Руководство пользователя по эксплуатации

версия 31 ред. от 25.01.2021

Листов 75

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

ОС	–	операционная система
ПК	–	программный комплекс
СОВ	–	система обнаружения вторжений
ID	–	идентификатор
IP	–	(англ. Internet Protocol) – межсетевой протокол
MAC	–	(англ. Media Access Control) – управление доступом к среде
SID	–	(англ. Security IDentifier) – идентификатор безопасности

АННОТАЦИЯ

Настоящее руководство пользователя по эксплуатации предназначено для технических специалистов и пользователей, которые выполняют конфигурирование и мониторинг работы InfoWatch ARMA Management Console версии 1.0.1.

Руководство пользователя по эксплуатации содержит описание графического и консольного интерфейса, доступных функций с подробным описанием их настройки и использования, а также принципов работы с InfoWatch ARMA Management Console.

Перед эксплуатацией InfoWatch ARMA Management Console пользователю необходимо изучить настоящее руководство.

1 НАЗНАЧЕНИЕ ПРОГРАММЫ

InfoWatch ARMA Management Console представляет собой единый центр управления решениями InfoWatch ARMA и реагирования на инциденты и решает следующие задачи:

- расследование инцидентов ПК «InfoWatch ARMA Industrial Firewall»;
- централизованное управление ПК «InfoWatch ARMA Industrial Firewall»;
- доступ к веб-интерфейсу управляемых устройств ПК «InfoWatch ARMA Industrial Firewall»;
- управление правилами СОВ на ПК «InfoWatch ARMA Industrial Firewall»;
- управление конфигурацией ПК «InfoWatch ARMA Industrial Firewall»;
- управление списком устройств сети;
- построение карты сети:
  - по анализу трафика (по производителю, по типу ОС, по назначению устройства);
  - отображение групп устройств;
  - отображение несанкционированных сетевых узлов (хостов);
  - отображение несанкционированных информационных потоков;
  - отображение информации об устройстве (IP, MAC-адрес, наименование и производитель сетевой карты);
- управление учетными записями и ролями InfoWatch ARMA Management Console.

2 НАЧАЛО РАБОТЫ

2.1 Базовая настройка сетевых интерфейсов

Адрес по умолчанию выдается по DHCP для каждого интерфейса у InfoWatch ARMA Management Console.

Для того чтобы задать IP-адрес для сетевого интерфейса необходимо:

1. Зайти в консольный интерфейс, используя пользователя по умолчанию (логин – root, пароль – root).

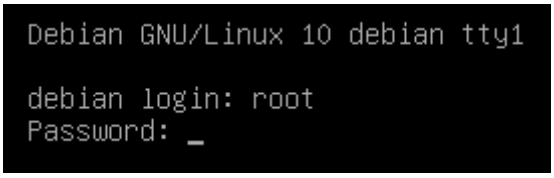


Рисунок 1 – Вход в консольный интерфейс

2. Выполнить команду *nano /etc/network/interfaces*
3. Задать параметры в секции #The primary network interface согласно рисунку ниже (Рисунок 2) и сохранить изменения, нажав комбинации клавиш «Ctrl+O», а затем «Ctrl+X».

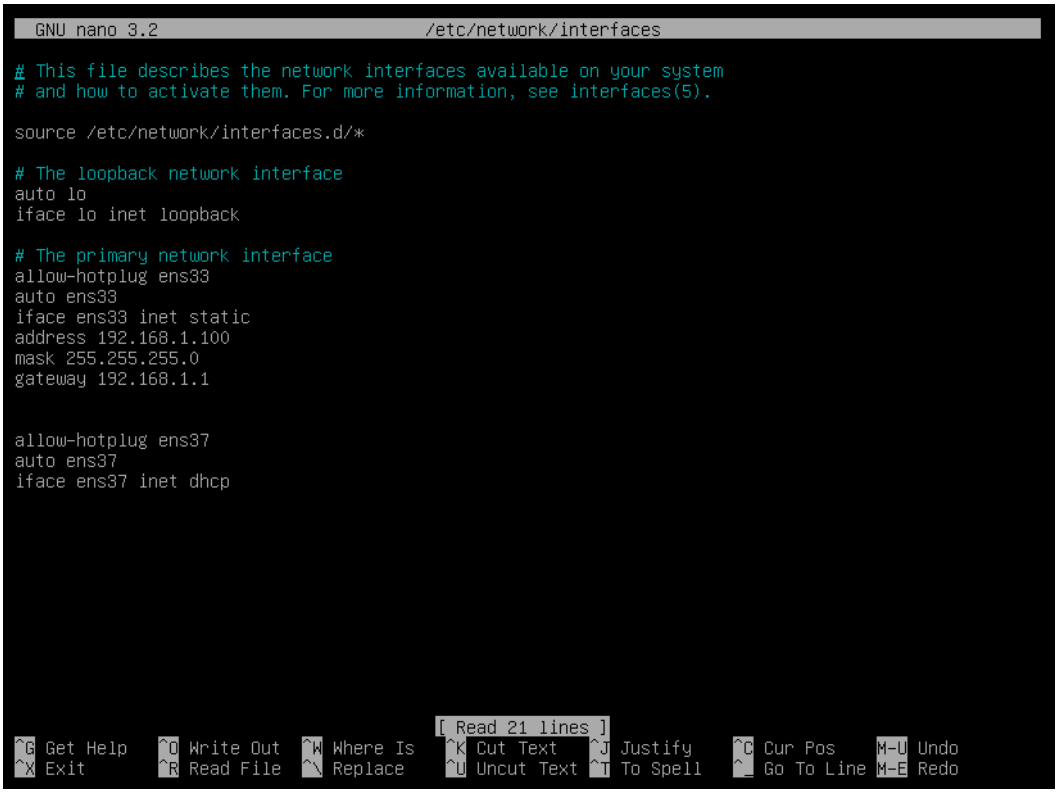
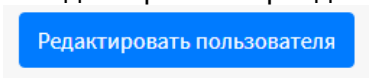


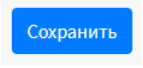
Рисунок 2 – Настройка сетевого интерфейса

4. Выполнить команду *service networking restart*.
5. Затем с помощью команды *ip a* убедиться в том, что настройки применились.

2.2 Изменение пароля по умолчанию

Для изменения пароля по умолчанию пользователя консольного интерфейса необходимо зайти в консольный интерфейс InfoWatch ARMA Management Console, используя пользователя по умолчанию (логин – root, пароль – root). После успешного входа необходимо выполнить команду *passwd*, указать новый пароль, нажать «Enter», повторить пароль, нажать «Enter».

Для изменения пароля по умолчанию пользователя веб-интерфейса необходимо зайти в веб-интерфейс InfoWatch ARMA Management Console, используя пользователя по умолчанию (логин – admin, пароль – nimda). После успешного входа перейти в раздел «Профиль пользователя», нажав на кнопку  , нажать на 

и в полях «Пароль» и «Подтверждение пароля» задать новый пароль и нажать на 

.

2.3 Подключение к InfoWatch ARMA Management Console

Для доступа к веб-интерфейсу управления InfoWatch ARMA Management Console необходимо:

– открыть веб-браузер (для ОС Windows: Chrome, Firefox, Internet Explorer (v8-v11); для ОС Linux: Chrome для Linux, Firefox для Linux);

– ввести IP-адрес, установленный при первоначальной настройке InfoWatch ARMA Management Console (по умолчанию используется получение по DHCP).

Для начала работы с системой необходимо ввести аутентификационные данные (по умолчанию логин – admin, пароль – nimda) и нажать на кнопку «Войти» (Рисунок 3).

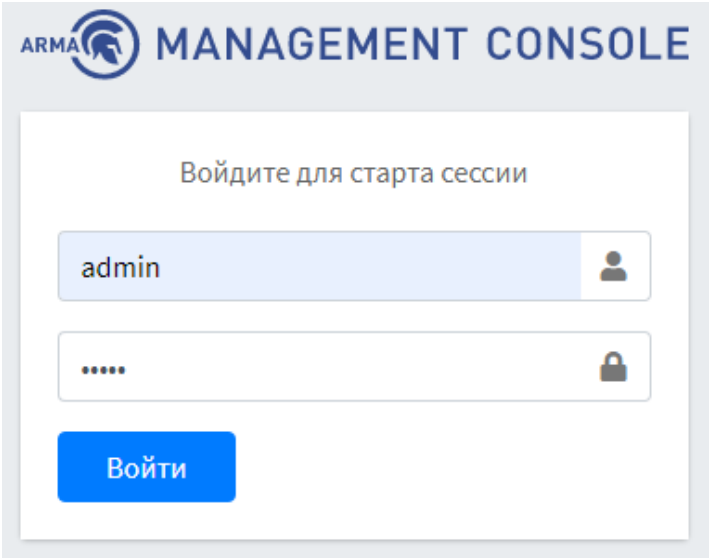


Рисунок 3 – Вход в систему

После входа в систему открывается стартовая панель («Обзорная панель») (Рисунок 4).

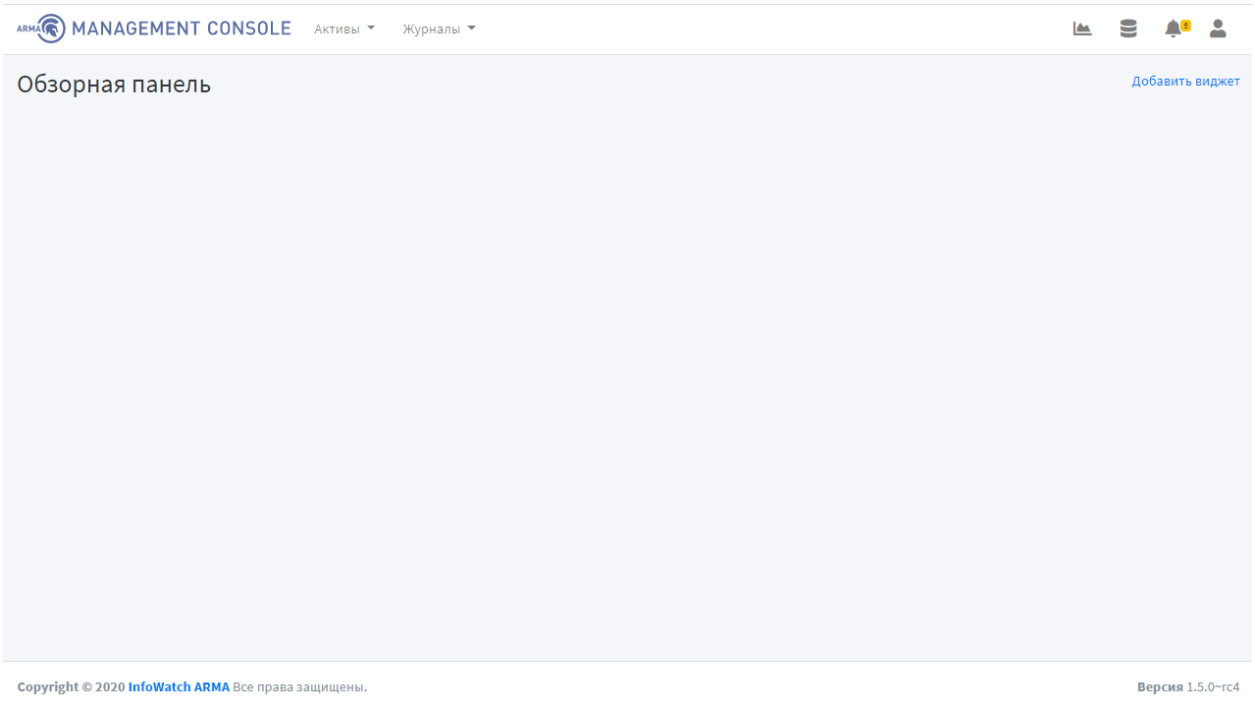


Рисунок 4 – Обзорная панель

Информация о порядке работы в InfoWatch ARMA Management Console изложена в следующих разделах:

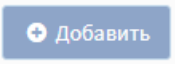
- Просмотр журналов событий (раздел 3);
- Расследование инцидентов (раздел 4);
- Управление системами защиты (раздел 5);
- Управление источниками события (раздел 6);
- Управление списком устройств сети (раздел 7);
- Настройка карты сети (раздел 8);
- Управление учетными записями и ролями системы (раздел 9);
- Управление стартовой панелью (раздел 10);
- Сообщения пользователю (раздел 11).

2.4 Добавление источника событий

Для возможности подключения InfoWatch ARMA Firewall к InfoWatch ARMA Management Console необходимо выполнить следующие шаги:

1. В InfoWatch ARMA Firewall создать пользователя с правами администратора и с ключом API.
2. В InfoWatch ARMA Management Console добавить источник событий.
3. В InfoWatch ARMA Firewall настроить экспорт событий по Syslog.

2.4.1 Создание пользователя

В InfoWatch ARMA Firewall перейти в раздел доступа к системе («Система» - «Доступ» - «Пользователи») и нажать на кнопку 

.

В поле «Имя пользователя» необходимо ввести имя «arma». В поле «Пароль» необходимо задать пароль и подтвердить его. В пункте «Членство в группе»

выбрать группу «admins» и, нажав на стрелочку «вправо», добавить группу для создаваемого пользователя и нажать на «Сохранить». После сохранения данных страница с настройками обновится и появится возможность добавления ключа API.

Для создания ключа необходимо в пункте «Ключ API» нажать на +, после чего будет скачан файл в формате apikey.txt.

2.4.2 Добавление источника событий

В InfoWatch ARMA Management Console необходимо перейти в раздел управления системами защиты («Активы» - «Системы защиты»), нажать на кнопку Добавить устройство, заполнить поля согласно рисунку 3 и нажать на кнопку «Сохранить».

Примечание – в поле «Порт» необходимо указать любой произвольный, но свободный порт, начиная с 1500.

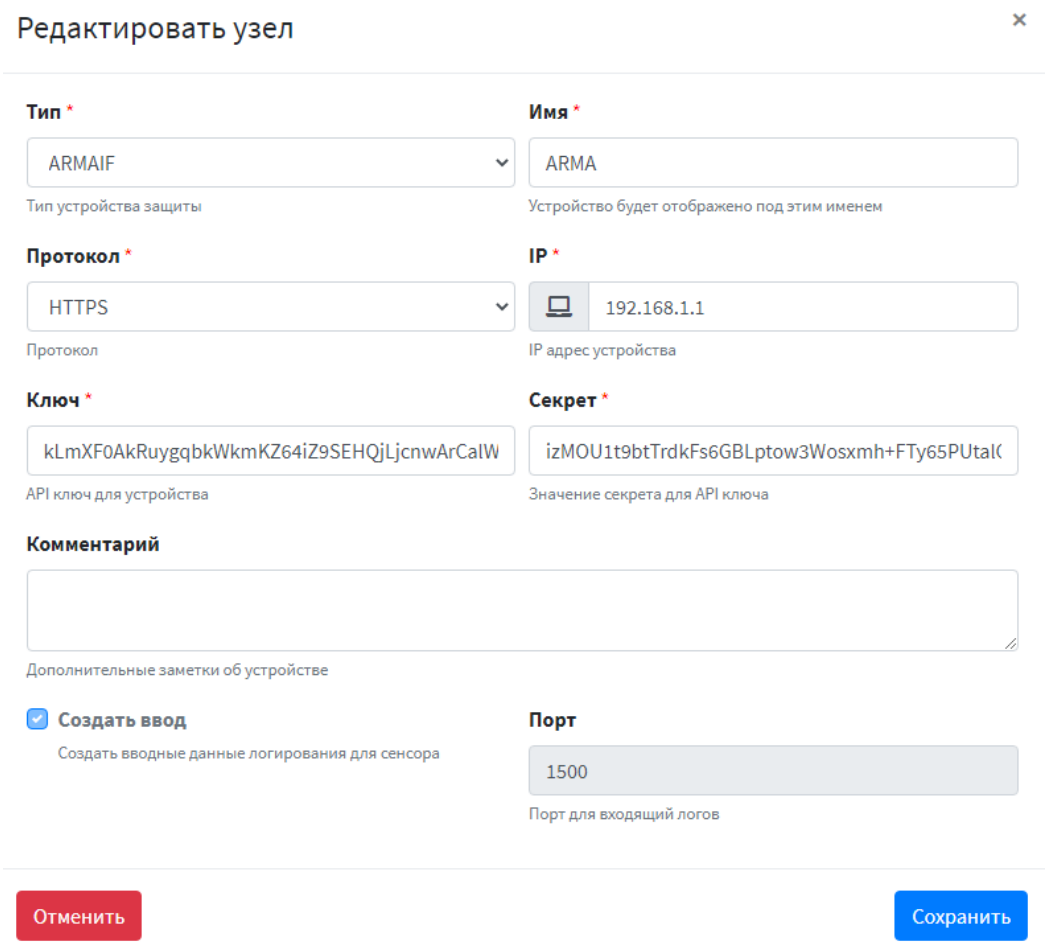


Рисунок 5 – Добавление нового устройства

Устройство добавлено и отображается в списке систем защиты (Рисунок 6).

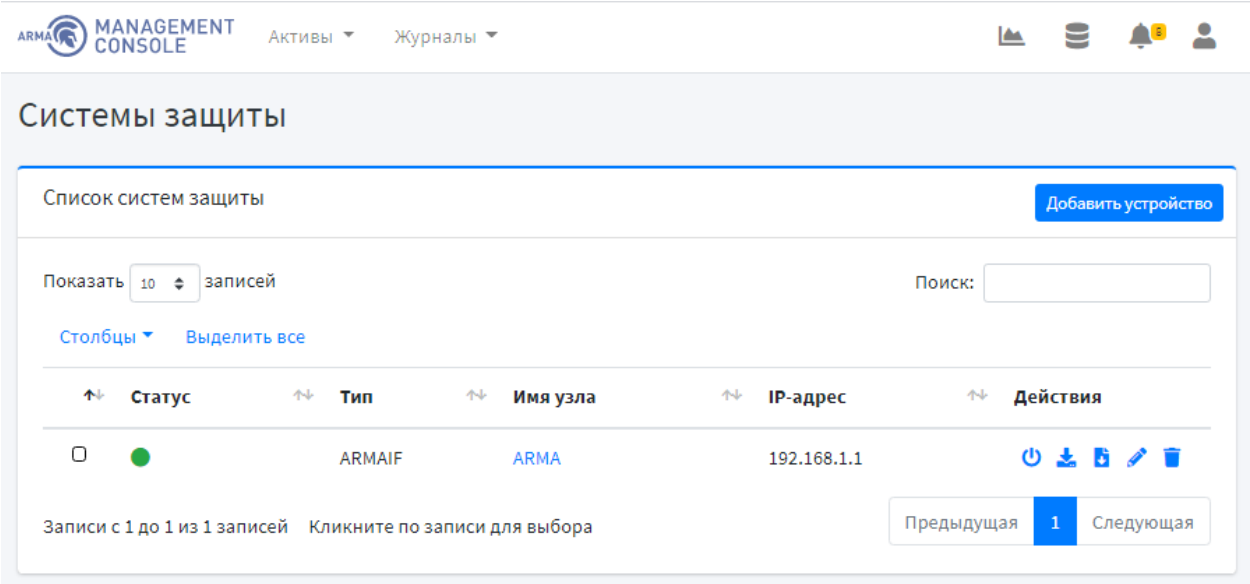


Рисунок 6 – Список систем защиты

2.4.3 Настройка экспорта событий по Syslog

В InfoWatch ARMA Firewall перейти в раздел настройки экспорта событий по Syslog («Система» - «Настройки» - «Экспорт событий»), нажать на +, заполнить поля согласно рисунку 5, нажать на «Сохранить», а затем на «Применить».

Примечание – в поле «Имя хоста» необходимо прописывать заданный адрес InfoWatch ARMA Management Console.

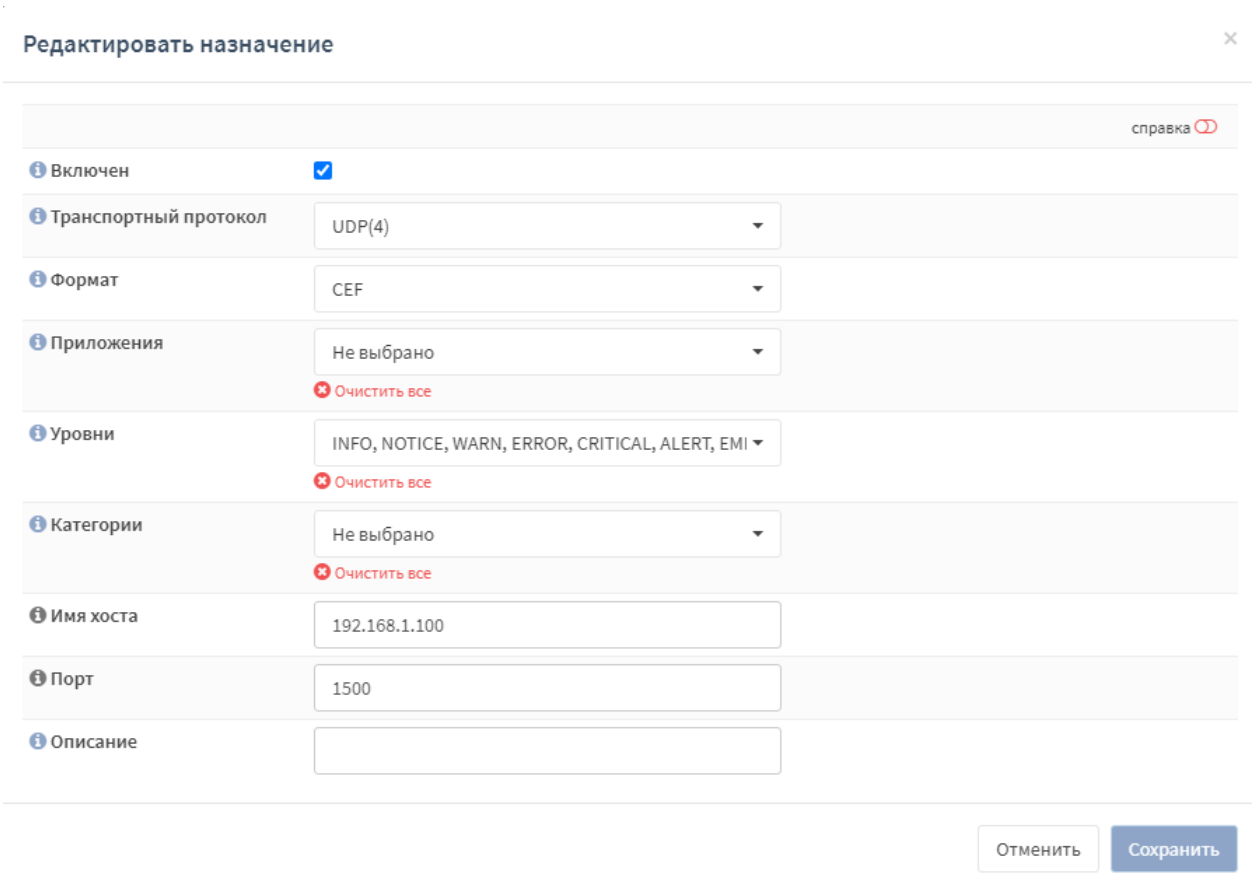


Рисунок 7 – Настройка экспорта событий по Syslog

3 ПРОСМОТР ЖУРНАЛОВ СОБЫТИЙ

Текущий раздел доступен пользователям с правом доступа «Может просматривать список событий». Описание добавления пользователя и назначение прав доступа приведены в разделе 9 настоящего документа.

Для просмотра журнала событий необходимо перейти на страницу «Журналы» - «Журнал событий» (Рисунок 8).

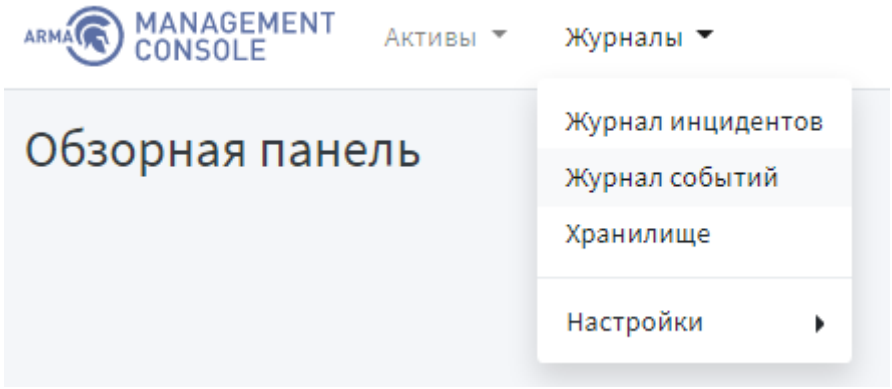


Рисунок 8 – Переход в журнал событий

3.1 Описание журнала событий

В журнале событий отображаются события систем защиты, подключенных к InfoWatch ARMA Management Console.

Страница «Журнал событий» позволяет просматривать журнал событий в формате таблицы, которая содержит следующие данные (Рисунок 9):

- дата;
- ID события;
- сообщение;
- критичность;
- категория;
- IP источника;
- IP получателя.

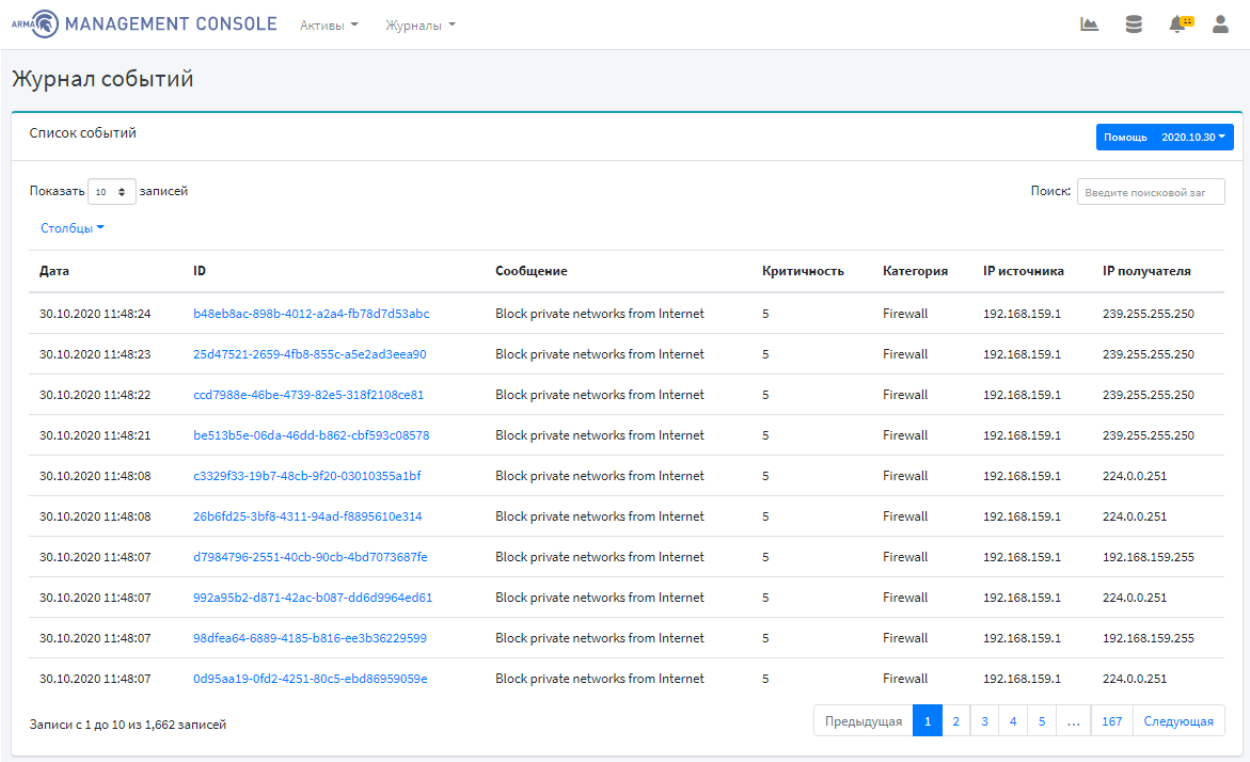


Рисунок 9 – Журнал событий

Данные о событиях можно настраивать вручную. Для этого необходимо нажать на «Столбцы» и в выпадающем списке выбрать/убрать данные, которые будут отображаться в таблице (Рисунок 10).

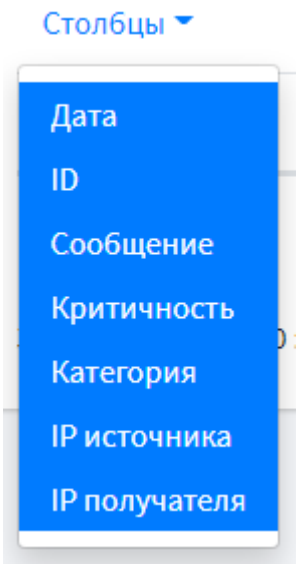


Рисунок 10 – Выбор данных о событиях

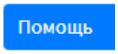
Для выбора конкретной даты отображения данных таблицы событий необходимо нажать на кнопку 

в правом верхнем углу страницы.

