Общество с ограниченной ответственностью «АСП Лабс»

Программное обеспечение автоматизированного рабочего места оператора информационной безопасности программного комплекса «Аркан» (ПО АРМ ИБ ПК«Аркан»)

Руководство пользователя СТРЦ.501540.001-01 РП 01

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

МЭ	–	межсетевой экран
ПК	–	программный комплекс
ПЛК	–	программируемый логический контроллер
ПО	–	программное обеспечение
САЗ	–	система анализа защищенности
СВТ	–	средство вычислительной техники
СЗИ	–	средство защиты информации
СОВ	–	система обнаружения вторжений
СПВ	–	средство предотвращения вторжений
ТС	–	техническое средство
ТП	–	технологический процесс
УЗ	–	устройство защиты (устройство ПАК «Аркан-М»)

АННОТАЦИЯ

Руководство пользователя описывает работу с программным обеспечением (ПО) автоматизированного рабочего места информационной безопасности (АРМ ИБ) ПК «Аркан». Настоящее руководство предназначено для технических специалистов и пользователей и содержит условия и правила запуска и остановки ПО, описание диалога с оператором и сообщения оператору. Пользователь ПО АРМ ИБ ПК «Аркан» должен изучить настоящее руководство и иную эксплуатационную документацию. ПО АРМ ИБ ПК «Аркан» используется для управления продуктами ПАК «Аркан-М» и ПАК «Аркан-К». При этом предоставляется единый унифицированный интерфейс. Пользовательский интерфейс подключается либо к ПАК «Аркан-М» и позволяет управлять им, либо к ПАК «Аркан-К». В зависимости от этого системные настройки будут позволять управление тем устройством, к которому произведено подключение. Программный комплекс «Аркан» функционально состоит из модуля устройства защиты и сервера. В данном руководстве описан интерфейс ПК «Аркан». На основе ПК «Аркан» функционируют два продукта ПАК «Аркан-М» (где совмещены оба модуля ПК «Аркан») и ПАК «Аркан-К» (вынесенный на отдельное устройство модуль сервера).

1. НАЗНАЧЕНИЕ ПРОГРАММЫ

1. ПО АРМ ИБ ПК «Аркан» предназначено для настройки продуктов ПАК «Аркан-К» и ПАК «Аркан-М», оповещения об инцидентах безопасности и просмотра событий.
2. ПО АРМ ИБ ПК «Аркан» обеспечивает выполнение следующих задач:
    - управление несколькими ПАК «Аркан-М»;
    - мониторинг системы контроля целостности ПАК «Аркан-М»;
    - централизованный сбор и обработку информации;
    - агрегирование событий безопасности;
    - генерацию и управление инцидентами ИБ;
    - отображение событий, происходящих в системе.

2. СОСТАВ ПРОГРАММНОГО КОМПЛЕКСА

1. ПО АРМ ИБ ПК «Аркан» состоит из файла установки ПО и сертификатов для подключения.
2. Установка ПО описана в документе «Руководство администратора».
3. Комплекс программного обеспечения предоставляет следующие возможности.

Таблица 1. Фонкционал ПО

N п/п	Функционал
1	Разделение функций по управлению (администрированию) системой защиты – разный уровень доступа у администратора и пользователя. Ограничение действий пользователей в соответствии с ролями, поддержка ролевой модели доступа. Аутентификация с использованием пары логин/пароль и сертификата
2	Контроль деятельности пользователей ПК «Аркан»: изменение конфигурации системы, запросы на просмотр информации о конфигурации системы. Запись указанных событий
3	Возможность задания времени, возможность синхронизации времени по протоколу NTP
4	Ограничение доступа пользователей по имени пользователя
5	Обеспечение доверенного канала связи между устройством защиты и сервером
6	Отображение текущих сетевых соединений
7	Обновление базы решающих правил (сигнатур)
8	Разбор пакетов сетевого трафика промышленных протоколов
9	Информирование о возникновении инцидента ИБ
10	Обнаружение незарегистрированного сетевого устройства
11	Обнаружение факта «Сканирование сети»
12	Обнаружение атаки ARP-Spoofing (При развертывании системы начинается процесс формирование таблицы соответствия MAC-адресов и IP-адресов. При изменении MAC-адреса для какого-либо IP-адреса выдается оповещение об атаке ARP-Spoofing)
13	Обнаружение атаки «Flooding» (статистический анализ)
14	Обнаружение атаки «Эксплуатация известных уязвимостей»
15	Обнаружение использования запрещенных политикой функций промышленных протоколов (с помощью использования межсетевого экранирования компонентом L7)
16	Обнаружение изменения программы управления ПЛК, атак на изменение параметров ПЛК в том числе по промышленным протоколам, изменения ОС ПЛК (для тех, для которых на данный момент существуют сигнатуры для обнаружения)

N п/п	Функционал
17	Обнаружение политикой запрещенного информационного потока.[1] (аналогичен п. 18, но в режиме мониторинга)
18	Возможность фильтрации трафика на основе идентификаторов протоколов транспортного уровня (TCP, UDP)
19	Возможность фильтрации по IPv4 адресу и/или физическому адресу устройств
20	Восстановление работоспособности устройства защиты после аварийного отключения питания (выключения устройства)
21	Возможность уведомления пользователей об инциденте через графический интерфейс пользователя.
22	Выборочный просмотр журналов событий и инцидентов (поиск, сортировка, упорядочение данных)
23	Контроль целостности файлов на УЗ
24	Межсетевое экранирование по полям и/или функциям промышленных протоколов: - Modbus TCP; - IEC 60870-5-104; - OPC UA; - OPD DA;
25	Возможность анализа (разбора) информации по протоколам: - Modbus TCP; - DNP3; - Profinet; - S7COMM; - COTP; - IEC 60870-5-104; - OPC UA; - OPC DA;
26	Выбор совокупности регистрируемых системных событий безопасности
27	Экспорт инцидентов по протоколу syslog в формате вида: 13:14:52 SA1 CEF:0 | ASPLabs | ASAP | 1.3 | 1 | In work SA - {u’Node': 1, u’To': u'192.168.29.74', u’From': u'192.168.29.73'} | 5 | msg={"rev": 3, "category": "Attempted Information Leak", "severity": 2, "gid": 1, "proto": "TCP", "signature": "ET SCAN NMAP -sS window 1024", "signature_id": 2009582, "action": "allowed"}
28	Экспорт инцидентов по E-mail (по протоколу SMTP)

N п/п	Функционал
29	Мониторинг состояния по SNMPv3 следующих поддеревьев OID: .iso.org.dod.internet.mgmt.mib-2.system .iso.org.dod.internet.mgmt.mib-2.ip .iso.org.dod.internet.mgmt.mib-2.interfaces .iso.org.dod.internet.mgmt.mib-2.3 .iso.org.dod.internet.mgmt.mib-2.icmp .iso.org.dod.internet.mgmt.mib-2.tcp .iso.org.dod.internet.mgmt.mib-2.udp .iso.org.dod.internet.mgmt.mib-2.snmp .iso.org.dod.internet.mgmt.mib-2.host .iso.org.dod.internet.mgmt.mib-2.ifMIB .iso.org.dod.internet.mgmt.mib-2.ipv6MIB
30	Сегментация на канальном уровне (объединение интерфейсов на канальном уровне в «мосты»)
31	Возможность работы в двух режимах: - Режиме межсетевого экрана (блокирования) - Режиме системы обнаружения вторжений (мониторинга)

[1] Запрещенный (или неразрешенный) информационный поток – информационный поток, который запрещен в соответствии с политикой безопасности организации

3. СИСТЕМНЫЕ ТРЕБОВАНИЯ

Состав используемых технических (аппаратных) средств для ПО АРМ ИБ ПК «Аркан» должен иметь следующие характеристики:

Таблица 2. Характеристики ПК

Наименование СВТ	**Технические характеристики**
Автоматизированное рабочее место (АРМ) оператора	- процессор - Intel Atom 1500 МГц и выше; - оперативной памяти - 2 Гб или больше; - жесткий диск - 60 Гб или больше, SATA/SCSI; - сетевое оборудование - наличие не менее одного сетевого интерфейса 10/100/1000 Base-T;

Состав используемых программных средств для ПО АРМ ИБ ПК «Аркан» должен иметь следующие характеристики: ОС Windows 7 и выше или ОС Ubuntu 16.04 и выше. Дата в формате «ДД.ММ.ГГГГ» без перевода на летнее время, в «оформлении рабочего стола» размер шрифта «обычный». Разделитель целой и дробной части числа - «запятая».

4. ТРЕБОВАНИЯ К ОПЕРАТОРУ

Оператор должен:

- быть допущен к управлению АРМ на объекте установки;
- обладать практическими навыками работы с используемой операционной системой (ОС);
- обладать базовыми знаниями о работе средств защиты информации (СЗИ) и принципах их построения;
- обладать базовыми знаниями информационной безопасности;
- обладать базовыми знаниями принципов построения сетей передачи данных;
- обладать знаниями английского языка, достаточными для чтения технической документации;
- знать внутренние требования политики безопасности компании.

5. ВЫПОЛНЕНИЕ ПРОГРАММЫ

5.1. ЗАПУСК И АВТОРИЗАЦИЯ

Запуск ПО АРМ ИБ ПК «Аркан» производится двойным щелчком по ярлыку на рабочем столе Windows (Ярлык запуска ПО АРМ ИБ ПК «Аркан»). Так же возможен запуск через кнопку «Пуск», где в пункте «Программы» необходимо выбрать подпункт «ПО АРМ ИБ ПК «Аркан»».

Рисунок 1. Ярлык запуска ПО АРМ ИБ ПК «Аркан»

Если рабочее место и все подключения сетевых модулей настроены корректно, то после запуска «ПО АРМ ИБ ПК «Аркан»» оператору будет предложено ввести логин, пароль, имя и порт сервера, выбрать сертификаты и ключи. Программа сохраняет все данные для входа, кроме пароля (Ярлык запуска ПО АРМ ИБ ПК «Аркан»).

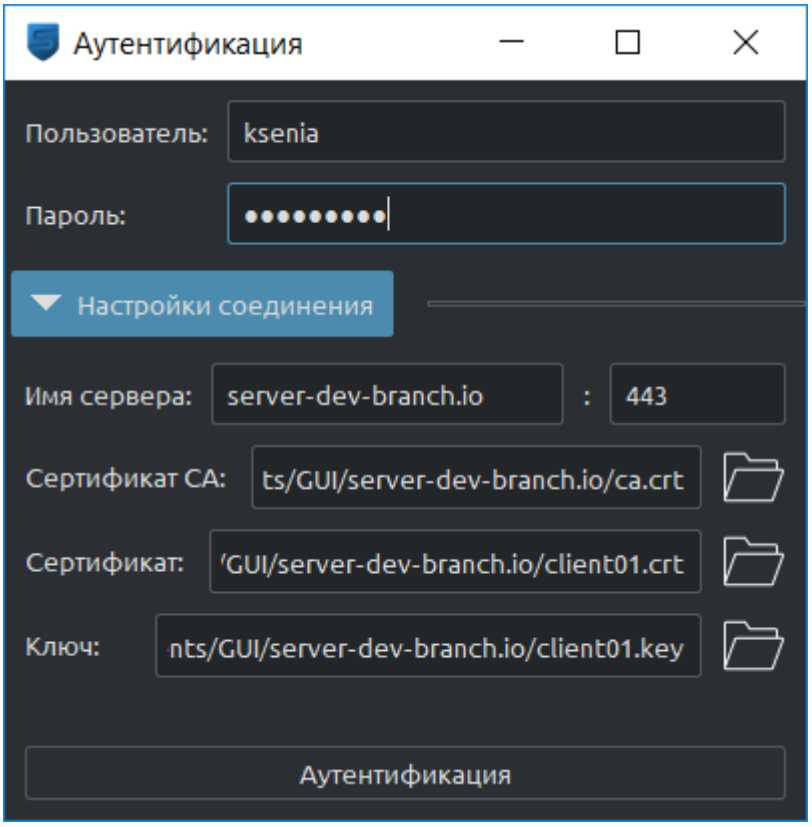


Рисунок 2. Ярлык запуска ПО АРМ ИБ ПК «Аркан»

Аутентификация пользователя производится на основе как пары логин/пароль, так и электронного сертификата. Электронный сертификат передается вместе с комплексом ПО и устанавливается поставщиком. В случае ввода неверного логина и пароля пользователь получит следующую ошибку (Пример ошибки при входе в систему).

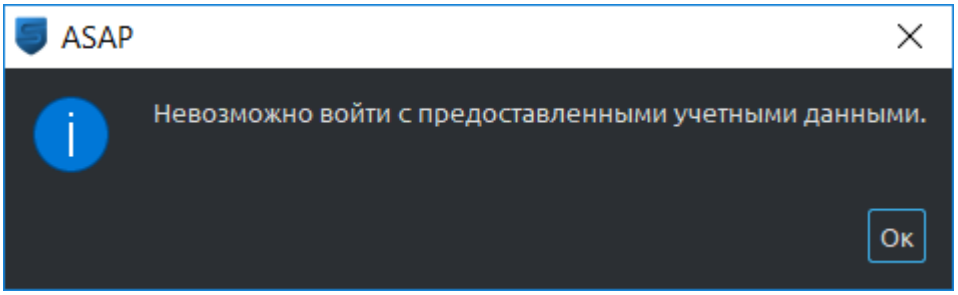


Рисунок 3. Пример ошибки при входе в систему

Если учетные данные введены верно, то начнется процесс запуска «ПО АРМ ИБ ПК «Аркан»».

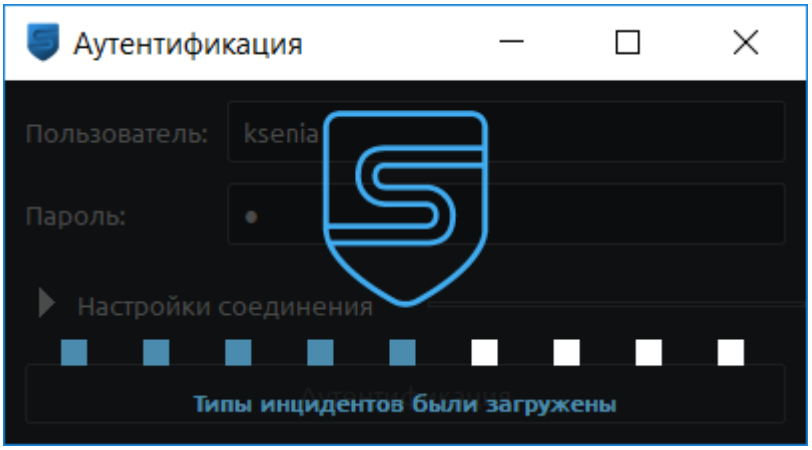


Рисунок 4. Процесс запуска «ПО АРМ ИБ ПК «Аркан»»

Функционал, доступный пользователю, зависит от его прав. Имеется три типа пользователей: «Администратор», «Оператор» и «Рабочий». ПК «Аркан» ограничивает подключение с одного и того же логина с разных IP-адресов. «Администратор» – пользователь, которому доступен следующий функционал ПК «Аркан»:

- управлять пользовательскими данными;
- добавлять/изменять/удалять правила МЭ, СОВ и СПВ;
- отображатьфильтрации атрибутов безопасности;
- производить модификации действий, предпринимаемых при нарушениях ограничений;
- управлять устройствами защиты (ПАК «Аркан-М»);
- настраивать интеграцию с внешними сервисами по протоколам SNMPv3, SMTP, Syslog, NTP;
- управлять настройками ПАК «Аркан-К»;
- обновлять базы решающих правил.

«Оператор» – пользователь, которому доступно наблюдение за состоянием системы и данными об инцидентах. «Рабочий» – пользователь, который предоставляет доступ к защищаемой сети (сегменту сети), в случае если пользователь аутентифицирован в ПО АРМ ИБ ПК «Аркан».

5.2. ИНТЕРФЕЙС

Вид главного окна программы после входа в систему представлен на рисунке ниже (Главное окно программы)

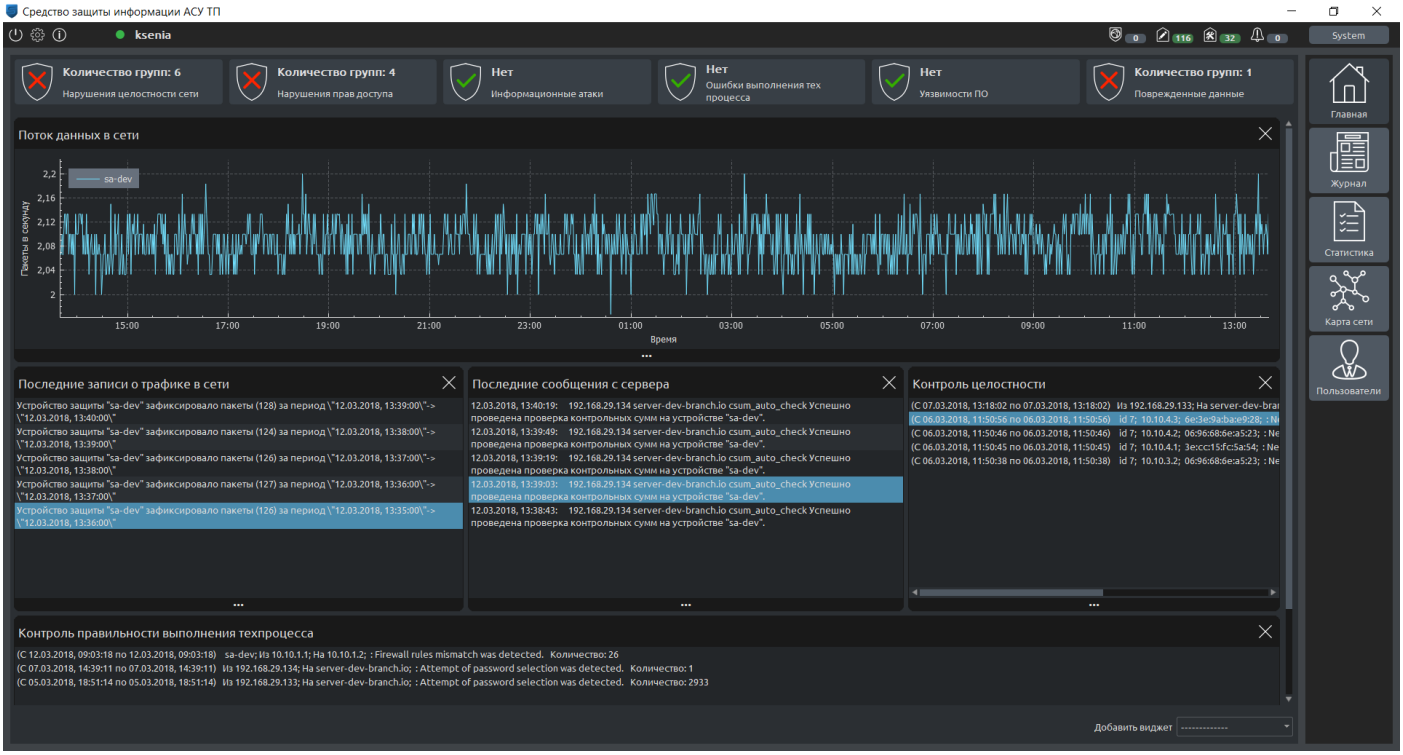


Рисунок 5. Главное окно программы

Главное окно состоит из панели навигации (справа), индикаторов состояния системы (верхняя часть), индикаторов уведомлений (справа сверху), информационной строки (снизу) и рабочей области. Кнопка «Выйти» позволяет свернуть программу и открыть окно входа в систему. Информационная строка отображает информацию о пользователе и сервере. Навигационная панель меняет информацию, отображаемую в рабочей области. Для того, чтобы полностью выйти из программы, необходимо кликнуть на значок программы на панели управления и выбрать «Выйти из системы» (Выход из системы).