Для выбора количества записей, отображаемых в таблице событий на странице «Журнал событий» необходимо нажать на кнопку 

в левом в верхнем углу страницы.

3.2 Поиск событий

Поле «Поиск» вверху таблицы событий позволяет осуществлять сквозной поиск по всем полям таблицы. Для выполнения поиска необходимо ввести одно из доступных полей, которые можно посмотреть, нажав на кнопку 

(Рисунок 11), и строку совпадения в поле «Поиск».

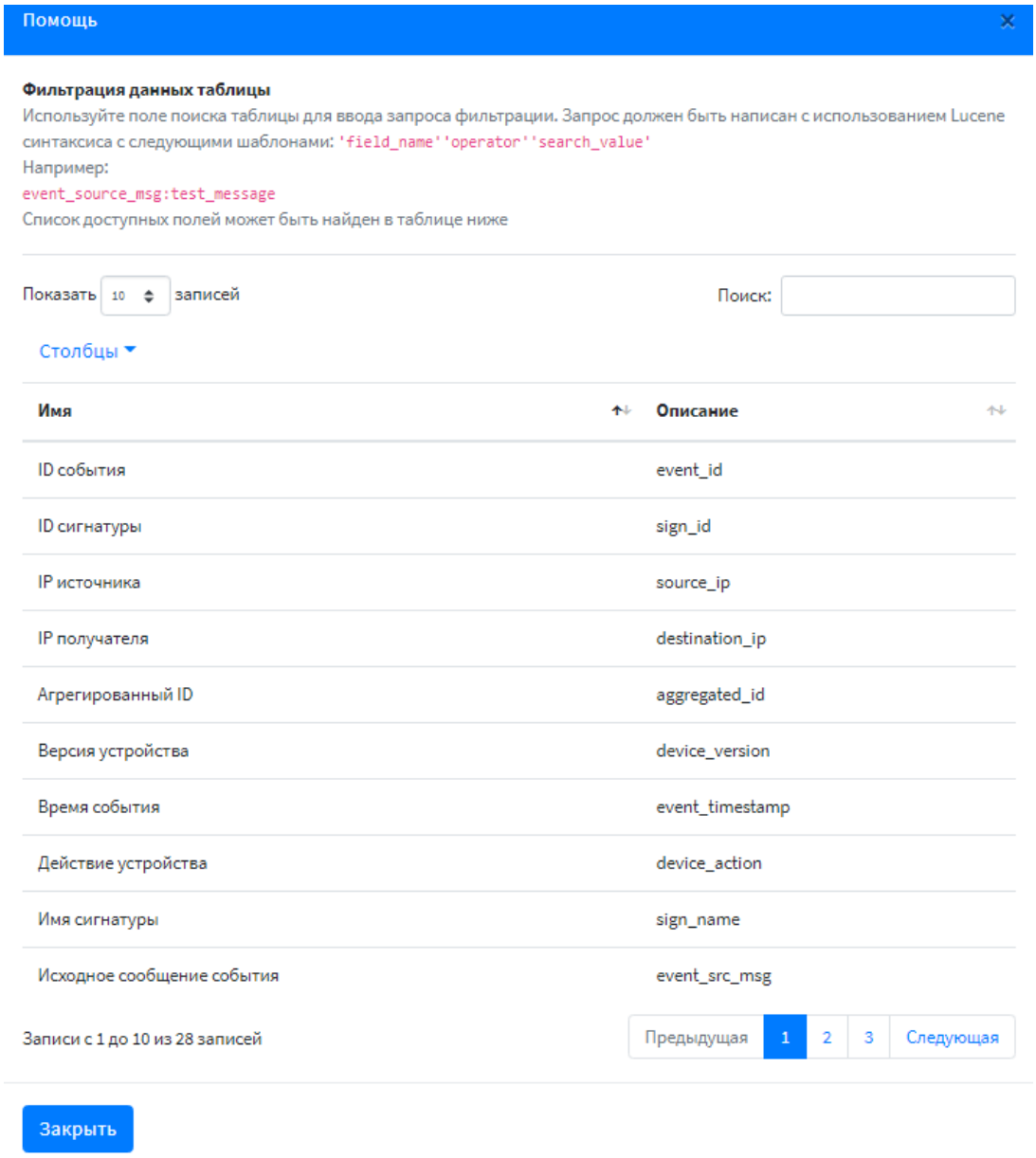


Рисунок 11 – Список доступных полей для поиска событий

3.3 Просмотр подробной информации о событии

Для просмотра подробной информации о событии необходимо перейти на страницу «Журнал событий». В таблице событий необходимо нажать на ссылку

идентификационного номера этого события (столбец «ID»), например, 6e6a9821-7cf3-43c4-9c4b-f7df567ab734. При нажатии на идентификационный номер события InfoWatch ARMA Management Console отобразит страницу подробной информации о событии со следующими разделами (Рисунок 12, Рисунок 13, Рисунок 14):

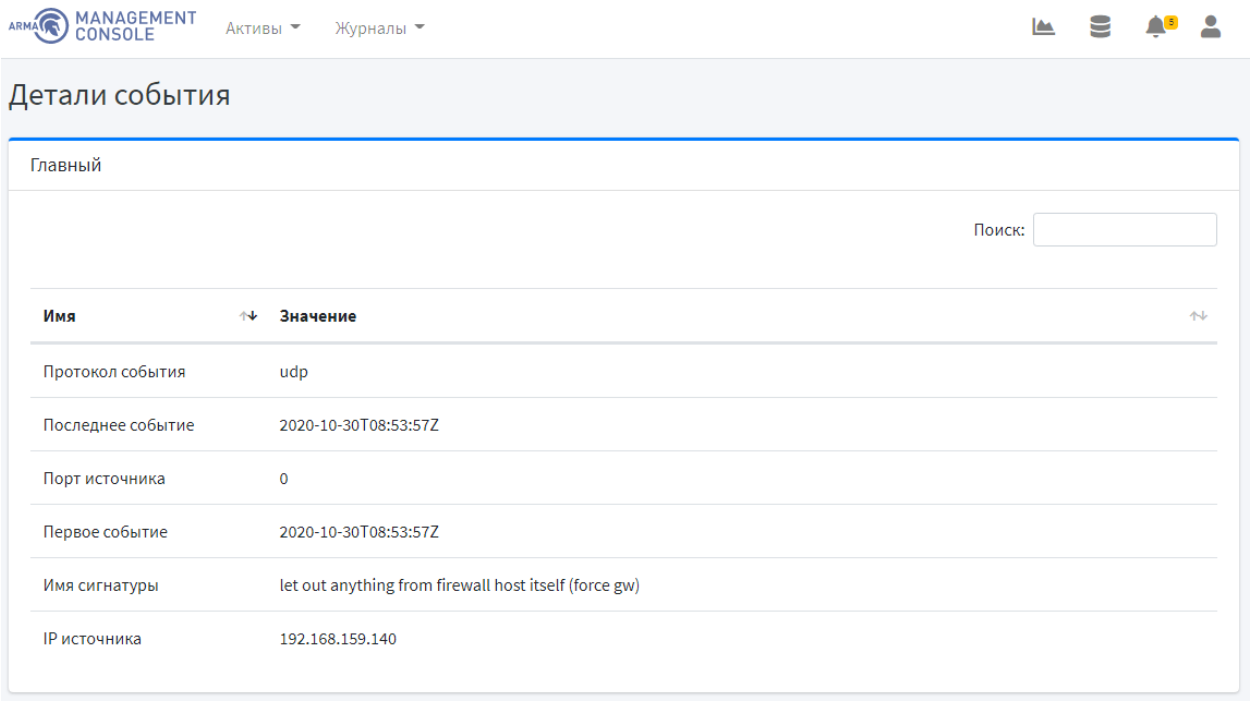


Рисунок 12 – Детали события. Основные

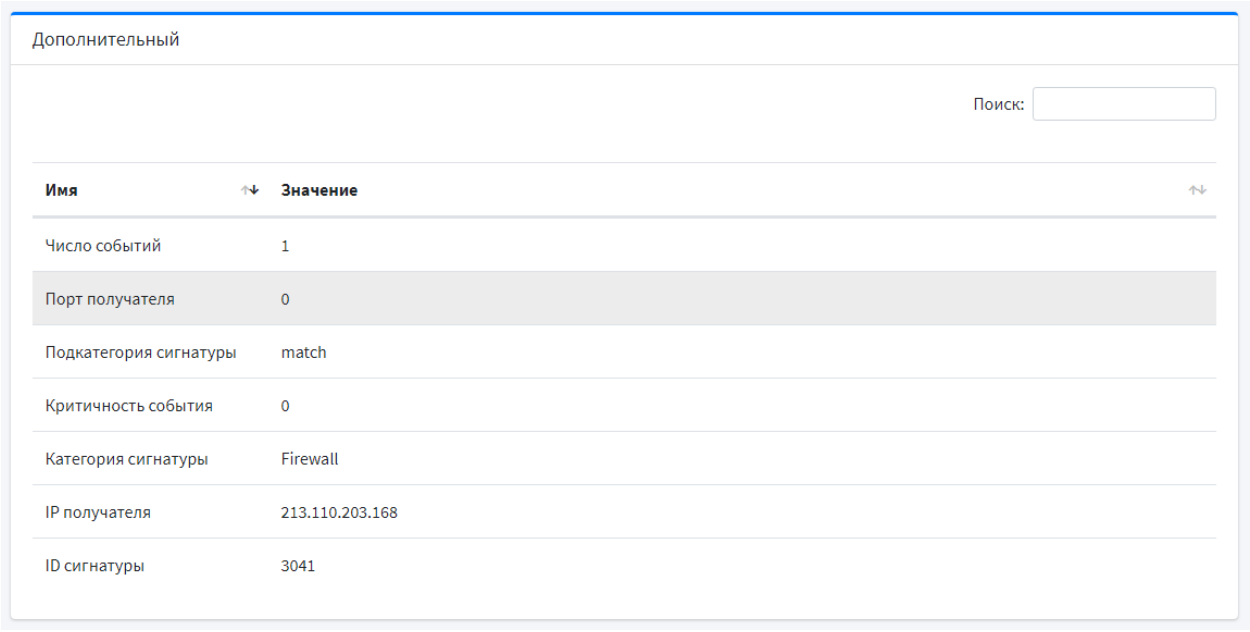


Рисунок 13 – Детали события. Дополнительные

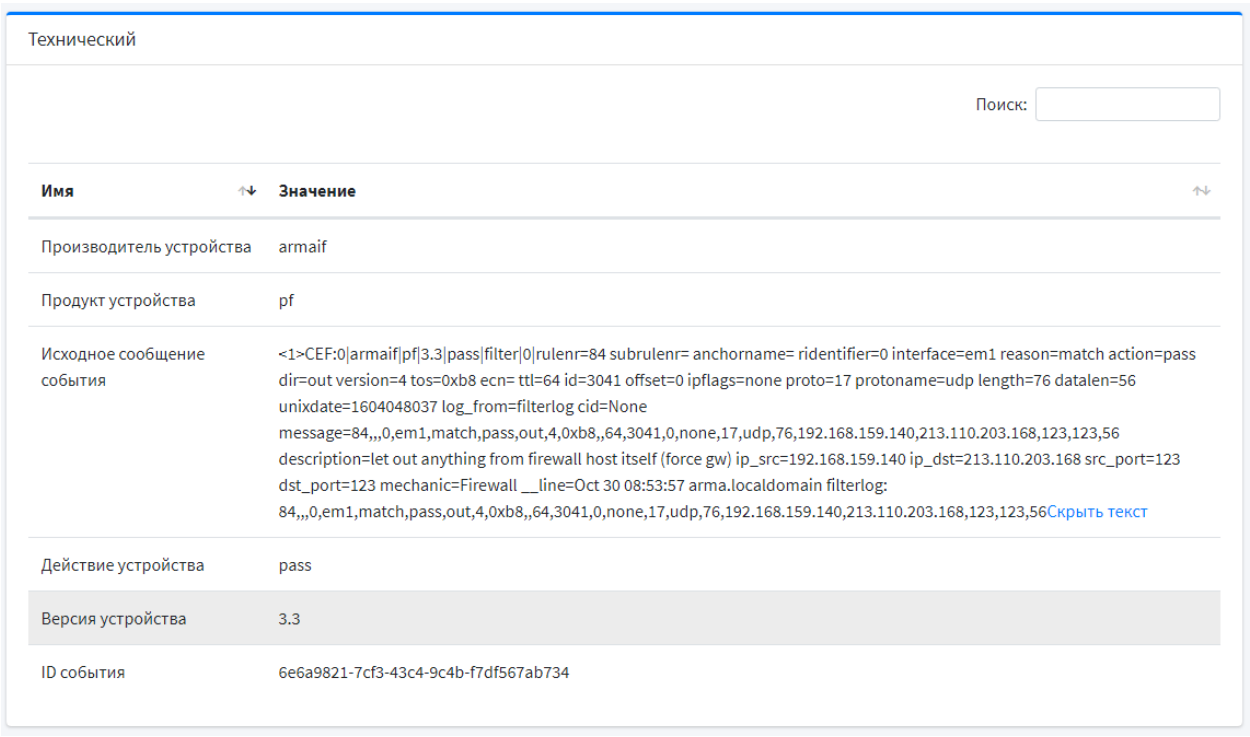


Рисунок 14 – Детали события. Технические

Поле «Поиск» вверху страницы позволяет осуществлять сквозной поиск по всей информации о событии. Для выполнения поиска необходимо ввести строку совпадения в поле «Поиск».

Таблица данных события позволяет производить сортировку по каждому столбцу. Для выполнения сортировки данных столбца таблицы необходимо нажать на кнопку рядом с названием соответствующего столбца.

4 РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ

Текущий раздел доступен пользователям с правом доступа «Может просматривать инциденты». Описание добавления пользователя и назначение прав доступа приведены в разделе 9 настоящего документа.

Пользователю с правом доступа «Может просматривать сетевые атаки» также отображаются инциденты, связанные с сетевыми атаками.

Пользователю с правом доступа «Может просматривать инциденты СОВ» также отображаются инциденты срабатывания правил СОВ.

Для просмотра журнала инцидентов необходимо перейти на страницу «Журналы» - «Журнал инцидентов» (Рисунок 15).

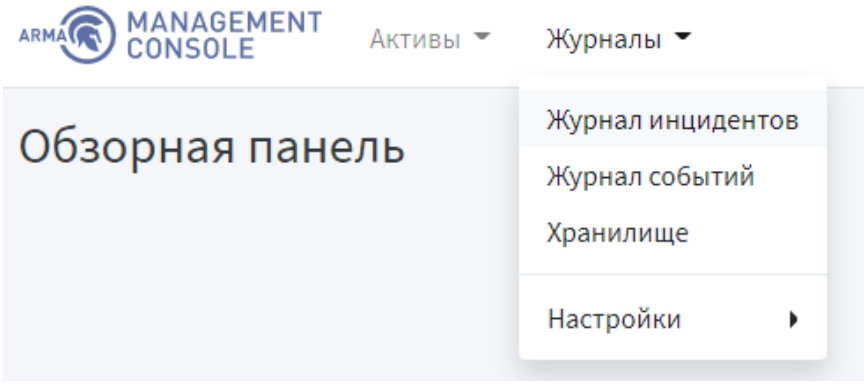


Рисунок 15 – Переход в журнал инцидентов

4.1 Уведомление о нерешенных инцидентах

Кнопка  в верхнем меню позволяет просматривать все уведомления InfoWatch ARMA Management Console.

При наличии/появлении нерешенных инцидентов появится уведомление об этом. Для просмотра нерешенных инцидентов, необходимо нажать на  , а затем выбрать уведомление об инцидентах (Рисунок 16). При нажатии на уведомление о нерешенных инцидентах InfoWatch ARMA Management Console отобразит страницу «Журналы» - «Журнал инцидентов» (Рисунок 17).

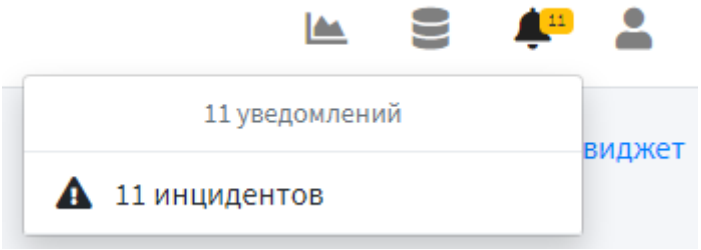


Рисунок 16 – Уведомление об инцидентах

4.2 Описание журнала инцидентов

В журнале инцидентов отображаются инциденты систем защиты, подключенных к InfoWatch ARMA Management Console.

Страница «Журнал инцидентов» позволяет просматривать журнал инцидентов в формате таблицы, которая содержит следующие данные (Рисунок 17).

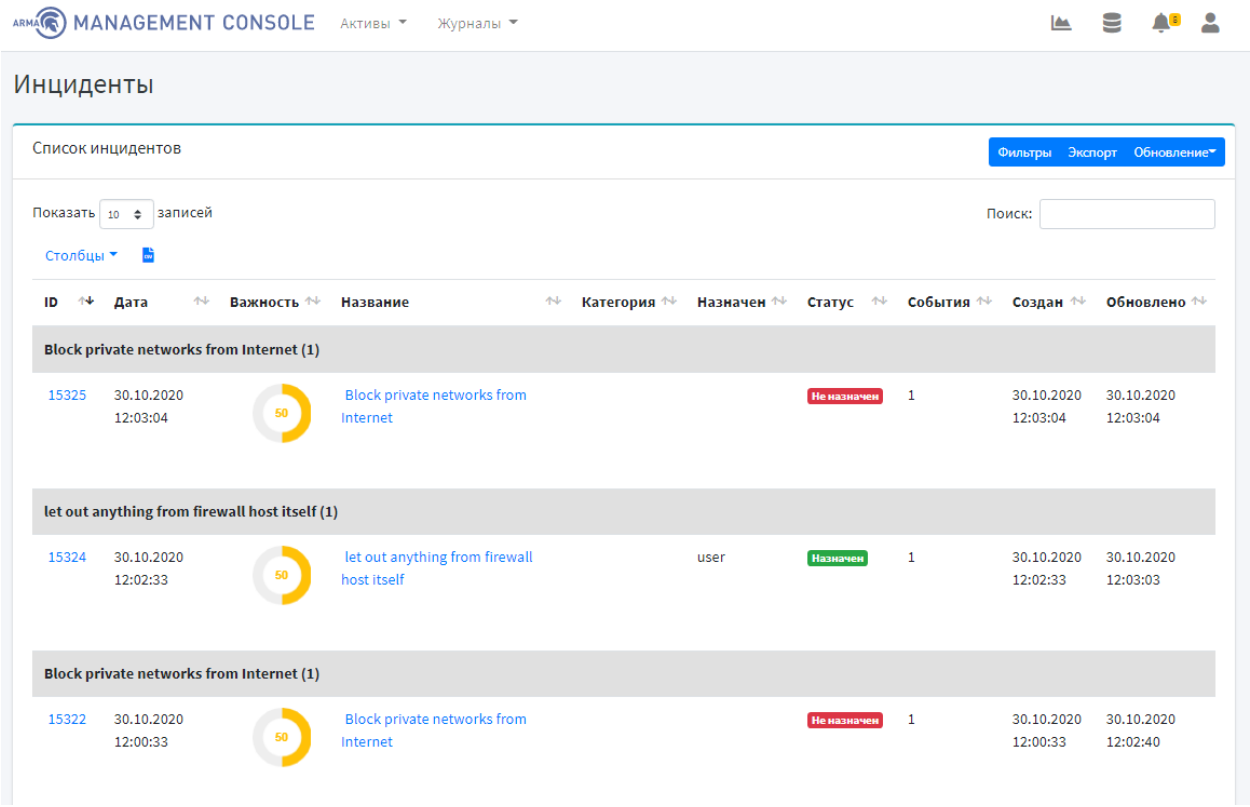
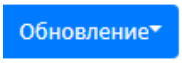
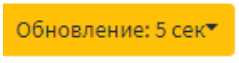


Рисунок 17 – Журнал инцидентов

InfoWatch ARMA Management Console поддерживает автоматическую группировку инцидентов.

Для выбора промежутка обновления данных таблицы инцидентов необходимо нажать на кнопку 

в правом верхнем углу страницы и выбрать частоту обновления данных. При выборе частоты обновления данных кнопка сменит вид 

.

Для выбора количества записей, отображаемых в таблице инцидентов на странице «Журнал инцидентов» необходимо нажать на кнопку 

в левом в верхнем углу страницы.

4.3 Поиск, сортировка и фильтрация инцидентов

Поле «Поиск» вверху таблицы событий позволяет осуществлять сквозной поиск по всем полям таблицы. Для выполнения поиска необходимо ввести строку совпадения в поле «Поиск».

Для фильтрации по определенным столбцам таблицы событий необходимо нажать кнопку Фильтры. Всплывающее окно позволяет задать фильтры отображения таблицы событий (Рисунок 18). В поле «Дата» необходимо выбрать промежуток времени отображения инцидентов. В поле «Важность» необходимо задать значение важности инцидентов. В поле «Категория» необходимо выбрать категорию инцидента. В поле «Назначен» необходимо выбрать пользователя, который назначается для решения инцидента. В поле «Статус» необходимо выбрать статус, отображаемых инцидентов. Для сброса фильтров необходимо нажать кнопку Сбросить. Для сохранения и применения фильтров необходимо нажать кнопку Применить.

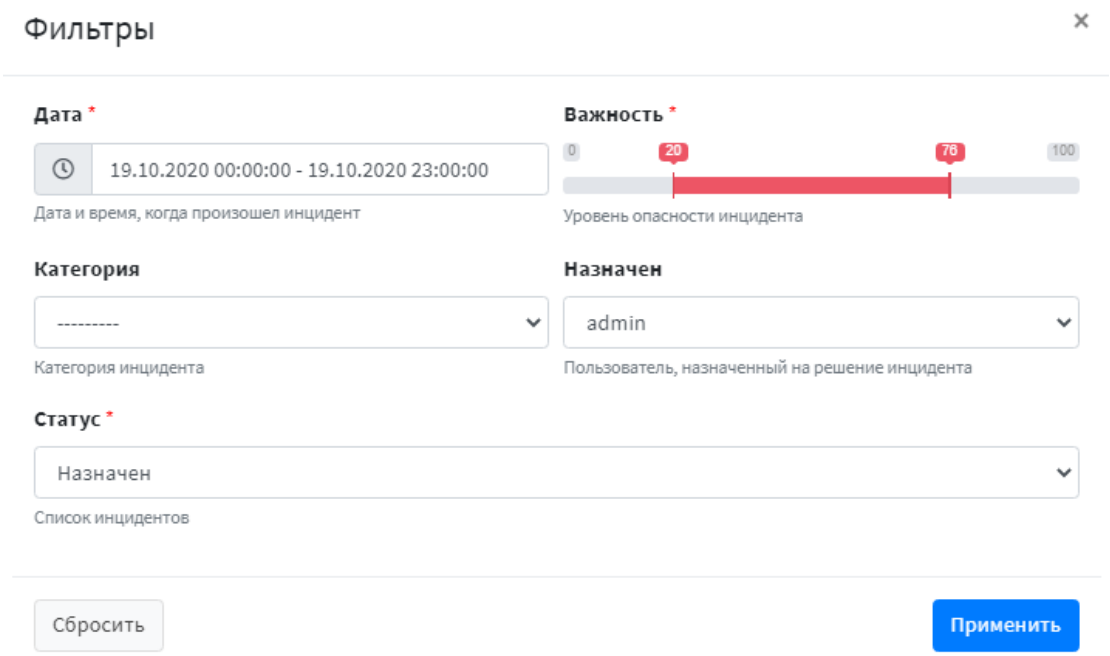


Рисунок 18 – Фильтры журнала инцидентов

Таблица позволяет производить сортировку по каждому столбцу. Для выполнения сортировки данных столбца таблицы необходимо нажать на кнопку ↑↓ рядом с названием соответствующего столбца.

4.4 Просмотр подробной информации об инциденте

Для просмотра подробной информации об инциденте необходимо перейти на страницу «Журнал инцидентов». В таблице инцидентов необходимо нажать на ссылку идентификационного номера этого инцидента (столбец «ID»), например, 15332. При нажатии на идентификационный номер инцидента InfoWatch ARMA Management Console отобразит страницу подробной информации об инциденте (Рисунок 19, Рисунок 20). Поля «Название», «Число событий», «Важность», «Описание» не редактируемые.

Для пользователя с правом доступа «Может назначать инциденты» и статусе инцидента отличным от значения «Решен», доступны для редактирования поля «Статус», «Крайний срок», «Назначен».

Для пользователя с правом доступа «Может работать с инцидентами» и статусе инцидента отличным от значения «Решен», доступны для редактирования поля «Статус», «Крайний срок», «Назначен», «Категория», «Комментарий».

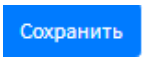
Для пользователя с правом доступа «Может изменять решенные инциденты» доступны для редактирования поля «Статус», «Крайний срок», «Назначен», «Категория», «Комментарий».

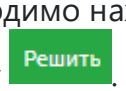
В поле «Статус» необходимо выбрать статус инцидента из следующих возможных:

- не назначен;
- назначен;
- отложен;
- решен;
- ложное срабатывание.

В поле «Категория» необходимо выбрать категорию инцидента. В поле «Крайний срок» необходимо выбрать крайний срок решения инцидента. В поле «Назначен» необходимо выбрать пользователя, назначенного для решения инцидента. В поле «Комментарий» необходимо ввести комментарий к инциденту. Далее отображается список событий, из которых сформирован инцидент, представленный в виде таблице со следующей информацией:

- дата события;
- сообщение;
- имя узла;
- продукт;
- IP источника;
- IP получателя.

Затем отображаются рекомендации по закрытию инцидента и последствия инцидента. Для сохранения изменений на странице «Детали инцидента» необходимо нажать кнопку 

. При решении инцидента необходимо нажать кнопку 

.

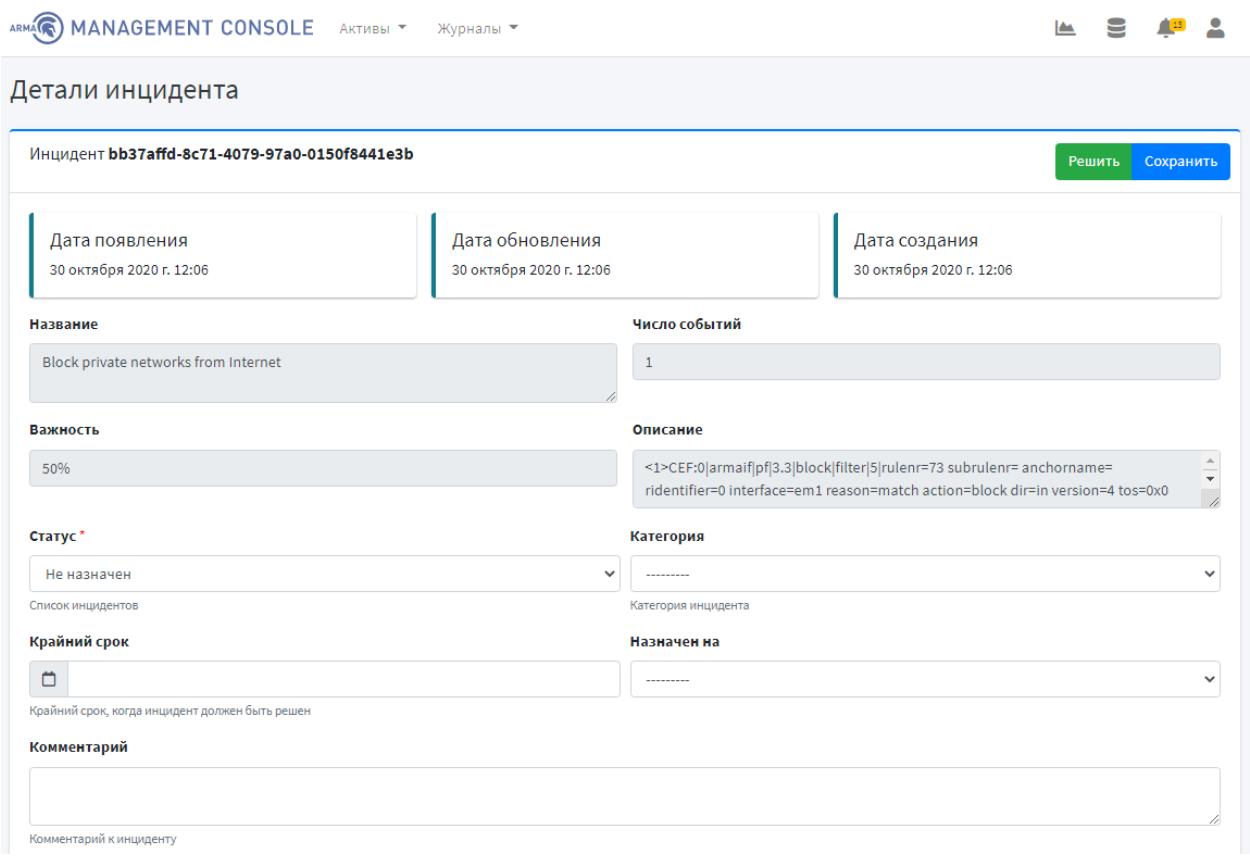


Рисунок 19 – Детали инцидента (1)

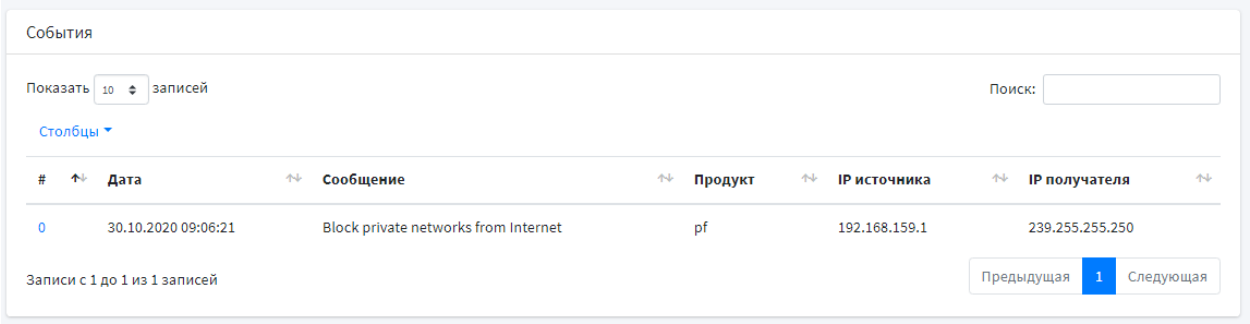
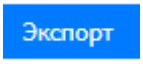


Рисунок 20 – Детали инцидента (2)

4.5 Экспорт инцидентов

4.5.1 Экспорт всей таблицы

Для того чтобы экспортировать всю таблицу инцидентов необходимо нажать на кнопку 

справа сверху таблицы.

4.5.2 Экспорт отфильтрованной таблицы в формате CSV

Для того чтобы скачать отфильтрованную таблицу инцидентов необходимо сначала задать фильтр (Рисунок 18), а затем нажать на кнопку 

слева сверху таблицы.

4.6 Управление инцидентами

Для работы с инцидентами с помощью InfoWatch ARMA Management Console предусмотрены следующие шаги:

– назначение пользователя для решения инцидента, даты до которой данный инцидент необходимо решить, изменение статуса инцидента, создание комментария для отображения мнения о данном инциденте;

– пользователь, назначенный для решения инцидента, исходя из результата проведенного расследования, должен изменить статус инцидента, в случае положительного решения инцидента — отметить инцидент как решенный.

4.6.1 Назначение пользователя для решения инцидента

Для назначения пользователей для решения инцидента необходимо перейти на страницу «Журнал инцидентов». В таблице инцидентов необходимо нажать на ссылку идентификационного номера этого инцидента (столбец «ID»), например, 15332 . При нажатии на идентификационный номер инцидента InfoWatch ARMA Management Console отобразит страницу подробной информации об инциденте (Рисунок 19).

Для пользователя с правом доступа «Может назначать инциденты» и статусе инцидента отличным от значения «Решен», доступны для редактирования поля «Статус», «Крайний срок», «Назначен».

Для пользователя с правом доступа «Может работать с инцидентами» и статусе инцидента отличным от значения «Решен», доступны для редактирования поля «Статус», «Крайний срок», «Назначен».

Для пользователя с правом доступа «Может изменять решенные инциденты» доступны для редактирования поля «Статус», «Крайний срок», «Назначен».

Для назначения пользователя на инцидент необходимо в поле «Статус» выбрать «Назначен». В поле «Назначен» необходимо выбрать пользователя, на которого будет назначен инцидент. В поле «Крайний срок» необходимо выбрать дату, до которой необходимо решить инцидент. Для сохранения настроек необходимо нажать кнопку Сохранить.

4.6.2 Внесение результата проведенного расследования

По результатам проведенного расследования пользователю необходимо перейти на страницу «Журнал инцидентов». В таблице инцидентов необходимо нажать на ссылку идентификационного номера этого инцидента (столбец «ID»), например, 15332 . При нажатии на идентификационный номер инцидента InfoWatch ARMA Management Console отобразит страницу подробной информации об инциденте (Рисунок 19).

Для пользователя с правом доступа «Может работать с инцидентами» и статусе инцидента отличным от значения «Решен», доступны для редактирования поля «Статус», «Комментарий».

Для пользователя с правом доступа «Может изменять решенные инциденты» доступны для редактирования поля «Статус», «Комментарий».

Для внесения результата проведенного расследования пользователю необходимо изменить статус в поле «Статус». В поле «Комментарий» необходимо ввести комментарий к инциденту. Для сохранения изменений необходимо нажать кнопку Сохранить.

В случае положительного решения инцидента, отметить инцидент как решенный. Для этого необходимо нажать кнопку Решить.

4.7 Просмотр архивов

Страница «Хранилище» позволяет просматривать архивы собранных инцидентов (Рисунок 21).

Для просмотра хранилища необходимо перейти на страницу «Журналы» - «Хранилище».

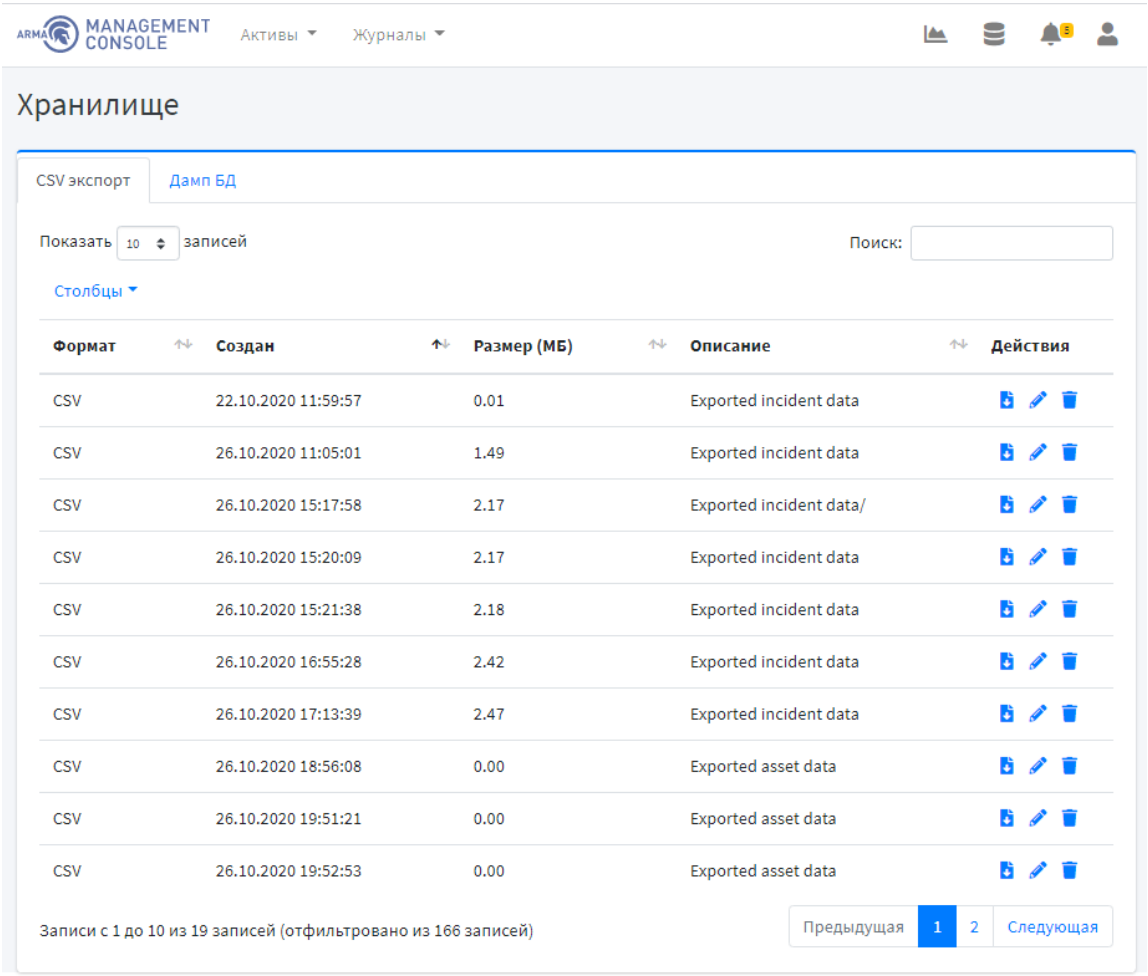


Рисунок 21 – Хранилище. CSV экспорт

Во вкладке «CSV экспорт» хранятся архивы собранных инцидентов в формате CSV. Во вкладке «Дамп БД» хранятся архивы собранных инцидентов, настроенных по ротации (Рисунок 22).

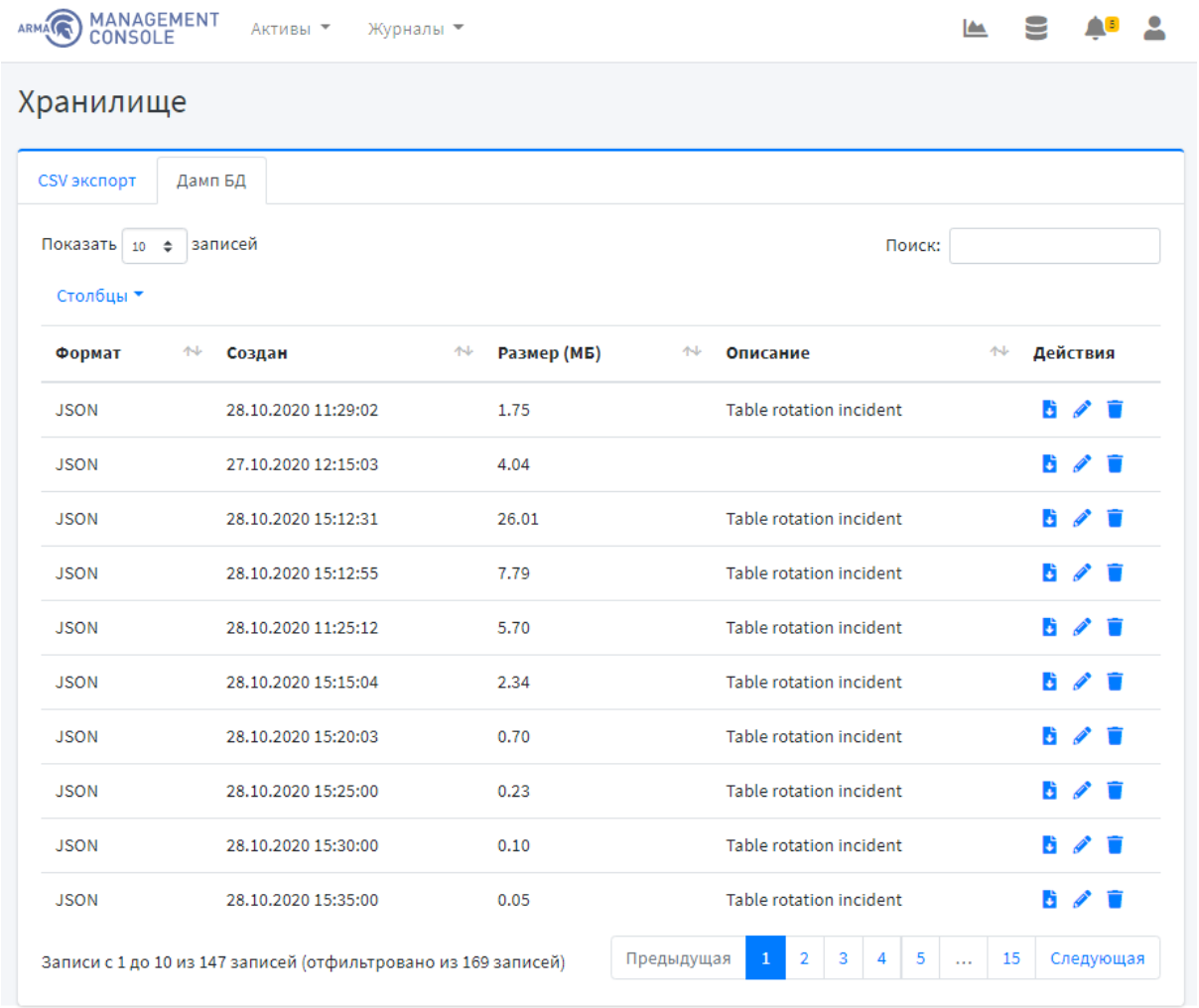


Рисунок 22 – Хранилище. Дамп БД

Для редактирования описания хранилища необходимо нажать кнопку напротив соответствующего хранилища и в разделе «Редактировать» изменить описание, а затем нажать на «Сохранить» (Рисунок 23). Для скачивания архива необходимо нажать кнопку (Рисунок 21).

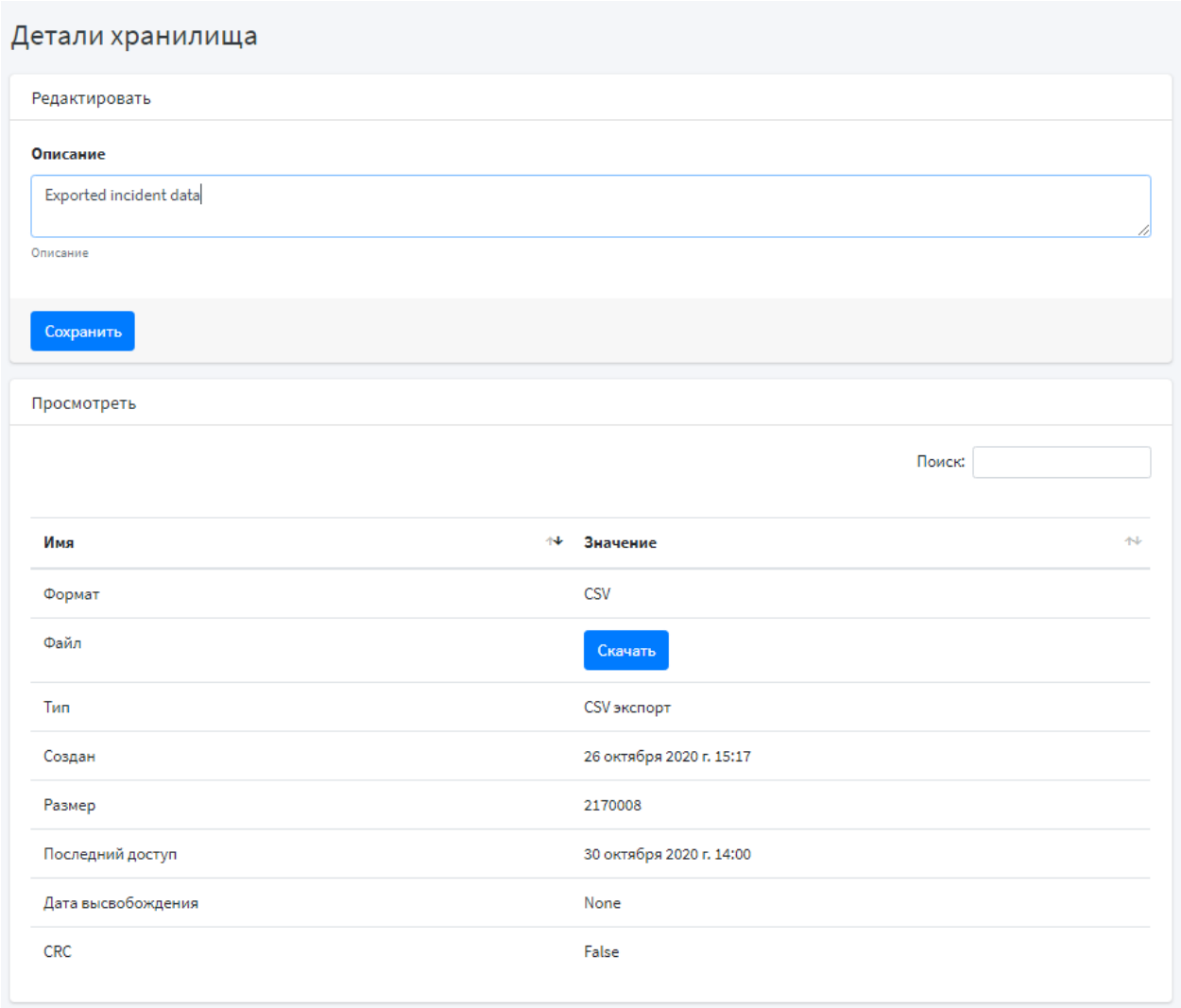


Рисунок 23 – Детали хранилища

4.8 Настройки

4.8.1 Настройка корреляции

Текущий раздел позволяет настраивать правила корреляции и просматривать их в формате таблицы. По умолчанию создано два правила корреляции (Рисунок 24).

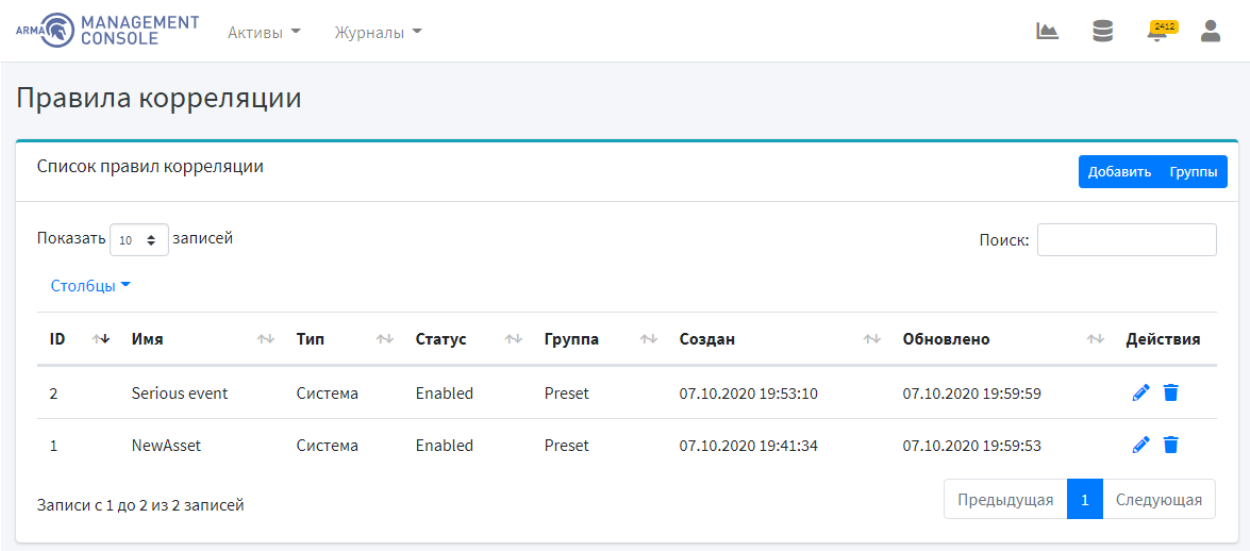


Рисунок 24 – Правила корреляции

Для добавления правила корреляции необходимо нажать на кнопку Добавить.

В разделе «Базовые настройки правила» в поле «Имя» необходимо ввести имя правила. В поле «Группа» необходимо выбрать группу правила. В поле «Глубина» необходимо указать глубину анализа. В поле «Описание» необходимо добавить описание правила. Для включения правила необходимо установить галочку напротив «Включено» (Рисунок 25).

В разделе «Условия» в поле «Тип» необходимо выбрать тип состояния («Совпадение», «Или», «И», «Регулярное выражение», «Больше или равно»). В поле «Поле» необходимо выбрать имя поля из выпадающего списка. В поле «Значение» необходимо ввести значение поля (Рисунок 25).

В разделе «Действия» для добавления действия необходимо нажать на кнопку Добавить, выбрать одно из предложенных действий и нажать на кнопку Добавить (Рисунок 26).

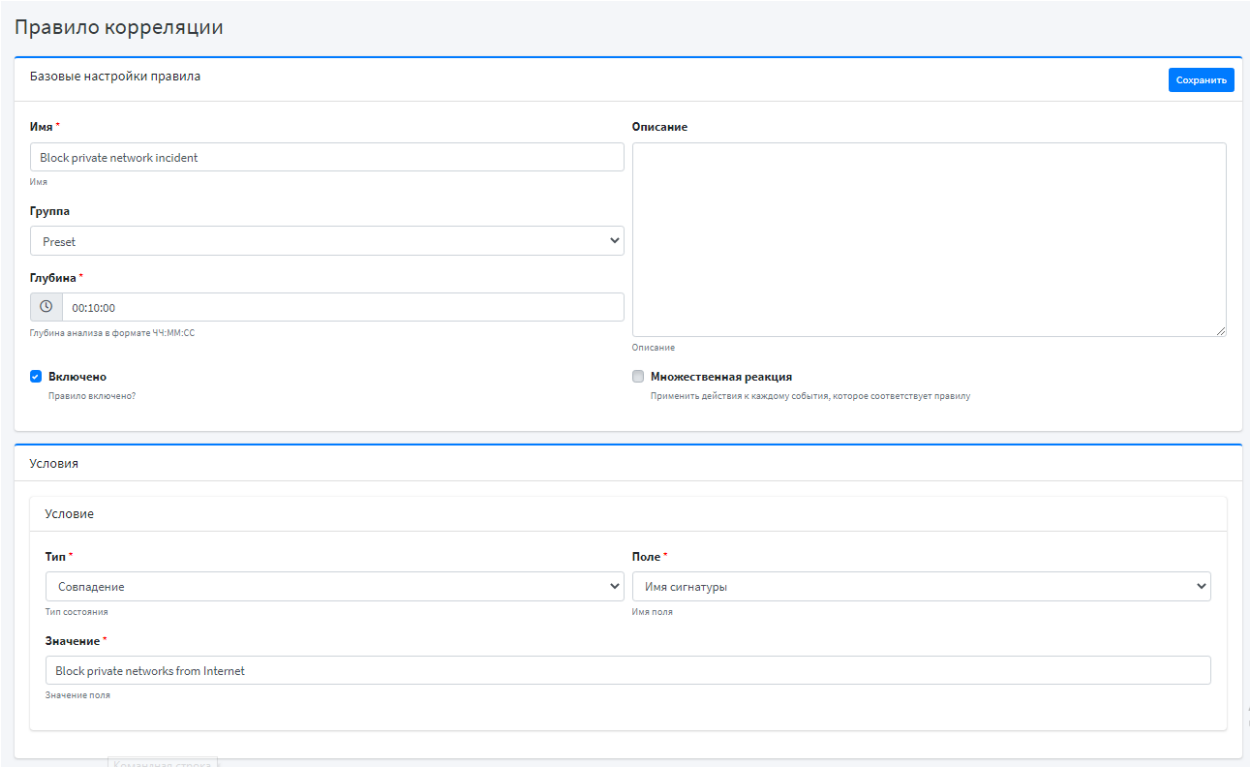


Рисунок 25 – Добавление правила корреляции

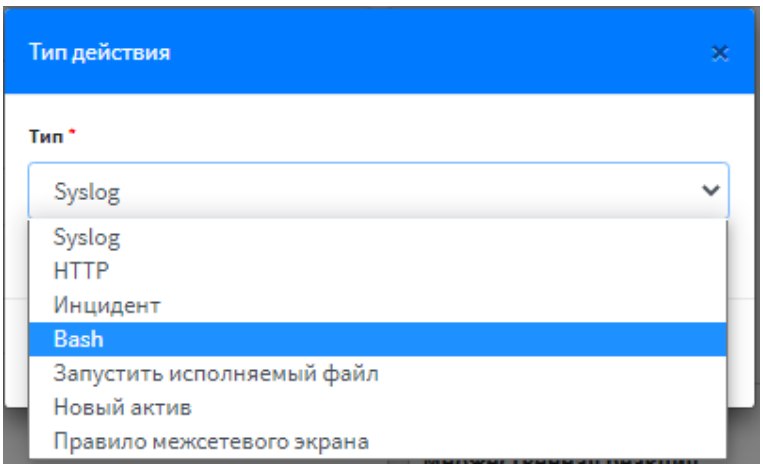


Рисунок 26 – Типы действий

При выборе действия «Syslog» появятся следующие поля для заполнения (Рисунок 27).

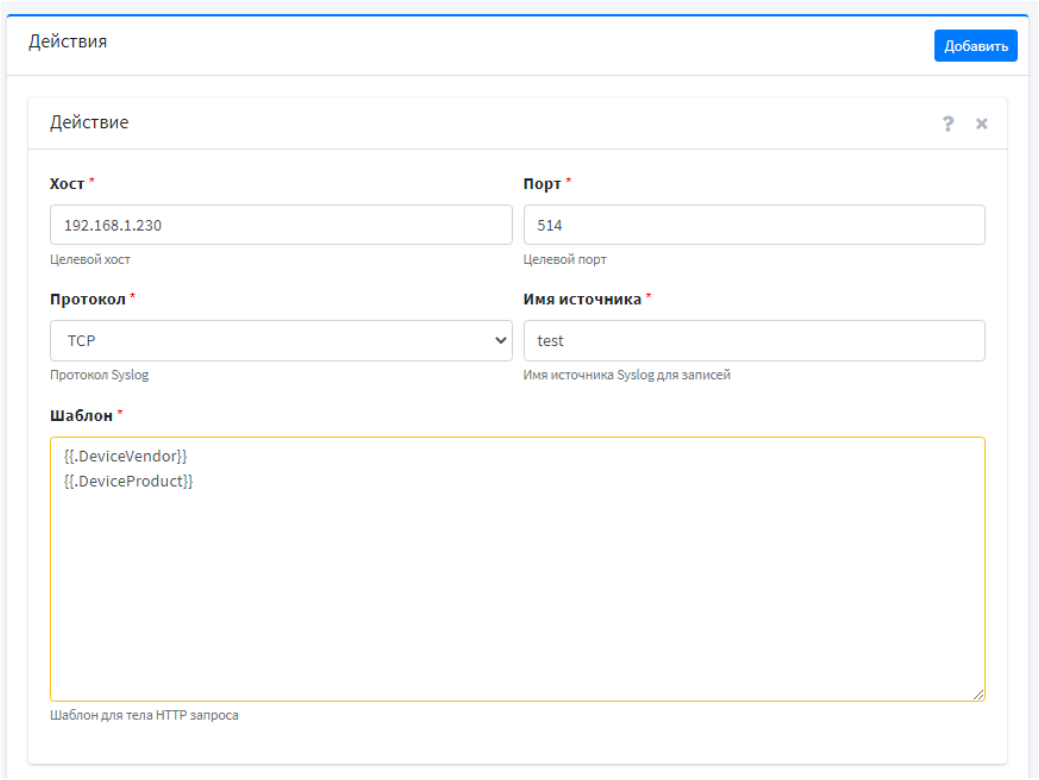


Рисунок 27 – Действие «Syslog»

В поле «Хост» необходимо указать целевой хост. В поле «Порт» необходимо указать целевой порт. В поле «Протокол» необходимо выбрать протокол syslog. В поле «Имя источника» необходимо указать имя источника syslog для записей. В поле «Шаблон» необходимо указать шаблон для http запроса.

При выборе действия «HTTP» появятся следующие поля для заполнения (Рисунок 28).

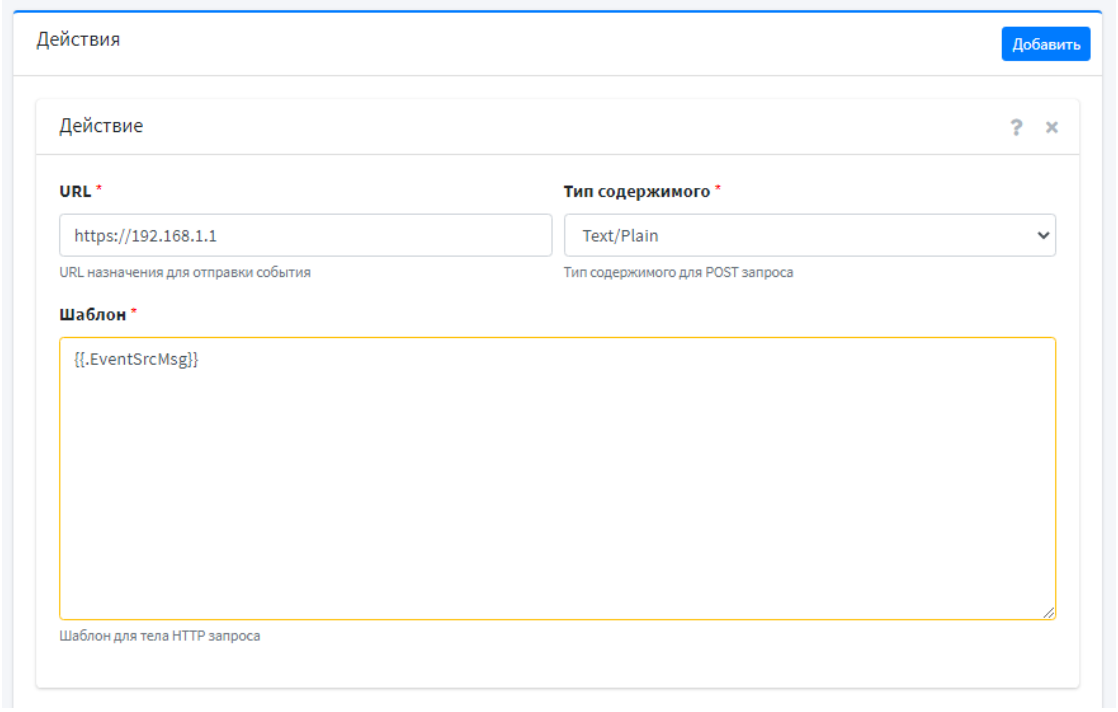


Рисунок 28 – Действие «HTTP»

В поле «URL» необходимо указать назначение для отправки события. В поле «Тип содержимого» выбрать тип содержимого для POST запроса («Text/Plain», «Application/Json»). В поле «Шаблон» необходимо указать шаблон для http запроса.