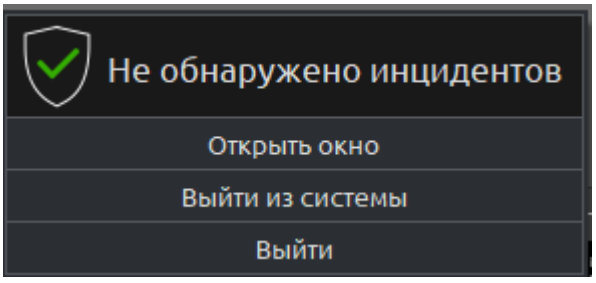
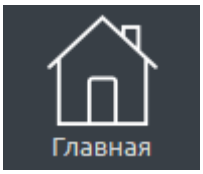
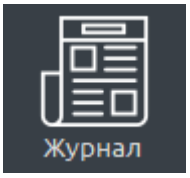
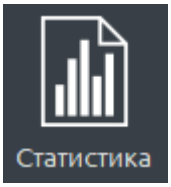
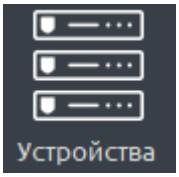
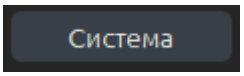


Рисунок 6. Выход из системы

Нажатие кнопок на панели навигации позволяет осуществить переход на соответствующий экран. В таблице Панель навигации подробно рассмотрены кнопки панели навигации.

Таблица 3. Панель навигации

Вид кнопки	Наименование	Функционал
	«Главная» («горячая клавиша» - Ctrl+0)	Выход в главный экран
	«Журнал» («горячая клавиша» - Ctrl+1)	Переход на экран с журналами и их настройками
	«Статистика» («горячая клавиша» - Ctrl+2)	Переход на экран просмотра статистики
	«Устройства» («горячая клавиша» - Ctrl+3)	Переход на экран с устройствами защиты, присутствующих в системе с возможностью их настройки, удаления и добавления
	«Пользователи» («горячая клавиша» - Ctrl+4)	Переход на экран управления пользователями
	«Система» («горячая клавиша» - Ctrl+5)	Переход на экран настройки системы (либо ПАК «Аркан-К», если управление производится через него)

Справа в верхнем углу расположены индикаторы уведомлений (Индикаторы уведомлений), нажав на которые можно сразу перейти на экран «Журнал» в следующие вкладки:

- события сети;
- события интерфейса;
- события системы;
- инциденты.

Рисунок 7. Индикаторы уведомлений

Слева в верхнем углу расположены кнопки управления программой (Кнопки управления программой), которая содержит следующие вкладки:

- «Выход из программы»;
- «Настройки интерфейса».

Вкладка «Выход из программы» (Рисунок 8) позволяет пользователю закрыть программу, завершить текущую сессию и свернуть программу.

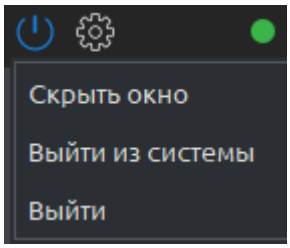


Рисунок 8. Кнопки управления программой

Во вкладке «Настройки интерфейса» (Настройки интерфейса) производятся настройки внешнего вида «Окна состояний», темы, языка, отображения уведомлений. Предоставляются возможности:

- отключить обновление «Последних сообщений с сервера»;
- отключить уведомления о нарушениях;
- изменить язык программы (применяется после перезагрузки программы);
- изменить тему программы (применяется после перезагрузки программы).

Рекомендуется использовать стандартные элементы управления.

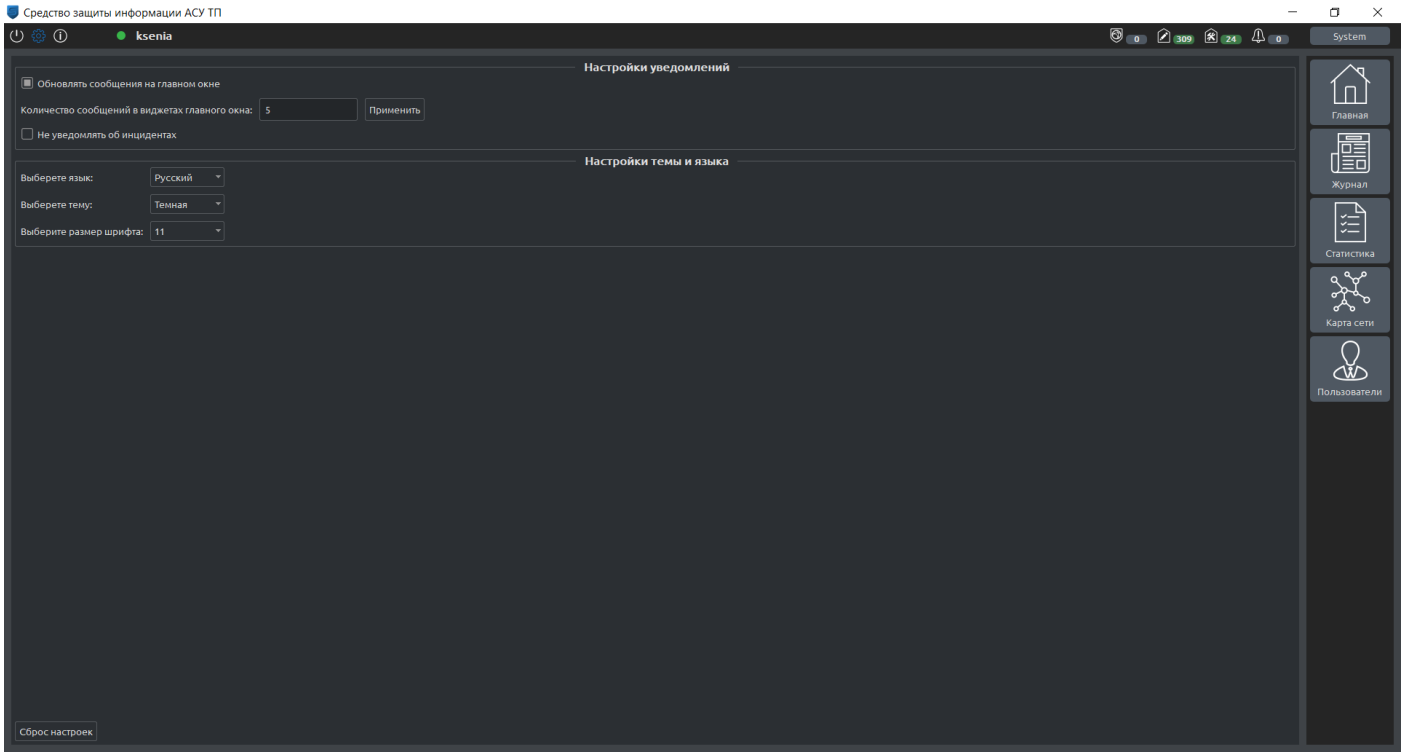


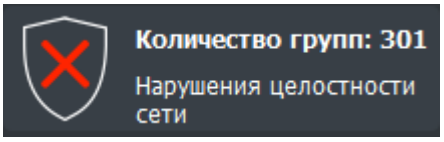
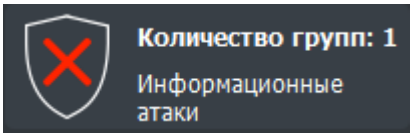
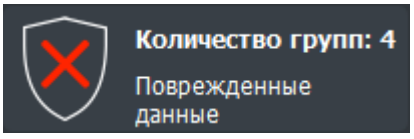
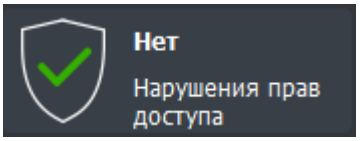
Рисунок 9. Настройки интерфейса

6. РАБОЧАЯ ОБЛАСТЬ

6.1. ГЛАВНАЯ

Окно состояний вызывается кнопкой «Главная» навигационной панели, а также при входе в систему (Главное окно программы). Вид окна можно изменить в настройках.
Окно включает в себя 6 информационных виджетов: «Индикаторы состояния системы», «Поток данных в сети», «Контроль правильности выполнения техпроцесса», «Последние записи о трафике в сети», «Последние сообщения с сервера» и «Контроль целостности». На виджетах в реальном времени выводится информация о последних (число задается в настройках) событиях. Всеми виджетами можно управлять, а именно, переместить, убрать или добавить. Виджет «Индикаторы состояния системы» отображает нерешенные события безопасности (Панель навигации).

Таблица 4. Панель навигации

Индикатор состояния системы	Описание (количество групп)
	нарушений в модуле контроля целостности сети
	компьютерных атак.[2]
	поврежденных файлов, обнаруженных системой контроля целостности
	нарушение правил межсетевого экранирования
*Примечание – группы формируются по типу, отправителю, получателю и другим свойствам. К нарушениям в модуле контроля целостности сети относятся: Новое устр-во, Конфликт IP, Изменение MAC, Подмена MAC	

Виджет «Поток данных в сети» отображает количество пакетов данных в секунду, проходящих через определенное УЗ в зависимости от времени (Поток данных в сети).

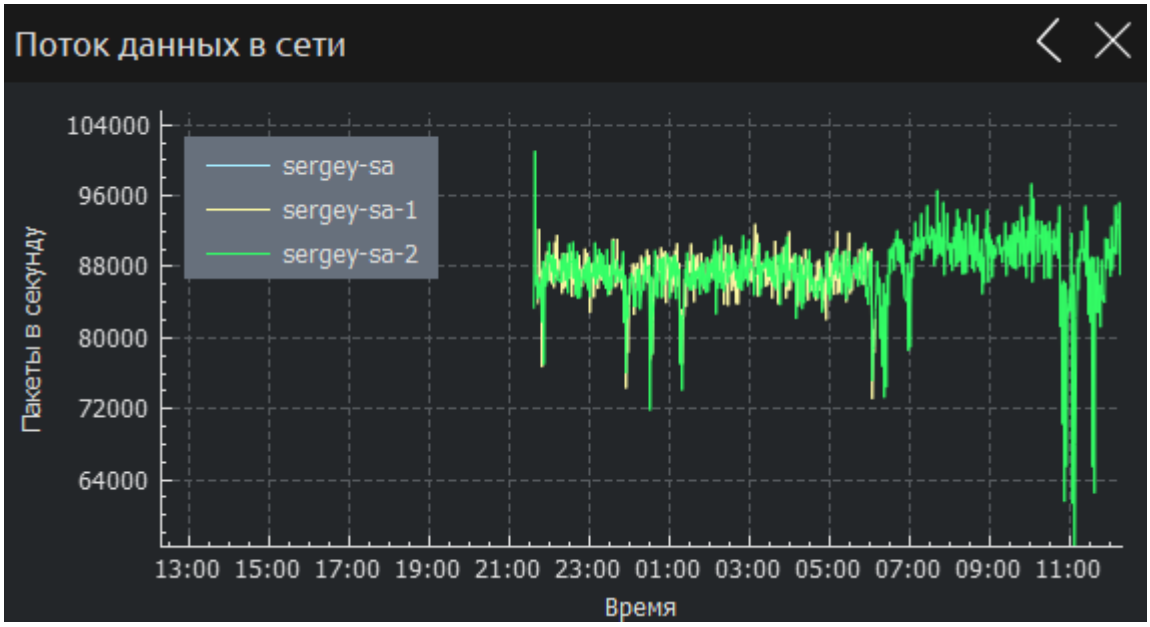


Рисунок 10. Поток данных в сети

Виджет «Контроль правильности выполнения техпроцесса» выводит сообщения о нарушениях, связанных с промышленным оборудованием и технологическим процессом. (Контроль правильности выполнения техпроцесса).

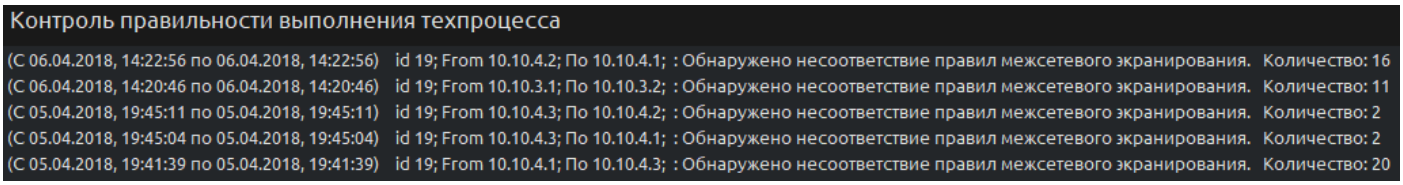


Рисунок 11. Контроль правильности выполнения техпроцесса

Виджет «Последние записи о трафике в сети» выводит ¬последние записи о трафике в сети согласно заданным правилам (Последние записи о трафике в сети).

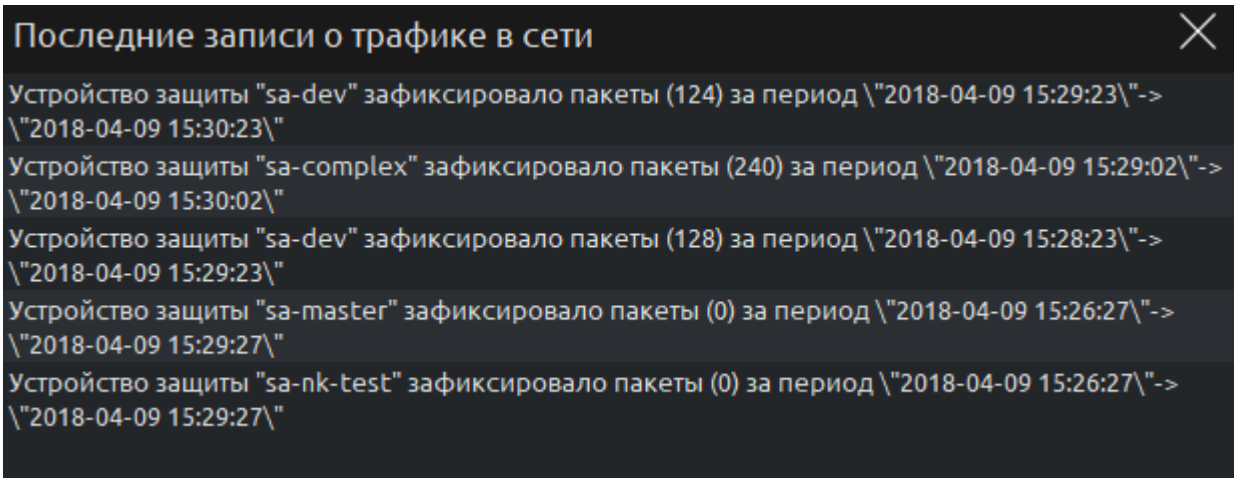


Рисунок 12. Последние записи о трафике в сети

Виджет «Последние сообщения с сервера» выводит последние записи журнала из таблицы

события системы (Последние сообщения с сервера).

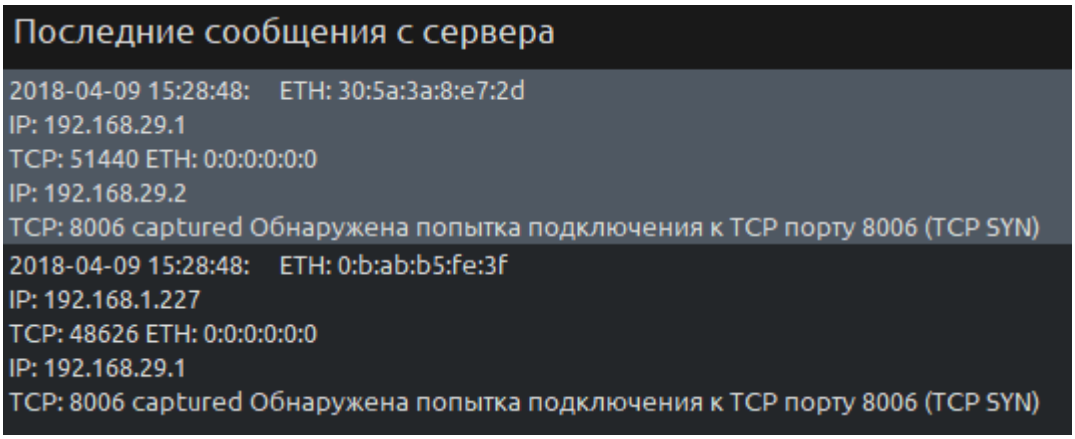


Рисунок 13. Последние сообщения с сервера

Виджет «Контроль целостности» – выводит сообщение в случае нарушения целостности УЗ (Контроль целостности).

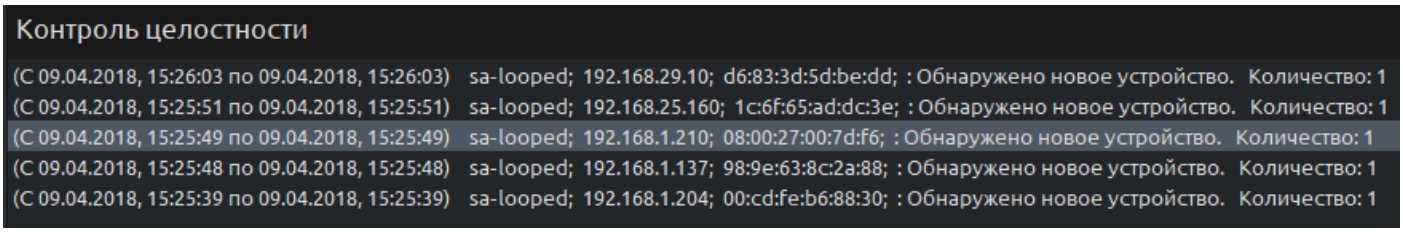


Рисунок 14. Контроль целостности

6.2. ЖУРНАЛ

Окно журнала вызывается нажатием на кнопку «Журнал» навигационной панели и делится на пять вкладок: «События сети», «События интерфейса», «События системы», «Инциденты», «Настройки инцидентов» (Журнал).

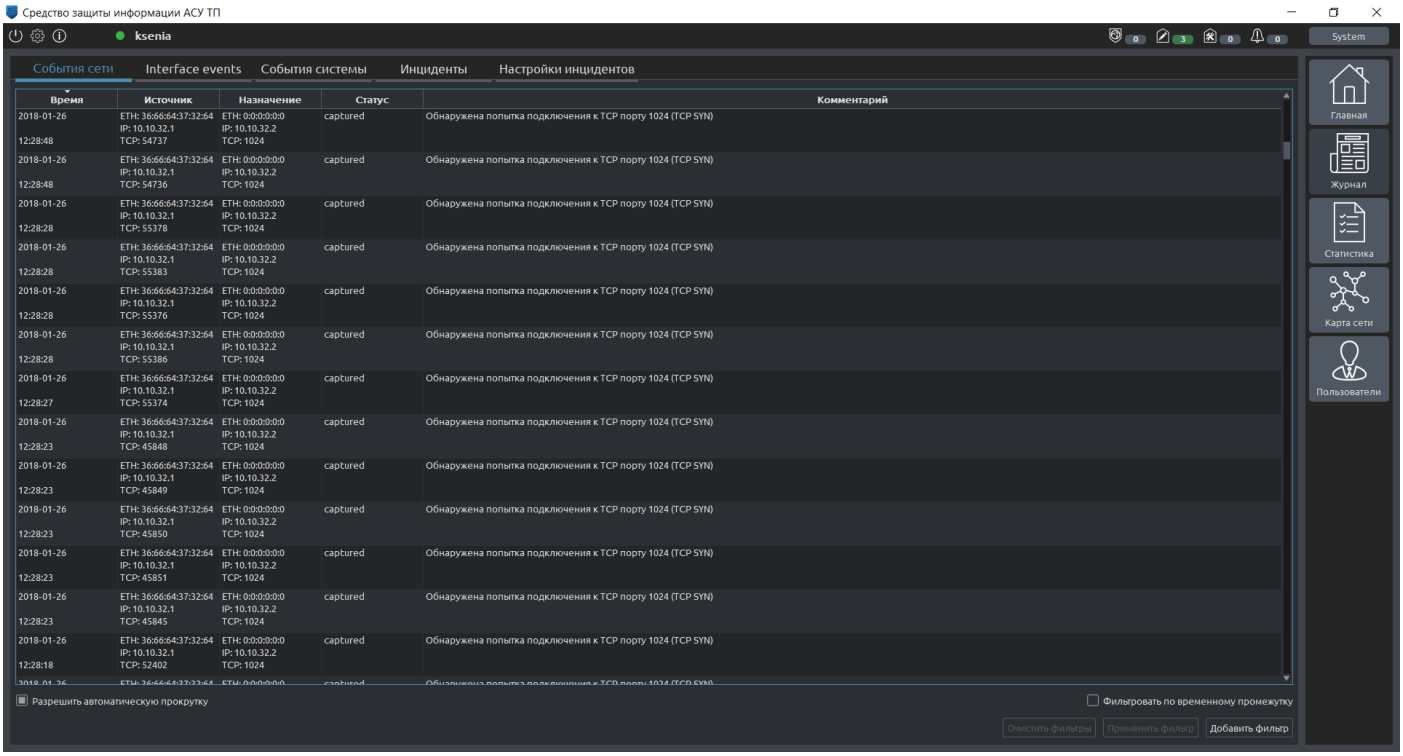


Рисунок 15. Журнал

6.2.1. СОБЫТИЯ СЕТИ

В данном журнале (События сети) отображается следующая информация:

- логирование TCP-соединений (с указанием IP-адресов источника и получателя);
- снимки пакетов технологического трафика (COTP, OPC UA, S7comm, Modbus TCP, PROFINET/RT, PROFINET/IO).