При выборе действия «Инцидент» появятся следующие поля для заполнения (Рисунок 29).

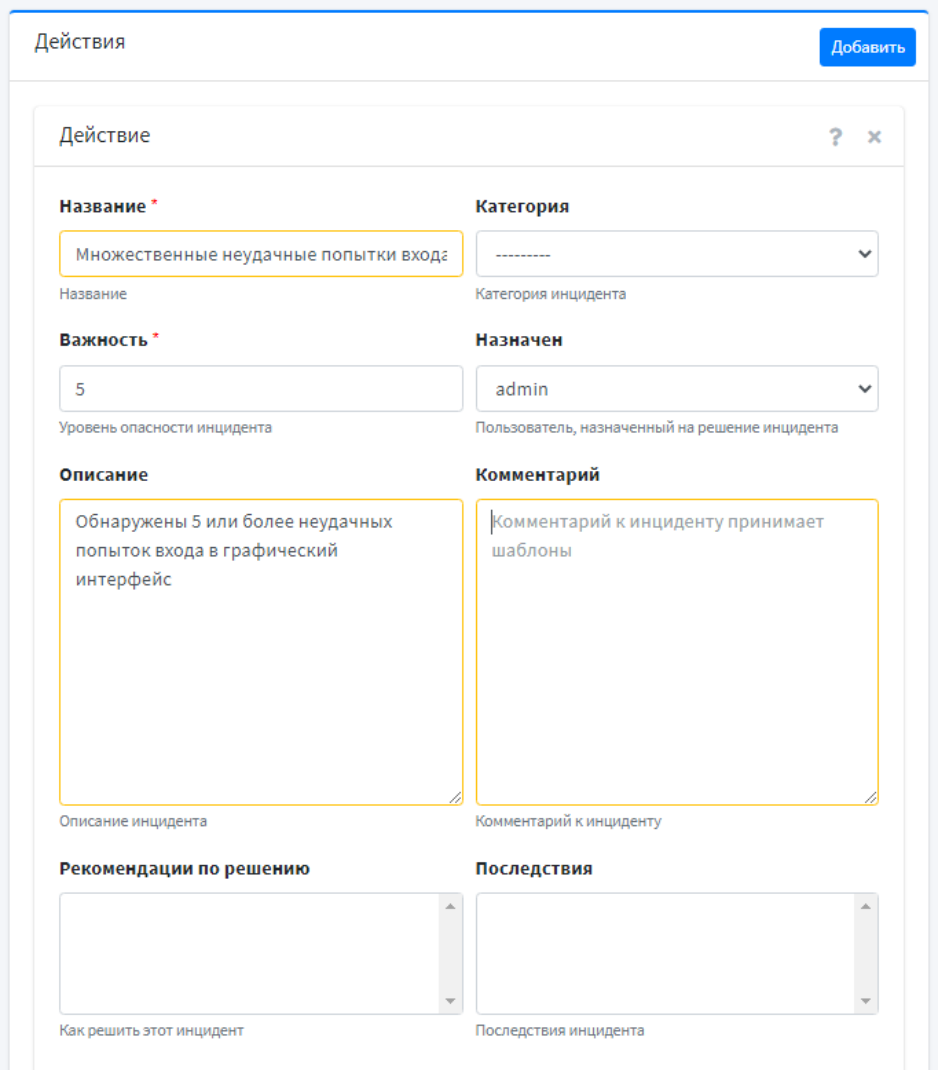


Рисунок 29 – Действие «Инцидент»

В поле «Название» необходимо ввести название инцидента. В поле «Категория» необходимо выбрать категорию инцидента. В поле «Важность» необходимо указать уровень опасности инцидента. В поле «Назначен» необходимо выбрать пользователя для решения инцидента. В поле «Описание» необходимо добавить описание инцидента. В поле «Комментарий» при необходимости добавить комментарий к инциденту. Поля «Рекомендации по решению» и «Последствия» не заполняются.

При выборе действия «Bash» появится поле «Тело», в котором необходимо прописать сценарий скрипта (Рисунок 30).

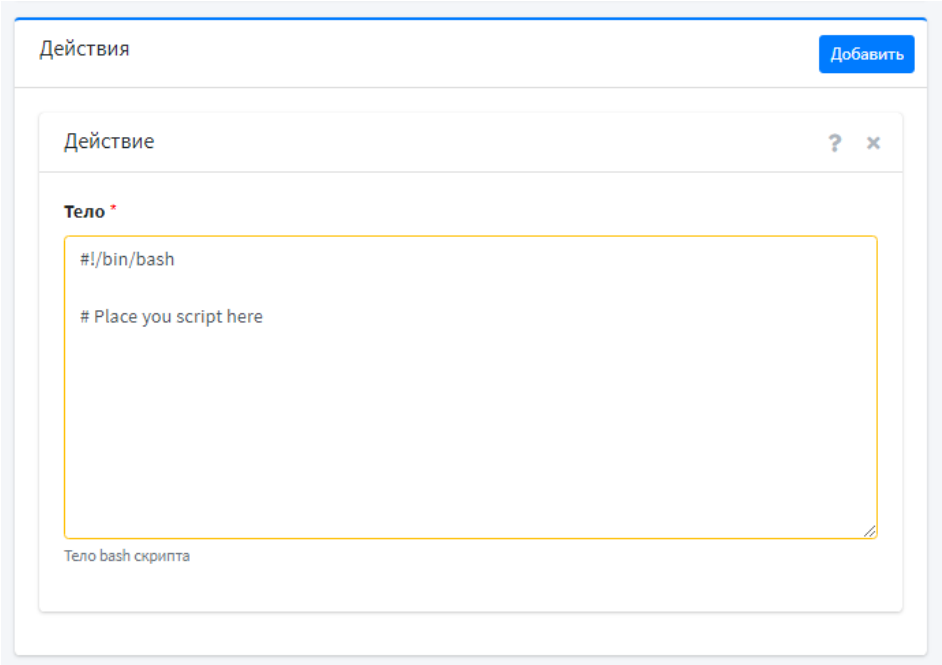


Рисунок 30 – Действие «Bash»

При выборе действия «Запустить исполняемый файл» появятся следующие поля (Рисунок 31).

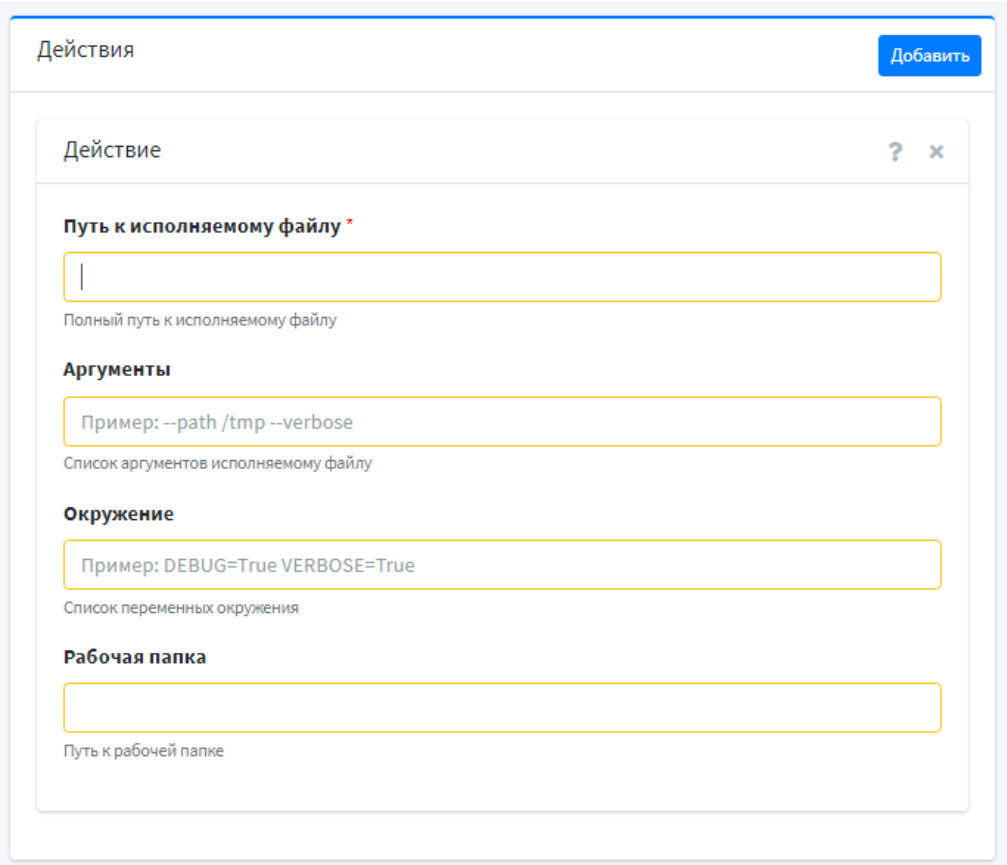


Рисунок 31 – Действие «Запустить исполняемый файл»

В поле «Путь к исполняемому файлу» необходимо указать полный путь к исполняемому файлу. В поле «Аргументы» необходимо указать список аргументов

к исполняемому файлу. В поле «Окружение» необходимо указать список переменных окружения. В поле «Рабочая папка» необходимо указать путь к рабочей папке.

При выборе действия «Новый актив» появятся следующие поля (Рисунок 32).

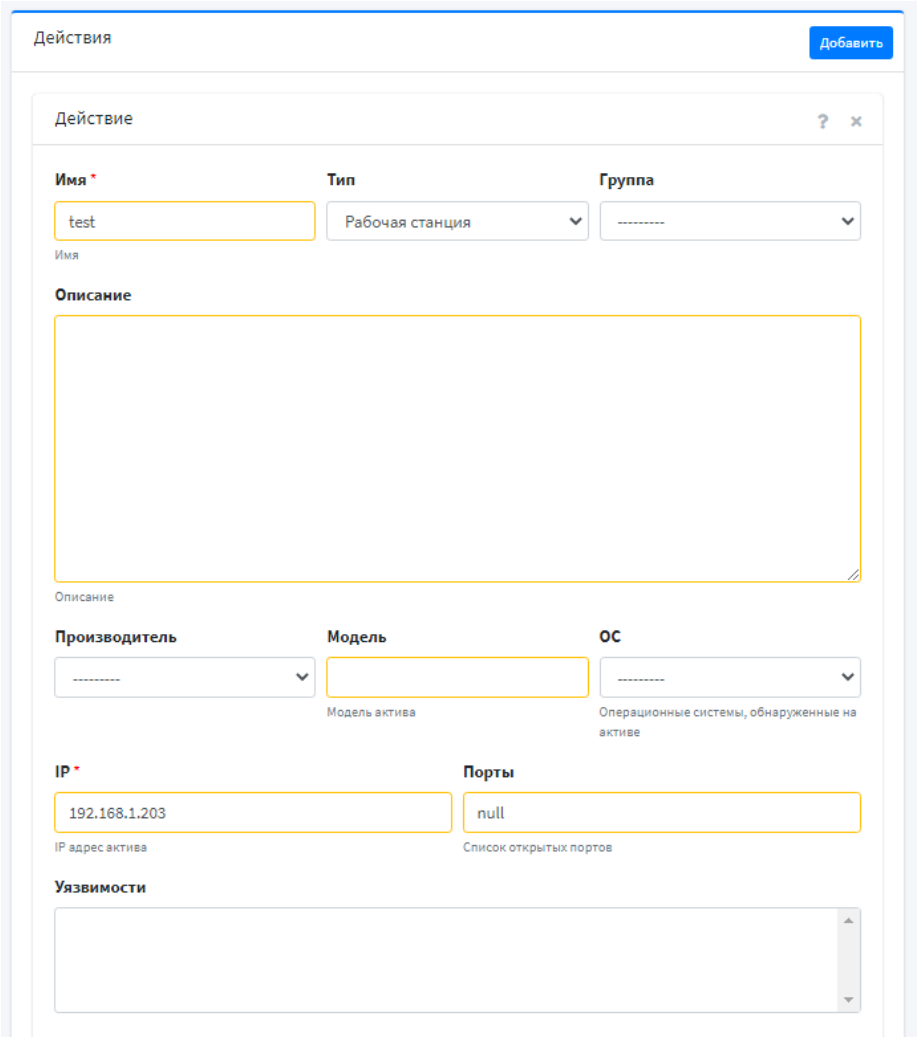


Рисунок 32 – Действие «Новый актив»

В поле «Имя» необходимо ввести имя актива. В поле «Тип» необходимо выбрать тип актива. В поле «Группа» необходимо выбрать группу. В поле «Описание» необходимо добавить описание актива. В поле «Производитель» необходимо выбрать производителя. В поле «Модель» необходимо указать модель актива. В поле «ОС» необходимо выбрать операционную систему, обнаруженную на активе. В поле «IP» необходимо ввести IP-адрес актива. В поле «Порты» необходимо указать список открытых портов. Поле «Уязвимости» не заполняется.

При выборе действия «Правило межсетевого экрана» появятся следующие поля (Рисунок 33).

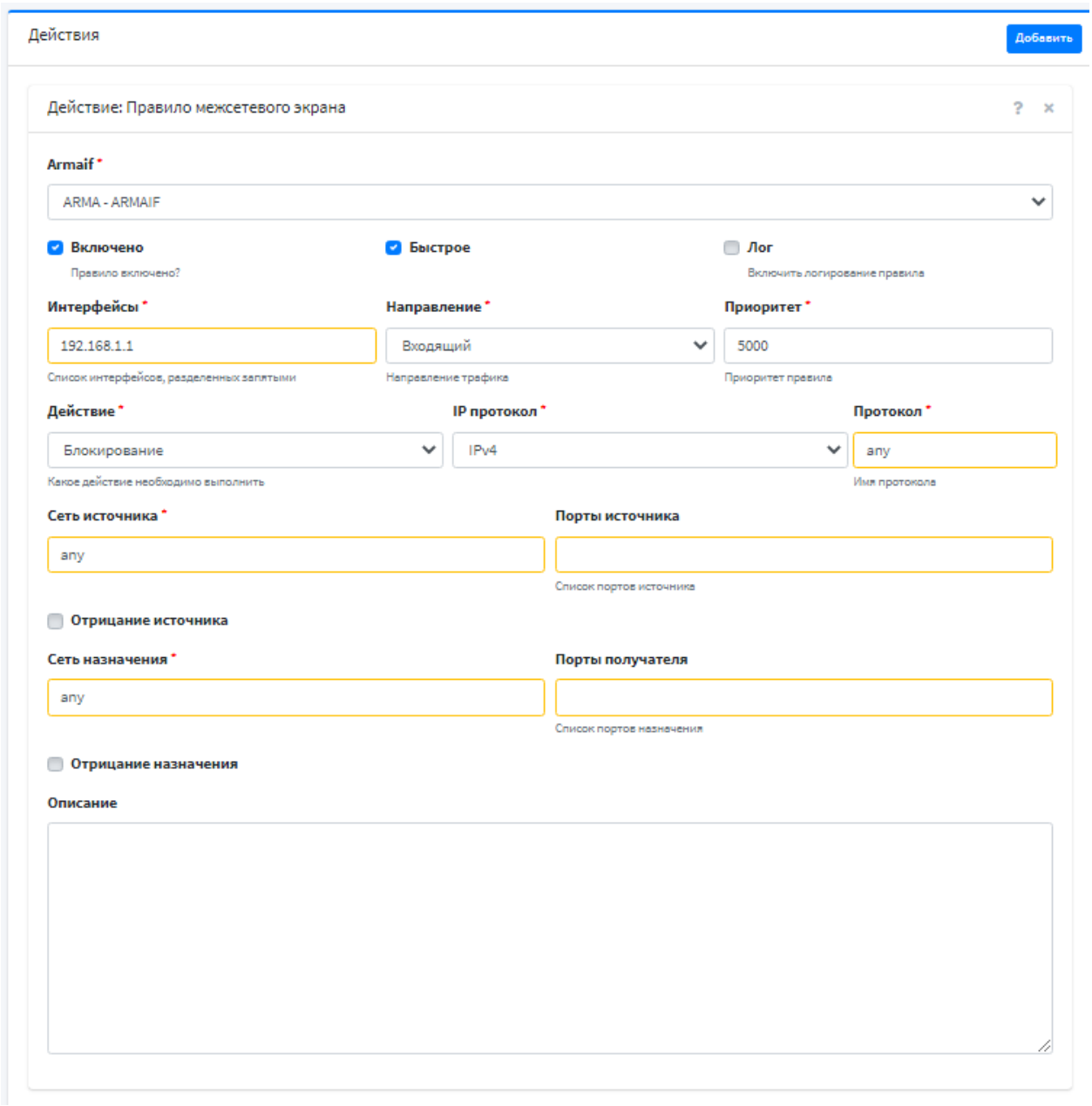


Рисунок 33 – Действие «Правило межсетевого экрана»

В поле «Armaif» необходимо выбрать систему защиты. Если правило включено необходимо установить галочку в поле «Включено». Для включения логирования правила необходимо установить галочку в поле «Лог». В поле «Интерфейс» необходимо указать список интерфейсов. В поле «Направление» необходимо выбрать направление трафика («входящий», «исходящий»). В поле «Приоритет» необходимо указать приоритет правила. В поле «Действие» необходимо выбрать действие («Разрешить», «Блокирование», «Отклонить»). В поле «IP протокол» необходимо выбрать версию протокола («Inet», «IPv4», «IPv6»). В поле «Протокол» необходимо указать название протокола. В поле «Сеть источника» необходимо указать сеть источника. В поле «Порты источника» необходимо указать порт источника. В поле «Сеть назначения» необходимо указать сеть назначения. В поле «Порты получателя» необходимо указать порт получателя. В поле «Описание» необходимо указать описание правила.

4.8.2 Настройка ротации журнала инцидентов

Текущий раздел позволяет настраивать ротацию инцидентов (Рисунок 34).

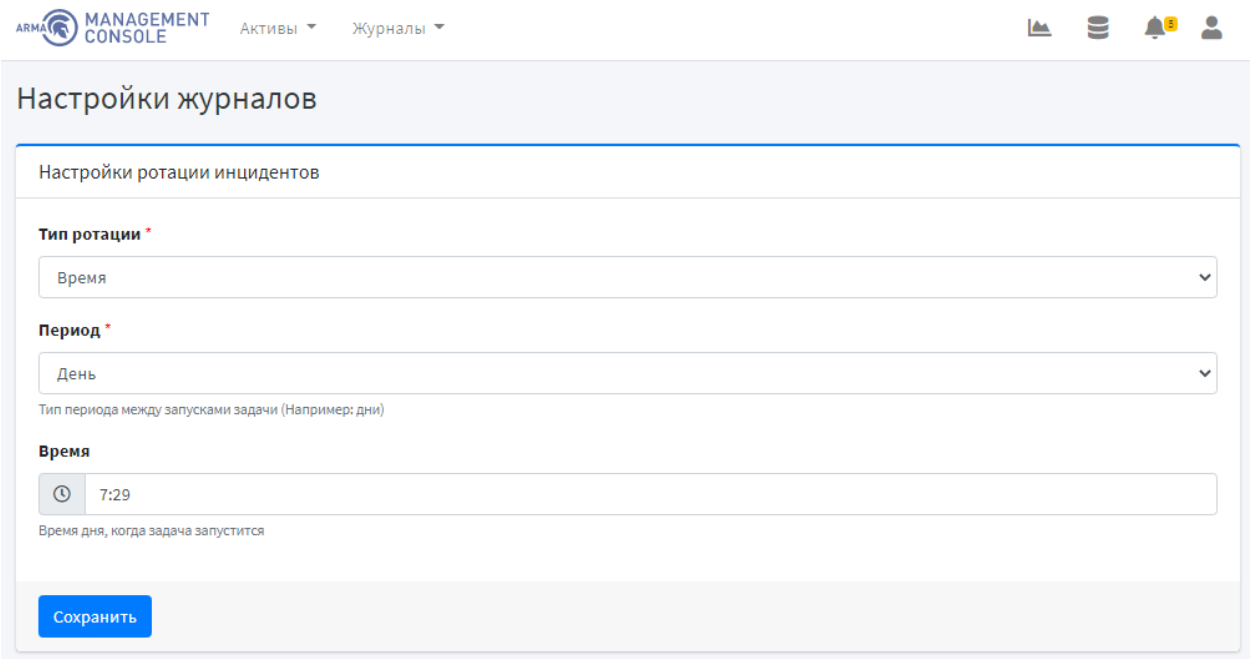


Рисунок 34 – Настройки ротации инцидентов по времени

В поле «Тип ротации» необходимо выбрать один из типов ротации – «Время», «Размер», «Отключено».

При выборе типа ротации «Время» в поле «Период» необходимо выбрать один из периодов времени – «День», «Неделя», «Месяц». При выборе периода «День» в поле «Время» необходимо указать время дня, когда будет запущена задача и нажать на кнопку Сохранить. При выборе периода «Неделя» необходимо выбрать день недели, в который будет запущена задача и нажать на кнопку Сохранить. При выборе периода «Месяц» необходимо выбрать месяц, в котором будет запущена задача и нажать на кнопку Сохранить.

При выборе типа ротации «Размер» в поле «Размер таблицы, когда происходит ротация» необходимо указать размер таблицы и нажать на кнопку (Рисунок 35).

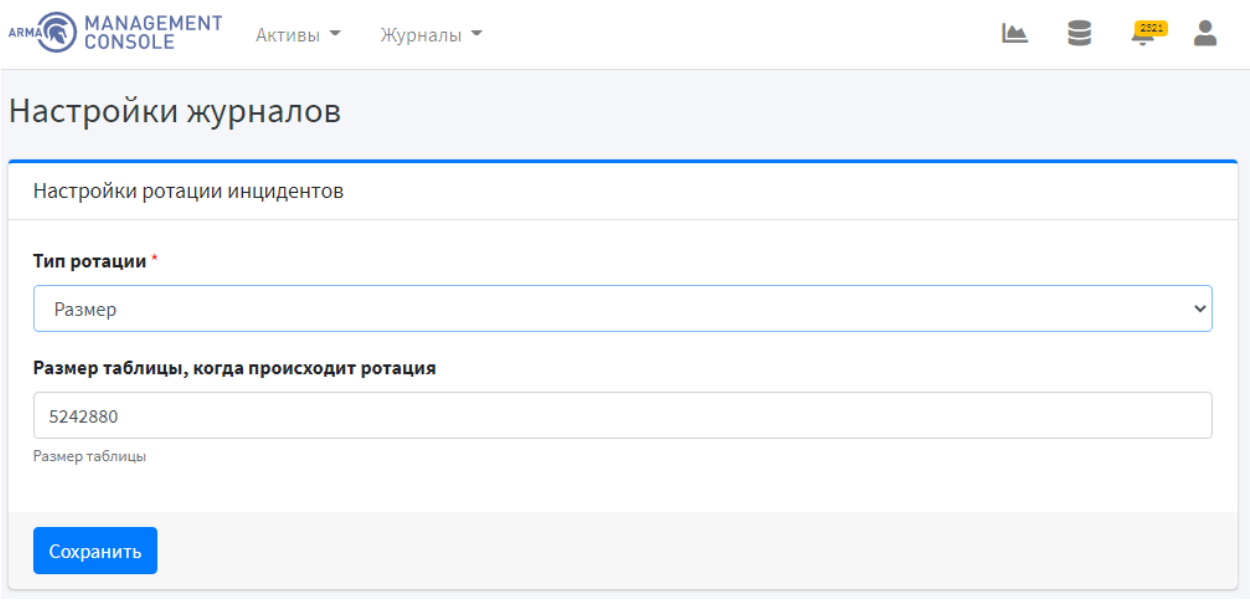


Рисунок 35 – Настройки ротации инцидентов по размеру

4.8.3 Настройка экспорта инцидентов

Текущий раздел позволяет настраивать экспорт событий по протоколам OPC UA и Syslog (Рисунок 36).

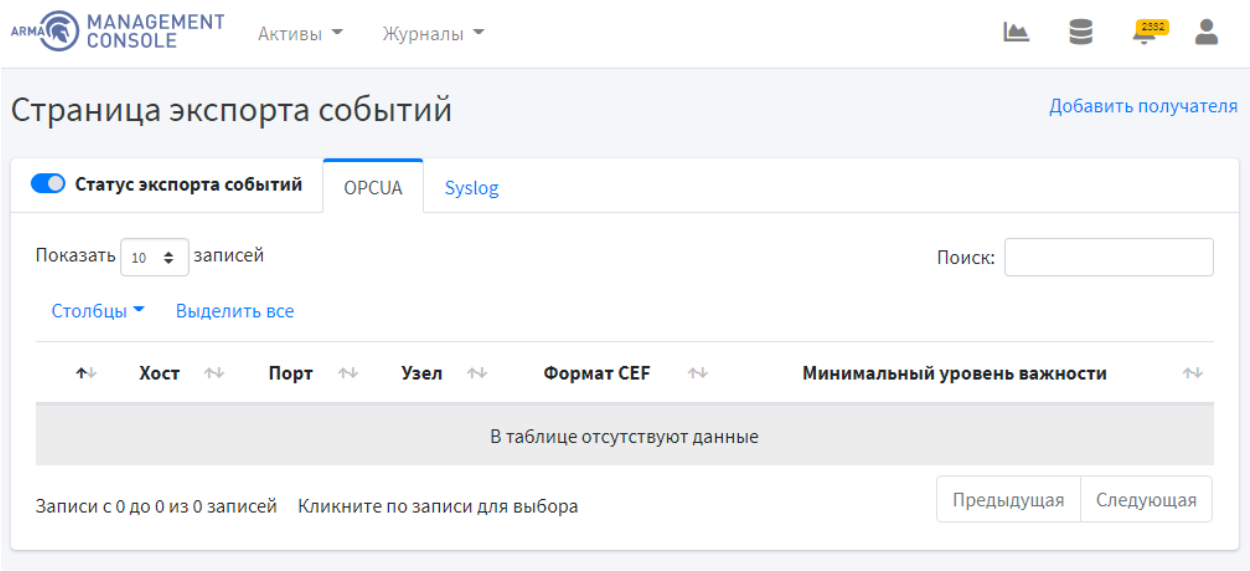


Рисунок 36 – Страница экспорта событий

Для включения/отключения экспорта событий необходимо нажать на кнопку / .

Для настройки экспорта событий по протоколам OPC UA и Syslog необходимо добавить получателя, нажав на кнопку Добавить получателя.

В поле «Тип» необходимо выбрать тип получателя и нажать на кнопку Следующий (Рисунок 37).

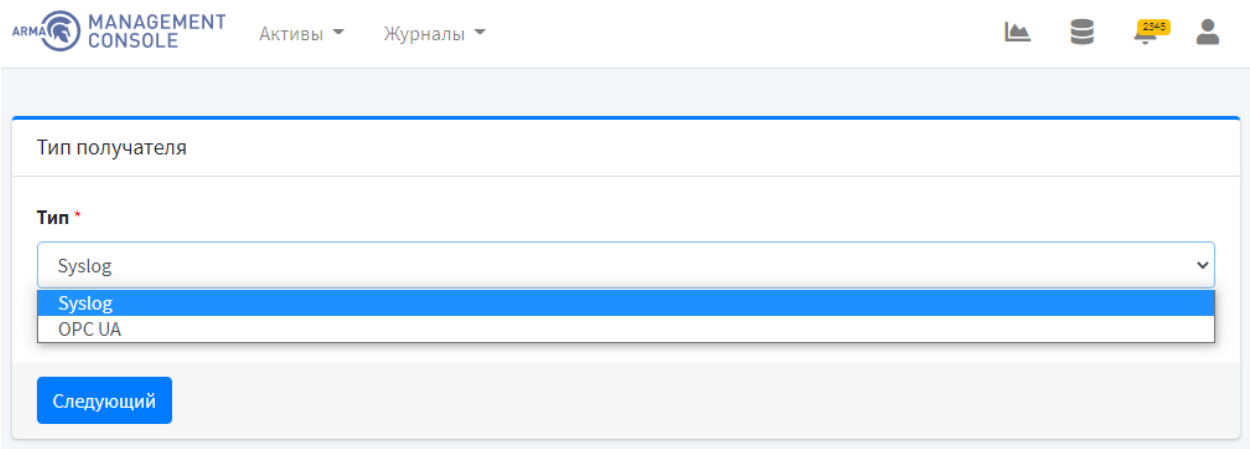


Рисунок 37 – Добавление получателя

В поле «Протокол отправки» необходимо выбрать протокол отправки, в поле «IP адрес хоста» ввести IP адрес получателя, в поле «Порт получателя» ввести порт получателя и нажать на кнопку Следующий (Рисунок 38).