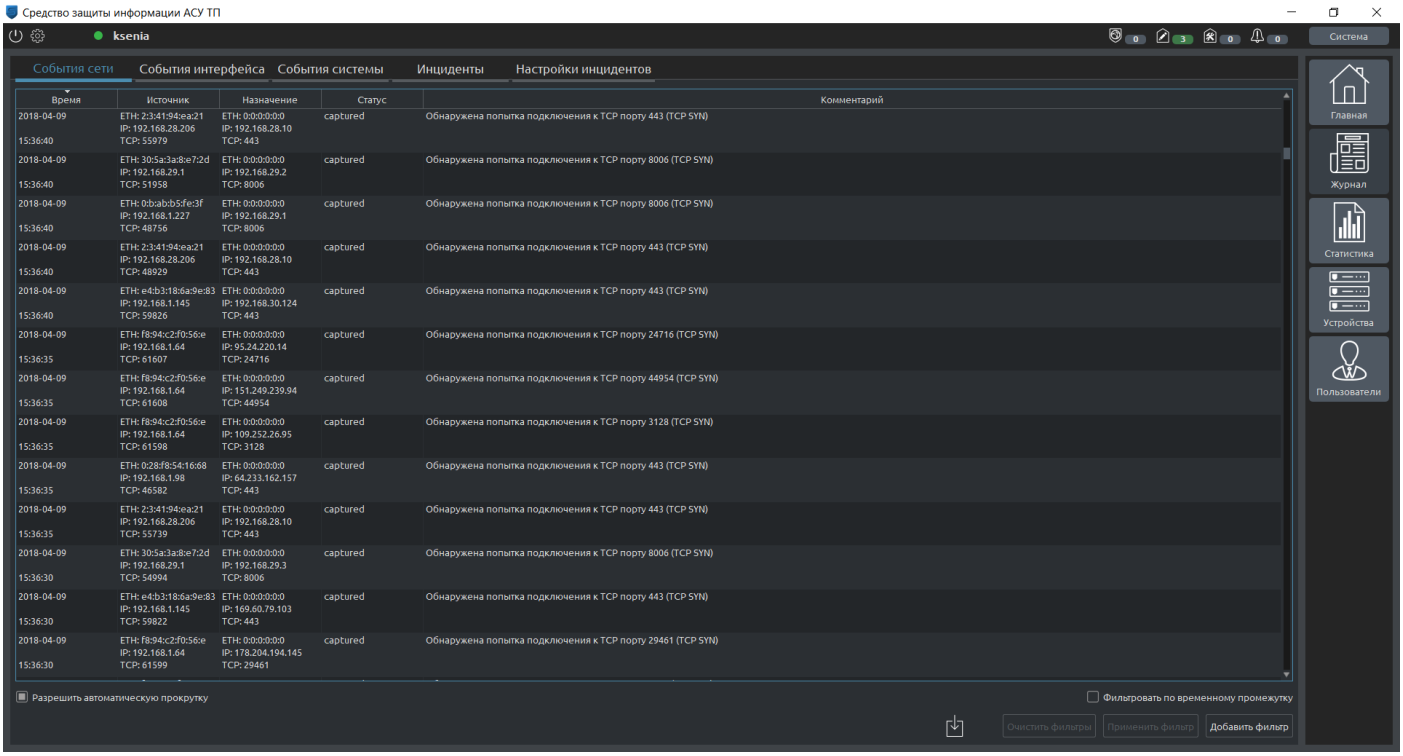


Рисунок 16. События сети

По умолчанию выводятся последние 1000 записей. В случае необходимости получить информацию по каким-то заданным параметрам можно использовать систему фильтрации (Система фильтрации).

Рисунок 17. Система фильтрации

Фильтровать можно по всем полям, перечисленным выше. При выборке по комментариям, она будет осуществлена по техническим комментариям (JSON). При активации фильтров журнал не обновляется в реальном времени. Используя постраничную навигацию можно посмотреть более 1000 записей.

6.2.2. СОБЫТИЯ ИНТЕРФЕЙСА

В данном журнале (События интерфейса) отображается следующая информация:

- загрузка данных;
- запросы на создание/удаление данных;
- запросы на обновление данных;
- запросы на получение данных;

- неуспешные попытки входа в систему пользователем;
- успешный вход пользователя в систему;
- успешное сохранение или обновление данных;
- успешное удаление данных;
- исключительные ситуации во время выполнения запроса;
- изменение системного времени на сервере;
- успешный выход пользователя из системы;
- пользовательские запросы на проверку контрольных сумм устройства защиты;
- автоматические запросы на проверку контрольных сумм устройства защиты.

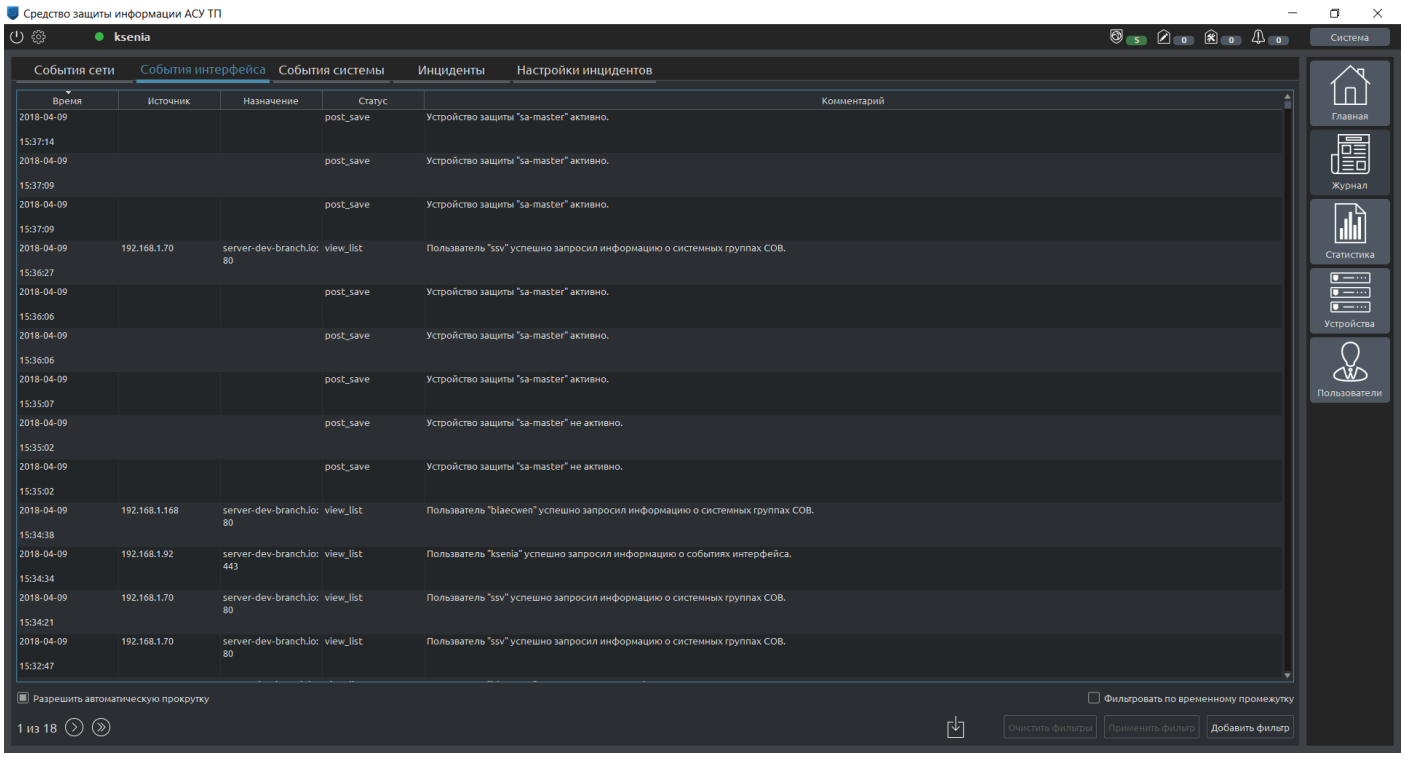


Рисунок 18. События интерфейса

6.2.3. СОБЫТИЯ СИСТЕМЫ

В данном журнале (События системы) отображается следующая информация:

- перезагрузка/выключение сервера;
- изменение конфигурации SYSLOG, Email, NTP;
- включение/выключение SYSLOG, Email;
- запуск ротации журналов;

- окончание ротации журналов;
- некорректное окончание ротации журналов;
- изменение системного времени;
- настройки и действия по добавлению новых устройств;
- события успешного/неудачного добавления нового устройства;
- этапы процесса добавления нового устройства (подключение по сети, добавление пользователей, проверка логина и пароля пользователей, проверка сертификатов и др.) с фиксацией результата выполненного этапа;
- ошибки при попытке добавления устройства защиты с неправильными настройками (неправильный сетевой адрес, неправильный логин и пароль, неправильные сертификаты, сертификаты с истекшим сроком действия).

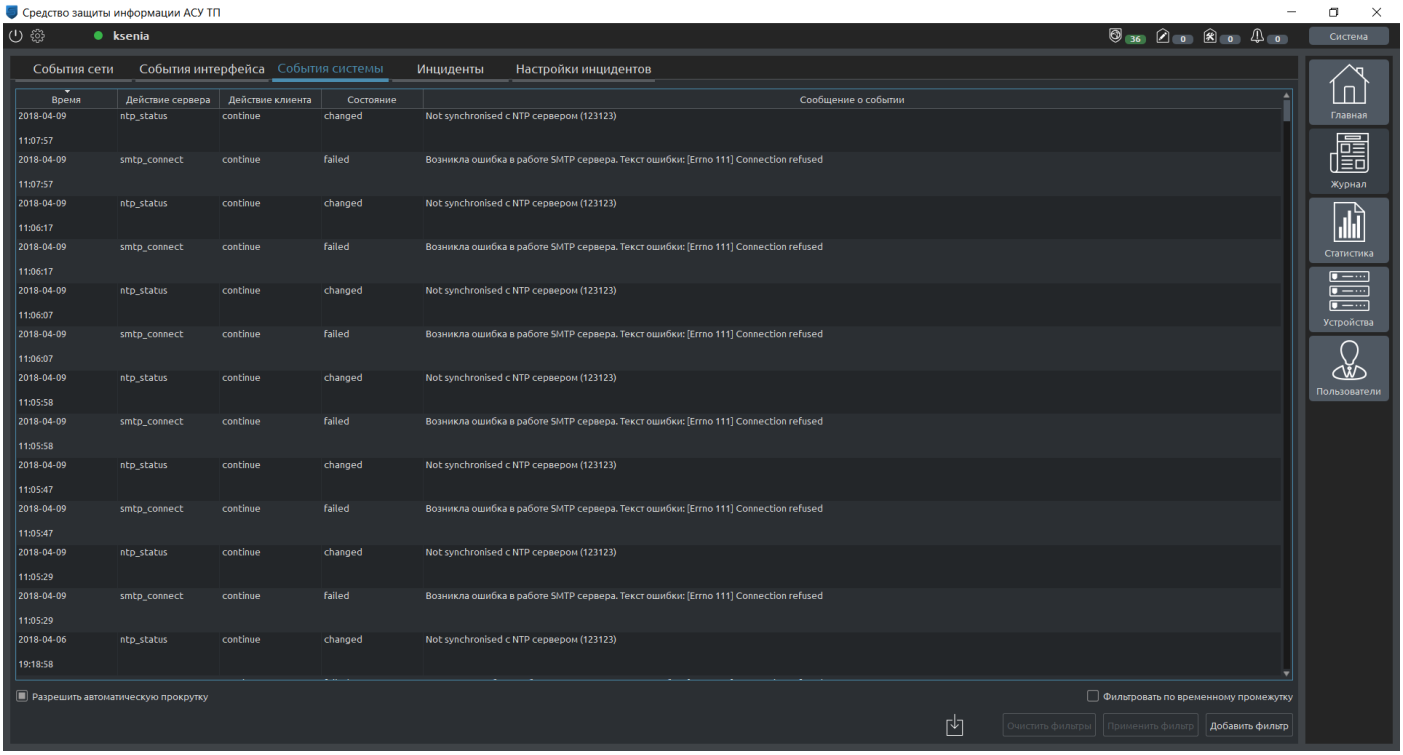


Рисунок 19. События системы

6.2.4. ИНЦИДЕНТЫ

В данном журнале (Инциденты) отображается следующая информация:

- обнаружено новое устройство (обнаружена новая пара MAC/IP адресов в сети);
- обнаружена атака ARP spoofing.[3] (обнаружено большое количество событий канального уровня, которые можно интерпретировать как атаку ARP spoofing);

- обнаружена информационная атака;
- обнаружен конфликт IP-адресов (обнаружена попытка двух устройств занять один IP-адрес, либо конфликт IP-адресов, либо связано с атакой);
- обнаружение применения metasploit;
- обнаружено нарушение правил межсетевого экранирования;
- обнаружено нарушение целостности устройства защиты;
- обнаружено нарушение целостности – несоответствие списку контролируемых файлов (системные сообщения, получен пустой список файлов ПО устройства защиты для проверки системой контроля целостности);
- обнаружено нарушение целостности – несоответствие пользователя устройству защиты (системные сообщения, возникающие, например, при копировании образа системы с одной аппаратной платформы на другую);
- обнаружено нарушение целостности – несоответствие временному интервалу;
- обнаружено нарушение целостности сети – потеряно соединение с ПЛК;
- обнаружено нарушение целостности сети – потеряно соединение со SCADA системой;
- обнаружено подключение к административному интерфейсу ПЛК;
- обнаружена информационная атака – изменение (чтение) прошивки ПЛК;
- вызвана проверка контрольной суммы для несуществующего устройства;
- некорректно сформирован запрос проверки контрольной суммы;
- не найден файл программного обеспечения, отвечающий за изменение времени;
- не выставлены права файла скрипта для изменения времени;
- не задана переменная сервера;
- нет возможности отменить задачу, так как не найдена TaskState;
- задано неверное значение переменной настроек сервера;
- обнаружено изменение MAC-адреса (обнаружен факт занятия IP-адреса новым устройством);
- обнаружена подмена MAC-адреса (MAC-адрес отправителя пакета не соответствует MAC-адресу, привязываемому к IP адресу);
- потеряна связь с активным устройством защиты (резервное УЗ потеряло соединение с активным УЗ);
- обнаружена попытка подбора пароля (пользователь 3 раза ввел неправильный пароль в течение 30 секунд (значения по умолчанию, возможно изменение)).

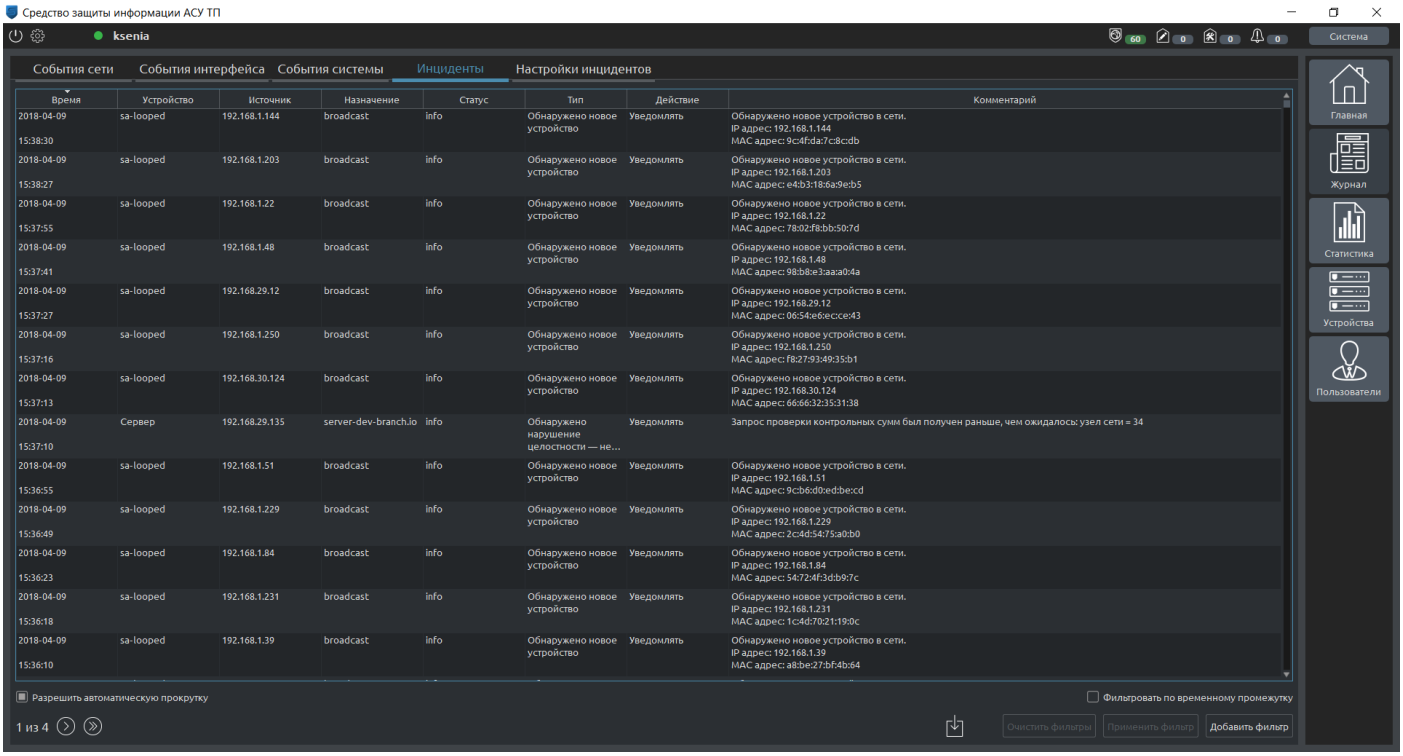


Рисунок 20. Инциденты

6.2.5. НАСТРОЙКА ИНЦИДЕНОВ

Вкладка «Настройки инцидентов» (Настройки инцидентов) доступна только при использовании учетной записи типа «Администратор».