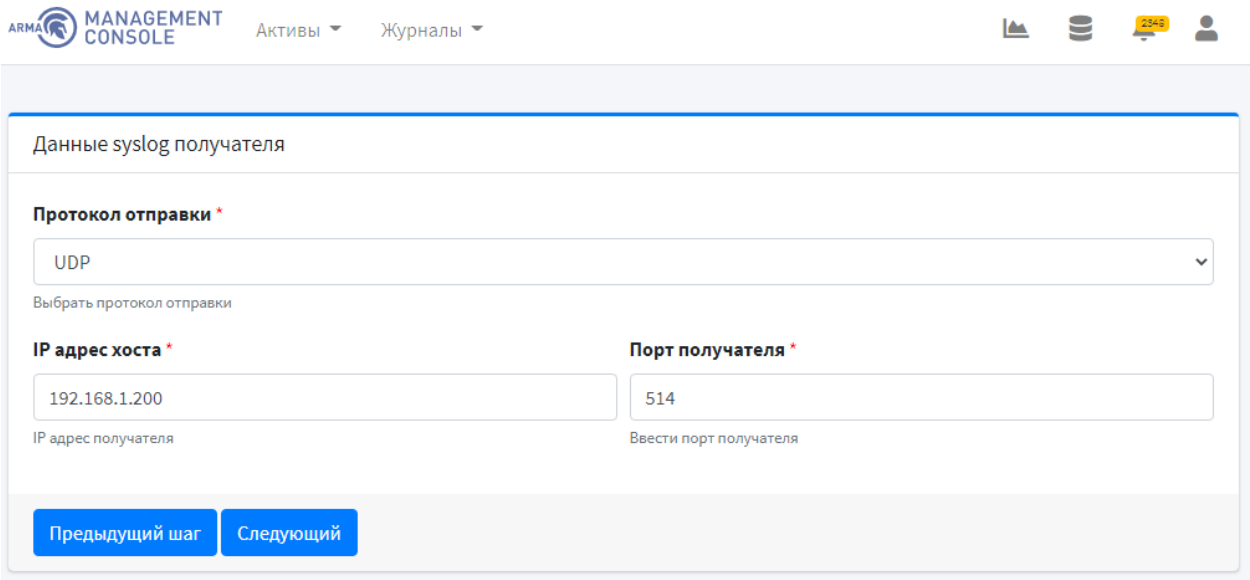


Рисунок 38 – Данные получателя

В поле «Минимальный уровень важности сообщения» необходимо выбрать минимальный уровень важности события для отправки и нажать на кнопку Сохранить (Рисунок 39).

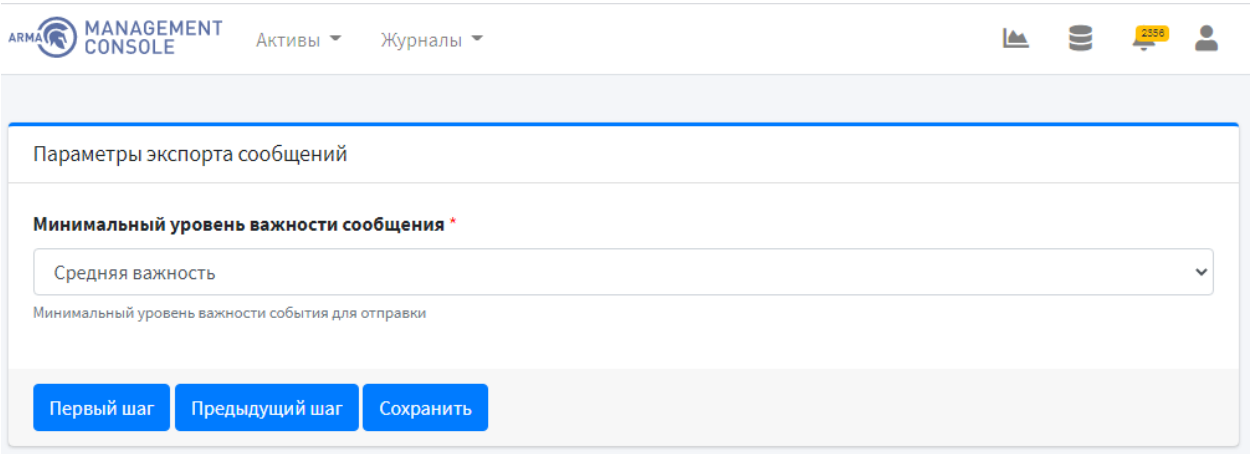


Рисунок 39 – Параметры экспорта сообщений

4.8.4 Формат сообщений при экспорте инцидентов через Syslog

4.8.4.1 Формат основного сообщения

<DateTime> <Host/IP> AMC: <MessageBody>

- **<DateTime>** - дата и время получения сообщения
- **<Host/IP>** - хост или IP адрес отправителя
- **<MessageBody>** - тело сообщения.

Пример такого сообщения:

Dec 17 17:26:32 172.18.0.10 AMC: CEF:0|InfoWatch ARMA|ARMAMC|1.0.1|Incident|test|5|cnt=1 rt=1608216295000 cs1=1c5f4516-27cb4714-af79-9643f8c18022 cs1Label=IncidentID start=1608216259000 end=1608216259000 msg=
<14>CEF:0|armaif|Suricata|2.0|429496728|suricataalert|8|unixdate\=1608216259 .676164 log_from\=suricata cid\=28775 gid\=1 signature\=429496728 rev\=1 msg\=test classification\=null priority\=3 proto\=TCP ip_src\=192.168.56.100 port_src\=80 ip_dst\=10.20.30.1 port_dst\=34568 mechanic\=IDS

4.8.4.2 Формат вложенного сообщения CEF

CEF:<Version>|<Device Vendor>|<Device Product>|<Device Version>|<Device Event Class ID>|<Name>|<Severity>|<Extension>

- **<Version>** - версия CEF
- **<Device Vendor>** - производитель источника логов (всегда InfoWatch ARMA)
- **<Device Product>** - название продукта, источника логов (всегда InfoWatch ARMA Management Console)
- **<Device Version>** - версия продукта, источника логов.
- **<Device Event Class ID>** - тип сообщения, всегда равен Incident
- **<Name>** - название инцидента
- **<Severity>** - серьезность инцидента от 0 до 10
- **<Extension>** - дополнительные поля представляющие собой пары ключ=значение. В значении, допускаются пробелы.
  - **cnt** - количество событий, сформировавших инцидент

- **rt** - время создания инцидента в формате unixtime в миллисекундах (пример: 1608216295000)
- **cs1** - уникальный идентификатор инцидента (пример: 1c5f451627cb-4714-af79-9643f8c18022)
- **cs1Label** - описание того, что записывается в cs1 (всегда IncidentID)
- **start** - время появления первого события для текущего инцидента в формате unixtime в миллисекундах (пример: 1608216295000)
- **end** - время появления последнего события для текущего инцидента в формате unixtime в миллисекундах (пример: 1608216295000)
- **msg** - описание инцидента, зависит от сформировавшего инцидент правила корреляции. Применяется экранирование символов \, = с помощью постановки символа \ перед такими символами

Пример такого сообщения:

CEF:0|InfoWatch ARMA|ARMAMC|1.0.1|Incident|test|5|cnt=1 rt=1608216295000 cs1=1c5f4516-27cb-4714-af79-9643f8c18022 cs1Label=IncidentID start=1608216259000 end=1608216259000 msg= <14>CEF:0|armaif|Suricata|2.0|429496728|suricataalert|8|unixdate\=1608216259 .676164 log_from\=suricata cid\=28775 gid\=1 signature\=429496728 rev\=1 msg\=test classification\=null priority\=3 proto\=TCP ip_src\=192.168.56.100 port_src\=80 ip_dst\=10.20.30.1 port_dst\=34568 mechanic\=IDS

В данном случае значение ключа msg в поле Extension представляет собой другое сообщение формата CEF:

<14>CEF:0|armaif|Suricata|2.0|429496728|suricataalert|8|unixdate=1608 216259.676164 log_from=suricata cid=28775 gid=1 signature=429496728 rev=1 msg=test classification=null priority=3 proto=TCP ip_src=192.168.56.100 port_src=80 ip_dst=10.20.30.1 port_dst=34568 mechanic=IDS

5 УПРАВЛЕНИЕ СИСТЕМАМИ ЗАЩИТЫ

Текущий раздел доступен пользователям с правом доступа «Может просматривать список сенсоров». Описание добавления пользователя и назначение прав доступа приведены в разделе 9 настоящего документа.

Для просмотра систем защиты необходимо перейти на страницу «Активы» - «Системы защиты» (Рисунок 40).

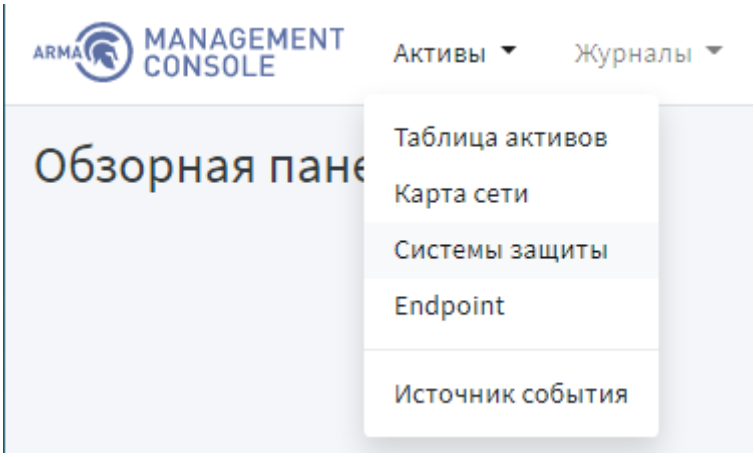


Рисунок 40 – Переход в системы защиты

5.1 Описание таблицы систем защиты

Страница «Системы защиты» позволяет просматривать системы защиты в формате таблицы, которая содержит следующие данные (Рисунок 41):

- статус;
- тип системы защиты;
- имя узла;
- IP-адрес;
- действия (отображаются только для пользователя с правом «Может управлять сенсорами»):
  - : перезагрузка системы управления;
  - : скачивание конфигурации на устройство;
  - : скачивание баз решающих правил СОВ;
  - : редактирование информации о системе защиты;
  - : удаление системы защиты из списка.

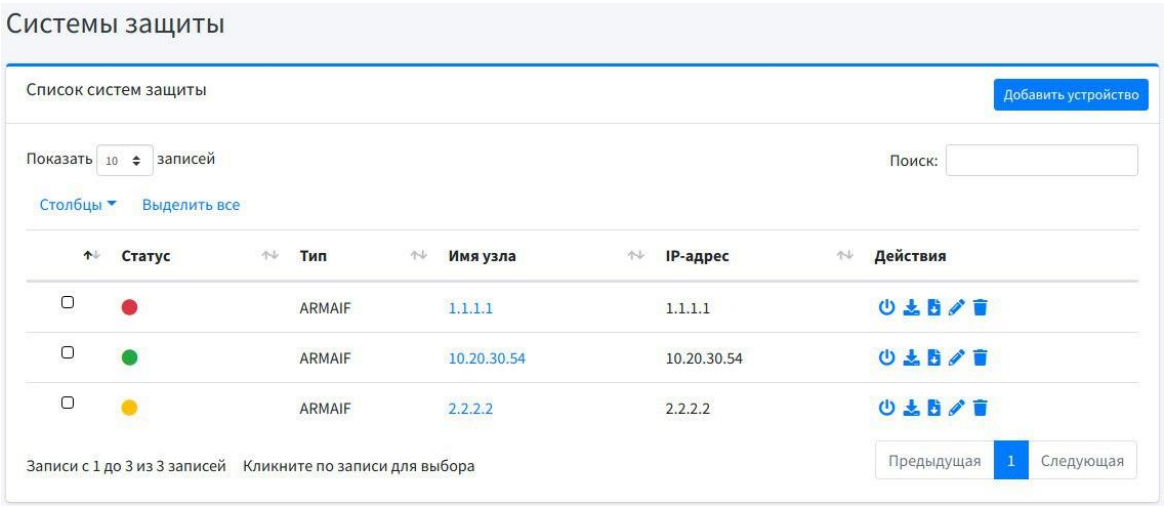


Рисунок 41 – Системы защиты

Для выбора количества записей, отображаемых в таблице систем защиты на странице «Системы защиты» необходимо нажать на кнопку 10 в левом в верхнем углу страницы.

Поле «Поиск» вверху таблицы инцидентов позволяет осуществлять сквозной поиск по всем полям таблицы. Для выполнения поиска необходимо ввести строку совпадения в поле «Поиск».

Таблица позволяет производить сортировку по каждому столбцу. Для выполнения сортировки данных столбца таблицы необходимо нажать на кнопку рядом с названием соответствующего столбца.

Для изменения столбцов, отображаемых в таблице, необходимо нажать на кнопку Столбцы .

Действия доступные для применения к нескольким системам защиты следующие (отображается только для пользователя с правом «Может управлять сенсорами»):

– : загрузка конфигурации на устройство;

– : загрузка баз решающих правил СОВ;

– : удаление системы защиты из списка.

Для применения действий ко всем системам защиты необходимо нажать на кнопку «Выделить все». Для применения действий к нескольким системам защиты необходимо поставить флажок в левом столбце напротив соответствующих систем защиты.

В столбце «Статус» отображается статус добавленных систем защиты, такие как:

– : в сети – система защиты включена и доступна;

– : не в сети – система защиты не доступна;

– : ошибка – произошла ошибка при подключении к системе защиты.

5.2 Добавление системы защиты

Текущий подраздел доступен только для пользователя с правом «Может добавлять системы защиты». Описание добавления пользователя и назначение прав доступа приведены в разделе 9 настоящего документа.

Для добавления системы защиты необходимо перейти на страницу «Активы» - «Системы защиты» и нажать кнопку Добавить устройство.

Всплывающее окно позволяет ввести необходимую информацию для подключения новой системы защиты (Рисунок 42).

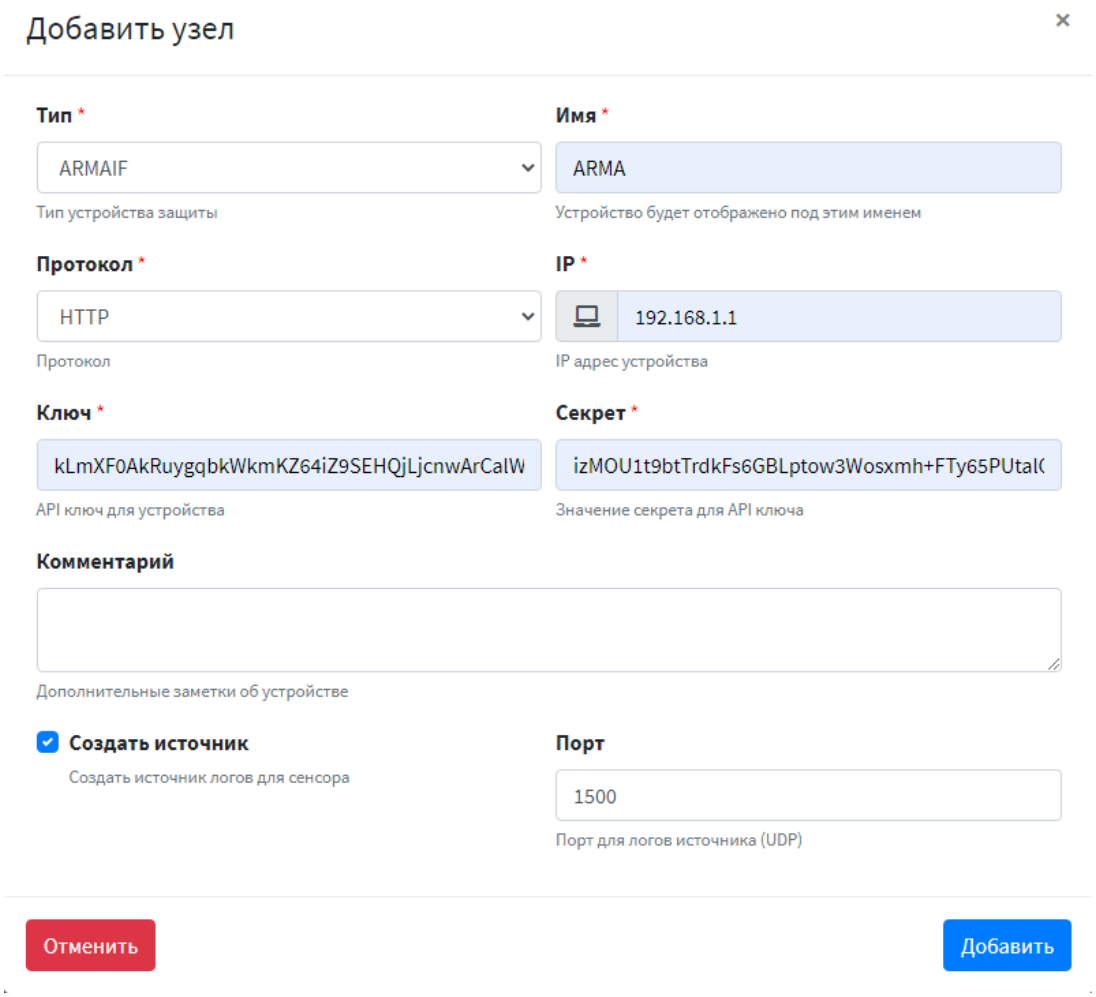


Рисунок 42 – Добавление нового устройства

В поле «Тип» необходимо выбрать тип системы защиты. В поле «Имя» необходимо ввести название системы защиты. В поле «Протокол» необходимо выбрать протокол подключения к системе защиты. В поле «IP» необходимо ввести IP-адрес подключаемой системы. В поле «Ключ» необходимо ввести ключ авторизации. В поле «Секрет» необходимо ввести «секрет» для API ключа. В поле «Комментарий» необходимо ввести комментарий к системе защиты. Для создания

источника события для системы защиты необходимо поставить галочку в поле «Создать источник». В поле «Порт» необходимо указать порт для входящих логов.

Для сохранения информации и добавления системы защиты необходимо нажать кнопку Добавить. Для отмены добавления нового устройства необходимо нажать кнопку Отменить.

5.3 Удаление системы защиты

Текущий подраздел доступен пользователям с правом доступа «Может управлять сенсорами». Описание добавления пользователя и назначение прав доступа приведены в разделе 8 настоящего документа.

Для удаления системы защиты необходимо перейти на страницу «Активы» - «Системы защиты». В таблице систем защиты необходимо нажать на напротив системы защиты, которую собираетесь удалить. После нажатия необходимо подтвердить удаление, нажав во всплывающем окне кнопку «Да».

Для удаления нескольких систем защиты необходимо перейти на страницу «Активы» - «Системы защиты». В таблице систем защиты необходимо выбрать несколько систем защиты (для выбора всех систем защиты нажать кнопку «Выделить все» вверху таблицы) и нажать на вверху таблицы. После нажатия необходимо подтвердить удаление, нажав во всплывающем окне кнопку «Да».

5.4 Редактирование основной информации о системе защиты

Текущий подраздел доступен пользователям с правом доступа «Может управлять сенсорами». Описание добавления пользователя и назначение прав доступа приведены в разделе 8 настоящего документа.

Для редактирования системы защиты необходимо перейти на страницу «Активы» - «Системы защиты» и нажать кнопку напротив системы защиты.

Всплывающее окно позволяет изменить необходимую информацию системы защиты (Рисунок 43).

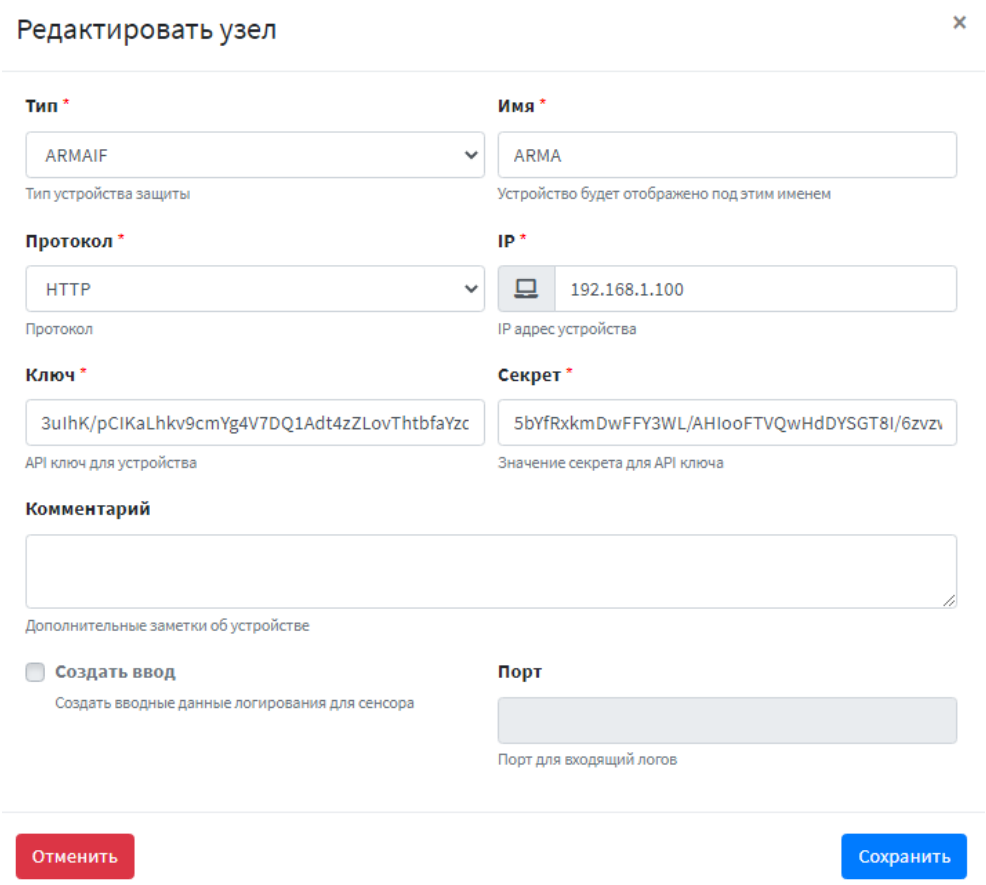


Рисунок 43 – Окно редактирования системы защиты

Для сохранения изменения информации о системе защиты необходимо нажать кнопку Сохранить. Для отмены добавления нового устройства необходимо нажать кнопку Отменить.

5.5 Работа с конфигурациями систем защиты

Текущий подраздел доступен пользователям с правом доступа «Может управлять сенсорами». Описание добавления пользователя и назначение прав доступа приведены в разделе 9 настоящего документа.

5.5.1 Скачивание конфигурации системы защиты

Для скачивания конфигурации системы защиты необходимо перейти на страницу «Активы» - «Системы защиты» и нажать кнопку напротив системы защиты. При успешном скачивании файла конфигурации появится всплывающее уведомление об этом.

5.5.2 Загрузка конфигурации на систему/системы защиты

Для загрузки файла конфигурации системы защиты необходимо перейти на страницу «Активы» - «Системы защиты». В таблице систем защиты необходимо выбрать системы защиты (для выбора всех систем защиты необходимо нажать

кнопку «Выделить все») и нажать на вверху таблицы. После нажатия необходимо выбрать файл конфигурации. При успешной загрузке конфигурации на систему/системы защиты в верхнем правом углу появится уведомление об этом.

5.6 Работа с правилами СОВ систем защиты

Текущий подраздел доступен пользователям с правом доступа «Может управлять сенсорами». Описание добавления пользователя и назначение прав доступа приведены в разделе 9 настоящего документа.

5.6.1 Скачивание правил СОВ системы защиты

Для скачивания привил СОВ системы защиты необходимо перейти на страницу «Активы» - «Системы защиты» и нажать кнопку напротив соответствующей системы защиты. При успешном скачивании файла правил СОВ появится всплывающее уведомление об этом.

5.6.2 Загрузка правил СОВ на систему/системы защиты

Для загрузки файла правил СОВ системы защиты необходимо перейти на страницу «Активы» - «Системы защиты». В таблице систем защиты необходимо выбрать соответствующие системы защиты (для выбора всех систем защиты необходимо нажать кнопку «Выделить все») и нажать на вверху таблицы. После нажатия необходимо выбрать файл правил СОВ. При успешной загрузке правил СОВ на систему/системы защиты в верхнем правом углу появится уведомление об этом.

5.7 Добавление Endpoint

Текущий подраздел доступен только для пользователя с правом «Может добавлять Endpoint». Описание добавления пользователя и назначение прав доступа приведены в разделе 9 настоящего документа.

Для добавления Endpoint необходимо перейти на страницу «Активы» - «Endpoint» и нажать кнопку Добавить (Рисунок 44).

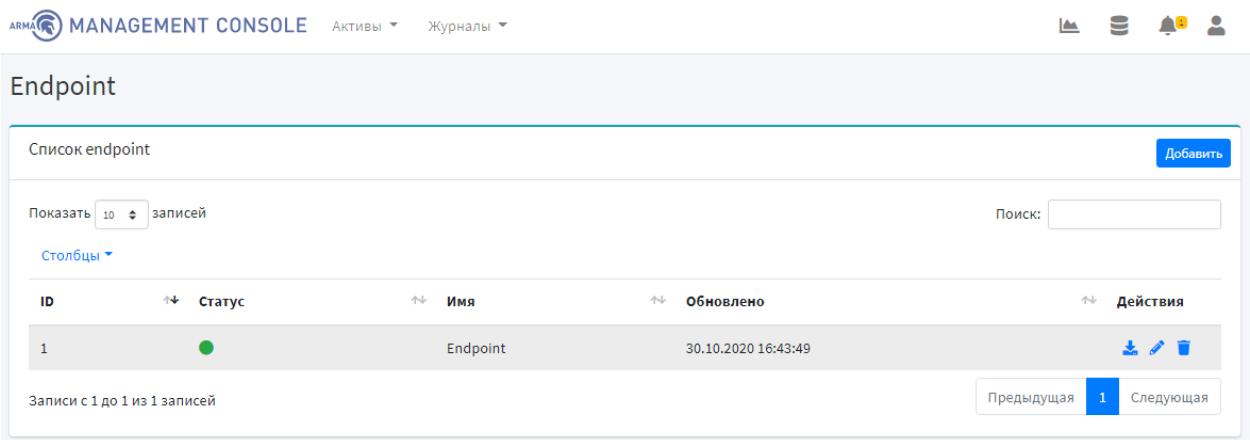


Рисунок 44 – Страница Endpoint

В поле «Имя» необходимо задать имя Endpoint. В поле «Описание» необходимо добавить описание Endpoint. Для создания источника события для Endpoint необходимо поставить галочку в поле «Создать источник». В поле «Порт» необходимо указать порт для входящих логов. В поле «IP» необходимо ввести адрес устройства. Для записи запущенных программ необходимо поставить галочку в поле «Режим обучения» (Рисунок 45).