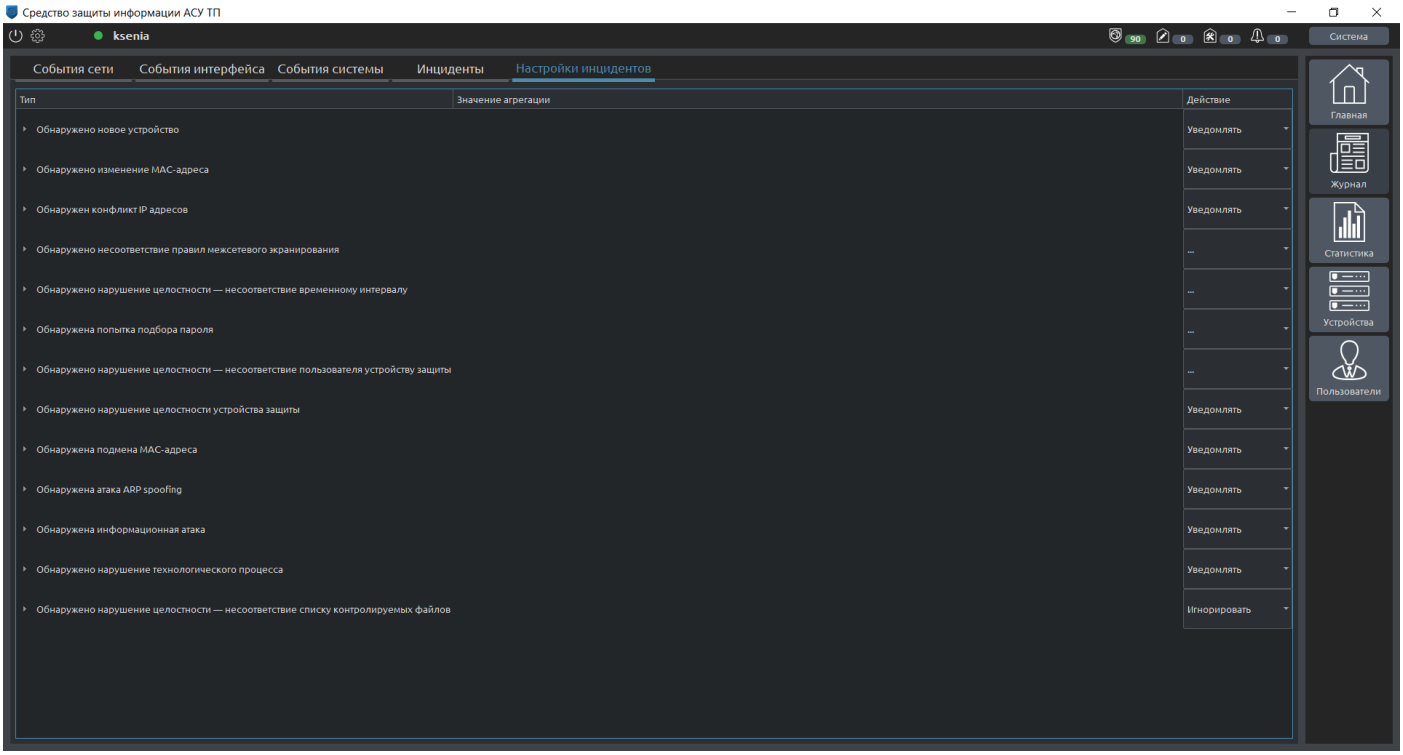


Рисунок 21. Настройки инцидентов

Данная вкладка разбита на две части:

1. «Дерево инцидентов» – имеет два уровня вложенности, на верхнем уровне в узлах расположены типы инцидентов, на втором – сгруппированные инциденты (группировка выполняется по полям, представленным на рисунке (Описание группы инцидентов), оно позволяет изменять состояние групп, тем самым, меняя отображаемую информацию на «Окне состояний» (Настройки инцидентов);
2. «Подробная информация о группе инцидентов» – описание произошедших событий, нарушающих безопасность (Описание группы инцидентов).

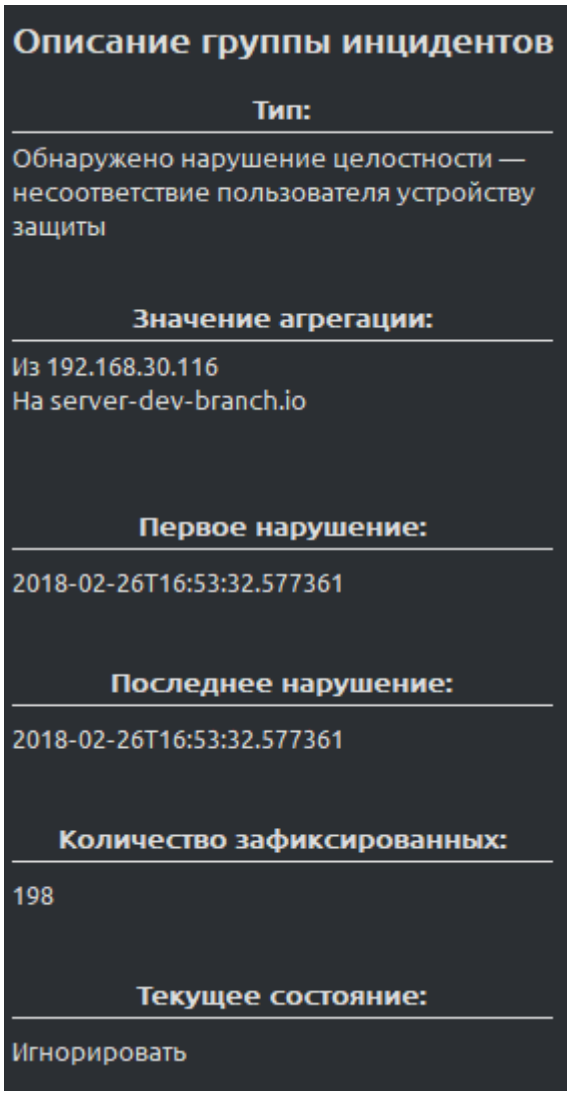


Рисунок 22. Описание группы инцидентов

Для конкретной группы инцидентов можно выбрать одно из трех состояний:

- «Уведомлять» – принадлежащие данной группе инциденты отображаются. В случае нового зафиксированного события будет выведено уведомление (Описание группы инцидентов), если не включена опция, отключающая уведомления.

- «Игнорировать» – принадлежащие данной группе инциденты не отображаются, уведомление не выводится.
- «Решено» – принадлежащие данной группе инциденты не отображаются. В случае нового зафиксированного события будет выведено уведомление, а группа перейдёт в состояние «Уведомлять».

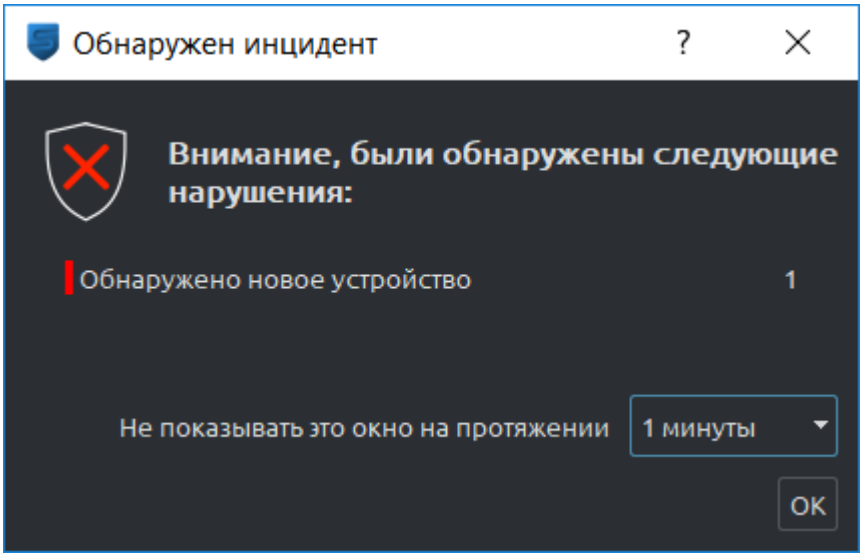


Рисунок 23. Описание группы инцидентов

6.3. СТАТИСТИКА

Окно статистики вызывается нажатием на кнопку «Статистика» навигационной панели и разделено на 5 вкладок: «События сети за время», «События интерфейса за время», «События системы за время», «Инциденты за время», «Инциденты по типам» (Статистика). Пользователь может указать день, за который необходимо получить статистику.

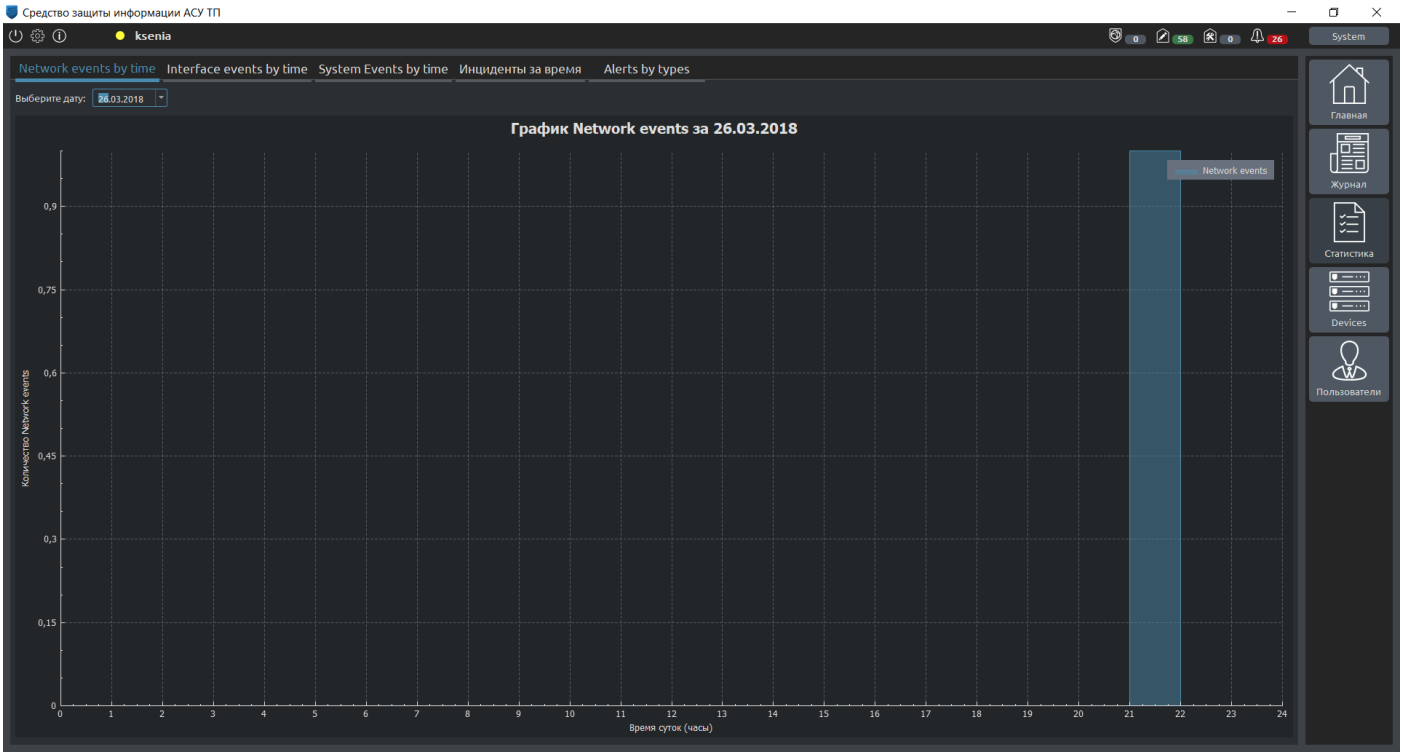


Рисунок 24. Статистика

Вкладки «События сети за время», «Инциденты за время»

Статистика представлена в виде графиков, отражающих количество определенных событий (Статистика) и инцидентов (Инциденты за время) за текущие сутки по часам.

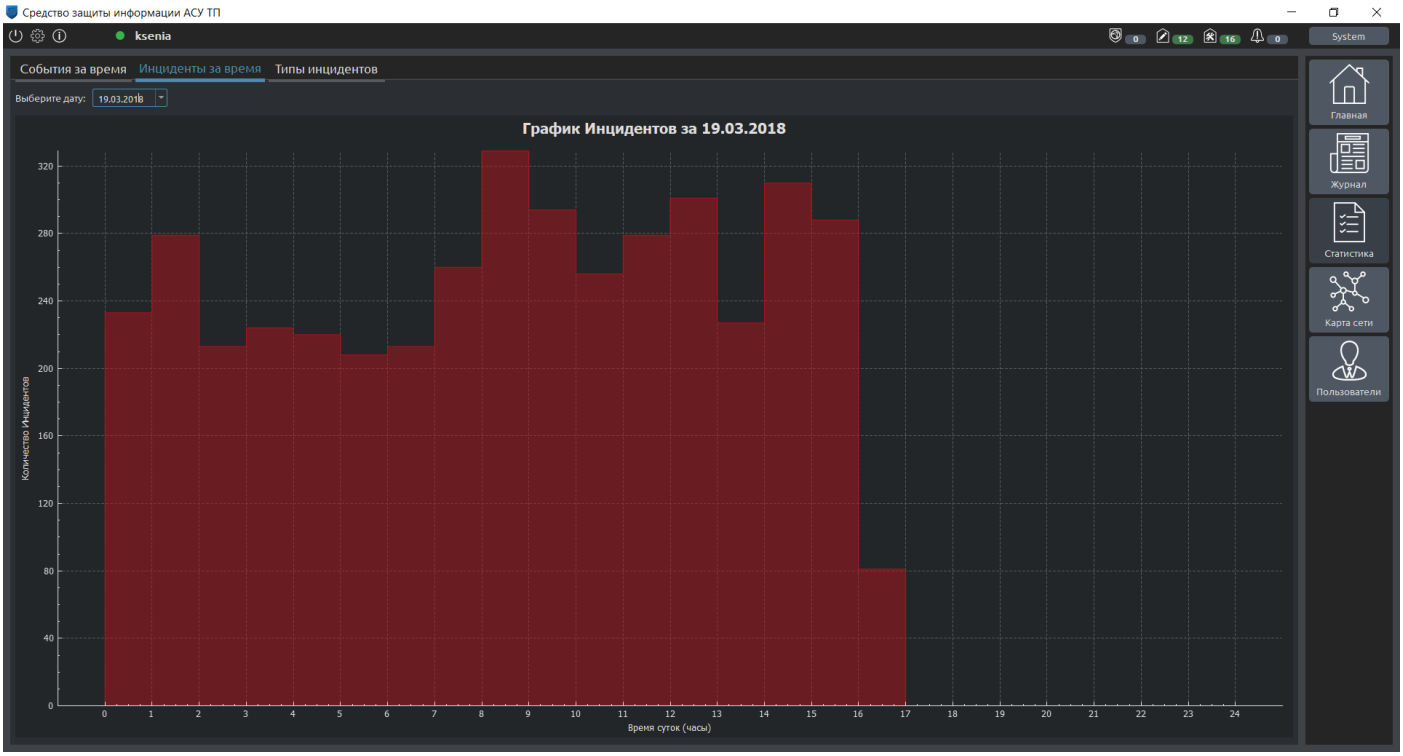


Рисунок 25. Инциденты за время

Вкладка «События интерфейса за время»

Вкладка «События интерфейса за время» (События интерфейса за время) отображает количество событий интерфейса за текущие сутки по часам.

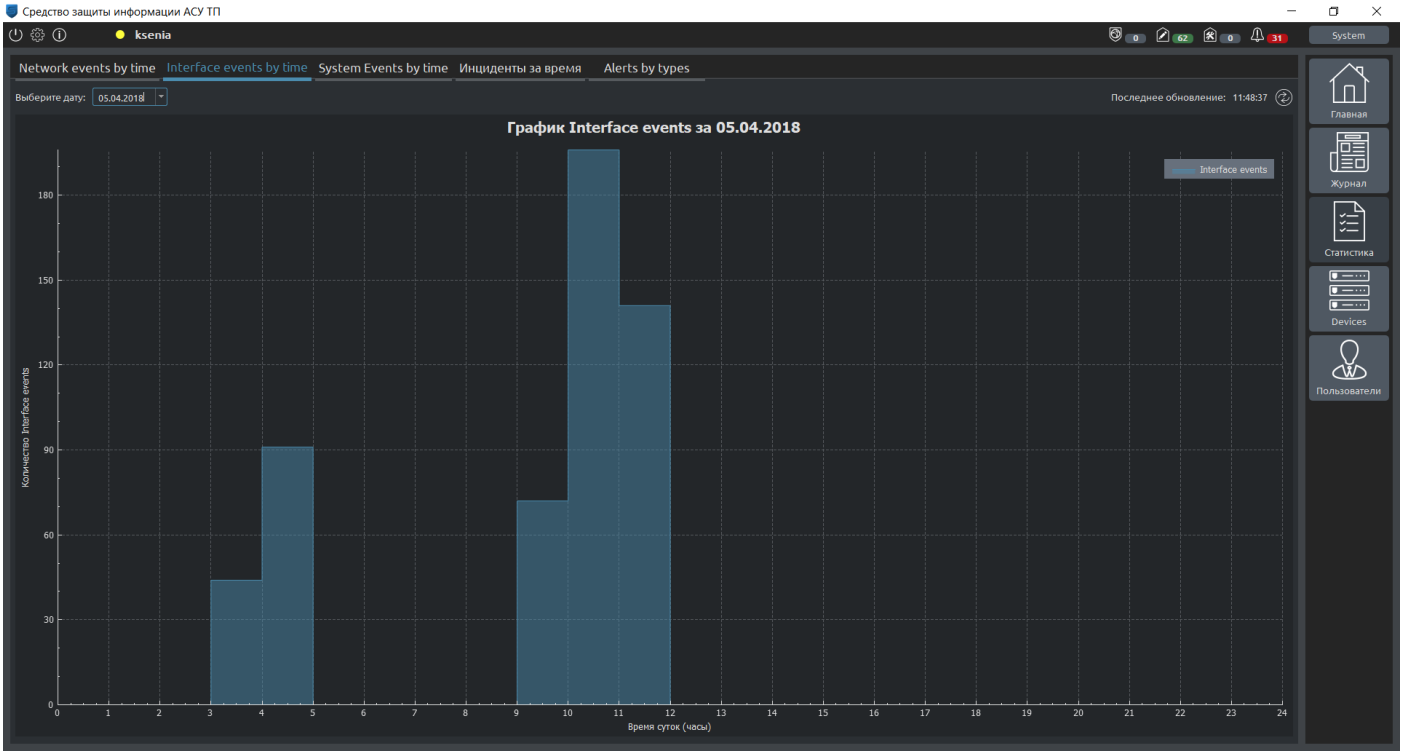


Рисунок 26. События интерфейса за время

Вкладка «События системы за время»

Вкладка «События системы за время» (События интерфейса за время) отображает количество событий системы за текущие сутки по часам.

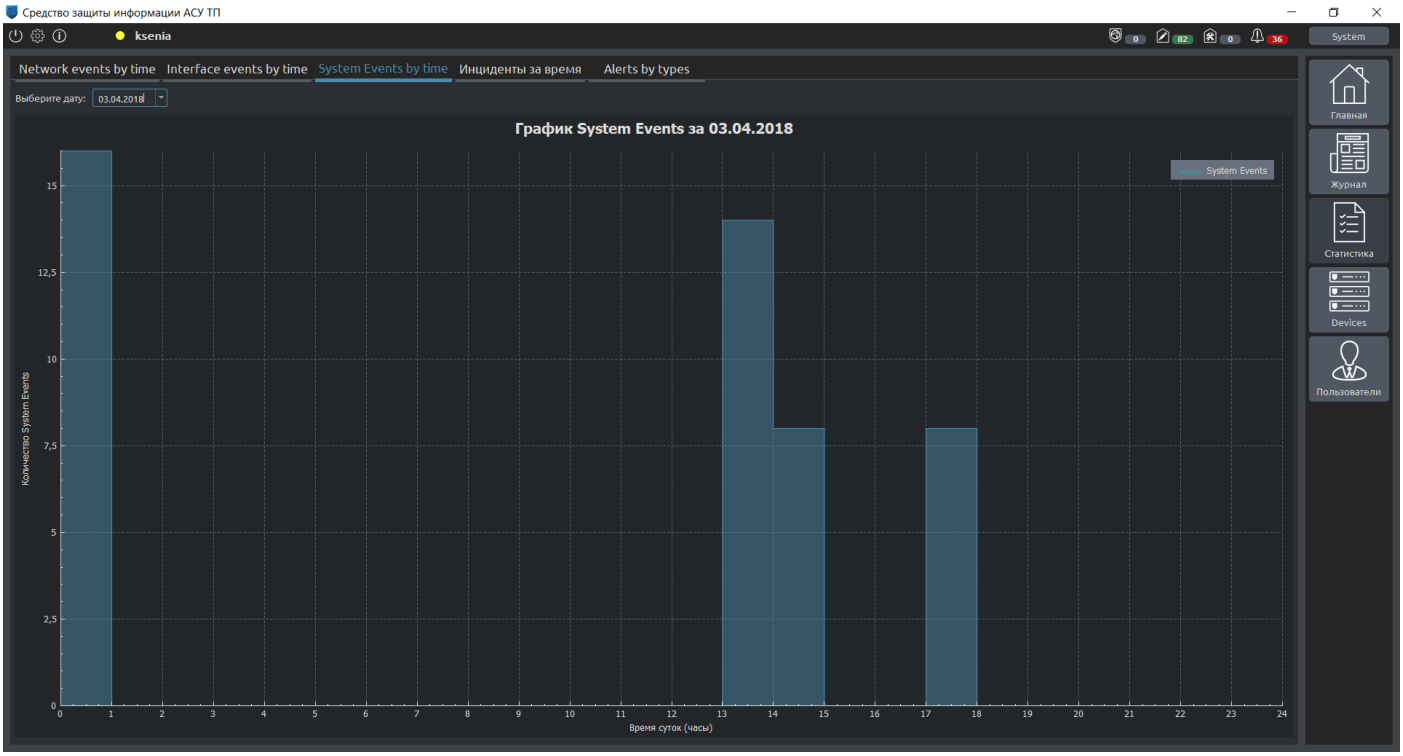


Рисунок 27. События интерфейса за время

Вкладка «Инциденты по типам»

Вкладка «Инциденты по типам» показывает распределение инцидентов, произошедших за все время по типу в виде графика (Инциденты по типам).

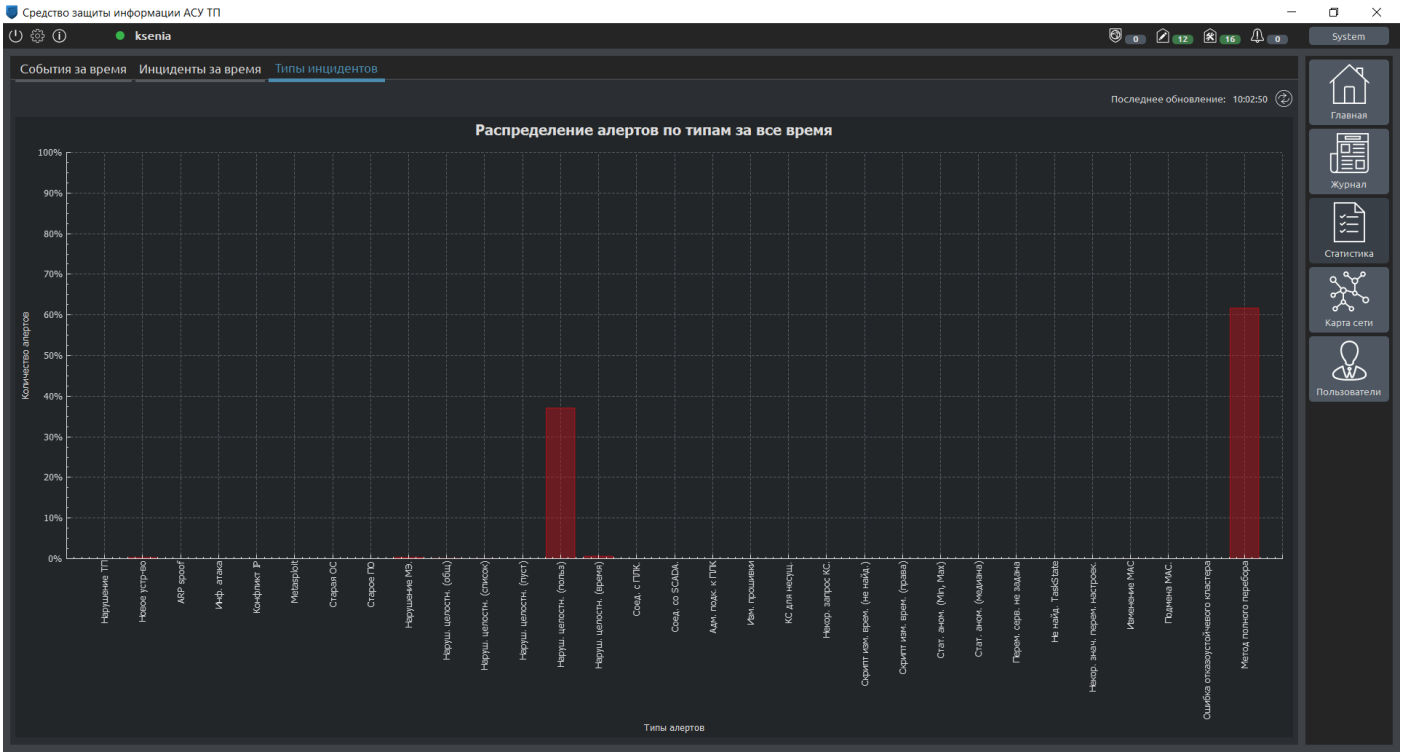


Рисунок 28. Инциденты по типам

6.4. УСТРОЙСТВА

Окно «Устройства» (Устройства) вызывается нажатием на кнопку «Устройства» навигационной панели и предоставляет информацию о всех устройствах защиты, подключенных к используемому серверу. Окно «Устройства» выполняет следующие функции:

- добавление нового устройства защиты;
- отображение базовой информации об устройстве;
- отображение всех доступных устройств;
- добавление нового и удаление имеющегося устройства;
- возможность выгружать файл конфигурации УЗ для добавленного на сервер УЗ.

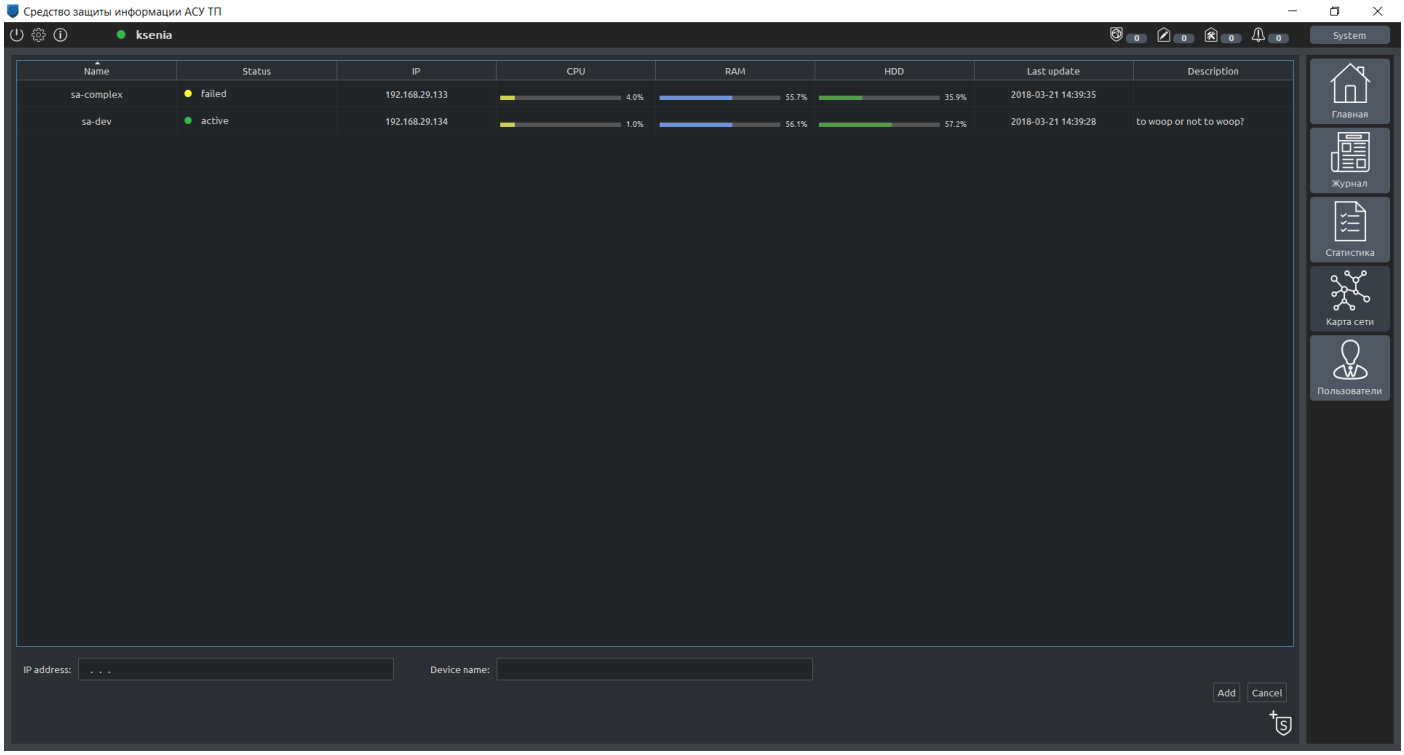


Рисунок 29. Устройства

На рисунке 29 отображена базовая информация об устройствах защиты:

- имя устройства;
- тип устройства;
- состояние работы устройства;
- адрес управления устройства;
- уровень загруженности процессора «CPU»;

- количество свободной оперативной памяти «RAM»;
- количество свободного места «HDD»;
- время последнего обновления информации об устройстве;
- описание устройства.

Так же можно добавлять/удалять новое устройство. Для добавления нового устройства нужно воспользоваться дополнительным полем (Добавление нового устройства), нажав на кнопку  , в котором нужно ввести IP-адрес и имя устройства защиты и нажать кнопку «Добавить». После создания УЗ необходимо провести операции, описанные в соответствующем разделе руководства администратора.

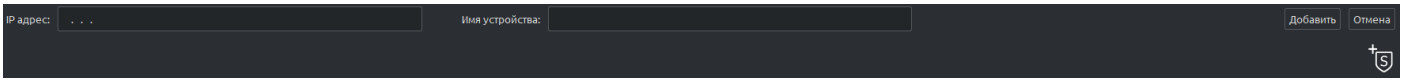


Рисунок 30. Добавление нового устройства

Для удаления устройства необходимо выбрать конкретное устройство, перейти в его настройки и в разделе «Удаление устройства» (Удаление устройства) нажать кнопку «Удалить» и подтвердить удаление, нажав «Да» (Подтверждение удаления устройства). После удаления устройства, УЗ продолжит работать в последней конфигурации, а последующее изменение конфигурации будет невозможно. Для возобновления возможности управления конфигурацией, необходимо воспользоваться руководством администратора.

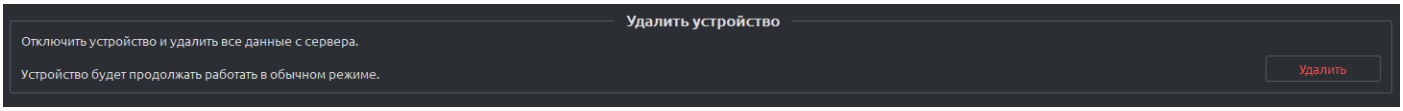


Рисунок 31. Удаление устройства

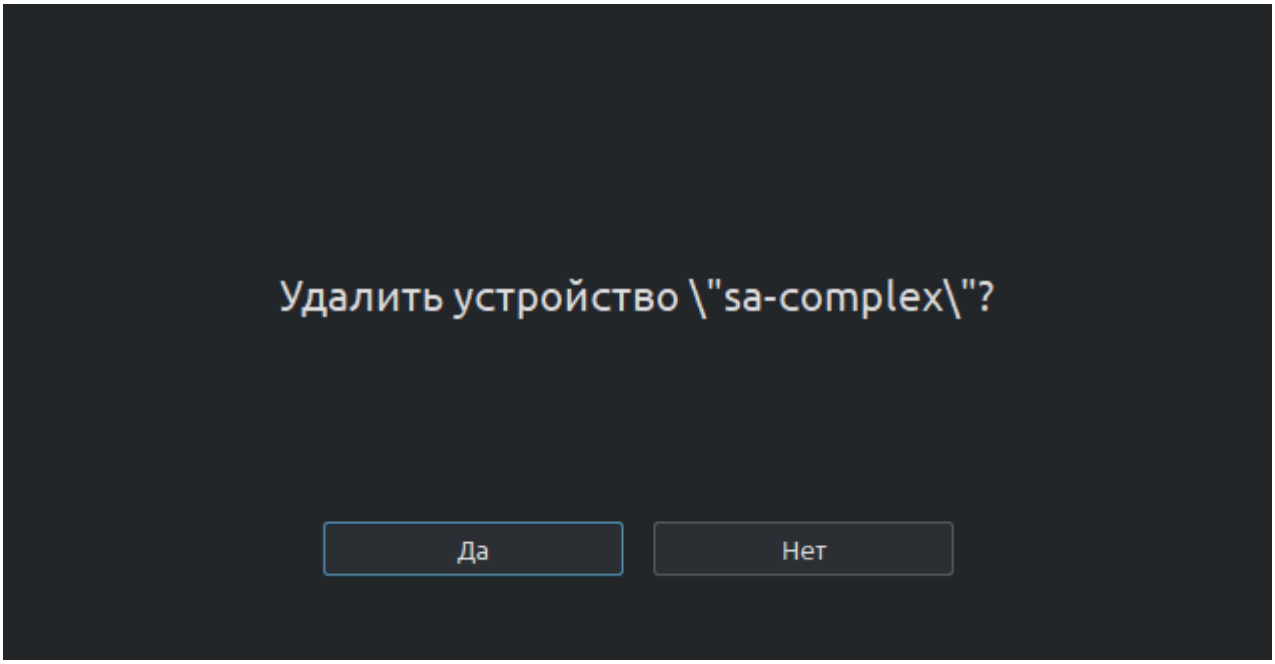


Рисунок 32. Подтверждение удаления устройства

Для администратора доступно окно настроек – по двойному нажатию на устройство (Подтверждение удаления устройства).

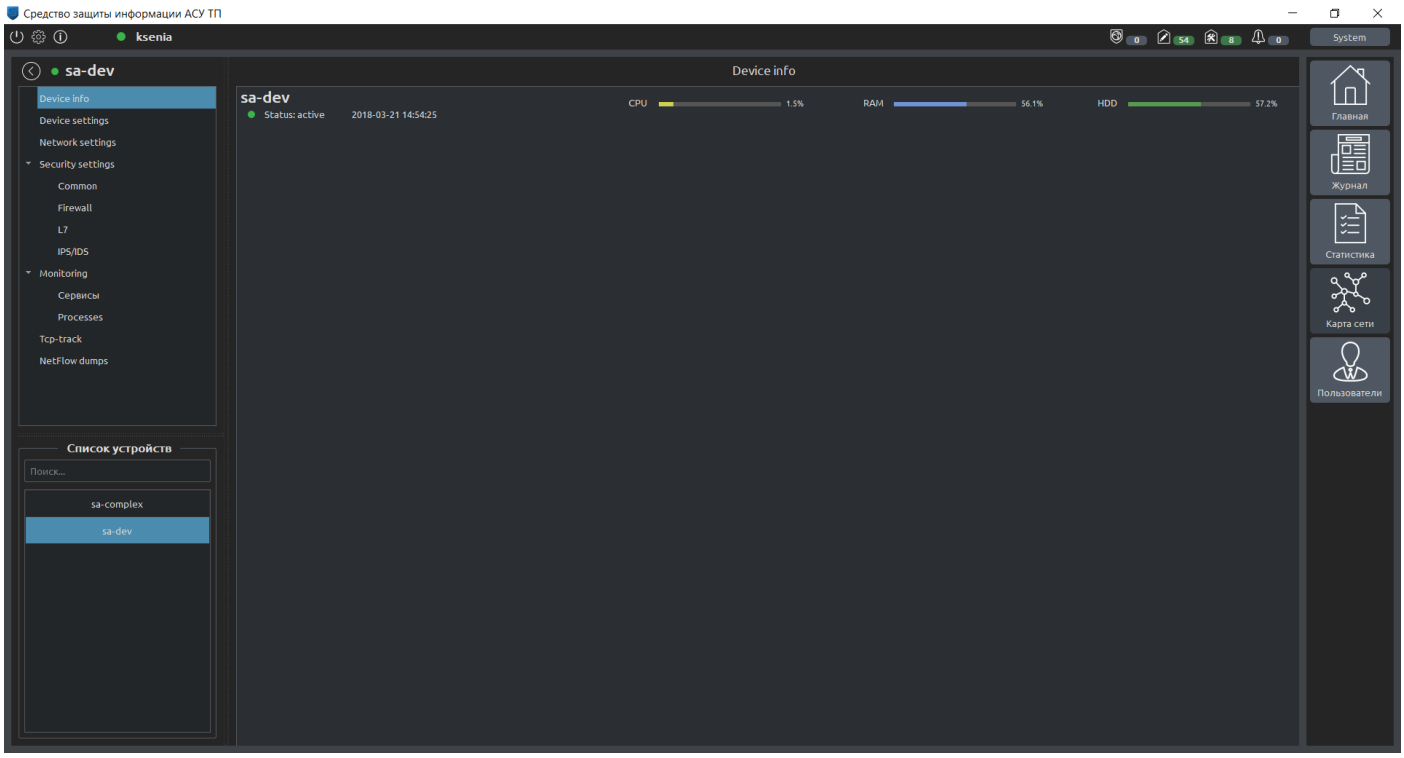


Рисунок 33. Подтверждение удаления устройства

Окно настроек состоит из 7 вкладок: «Информация об УЗ», «Настройки устройства» «Сетевые настройки», «Настройки безопасности», «Мониторинг», «TCP соединения», «Дампы трафика». Администратор может редактировать настройки одновременно нескольких устройств.

6.4.1. «ИНФОРМАЦИЯ ОБ УЗ»

Во вкладке «Информация об УЗ» представлена информация об устройстве защиты: состояние работы устройства, уровень загруженности процессора («CPU»), количество свободной оперативной памяти («RAM»), количество свободного места («HDD»).

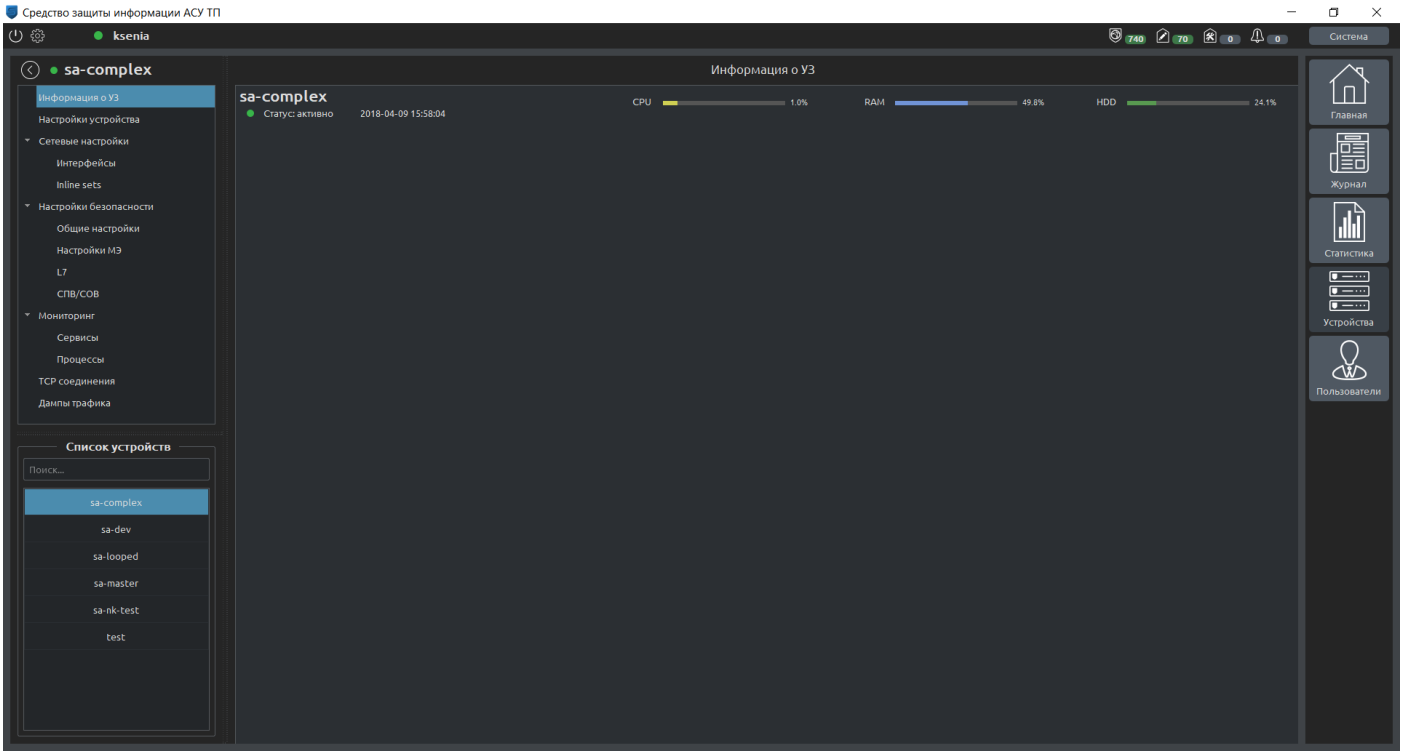


Рисунок 34. Подтверждение удаления устройства

6.4.2. «НАСТРОЙКИ УСТРОЙСТВА»

Во вкладке «Настройки устройства» (Настройки устройства) представлены настройки устройства защиты:

- пользовательское описание устройства;
- настройка SNMPv3;
- загрузка файла конфигурации для первоначальной настройки УЗ;
- удаление устройства.