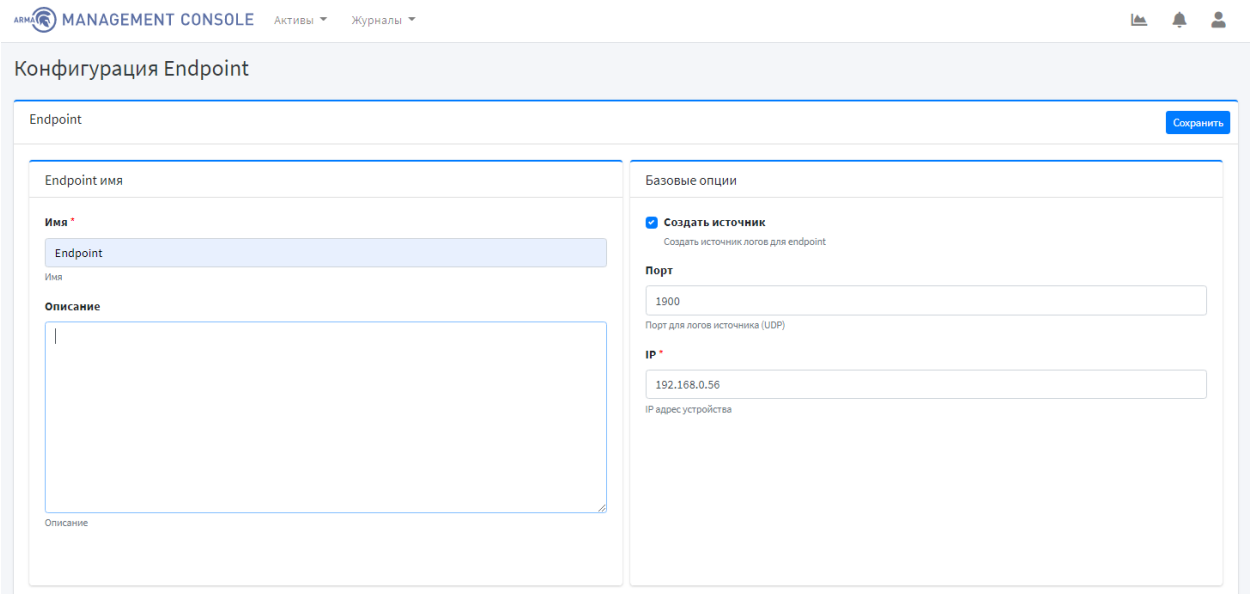


Рисунок 45 – Добавление Endpoint

В блоке «Директории для сканирования» необходимо добавить путь к файлу или папке, который будет сканироваться. Для включения контроля целостности и проверки чексумм по базе необходимо установить галочки в соответствующих полях «Включить контроль целостности» и «Включить проверку чексумм по базе». В поле «Таймаут создания события» необходимо задать частоту получения событий контроля целостности. В поле «Таймаут сканирования директории» необходимо задать частоту пересканирования директории (Рисунок 46).

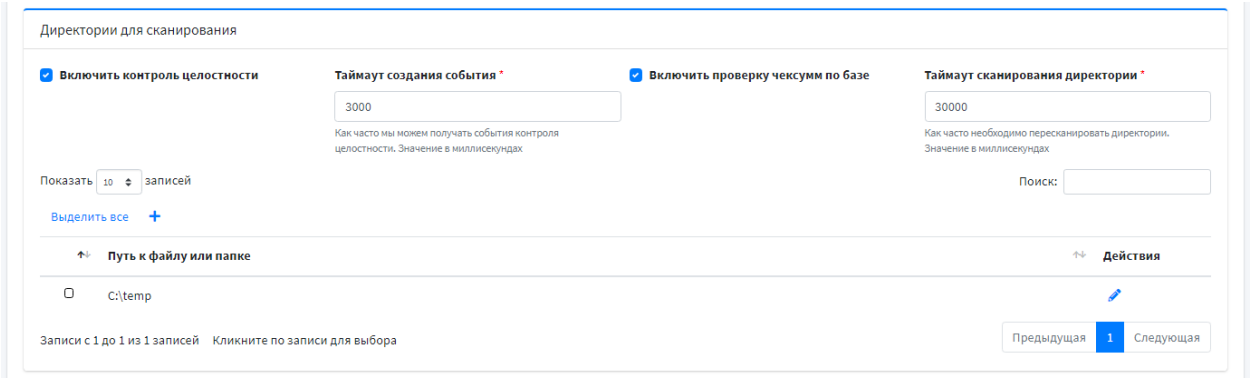


Рисунок 46 – Добавление Endpoint. Директории для сканирования

В блоке «Белый список приложений» необходимо указать путь к файлу или папке, доступ к которому будет разрешен. По умолчанию заданы пути, указанные на рисунке ниже (Рисунок 47). Для включения белого списка и принудительного обновления политики необходимо установить галочки в соответствующих полях

«Включить белый список» и «Включить gpupdate». При необходимости разрешения локальному администратору игнорировать белый список необходимо установить галочку в поле «Локальный администратор игнорирует белый список» (Рисунок 47).

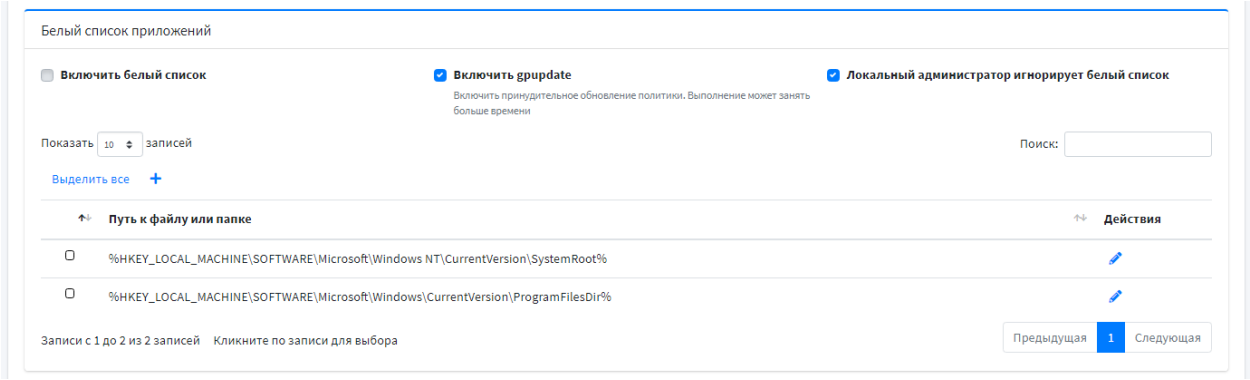


Рисунок 47 – Добавление Endpoint. Белый список приложений

Блок «Права доступа» позволяет настраивать различные права доступа. Для включения контроля устройств и принудительного обновления политики необходимо установить галочки в соответствующих полях «Включить контроль устройства» и «Включить gpupdate» (Рисунок 48).

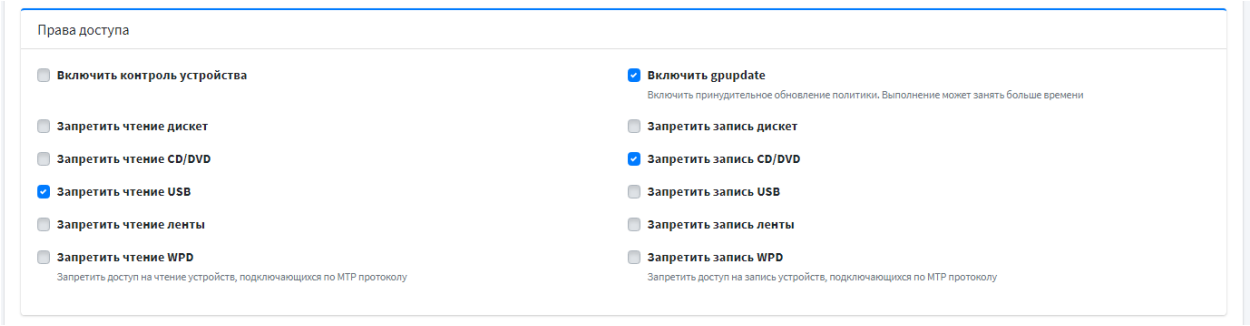


Рисунок 48 – Добавление Endpoint. Права доступа

Блок «GUI» позволяет включать контроль источников событий с помощью веб-интерфейса (Рисунок 49).

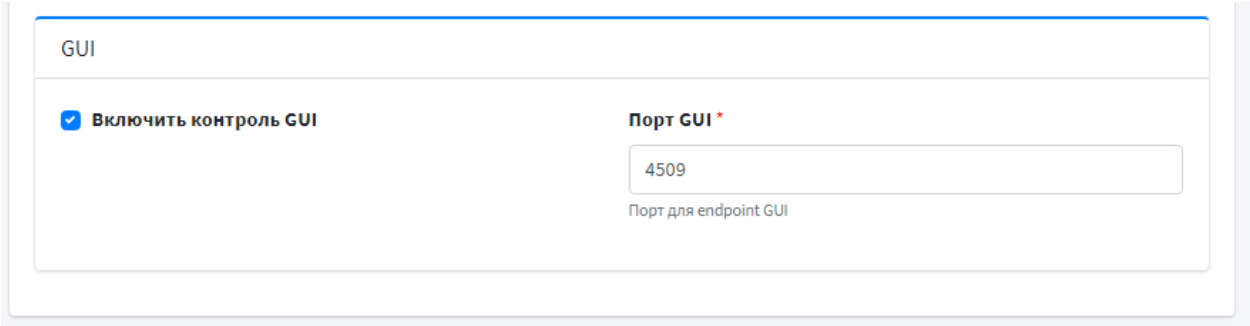


Рисунок 49 – Добавление Endpoint. GUI

6 УПРАВЛЕНИЕ ИСТОЧНИКАМИ СОБЫТИЯ

Текущий раздел позволяет настраивать связи логирования.

Для просмотра списка источников логов необходимо перейти на страницу «Активы» - «Источник события» (Рисунок 50).

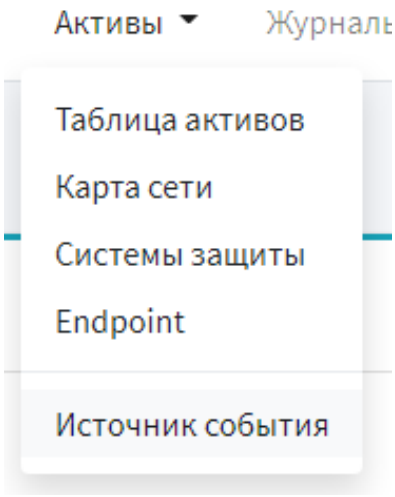


Рисунок 50 – Переход на страницу источников событий

Страница «Источник события» позволяет просматривать список источников логов в формате таблицы (Рисунок 51).

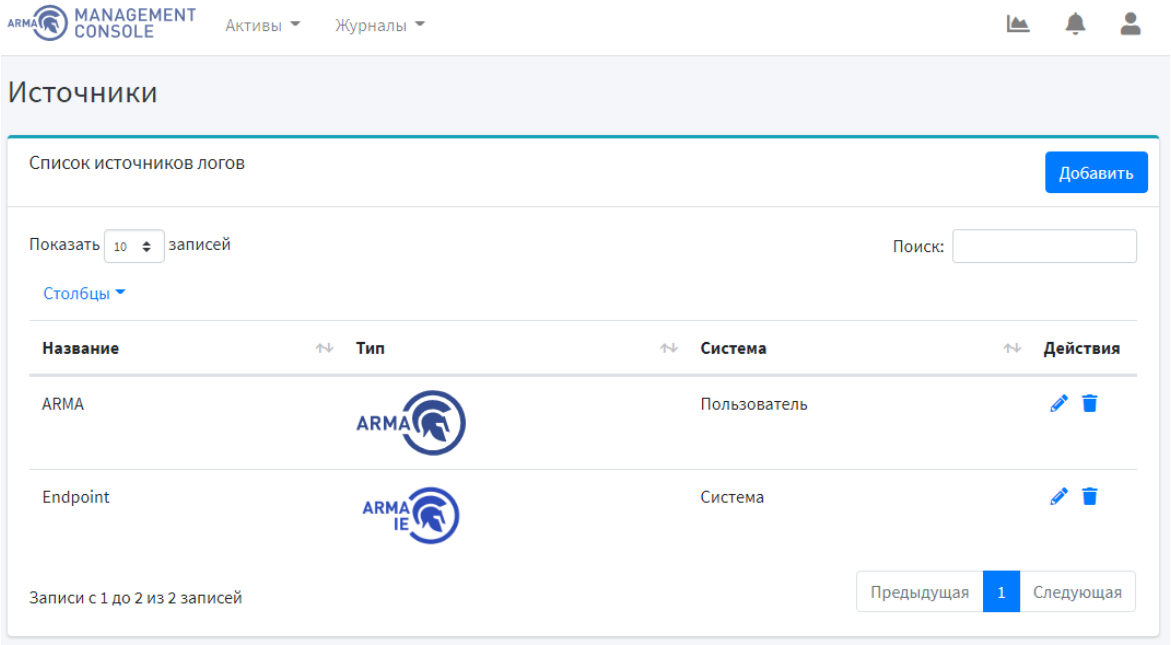
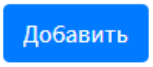


Рисунок 51 – Список источников логов

6.1 Добавление источника события

Для создания источника события необходимо нажать на кнопку 

. В поле «Имя» необходимо ввести название источника. В поле «Тип» необходимо выбрать тип источника логов (Рисунок 52).

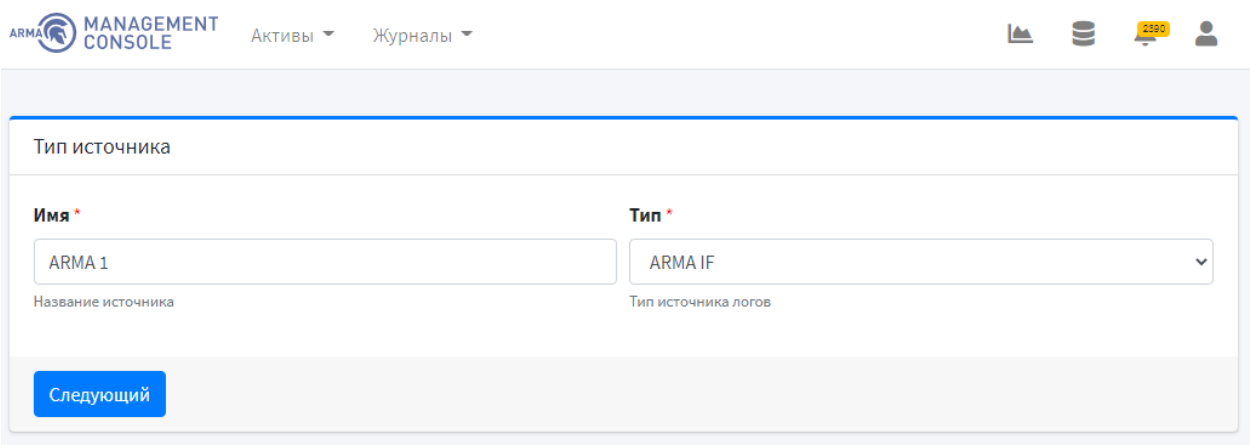


Рисунок 52 – Добавление источника события

Для перехода на второй шаг («Входные данные логов ARMA IF») необходимо нажать на кнопку Следующий, в поле «Порт» указать номер порта источника и затем нажать на кнопку Сохранить (Рисунок 53). Для возврата к предыдущему шагу необходимо нажать на соответствующую кнопку Предыдущий шаг.

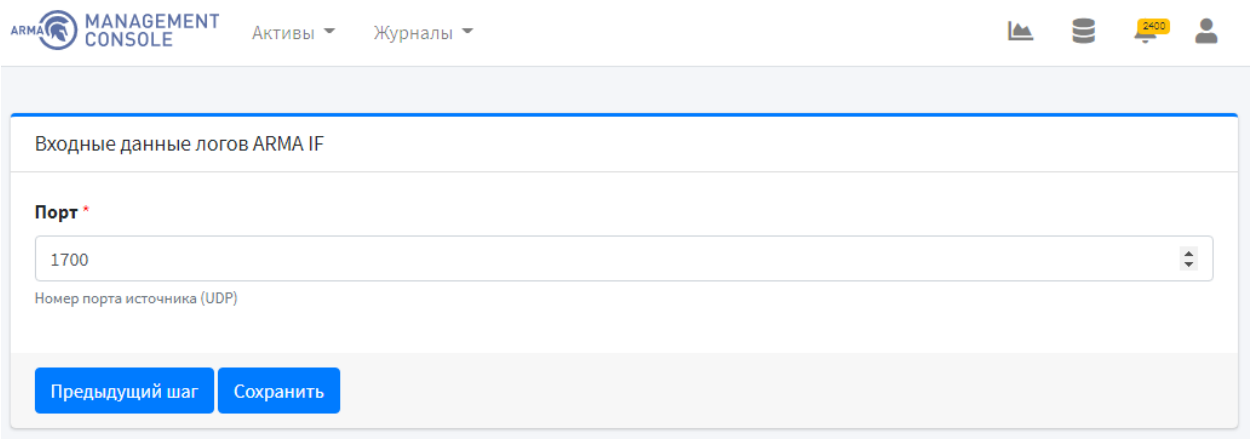


Рисунок 53 – Входные данные логов ARMA IF

7 УПРАВЛЕНИЕ СПИСКОМ УСТРОЙСТВ СЕТИ

Текущий раздел доступен пользователям с правом доступа «Может просматривать активы». Описание добавления пользователя и назначение прав доступа приведены в разделе 9 настоящего документа.

Для просмотра устройств сети необходимо перейти на страницу «Активы» - «Таблица активов» (Рисунок 54).

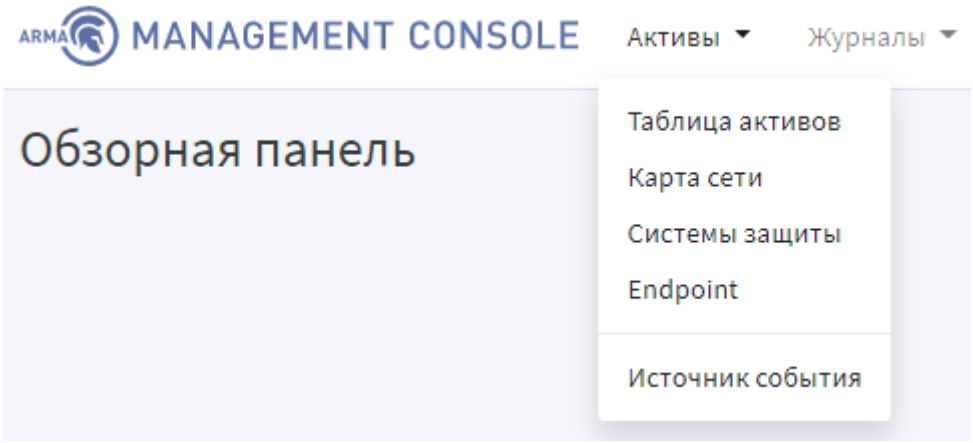


Рисунок 54 – Переход в таблицу активов

7.1 Описание таблицы устройств сети

Страница «Таблица активов» позволяет просматривать активы в формате таблицы, которая содержит следующие данные (Рисунок 55):

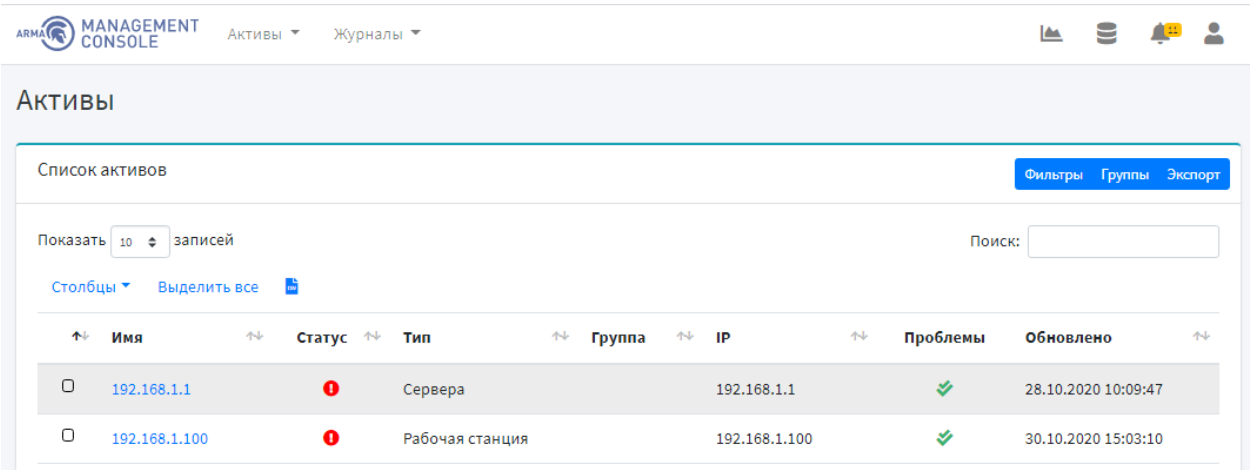


Рисунок 55 – Таблица активов

Для выбора количества записей, отображаемых в таблице на странице «Таблица активов» необходимо нажать на кнопку 10 в верхнем левом углу страницы.

7.2 Поиск, сортировка и фильтрация устройств сети

Поле «Поиск» вверху таблицы инцидентов позволяет осуществлять сквозной поиск по всем полям таблицы. Для выполнения поиска необходимо ввести строку совпадения в поле «Поиск».

Для фильтрации по определенным столбцам таблицы событий необходимо нажать кнопку Фильтры. Всплывающее окно позволяет задать фильтры отображения таблицы инцидентов (Рисунок 56). В поле «Группа» необходимо выбрать группу устройств сети. В поле «ОС» необходимо выбрать ОС устройства сети. В поле «Тип» необходимо выбрать тип актива. В поле «Статус актива» необходимо выбрать статус разрешенности актива. В поле «Обновлено» необходимо выбрать промежуток времени обнаружения устройства. Для закрытия окна задания фильтра необходимо нажать кнопку Закрыть. Для сохранения и применения фильтров необходимо нажать кнопку Применить.

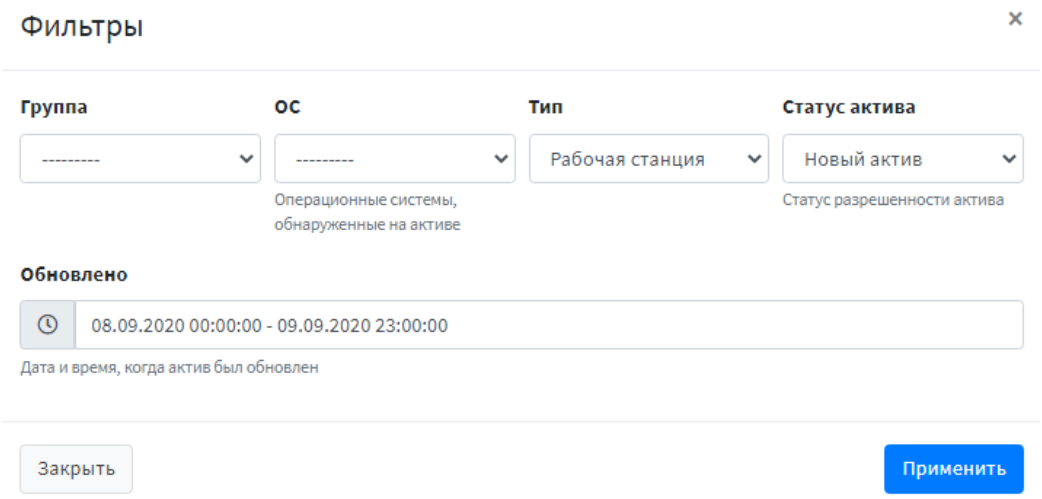


Рисунок 56 – Фильтрация списка активов

Таблица позволяет производить сортировку по каждому столбцу. Для выполнения сортировки данных столбца таблицы необходимо нажать на кнопку ↑↓ рядом с названием соответствующего столбца.

7.3 Редактирование основной информации об устройстве сети

Для редактирования основной информации об устройстве необходимо перейти на страницу «Таблица активов». В таблице активов необходимо нажать на ссылку названия этого устройства сети (столбец «Имя»), например, 192.168.1.1. При нажатии на название устройства сети InfoWatch ARMA Management Console отобразит страницу подробной информации об устройстве (Рисунок 57). В поле «Группы» необходимо выбрать группу сетевого устройства. В поле «Название» необходимо ввести название устройства. В поле «Описание» необходимо ввести название устройства. Для сохранения изменений необходимо нажать кнопку Сохранить.

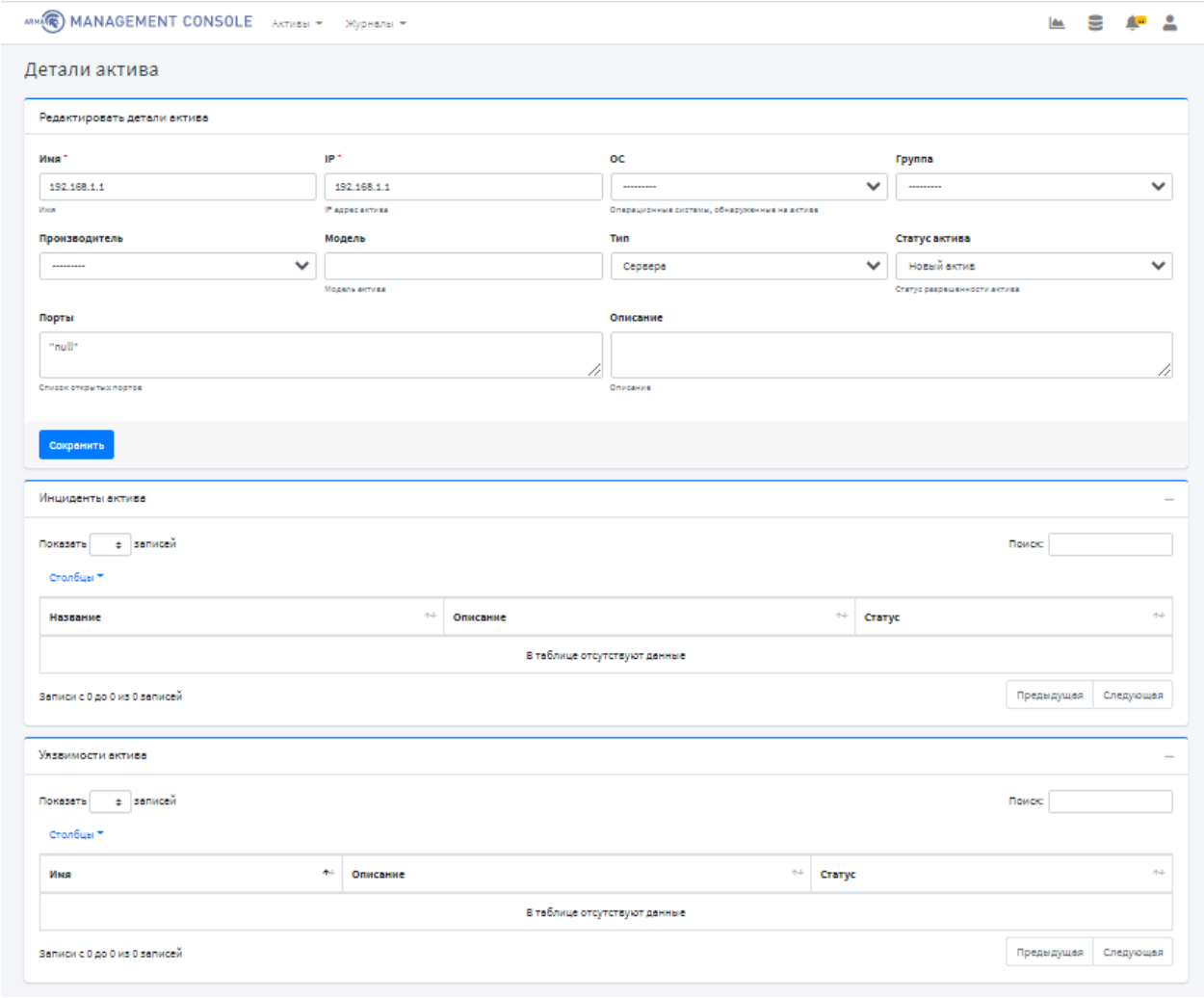


Рисунок 57 – Подробная информация об устройстве сети

7.4 Добавление группы устройств сети

Текущий подраздел доступен пользователям с правом доступа «Может редактировать группы активов». Описание добавления пользователя и назначение прав доступа приведены в разделе 9 настоящего документа.

Для добавления группы систем защиты необходимо перейти на страницу «Активы» - «Таблица активов» и нажать кнопку Группы. Во всплывающем окне отобразится список предустановленных групп (без возможности редактирования/удаления) и пользовательских групп (Рисунок 58). Для добавления новой группы необходимо нажать кнопку Добавить.

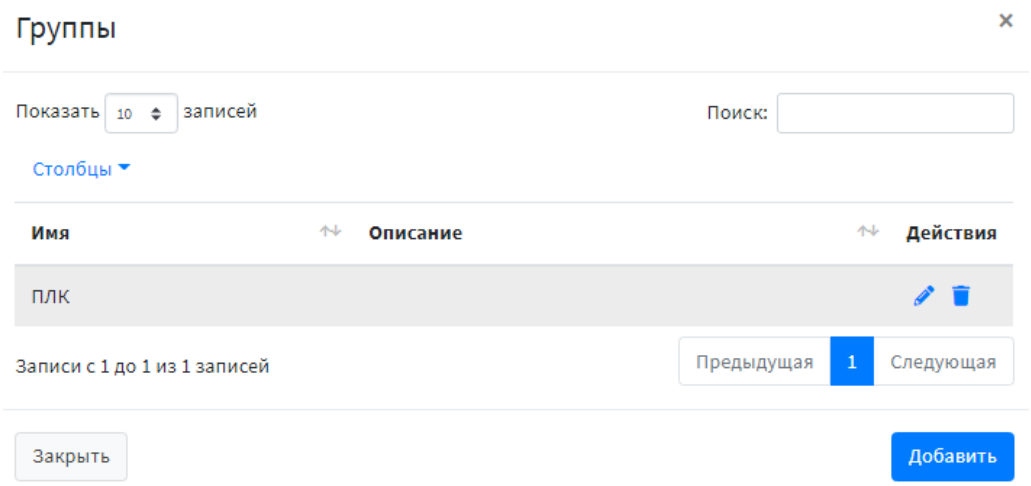


Рисунок 58 – Список групп активов

Окно добавления группы (Рисунок 59) позволяет ввести необходимую информацию для создания новой группы. В поле «Название» необходимо ввести название группы устройств сети. В поле «Описание» необходимо ввести описание группы устройств. Для закрытия окна добавления группы необходимо нажать кнопку Закрыть . Для сохранения группы устройств сети необходимо нажать кнопку Сохранить изменения . В случае успешного добавления группы появится уведомление об этом.