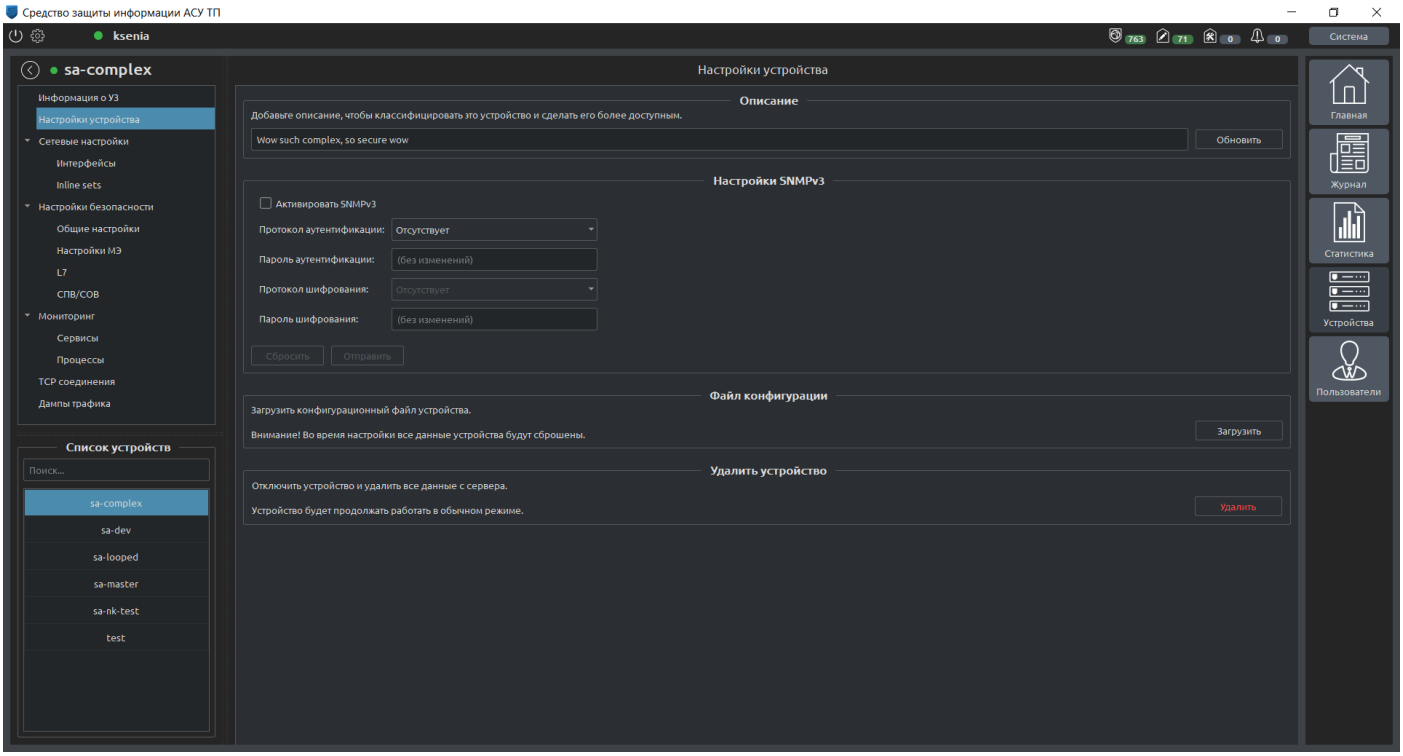


Рисунок 35. Настройки устройства

6.4.3. «СЕТЕВЫЕ НАСТРОЙКИ»

Данная вкладка состоит из вкладок «Интерфейсы» и «Мосты». Вкладка «Интерфейсы» (Сетевые настройки) предоставляет информацию о сетевых интерфейсах и позволяет редактировать их настройки: MTU, режим работы сетевых интерфейсов устройства Span/Inline. Информация о сетевых интерфейсах содержит следующие данные:

- имя интерфейса;
- тип интерфейса;
- группа, к которой он относится («Мост»);
- MAC-адрес;
- MTU значение;
- дуплекс значение;
- скорость;
- описание.

Также возможно редактирование сетевых настроек (Окно редактирования сетевых настроек).

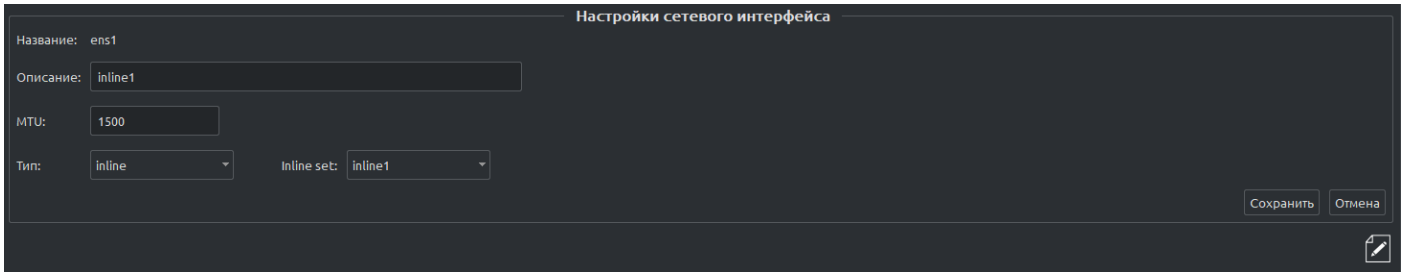


Рисунок 36. Окно редактирования сетевых настроек

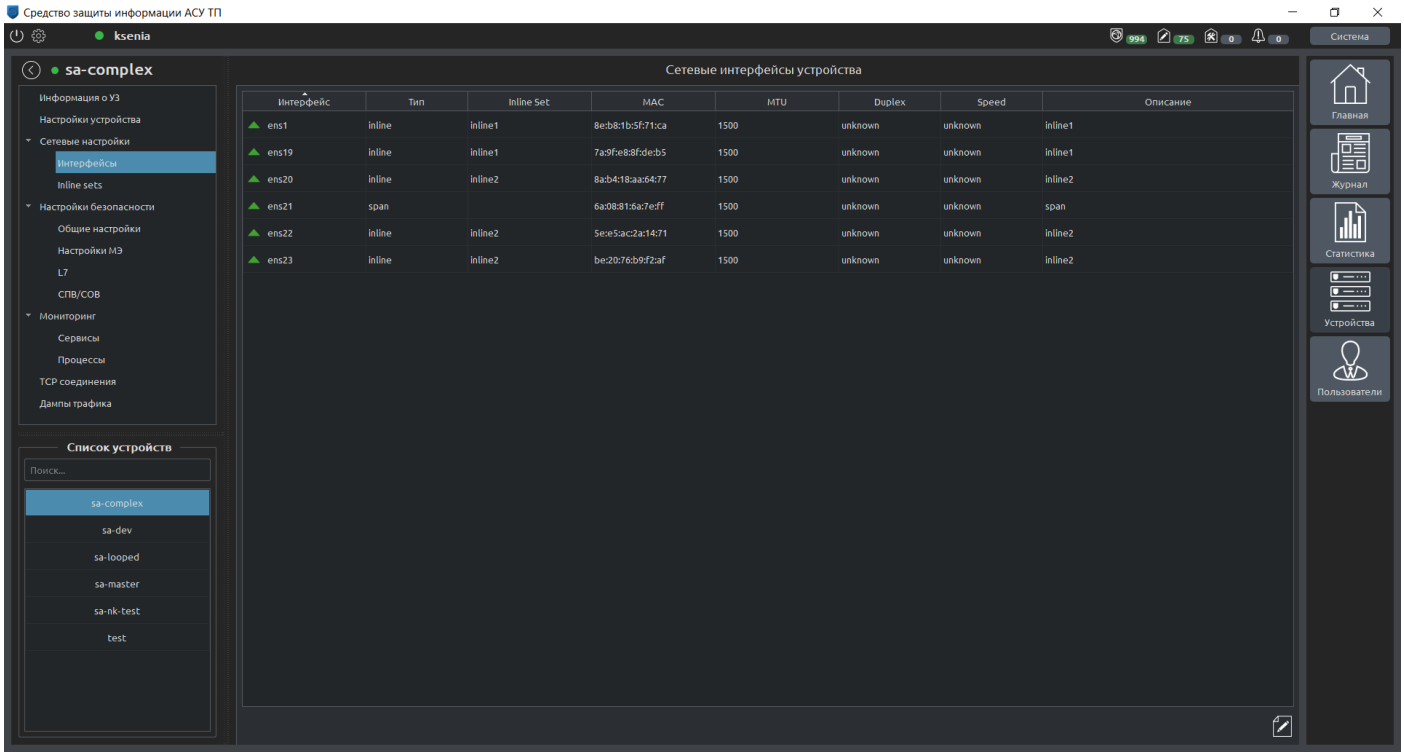


Рисунок 37. Сетевые настройки

Вкладка «Мосты» позволяет объединять интерфейсы в группы (которые по сути являются Bridge или Inline Set), а также предназначена для объединения интерфейсов в мосты и показывает уже созданные мосты. Если группа интерфейсов объединена в один мост (одну группу), то они работают как единое устройство второго уровня.

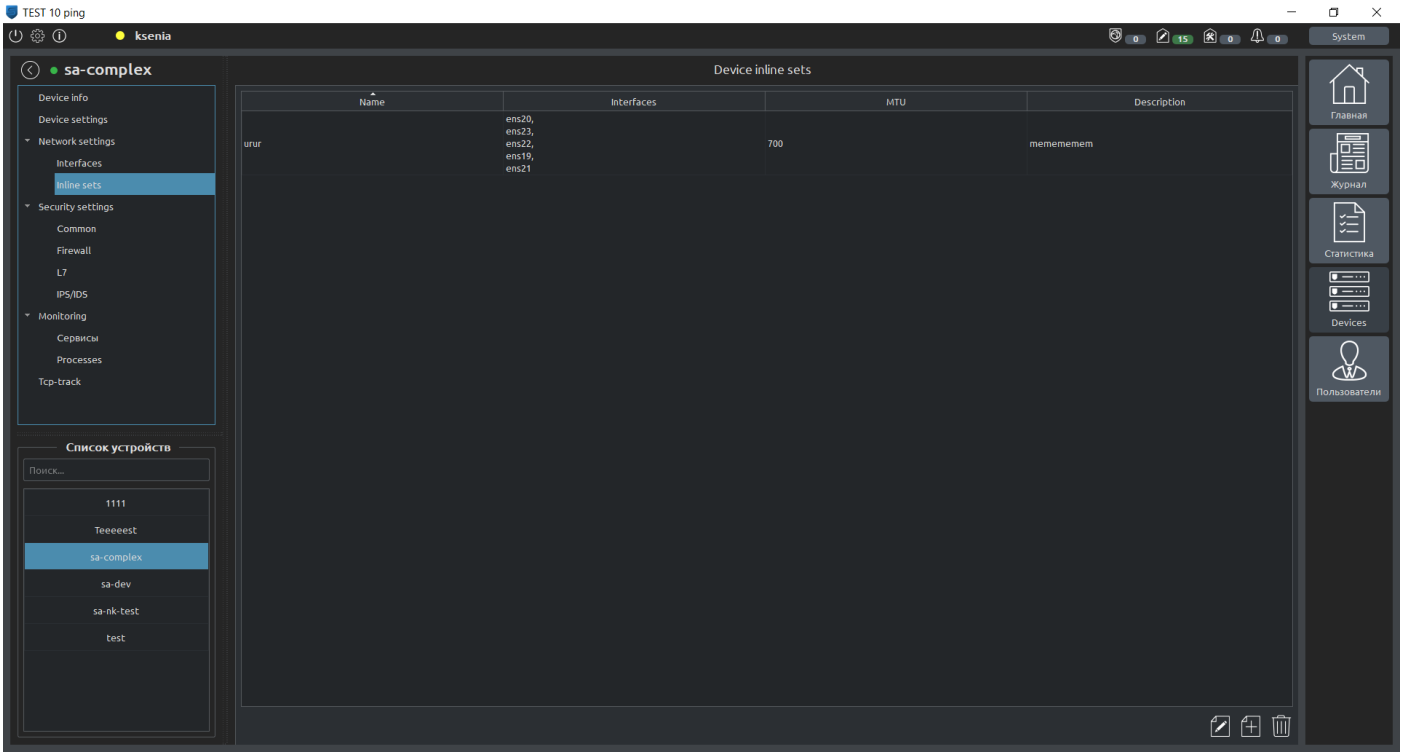


Рисунок 38. Inline Sets

6.4.4. «НАСТРОЙКИ БЕЗОПАСНОСТИ»

Вкладка «Настройки безопасности» содержит в себе следующие вкладки:

- «Общие настройки»;
- «Настройки МЭ»;
- «Настройки L7»;
- «Настройки СПВ/СОВ».

«Общие настройки» Вкладка «Общие настройки» (Общие настройки) позволяет конфигурировать опции устройства защиты и позволяет импортировать/экспортировать базу решающих правил для СОВ/СПВ. Список опций устройства защиты доступных для изменения:

- включить/отключить защиту;
- включить/отключить журналирование TCP соединений;
- включить/отключить блокировку вредоносных пакетов;
- включить/отключить преобразование сетевых адресов (NAT);
- изменить режим межсетевого экранирования (черный список/белый список).

Черный список – режим, при котором МЭ запрещает соединения, соответствующие правилам,

указанным в таблице правил МЭ. Белый список – режим, который разрешает соединения, указанные в таблице правил МЭ. Для добавления групп правил или обновления базы решающих правил необходимо нажать кнопку загрузки в правой нижней части блока и выбрать архив с системными группами правил, полученных от разработчика.

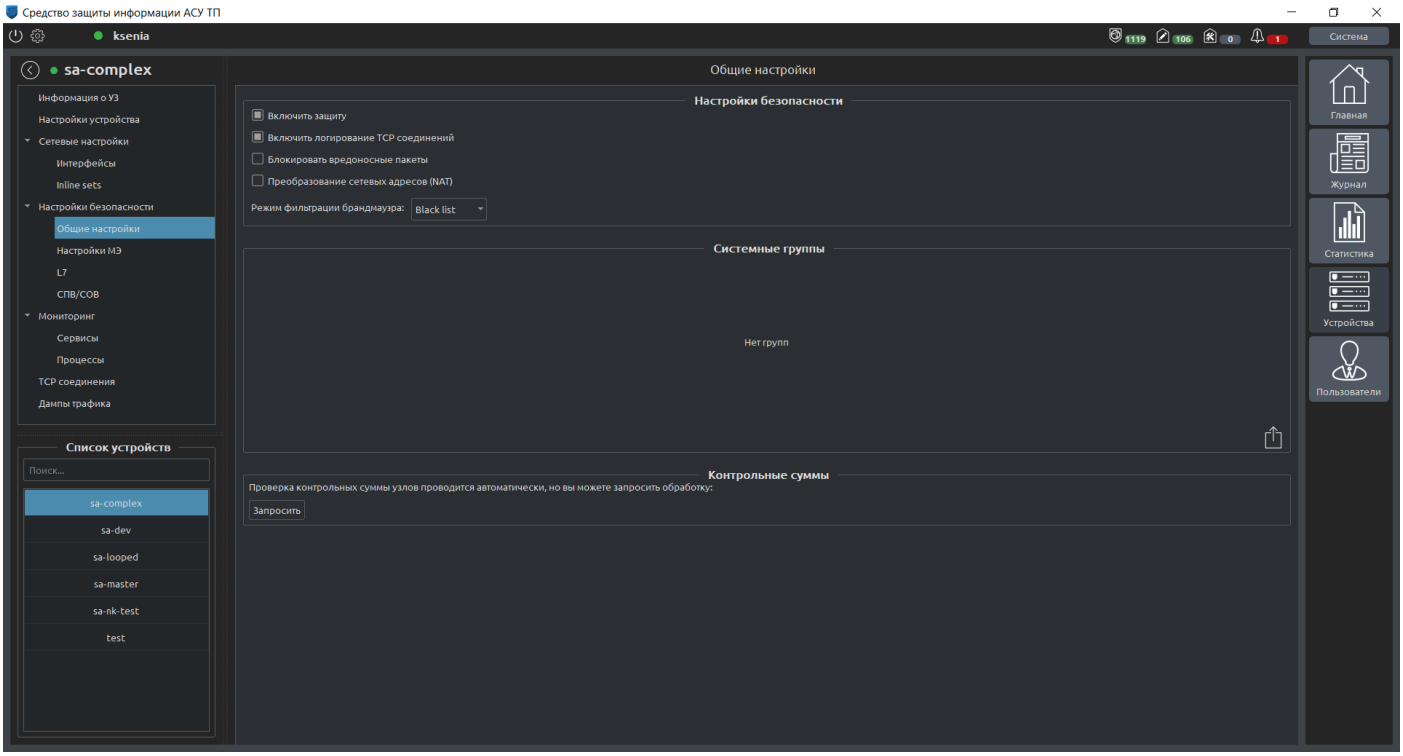


Рисунок 39. Общие настройки

«Настройки межсетевого экрана»

Во вкладке «Настройки межсетевого экрана» (Настройки межсетевого экрана) редактируется список правил межсетевого экранирования

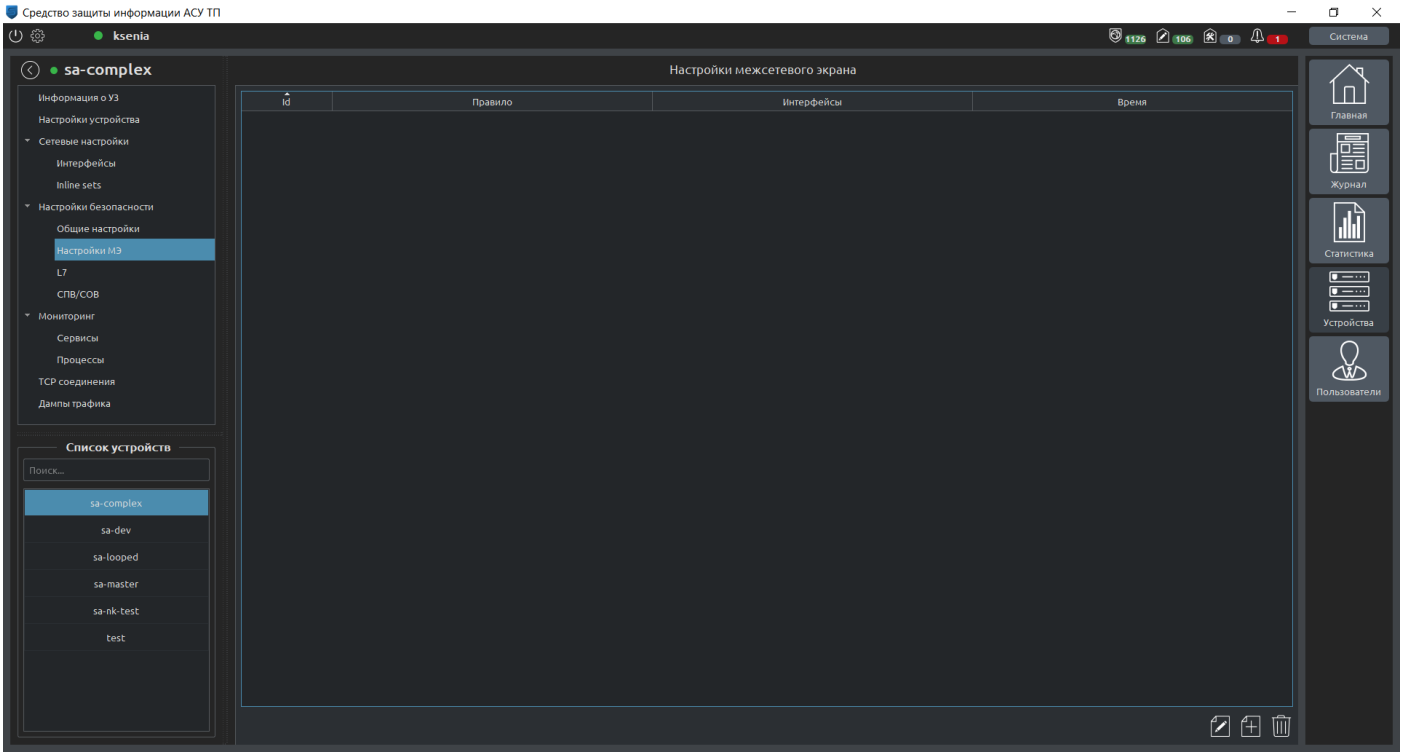


Рисунок 40. Настройки межсетевого экрана

«Настройки L7»

Вкладка «Настройки L7» (L7) позволяет настраивать правила фильтрации для прикладного уровня сети с помощью специализированного конструктора, поддерживающего добавление правил по следующим протоколам:

- Modbus TCP;
- IEC 60870-5-104;
- OPC UA;
- OPD DA.

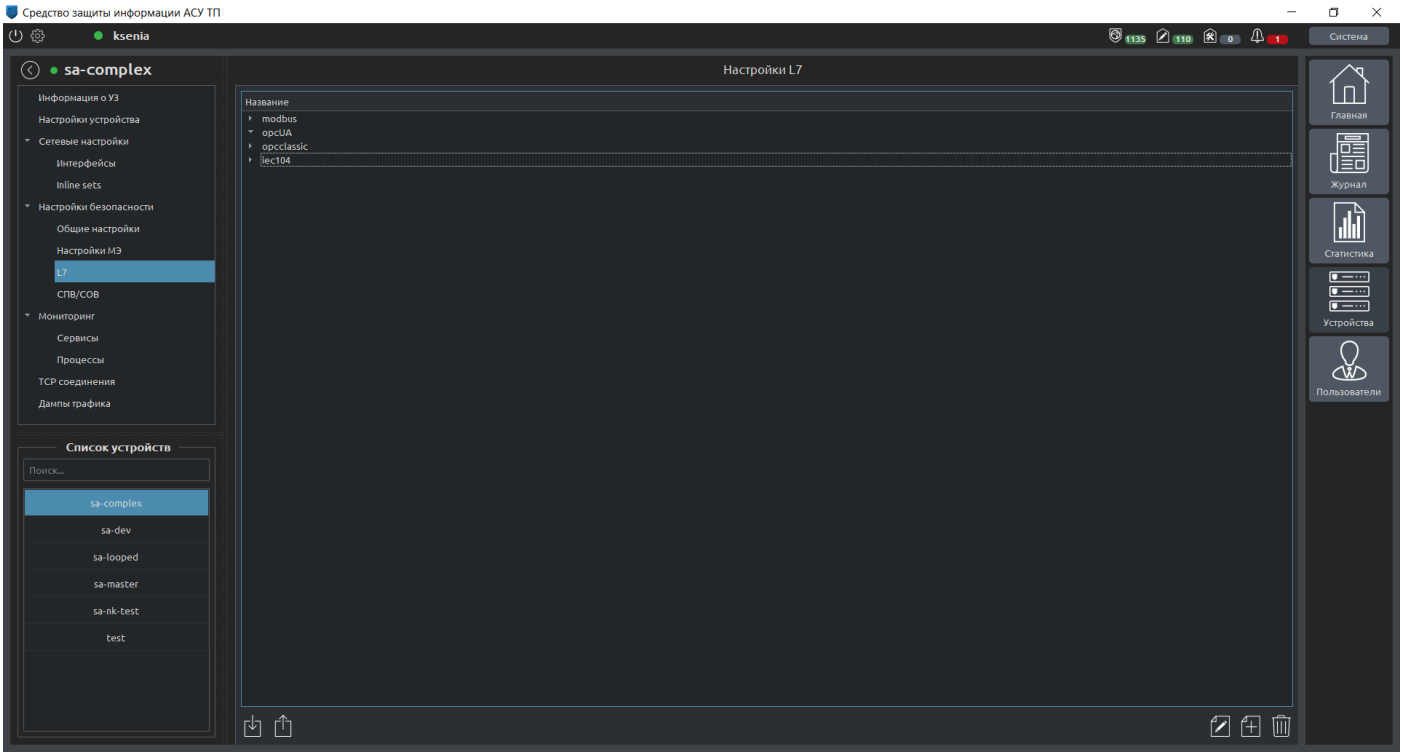


Рисунок 41. L7

«Настройки системы предотвращения и обнаружения вторжений (СПВ/СОВ)»

Вкладка «Настройки СПВ/СОВ» (Настройки СОВ/СПВ) представляет возможность настройки конкретного устройства защиты. Основное рабочее пространство вкладки представляет из себя список правил на сервере, которые применяются ко всем УЗ, входящих в состав ПК.

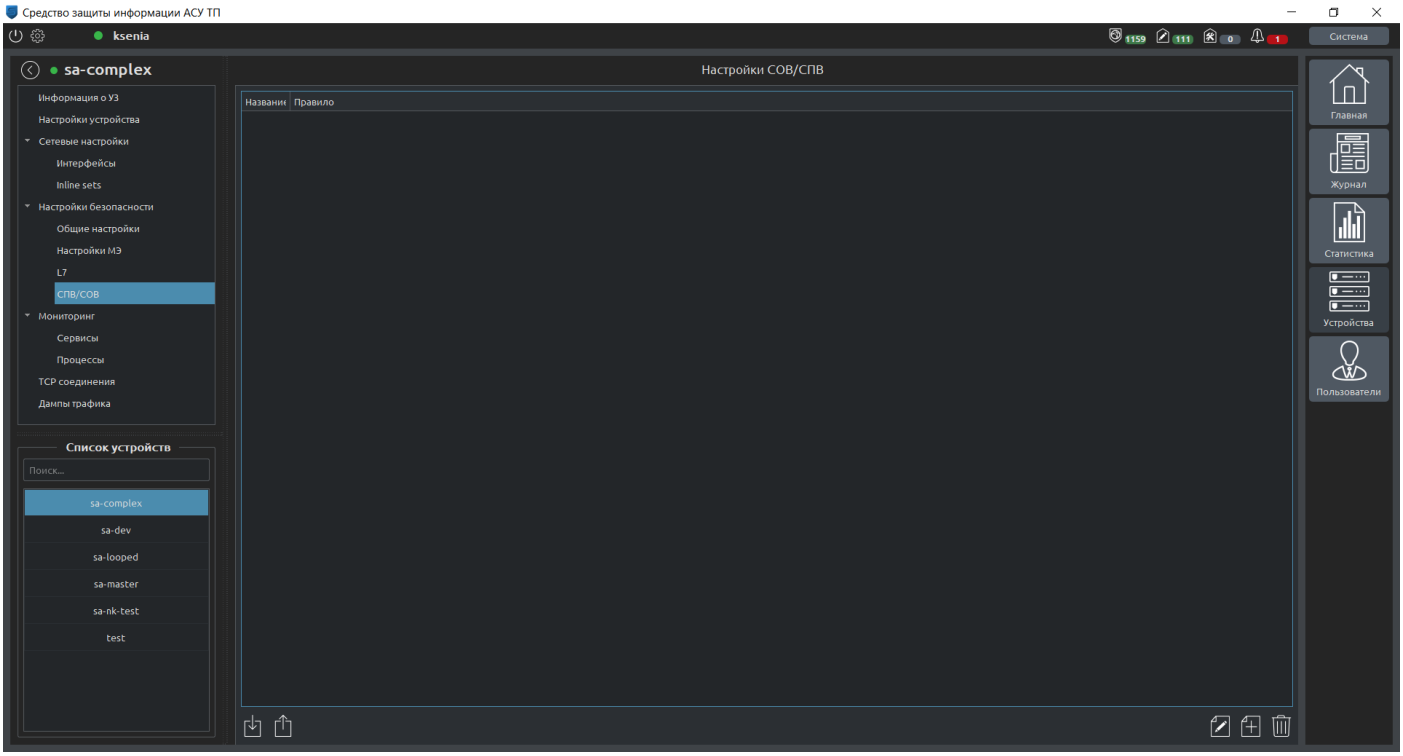


Рисунок 42. Настройки СОВ/СПВ

В основной рабочей области представлен список сгруппированных правил, которые можно редактировать, удалять и добавлять новые. При нажатии кнопки «+» откроется область добавления правил. После заполнения всех необходимых полей и нажатия на кнопку «Отправить изменения на сервер» правило станет активным на всех УЗ, входящих в состав в используемый сегмент ПК «Аркан».

В данном окне отображается список правил системы обнаружения вторжений, сгруппированный так, как удобно пользователю. Редактировать можно как группы (Редактор групп СПВ/СОВ), так и сами правила. Для вызова окон редактирования выполняется двойное нажатие.

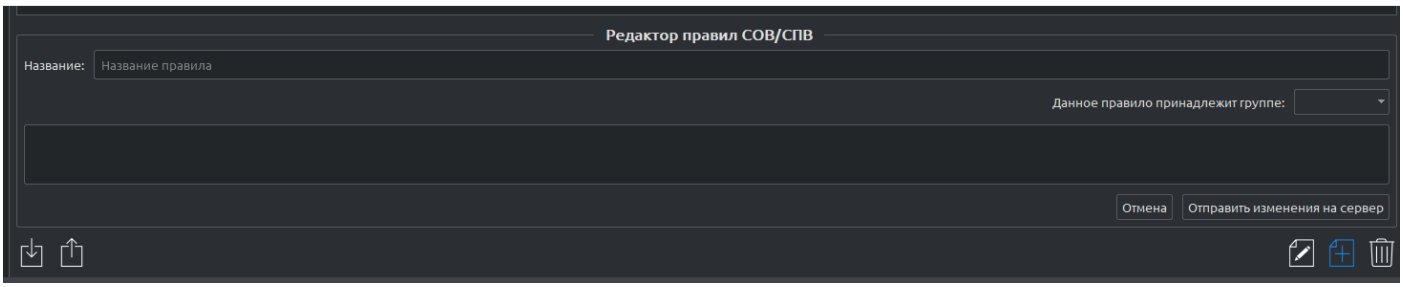


Рисунок 43. Редактор групп СПВ/СОВ

6.4.5. «МОНИТОРИНГ»

Вкладка «Мониторинг» включает в себя вкладки «Сервисы» и «Процессы».

«Сервисы»

Вкладка «Сервисы» (Сервисы) содержит список всех сервисов из состава ПК «Аркан», использующихся на УЗ. В таблице представлены имя сервисов, их тип, статус и время с последнего перезапуска.

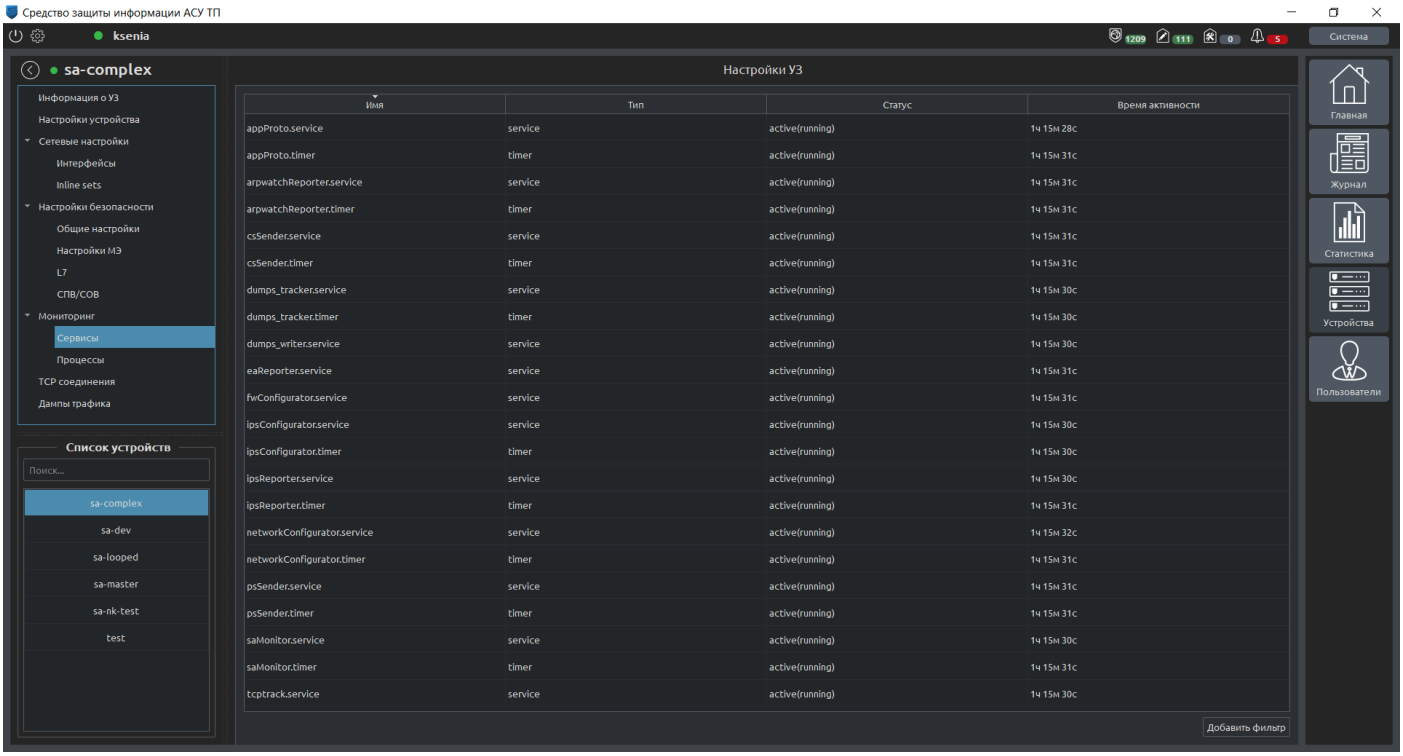


Рисунок 44. Сервисы

В штатном режиме работы системы все сервисы должны быть активны и работать без ошибок (статус active(running)), а состояние устройства защиты должно быть «Активно» и иметь индикатор активности зеленого цвета. В случае, если один из сервисов имеет статус, отличный от нормального (active(running)), необходимо обратиться к администратору.

Процессы»

Вкладка «Процессы» (Процессы) содержит список всех процессов.

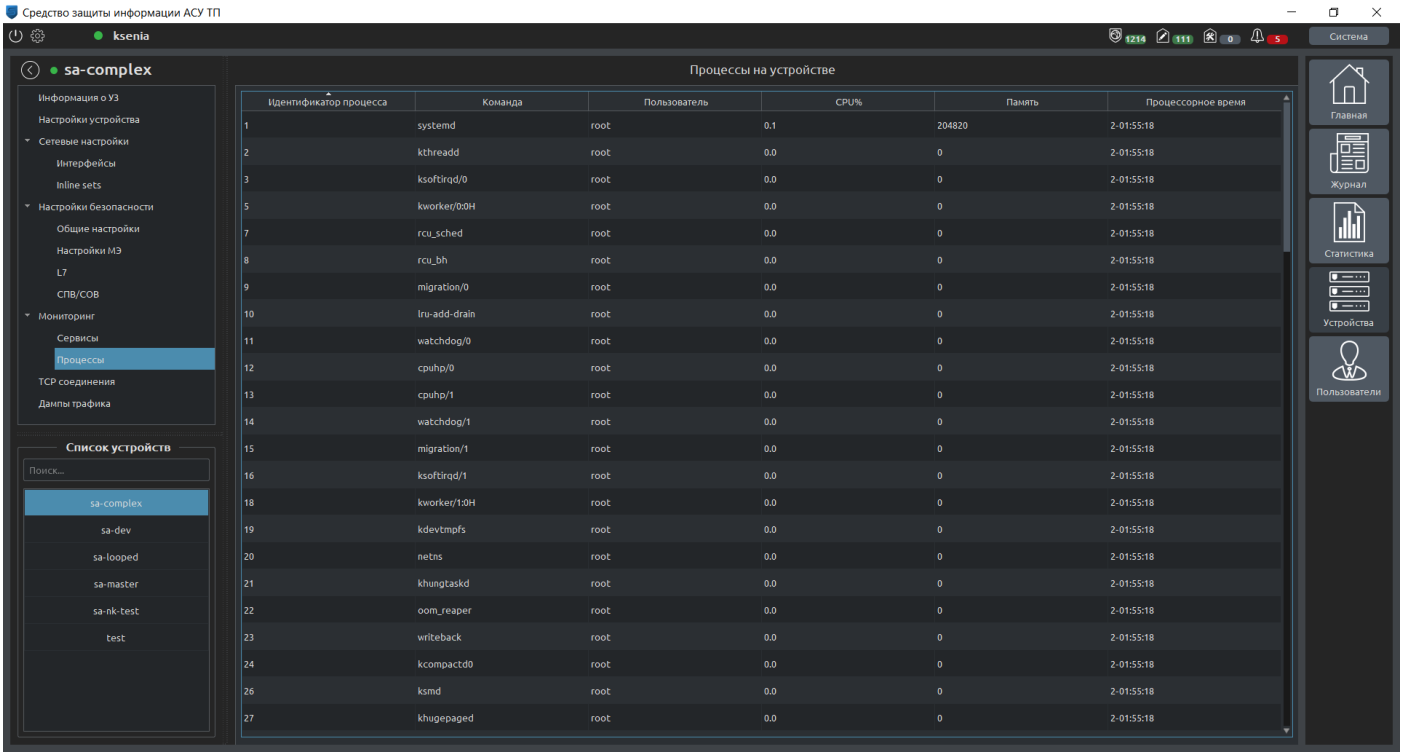


Рисунок 45. Процессы

Данная вкладка автоматически не обновляется, только по запросу пользователя. Первое обновление происходит при открытии настроек ПК.

6.4.6. «TCP СОЕДИНЕНИЯ»

Вкладка «TCP соединения» (TCP соединения) отображает текущие TCP сессии, проходящие через устройства защиты. Информация о текущих TCP сессиях представлена в виде таблицы со следующими столбцами:

- «Источник» (IP адрес и TCP порт устройства);
- «Назначение» (IP адрес и TCP порт устройства);
- «Состояние» (состояние сессии);
- «Время бездействия»;
- «Скорость, Б/с».