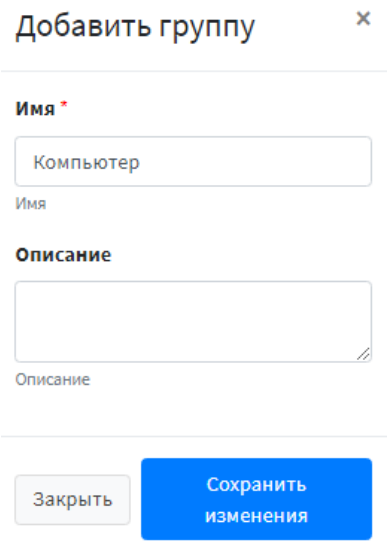


Рисунок 59 – Добавление группы устройств сети

7.5 Удаление группы устройств сети

Текущий подраздел доступен пользователям с правом доступа «Может редактировать группы активов». Описание добавления пользователя и назначение прав доступа приведены в разделе 9 настоящего документа.

Для удаления группы необходимо перейти на страницу «Активы» - «Таблица активов» и нажать кнопку Группы. Во всплывающем окне отобразится список предустановленных групп (без возможности редактирования/удаления) и пользовательских групп. Для удаления пользовательской группы необходимо нажать кнопку напротив соответствующей группы.

После нажатия на кнопку необходимо подтвердить удаление во всплывающем окне (Рисунок 60). Для этого необходимо нажать кнопку «ОК». В случае успешного удаления группы появится уведомление об этом.

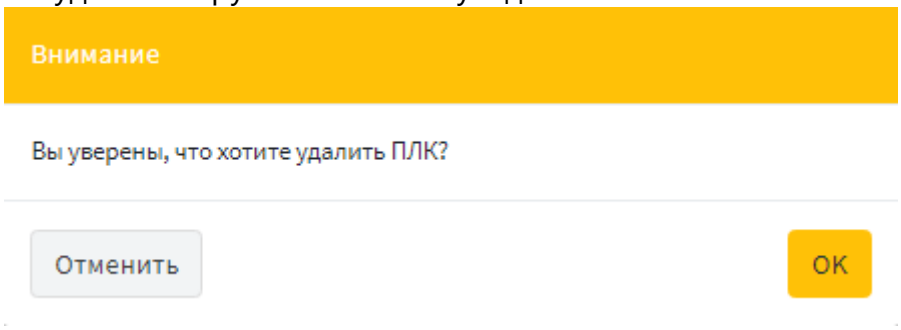


Рисунок 60 – Подтверждение удаления группы

7.6 Редактирование групп

Текущий подраздел доступен пользователям с правом доступа «Может редактировать группы активов». Описание добавления пользователя и назначение прав доступа приведены в разделе 9 настоящего документа.

Для редактирования группы необходимо перейти на страницу «Активы» - «Таблица активов» и нажать кнопку Группы. Во всплывающем окне отобразится список предустановленных групп (без возможности редактирования/удаления) и пользовательских групп. Для редактирования пользовательской группы необходимо нажать кнопку напротив группы.

Окно редактирования группы (Рисунок 61) позволяет ввести необходимую информацию о группе. В поле «Название» необходимо ввести название группы устройств сети. В поле «Описание» необходимо ввести описание группы устройств.

Для закрытия окна редактирования группы необходимо нажать кнопку Закрыть.

Для сохранения группы устройств сети необходимо нажать кнопку Сохранить изменения.

В случае успешного добавления группы появится уведомление об этом.

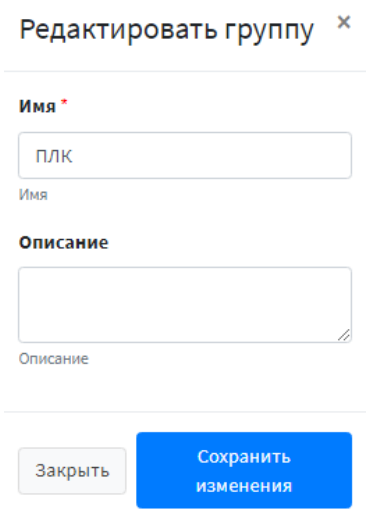


Рисунок 61 – Редактирование группы устройств сети

8 НАСТРОЙКА КАРТЫ СЕТИ

Текущий раздел доступен пользователям с правом доступа «Может просматривать структуру сети». Описание добавления пользователя и назначение прав доступа приведены в разделе 9 настоящего документа.

Для просмотра устройств сети необходимо перейти на страницу «Активы» - «Карта сети» (Рисунок 62).

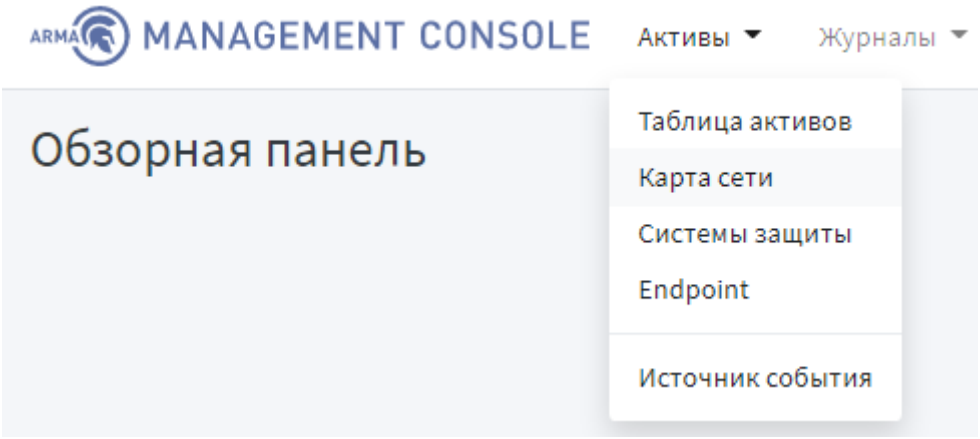


Рисунок 62 – Переход на карту сети

8.1 Описание карты сети

На странице «Активы» - «Карта сети» отображаются устройства сети и их связи (Рисунок 63) в соответствие с таблицей устройств сети на странице «Активы» - «Таблица активов» (Рисунок 55). Карта сети позволяет:

- просматривать все устройства сети;
- просматривать связи между устройствами сети;
- перемещать устройства сети;
- просматривать подробную информацию об устройстве сети.
- выбирать масштаб отображения карты сети;
- добавлять/удалять связи между устройствами.

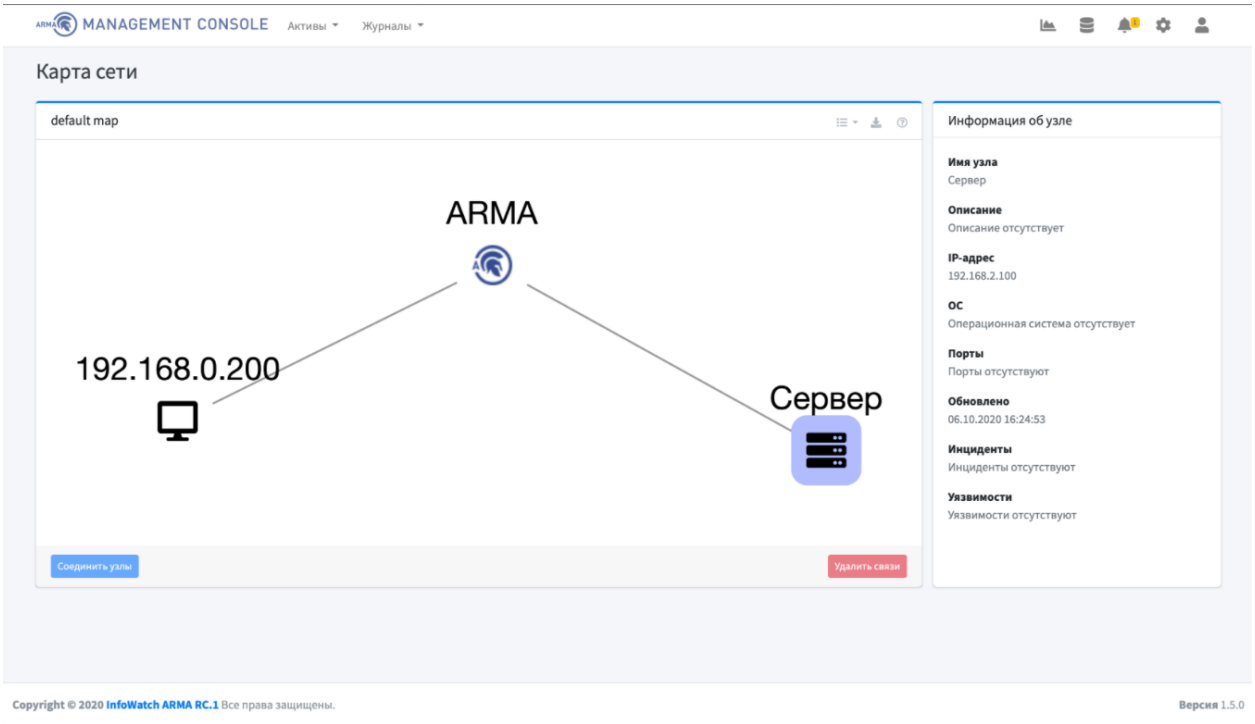


Рисунок 63 – Карта сети

Для перемещения устройства по карте сети необходимо зажать устройство левой клавишей мыши и передвинуть объект в другое место.

При нажатии на устройство сети открывается окно со следующей информацией:

- название узла;
- описание;
- IP-адрес узла;
- ОС;
- порты;
- обновлено;
- инциденты;
- уязвимости (отображаются только пользователю с правом доступа «Может просматривать уязвимости»).

8.2 Создание и удаление связей устройств

Для создания связей устройств сети необходимо перейти на страницу «Активы» - «Карта сети», выбрать устройства сети, которые необходимо соединить, и нажать кнопку Соединить узлы. Появится связь между устройствами.

Для удаления связей устройств сети необходимо перейти на страницу «Активы» - «Карта сети», выбрать устройства сети, связь которых необходимо удалить, и нажать кнопку Удалить связи, чтобы удалить связь между устройствами.

9 УПРАВЛЕНИЕ УЧЕТНЫМИ ЗАПИСЯМИ И РОЛЯМИ СИСТЕМЫ

9.1 Профиль пользователя

Для перехода на страницу «Профиль пользователя» необходимо нажать на  в верхнем меню, а затем выбрать «Профиль пользователя» (Рисунок 64).

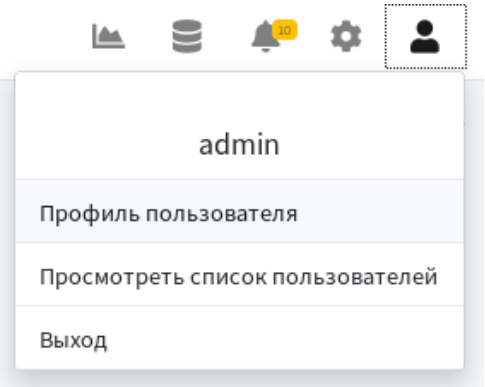


Рисунок 64 – Переход в профиль пользователя

Страница «Профиль пользователя» позволяет просматривать следующие данные о текущем пользователе (Рисунок 65):

- имя;
- адрес электронной почты;
- комментарий;
- временная зона;
- дата окончания срока действия;
- список групп, в которых состоит пользователь.

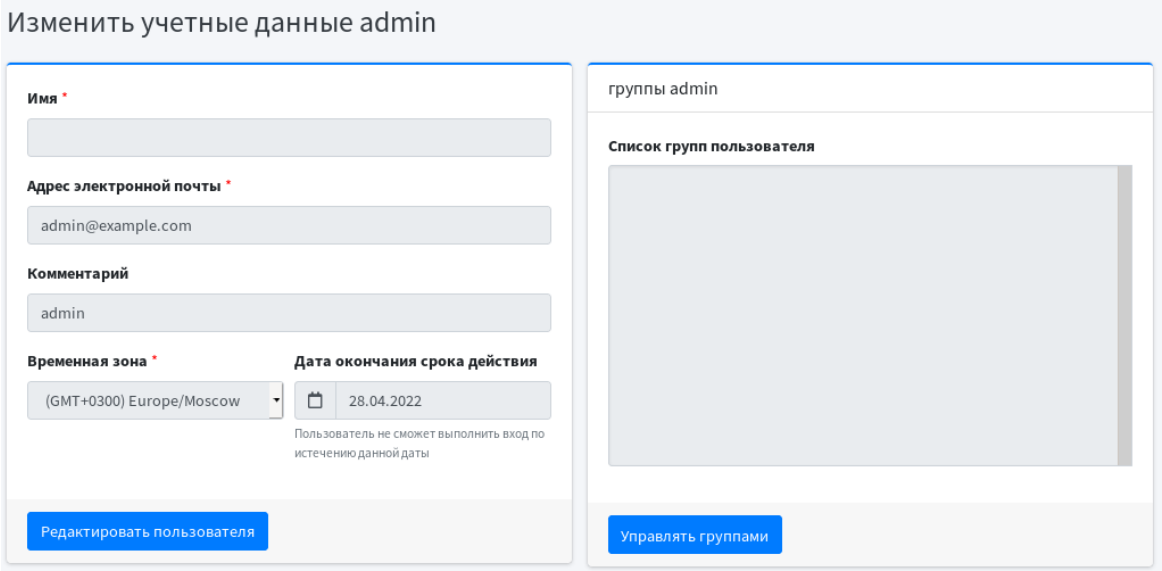


Рисунок 65 – Профиль текущего пользователя (просмотр)

9.2 Список пользователей

Текущий подраздел доступен пользователю с правом доступа «Может просматривать список пользователей». Описание добавления пользователя и назначение прав доступа приведены в текущем разделе (п. 9.2.2, п. 9.3).

Для перехода на страницу «Список пользователей» необходимо нажать на  в верхнем меню, а затем выбрать «Просмотреть список пользователей» (Рисунок 66).

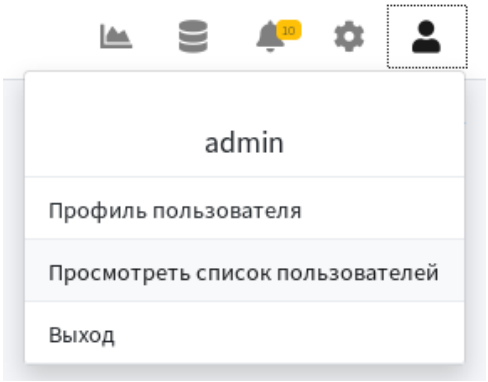


Рисунок 66 – Переход в список пользователей

Страница «Список пользователей» позволяет просматривать список учетных записей пользователей в формате таблицы, которая содержит следующие записи (Рисунок 67):

– имя пользователя (в виде ссылки отображается только пользователю с правом доступа «Может просматривать учетные данные пользователя»);

– имя;

– действия:

–  : редактировать (отображается только пользователю с правом доступа «Может редактировать учетные данные пользователя»);

–  : редактировать группы пользователя (отображается только пользователю с правом доступа «Может редактировать учетные данные пользователя»);

–  : удалить (отображается только пользователю с правом доступа «Может удалять пользователя»).

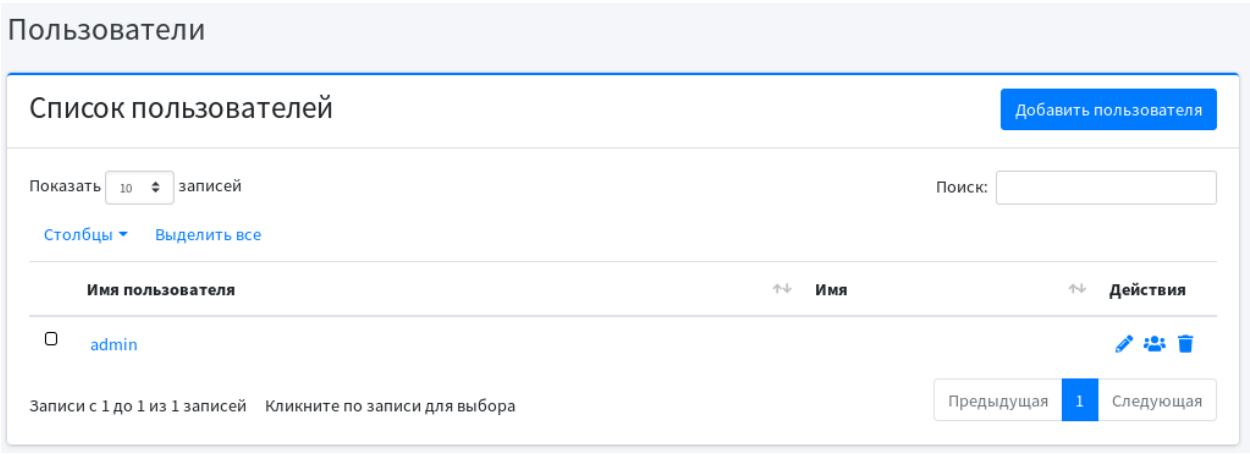


Рисунок 67 – Список пользователей

Для выбора количества записей, отображаемых в таблице пользователей на странице «Список пользователей» необходимо нажать на кнопку 10 в левом в верхнем углу страницы.

Поле «Поиск» вверху таблицы позволяет осуществлять сквозной поиск по всем полям таблицы. Для выполнения поиска необходимо ввести строку совпадения в поле «Поиск».

Таблица позволяет производить сортировку по каждому столбцу. Для выполнения сортировки данных столбца таблицы необходимо нажать на кнопку рядом с названием соответствующего столбца.

9.2.1 Просмотр учетной записи пользователя

Текущий подраздел доступен пользователю с правом доступа «Может просматривать учетные данные пользователя». Описание добавления пользователя и назначение прав доступа приведены в текущем разделе (п. 9.2.2, п. 9.3).

Для просмотра информации учетной записи пользователей необходимо нажать на в верхнем меню, а затем выбрать «Посмотреть список пользователей». Затем в таблице пользователей нажать на ссылку в столбце «Имя пользователя» соответствующего пользователя.

Страница «Изменить учетные данные пользователя» позволяет просматривать информацию о пользователе (Рисунок 65):

- имя;
- адрес электронной почты;
- комментарий;
- временная зона;
- дата окончания срока действия;
- список групп, в которых состоит пользователь.

Для пользователя с правом доступа «Может редактировать учетные данные пользователя» на странице будет отображаться кнопка Редактировать пользователя. При

нажатии на кнопку отображается страница «Редактировать пользователя» (подробнее описано в подразделе 9.2.3).

Для пользователя с правом доступа «Может редактировать права пользователя» на странице будет отображаться кнопка Управлять группами. При нажатии на кнопку отображается страница «Управление группами» (подробнее описано в подразделе 9.3).

9.2.2 Добавление учетной записи пользователя

Текущий подраздел доступен пользователю с правом доступа «Может добавлять новых пользователей». Описание добавления пользователя и назначение прав доступа приведены в текущем разделе (п. 9.2.2, п. 9.3).

Для добавления учетной записи пользователя необходимо нажать на в верхнем меню и выбрать «Просмотреть список пользователей». Затем нажать кнопку Добавить пользователя (Рисунок 67).

Страница «Добавление нового пользователя» позволяет ввести необходимую информацию для добавления учетной записи пользователя (Рисунок 68).

В поле «Имя пользователя» необходимо ввести имя пользователя для входа в систему (необходимо, чтобы имя пользователя было оригинальным в InfoWatch ARMA Management Console, так как имя пользователя является идентификатором пользователя в InfoWatch ARMA Management Console). В поле «Имя» необходимо ввести полное имя пользователя. В поле «Адрес электронной почты» необходимо ввести адрес электронной почты пользователя. В поле «Пароль» и «Подтверждение пароля» необходимо ввести пароль пользователя. В поле «Комментарий» необходимо ввести комментарий к пользователю. Для сохранения и добавления пользователя необходимо нажать кнопку Сохранить. Появится сообщение об успешном добавлении учетной записи пользователя.

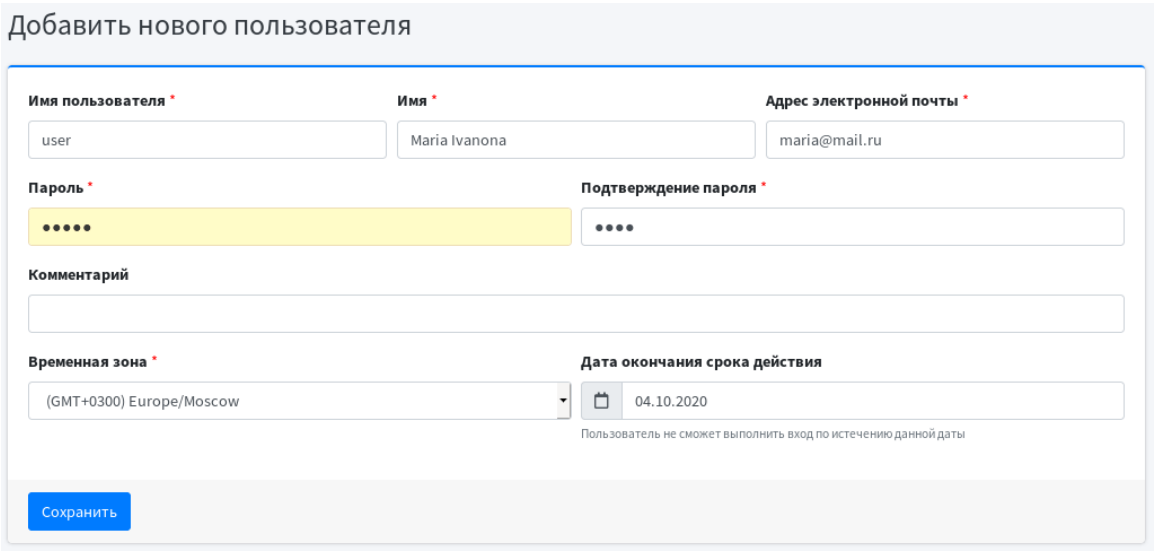


Рисунок 68 – Добавление пользователя

9.2.3 Редактирование учетной записи пользователя

Текущий подраздел доступен пользователю с правом доступа «Может редактировать учетные данные пользователя». Описание добавления пользователя и назначение прав доступа приведены в текущем разделе (п. 9.2.2, п. 9.3).

Для редактирования учетной записи пользователей необходимо нажать на в верхнем меню, а затем выбрать «Просмотреть список пользователей». Затем в таблице пользователей нажать на в столбце «Действия» соответствующего пользователя.

Страница «Редактирование пользователя» позволяет редактировать информацию учетной записи пользователя (Рисунок 69).

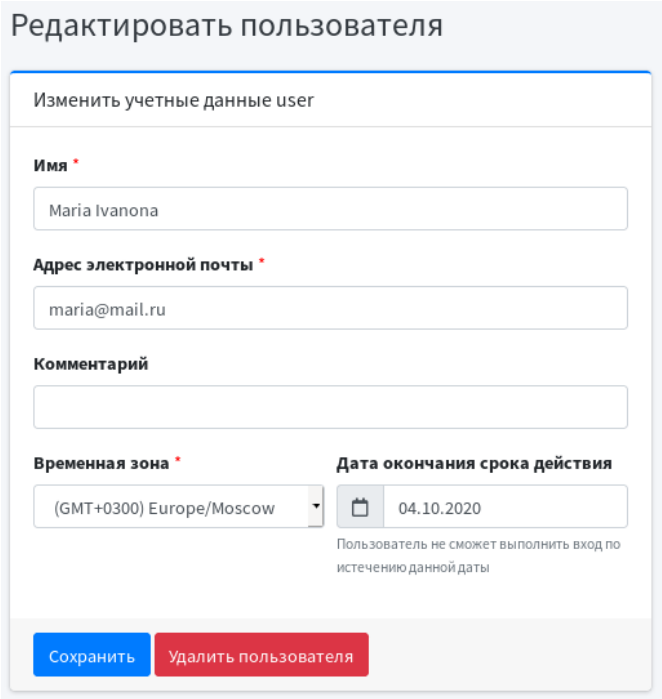


Рисунок 69 – Редактирование учетной записи пользователя

В поле «Имя» необходимо ввести полное имя пользователя. В поле «Адрес электронной почты» необходимо ввести адрес электронной почты пользователя. В поле «Комментарий» необходимо ввести комментарий к пользователю. В поле «Дата окончания срока действия» необходимо ввести дату, по истечении которой учетная запись будет недоступна. Для сохранения и добавления пользователя необходимо нажать кнопку Сохранить.

Для удаления пользователя необходимо нажать кнопку Удалить пользователя, а затем подтвердить удаление.

9.2.4 Удаление учетной записи

Текущий подраздел доступен пользователю с правом доступа «Может удалить пользователя». Описание добавления пользователя и назначение прав доступа приведены в текущем разделе (п. 9.2.2, п. 9.3).

Для удаления учетной записи пользователей необходимо нажать на в верхнем меню, а затем выбрать «Просмотреть список пользователей» (Рисунок 67).

Для удаления одной учетной записи пользователя в таблице пользователей нажать на в столбце «Действия» соответствующего пользователя. Появится всплывающее окно подтверждения удаления (Рисунок 70). Для подтверждения удаления необходимо нажать кнопку «OK».

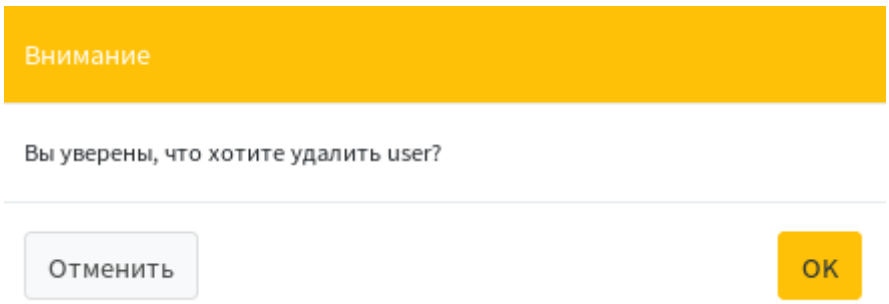


Рисунок 70 – Подтверждение удаления учетной записи пользователя

Для удаления нескольких учетных записей пользователя в таблице пользователей необходимо выбрать соответствующих пользователей (Рисунок 71) и нажать кнопку сверху. Появится всплывающее окно подтверждения удаления (Рисунок 72). Для подтверждения удаления необходимо нажать кнопку «OK».

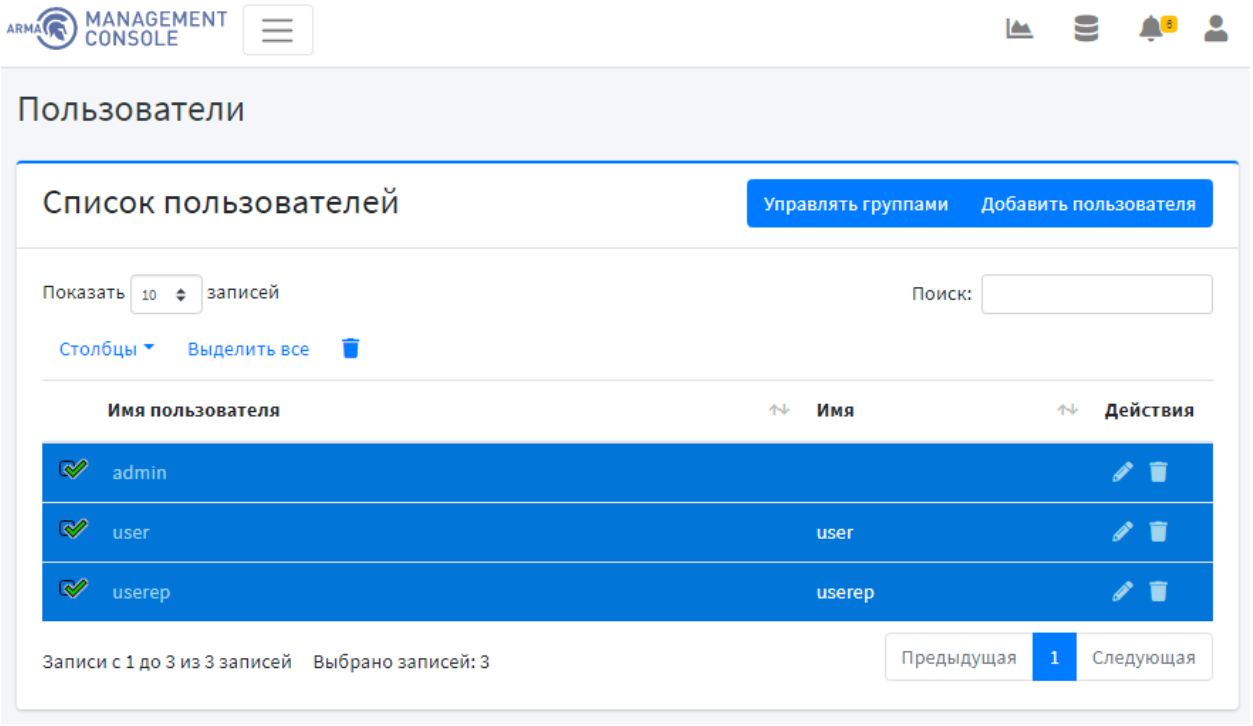


Рисунок 71 – Выбор нескольких учетных записей пользователей

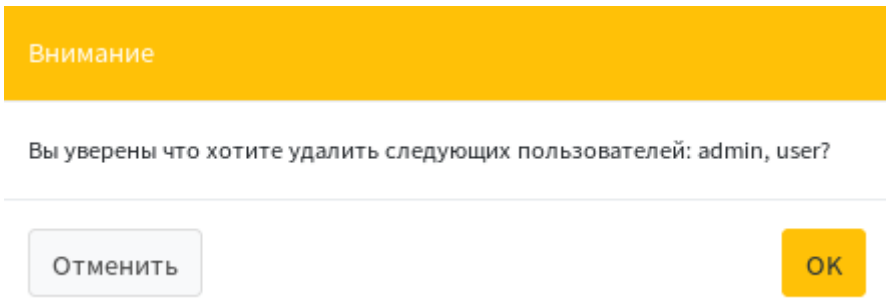


Рисунок 72 – Подтверждение удаления нескольких учетных записей

9.3 Управление правами пользователей

Текущий подраздел доступен пользователю с правом доступа «Может редактировать права пользователя».

Для возможности управления группами пользователей необходимо нажать на в верхнем меню, а затем выбрать «Просмотреть список пользователей». Затем в таблице пользователей нажать на в столбце «Действия» соответствующего пользователя.

На странице «Редактирование пользователя» нажать кнопку Управлять группами. При нажатии на кнопку отображается страница «Управление группами» (Рисунок 73).

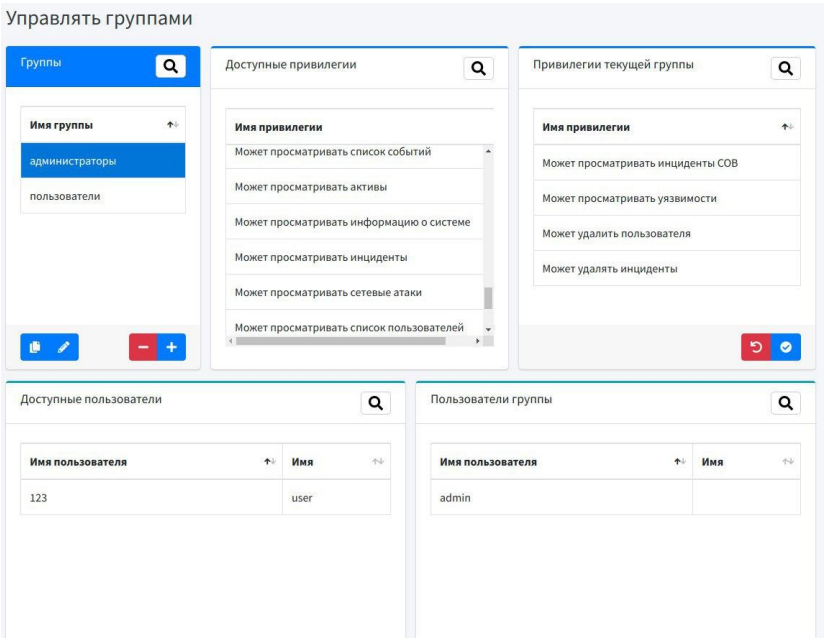


Рисунок 73 – Управление группами

Кнопка позволяет осуществлять сквозной поиск по всем полям соответствующих таблиц. Для выполнения поиска необходимо нажать кнопку ввести строку совпадения в поле соответствующее поле.

Все таблицы позволяют производить сортировку по каждому столбцу. Для выполнения сортировки данных столбца таблицы необходимо нажать на кнопку  рядом с названием соответствующего столбца.

Таблица «Группы» страницы «Управлять группами» отображает список настроенных групп. Возможны следующие действия с элементами таблицы:

–  : скопировать выбранную группу;

–  : редактировать выбранную группу;

–  : удалить выбранную группу;

–  : добавить группу.

Таблица «Доступные привилегии» отображает невыбранные права доступа для просматриваемой группы. Для выбора привилегий необходимо нажать на привилегию. При нажатии привилегия исчезнет из таблицы «Доступные привилегии» и появится в таблице «Привилегии текущей группы».

Таблица «Привилегии текущей группы» отображает права доступа для просматриваемой группы. Для удаления привилегий из группы необходимо нажать на привилегию. При нажатии привилегия исчезнет из таблицы «Привилегии текущей группы» и появится в таблице «Доступные привилегии». Для сохранения изменений привилегий группы необходимо нажать  . Для отмены изменения привилегий в группе необходимо нажать  .

Таблица «Доступные пользователи» отображает список пользователей, которые не являются участниками просматриваемой группы. Для добавления пользователя в группу необходимо нажать на этого пользователя. При нажатии пользователь исчезнет из таблицы «Доступные пользователи» и появится в таблице «Пользователи группы».

Таблица «Пользователи группы» отображает список пользователей, состоящих в просматриваемой группе. Для удаления пользователя из группы необходимо нажать на пользователя. При нажатии пользователь исчезнет из таблицы «Пользователи группы» и появится в таблице «Доступные пользователи». Для сохранения изменений необходимо нажать  . Для отмены изменения необходимо нажать  .

9.3.1 Права доступа в системе

В InfoWatch ARMA Management Console доступны следующие права доступа:

1. Управление пользователями:

- может просматривать список пользователей;
- может просматривать учетные данные пользователя;
- может редактировать учетные данные пользователя;
- может удалить пользователя;
- может добавлять новых пользователей;
- может редактировать права пользователя;

- может редактировать группы;
- может добавлять группы;
- может удалять группы.

2. Инциденты:

- может просматривать уязвимости;
- может назначать инциденты;
- может работать с инцидентами;
- может изменять решенные инциденты;
- может удалять инциденты;
- может добавлять настройки ротации инцидентов;
- может удалять настройки ротации инцидентов;
- может изменять настройки ротации инцидентов;
- может просматривать сетевые атаки.

3. Обзорная панель:

- может просматривать информацию о системе;
- может добавлять виджеты;
- может просматривать виджеты;
- может удалять виджеты.

4. События:

- может просматривать список событий;
- может скачивать журналы.

5. Таблица активов:

- может просматривать активы;
- может редактировать актив;
- может редактировать группы активов.

6. Карта сети:

- может просматривать структуру сети;
- может просматривать уязвимости сети.

7. Системы защиты:

- может просматривать список систем защиты;
- может добавлять системы защиты;
- может управлять системами защиты.

8. Источники:

- может добавлять источники;
- может просматривать список источников;
- может удалять источники.

9. Endpoint:

- может добавлять Endpoint;
- может изменять конфигурацию Endpoint;
- может просматривать список Endpoint;
- может скачивать конфигурацию Endpoint.

10. Корреляция:

- может работать с правилами корреляции.

9.3.2 Добавление группы пользователей

Для добавления группы пользователей необходимо нажать на в верхнем меню, а затем выбрать «Просмотреть список пользователей». Затем в таблице пользователей нажать на в столбце «Действия» соответствующего пользователя.

На странице «Редактирование пользователя» нажать кнопку Управлять группами. При нажатии на кнопку отображается страница «Управление группами».

Для добавления группы пользователей в таблице «Группы» страницы «Управлять группами» необходимо нажать кнопку .

Во всплывающем окне «Добавить новую группу» (Рисунок 74) в поле «Новое имя группы» необходимо ввести название группы пользователей. Для сохранения и создания новой группы пользователей необходимо нажать кнопку Сохранить изменения. Для отмены создания новой группы пользователей необходимо нажать Закрыть.

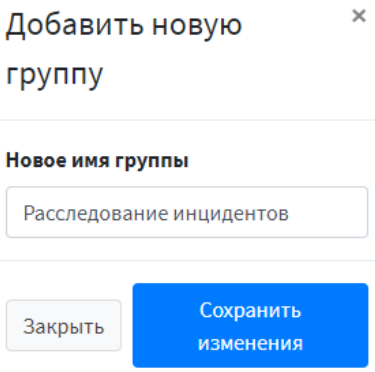


Рисунок 74 – Добавление группы пользователей

При успешном создании группы пользователей появится уведомление об этом, и группа появится в таблице «Группы». Для дальнейшего редактирования группы пользователей необходимо выбрать (нажать на) соответствующую группу в списке групп пользователей.

Для выбора привилегий необходимо нажать на привилегию в таблице «Доступные привилегии». При нажатии привилегия исчезнет из таблицы «Доступные привилегии» и появится в таблице «Привилегии текущей группы».

Для удаления привилегий из группы необходимо нажать на привилегию в таблице «Привилегии текущей группы». При нажатии привилегия исчезнет из таблицы «Привилегии текущей группы» и появится в таблице «Доступные привилегии». Для сохранения изменений привилегий группы необходимо нажать . Для отмены изменения привилегий в группе необходимо нажать .

Таблица «Доступные пользователи» отображает список пользователей, которые не являются участниками просматриваемой группы. Для добавления пользователя в группу необходимо нажать на этого пользователя. При нажатии

пользователь исчезнет из таблицы «Доступные пользователи» и появится в таблице «Пользователи группы».

Таблица «Пользователи группы» отображает список пользователей, состоящих в просматриваемой группе. Для удаления пользователя из группы необходимо нажать на пользователя. При нажатии пользователь исчезнет из таблицы «Пользователи группы» и появится в таблице «Доступные пользователи». Для сохранения изменений необходимо нажать . Для отмены изменения необходимо нажать .

9.3.3 Редактирование группы пользователя

Для редактирования группы пользователей необходимо нажать на в верхнем меню, а затем выбрать «Просмотреть список пользователей». Затем в таблице пользователей нажать на в столбце «Действия» соответствующего пользователя.

На странице «Редактирование пользователя» нажать кнопку Управлять группами. При нажатии на кнопку отображается страница «Управление группами».

Во всплывающем окне «Переименовать группу» (Рисунок 75) в поле «Новое имя группы» необходимо ввести название группы пользователей. Для сохранения изменений группы пользователей необходимо нажать кнопку Сохранить изменения. Для отмены создания новой группы пользователей необходимо нажать Закрыть.

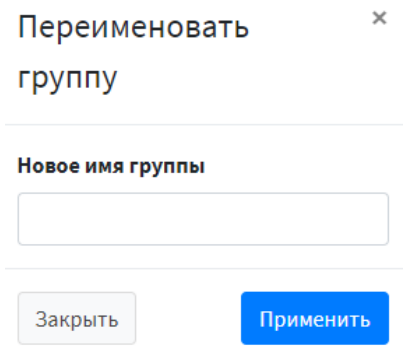


Рисунок 75 – Редактирование группы пользователей

При успешном изменении группы пользователей появится уведомление об этом. Для дальнейшего редактирования группы пользователей необходимо выбрать (нажать на) соответствующую группу в списке групп пользователей.

Для выбора привилегий необходимо нажать на привилегию в таблице «Доступны привилегии». При нажатии привилегия исчезнет из таблицы «Доступные привилегии» и появится в таблице «Привилегии текущей группы».

Для удаления привилегий из группы необходимо нажать на привилегию в таблице «Привилегии текущей группы». При нажатии привилегия исчезнет из таблицы «Привилегии текущей группы» и появится в таблице «Доступные

привилегии». Для сохранения изменений привилегий группы необходимо нажать . Для отмены изменения привилегий в группе необходимо нажать .

Таблица «Доступные пользователи» отображает список пользователей, которые не являются участниками просматриваемой группы. Для добавления пользователя в группу необходимо нажать на этого пользователя. При нажатии пользователь исчезнет из таблицы «Доступные пользователи» и появится в таблице «Пользователи группы».

Таблица «Пользователи группы» отображает список пользователей, состоящих в просматриваемой группе. Для удаления пользователя из группы необходимо нажать на пользователя. При нажатии пользователь исчезнет из таблицы «Пользователи группы» и появится в таблице «Доступные пользователи». Для сохранения изменений необходимо нажать . Для отмены изменения необходимо нажать .

9.3.4 Удаление группы пользователей

Для удаления группы пользователей необходимо нажать на в верхнем меню, а затем выбрать «Просмотреть список пользователей». Затем в таблице пользователей нажать на в столбце «Действия» соответствующего пользователя.

На странице «Редактирование пользователя» нажать кнопку Управлять группами. При нажатии на кнопку отображается страница «Управление группами».

Для удаления группы пользователей в таблице «Группы» страницы «Управлять группами» необходимо выбрать (нажать) группу пользователей и нажать кнопку . И подтвердить удаление во всплывающем окне (Рисунок 76), нажав кнопку «Да».

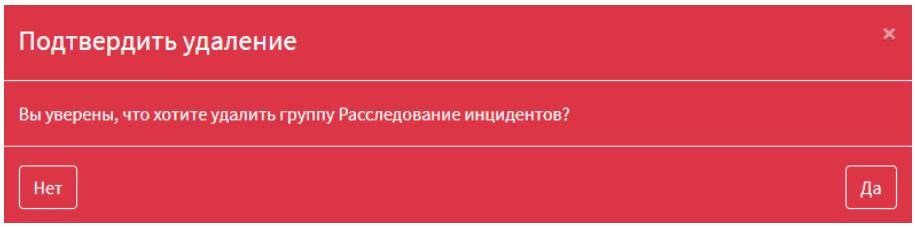


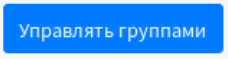
Рисунок 76 – Подтверждение удаления группы пользователей

9.3.5 Назначение ролей учетным записям пользователей

Назначение ролей учетных записей пользователей в InfoWatch ARMA Management Console производится по средствам добавления групп пользователей с заданными привилегиями.

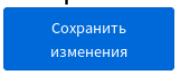
Для добавления группы пользователей необходимо нажать на в верхнем меню, а затем выбрать «Просмотреть список пользователей». Затем в таблице

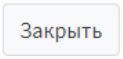
пользователей нажать на  в столбце «Действия» соответствующего пользователя.

На странице «Редактирование пользователя» нажать кнопку 

. При нажатии на кнопку отображается страница «Управление группами».

Для добавления группы пользователей в таблице «Группы» страницы «Управлять группами» необходимо нажать кнопку  .

Во всплывающем окне «Добавить новую группу» (Рисунок 74) в поле «Новое имя группы» необходимо ввести название группы пользователей. Для сохранения и создания новой группы пользователей необходимо нажать кнопку 

. Для отмены создания новой группы пользователей необходимо нажать 

.

При успешном создании группы пользователей появится уведомление об этом, и группа появится в таблице «Группы». Для дальнейшего редактирования группы пользователей необходимо выбрать (нажать на) соответствующую группу в списке групп пользователей.

Для выбора привилегий необходимо нажать на привилегию в таблице «Доступные привилегии». При нажатии привилегия исчезнет из таблицы «Доступные привилегии» и появится в таблице «Привилегии текущей группы».

Для удаления привилегий из группы необходимо нажать на привилегию в таблице «Привилегии текущей группы». При нажатии привилегия исчезнет из таблицы «Привилегии текущей группы» и появится в таблице «Доступные привилегии». Для сохранения изменений привилегий группы необходимо нажать  . Для отмены изменения привилегий в группе необходимо нажать  .

Таблица «Доступные пользователи» отображает список пользователей, которые не являются участниками просматриваемой группы. Для добавления пользователя в группу необходимо нажать на этого пользователя. При нажатии пользователь исчезнет из таблицы «Доступные пользователи» и появится в таблице «Пользователи группы».

Таблица «Пользователи группы» отображает список пользователей, состоящих в просматриваемой группе. Для удаления пользователя из группы необходимо нажать на пользователя. При нажатии пользователь исчезнет из таблицы «Пользователи группы» и появится в таблице «Доступные пользователи». Для сохранения изменений необходимо нажать  . Для отмены изменения необходимо нажать  .

10 УПРАВЛЕНИЕ СТАРТОВОЙ ПАНЕЛЬЮ

Для просмотра страницы «Обзорная панель» необходимо нажать на кнопку в верхнем меню или на логотип InfoWatch ARMA Management Console.

Страница «Обзорная панель» позволяет просматривать виджеты со следующей информацией (Рисунок 77):

– системная информация (отображается только для пользователя с правом доступа «Может просматривать информацию о системе»):
  – использование процессора;
  – информация об объеме памяти;
  – использование памяти;
– системные службы.

InfoWatch ARMA Management Console позволяет каждому пользователю настраивать индивидуальное отображение виджетов – выбирать удобное местоположение виджетов на странице, а также их масштаб.

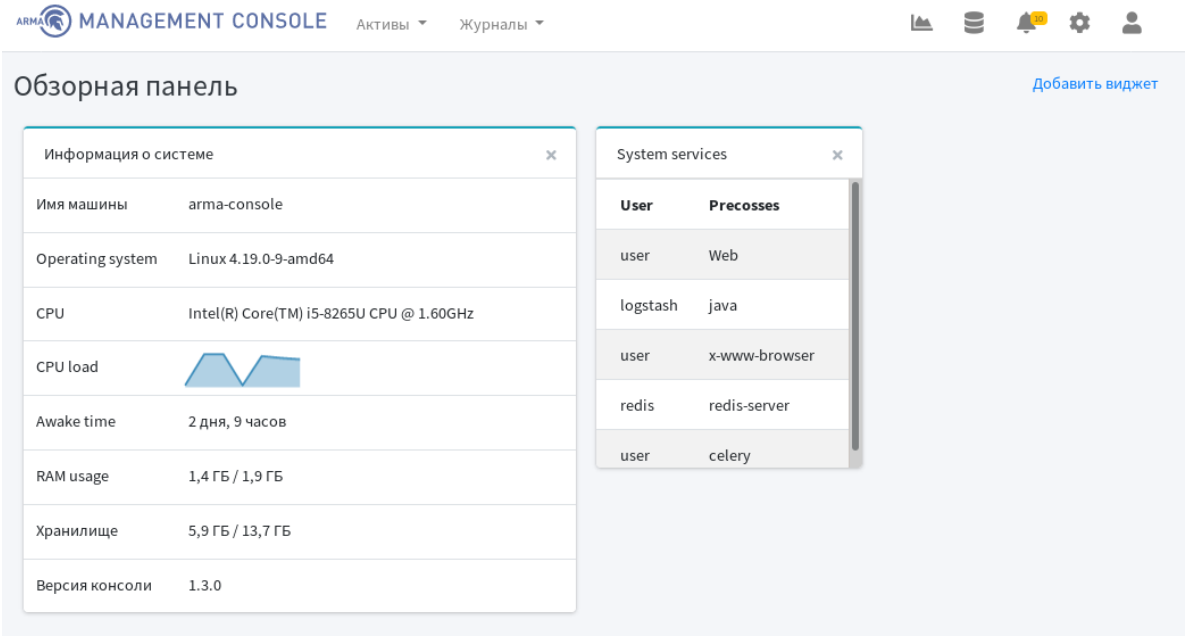


Рисунок 77 – Обзорная панель

Для добавления нового виджета необходимо нажать кнопку Добавить виджет. Во всплывающем окне «Добавить новый виджет» в поле «Тип виджета» необходимо выбрать тип добавляемого виджета (Рисунок 78).

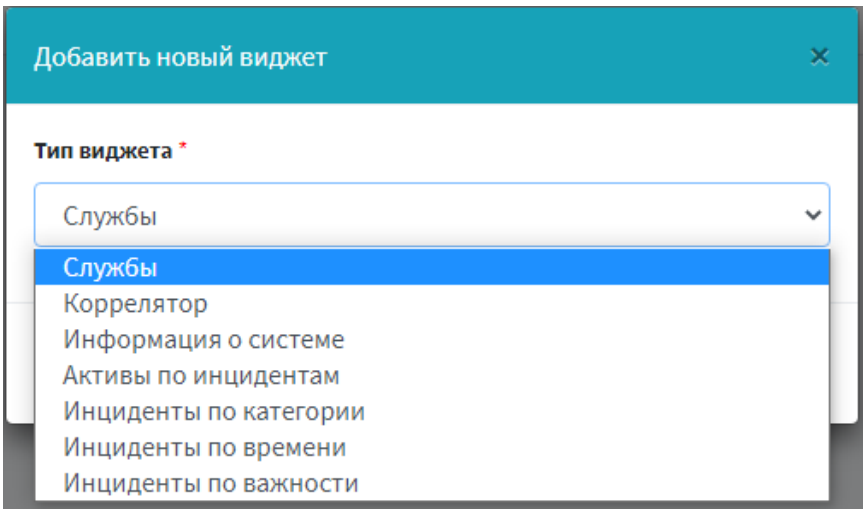


Рисунок 78 – Типы виджетов

Для добавления виджета необходимо нажать на кнопку Добавить (Рисунок 79).

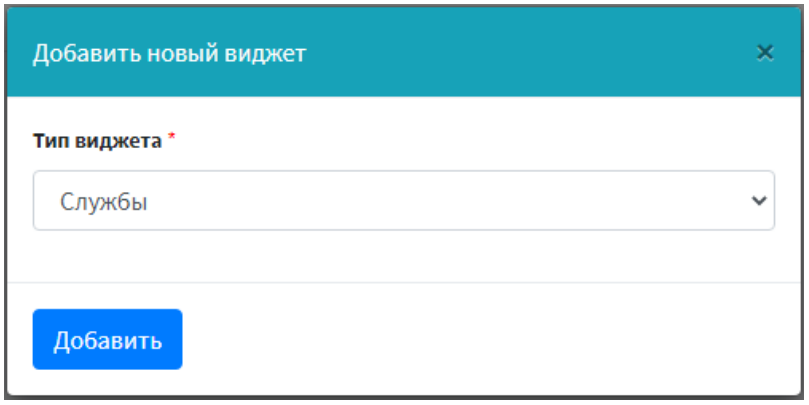


Рисунок 79 – Добавление виджета

11 СООБЩЕНИЯ ПОЛЬЗОВАТЕЛЮ

11.1 Предупреждения всплывающие при необходимости подтверждения действий.

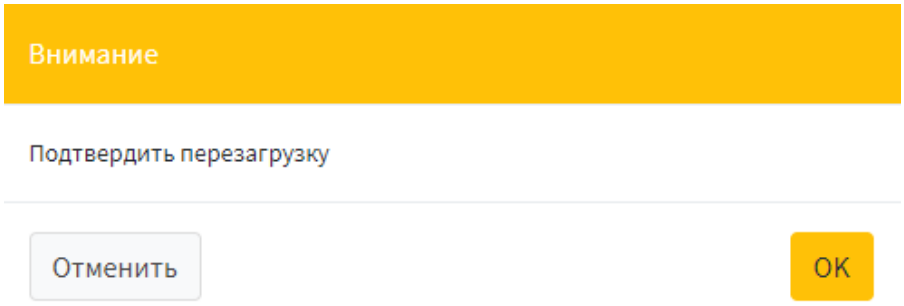


Рисунок 80 – Подтверждение перезагрузки

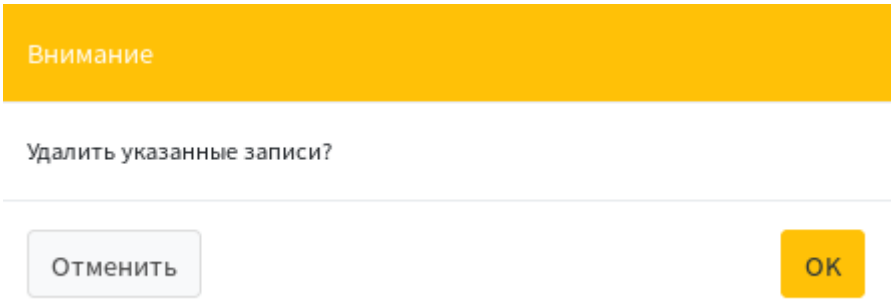


Рисунок 81 – Подтверждение удаления записей

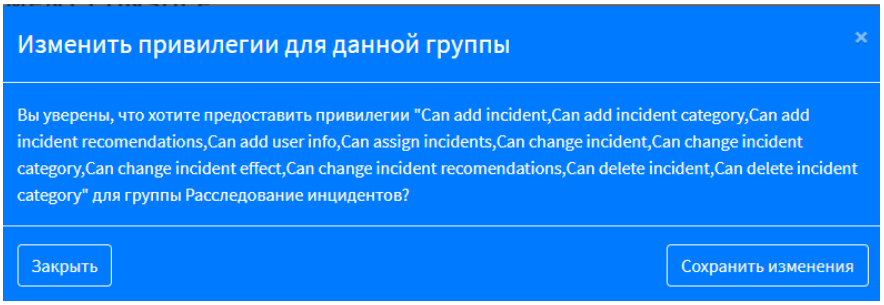


Рисунок 82 – Подтверждение изменений привилегий для группы

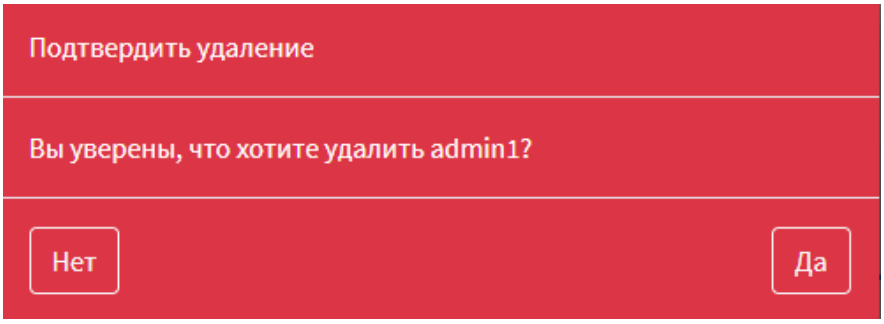


Рисунок 83 – Подтверждение удаления пользователя

11.2 Предупреждения при любом неправильном вводе в поле.

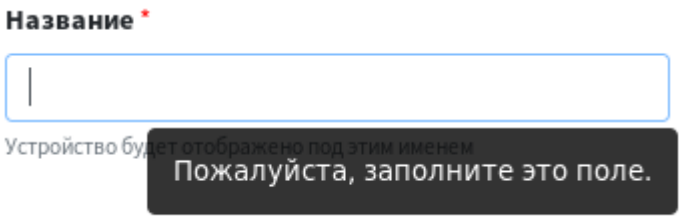


Рисунок 84 – Предупреждение о неправильном вводе в поле (1)

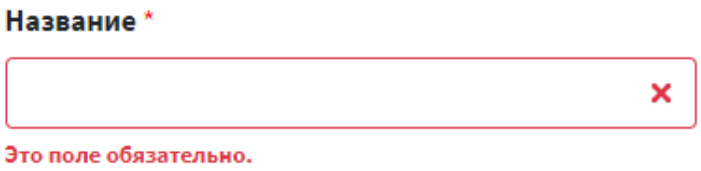


Рисунок 85 – Предупреждение о неправильном вводе в поле (2)

Рисунок 86 – Предупреждение о неправильном вводе в поле (3)

11.3 Предупреждения при применении настроек.

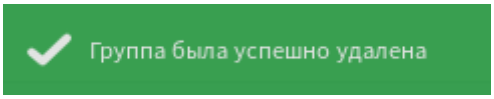


Рисунок 87 – Добавление группы

Рисунок 88 – Обновление актива

Рисунок 89 – Создание пользователя

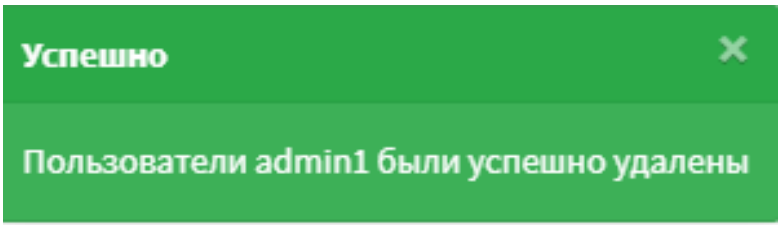


Рисунок 90 – Удаление пользователя

Рисунок 91 – Загрузка конфигурации/правил СОВ

Рисунок 92 – Ожидание скачивания

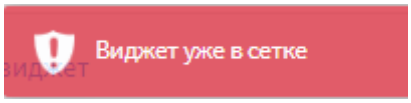


Рисунок 93 – Предупреждение о существующем виджете