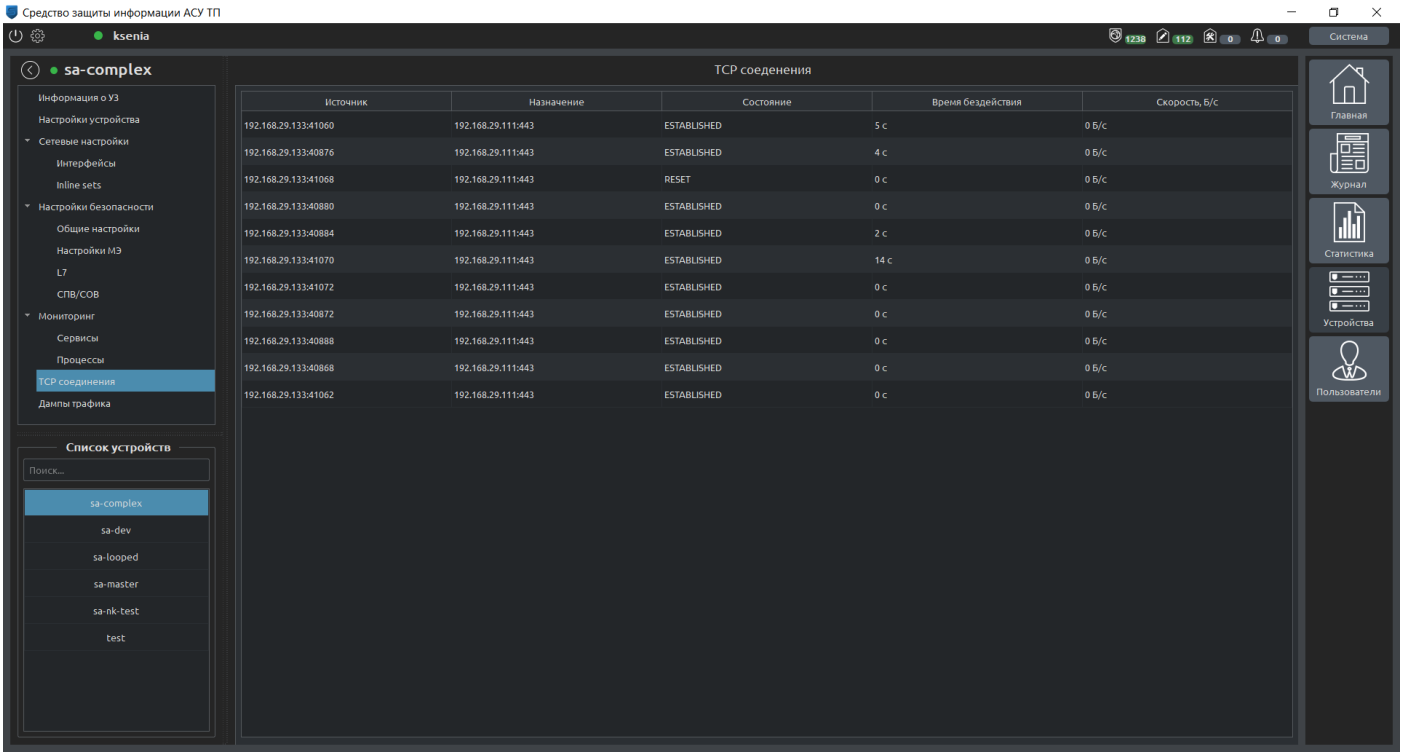


Рисунок 46. TCP соединения

6.4.7. «ДАМПЫ ТРАФИКА»

Во вкладке «Дампы трафика» пользователю предоставляется возможность сохранять записи трафика в файлы в формате «.pcap» (Дампы трафика). Дампы трафика доступны только для одного управляемого устройства ПАК «Аркан-М». (то есть когда сервер ПК «Аркан» установлен на том же устройстве).

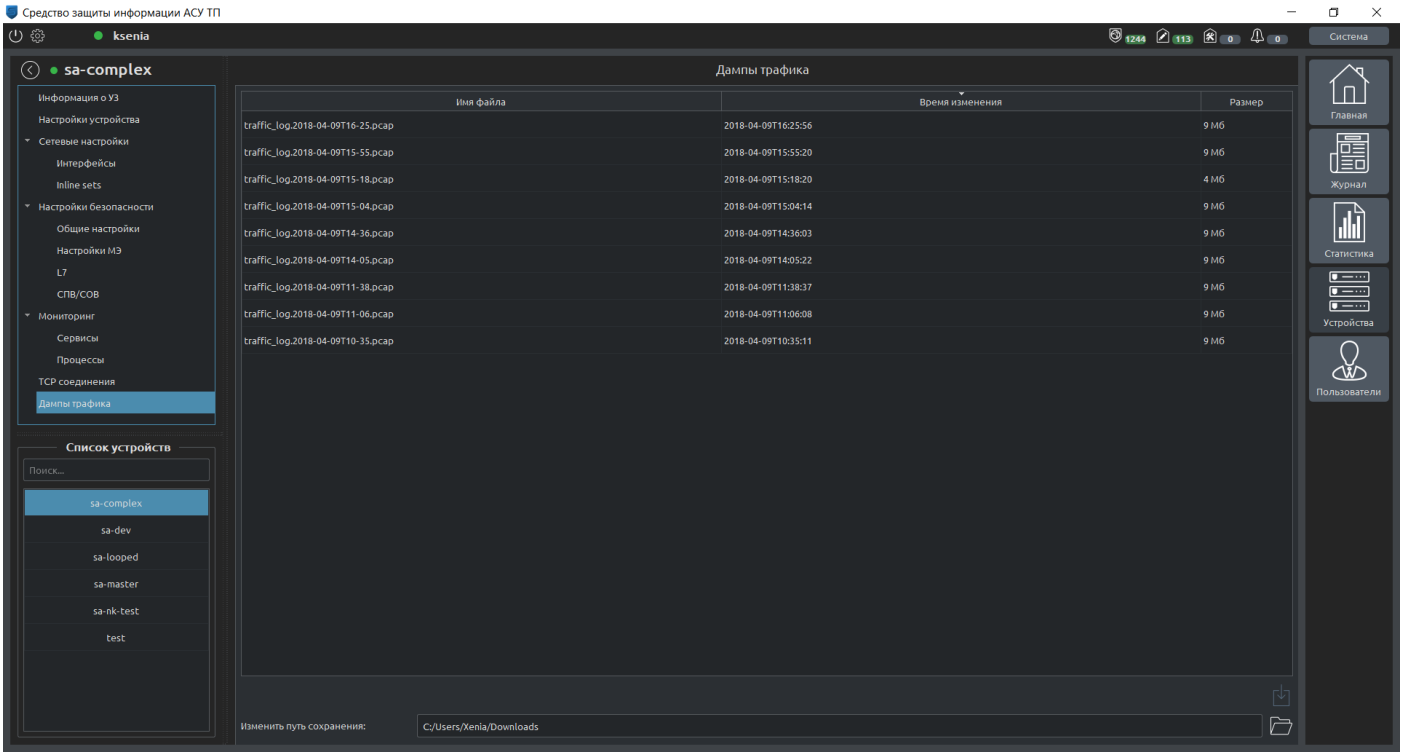


Рисунок 47. Дампы трафика

Чтобы сохранить запись трафика в файл необходимо:

1. При необходимости изменить путь сохранения файлов. Сделать это возможно двумя способами:
   a. Нажав кнопку «открыть»  и выбрать путь сохранения файла;
   b. Ввести путь для сохранения файлов вручную.
2. Выбрать необходимые файлы в таблице. Файлы, недоступные для загрузки (выделенные цветом) выбрать невозможно. После выделения как минимум одного файла необходимо нажать кнопку «загрузить»  .
3. Нажать кнопку «загрузить»  . После нажатия кнопки начнется процесс загрузки. Состояние процесса загрузки будет отражено на шкале прогресса в нижнем крае экрана (Дампы трафика). После завершения загрузки будет отображено сообщение, информирующее об успешно загруженных файлах (Дампы трафика).

После нажатия кнопки начнется процесс загрузки. Состояние процесса загрузки будет отражено на шкале прогресса в нижнем крае экрана (Дампы трафика). После завершения загрузки будет отображено сообщение, информирующее об успешно загруженных файлах (Дампы трафика).

6.5. ПОЛЬЗОВАТЕЛИ

Пункт меню (справа) «Пользователи» состоит из вкладок «Пользователи» и «Сессии».

6.5.1. «ПОЛЬЗОВАТЕЛИ»

Доступ к вкладке «Пользователи» (Пользователи) имеет только администратор. Вкладка позволяет управлять списком пользователей: создавать пользователей, редактировать и удалять.

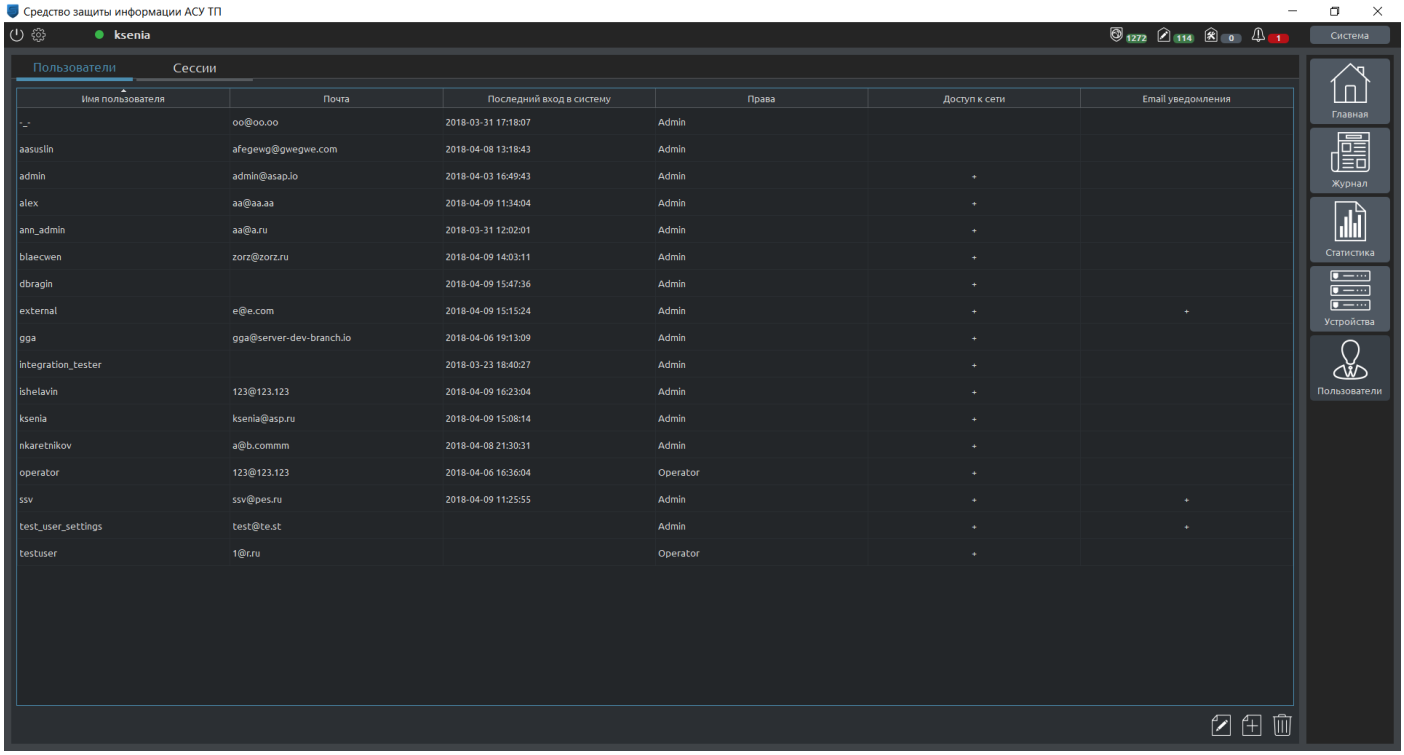


Рисунок 48. Пользователи

Записи о пользователях представлены в виде таблицы с полями:

- «Имя пользователя»;
- «Почта»;
- «Последний вход в систему»
- «Права» (администратор/оператор/рабочий);
- «Доступ к сети»;
- «E-mail уведомления».

Таблица не редактируемая, для изменения информации и добавления нового пользователя используется специальное окно (Пользователи). Для его вызова необходимо либо нажать на

значок редактирования для конкретного пользователя, либо на значок «Добавить» под таблицей.Настройка «Доступ к сети» предназначена для ограничения доступа пользователей через «Аркан-М», установленный в режиме блокирования. Данная функция активируется, если настроена работа в режиме белого списка – «White list» («Настройки безопасности»). В таком случае для каждого пользователя, имеющего права на доступ к сети, определяется текущий IP адрес и добавляется правило для разрешения пропуска сетевого трафика от данной машины. Данные правила помечаются специальной пометкой «(auto)». Подробнее данный режим рассмотрен в пункте 7.8 (Ограничение доступа по имени пользователя) документа.

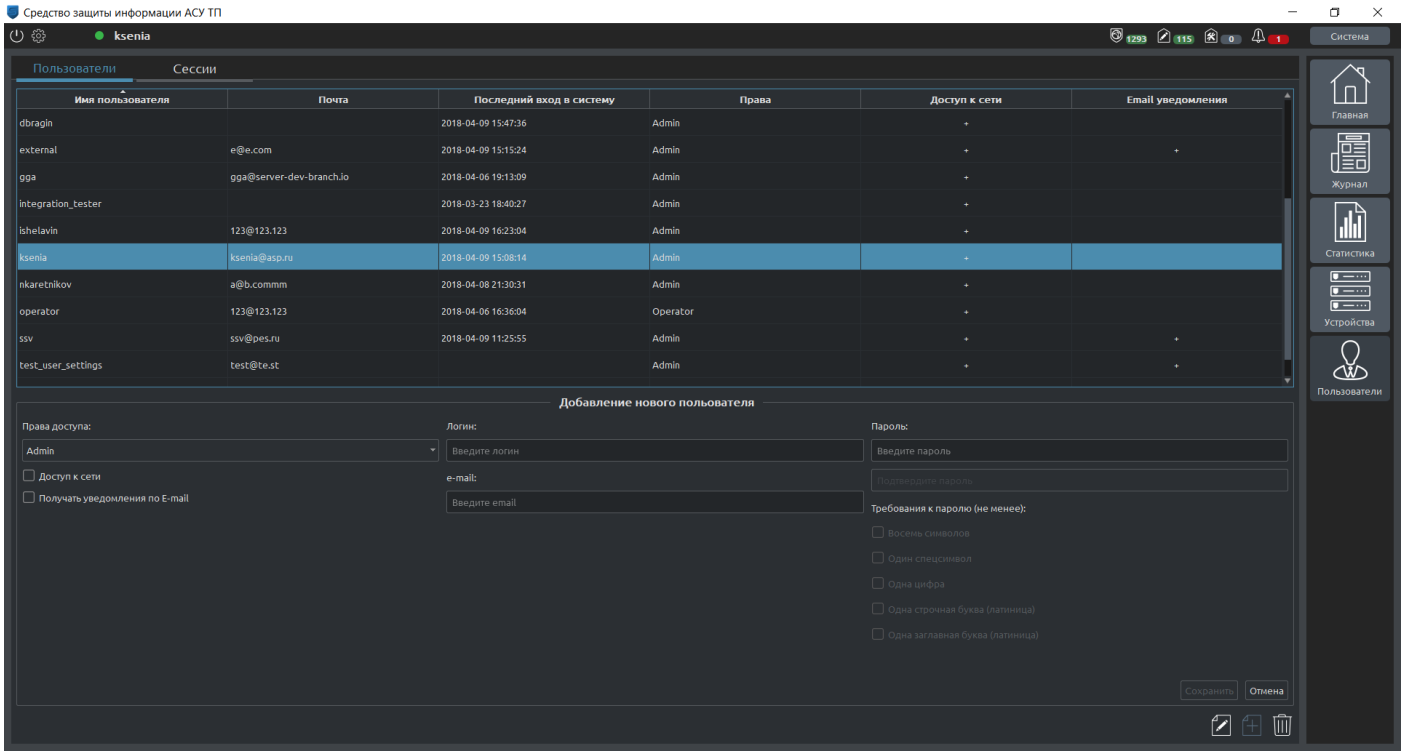


Рисунок 49. Окно редактирования/добавления пользователя

Удаление пользователя производится нажатием на значок удаления в строке пользователя (Удаление пользователя) или на значок удаления под таблицей для удаления группы выделенных пользователей.

Поддерживается три типа пользователей:

- «Администратор»;
- «Оператор»;
- «Рабочий».

Роль «Администратор» предназначена для предоставления административных прав. Пользователь с данными правами имеет доступ ко всему функционалу программного обеспечения.

Роль «Оператор» предназначена для предоставления пользователю прав для мониторинга событий и инцидентов.

Роль «Рабочий» предназначена для ограничения доступа пользователя к сети через ПАК «Аркан-М», работающий в режиме блокирования посредством настройки «Доступ к сети». Данный пользователь не имеет прав на работу с настройкой устройств и просмотра журналов, а интерфейс сворачивается автоматически сразу после входа пользователя.

Подтверждение удаления пользователя не осуществляется, за исключением случая, когда пользователь удаляет сам себя.

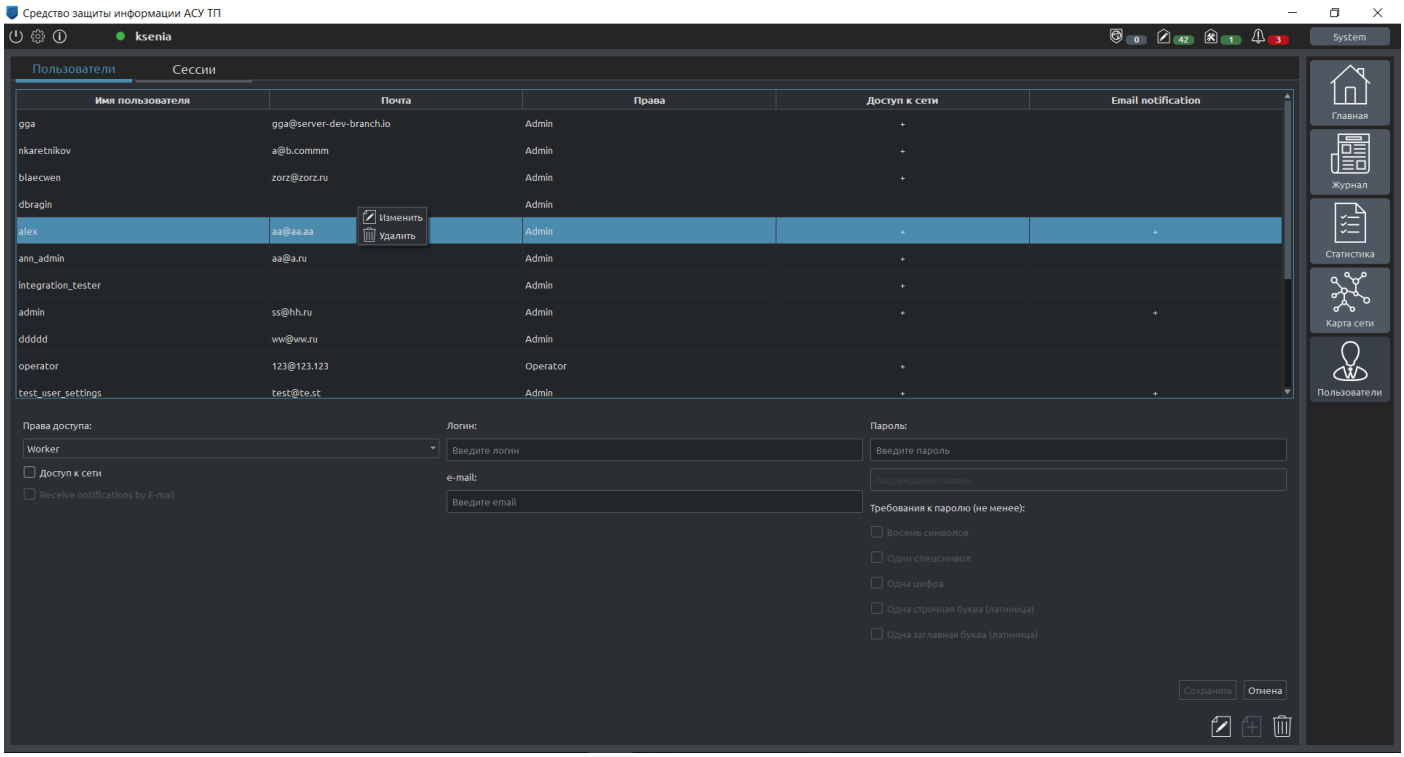


Рисунок 50. Удаление пользователя

6.5.2. «СЕССИИ»

Вкладка «Сессии» (Сессии) позволяет просматривать активные сессии пользователей, разделенных по группам: операторы и администраторы.

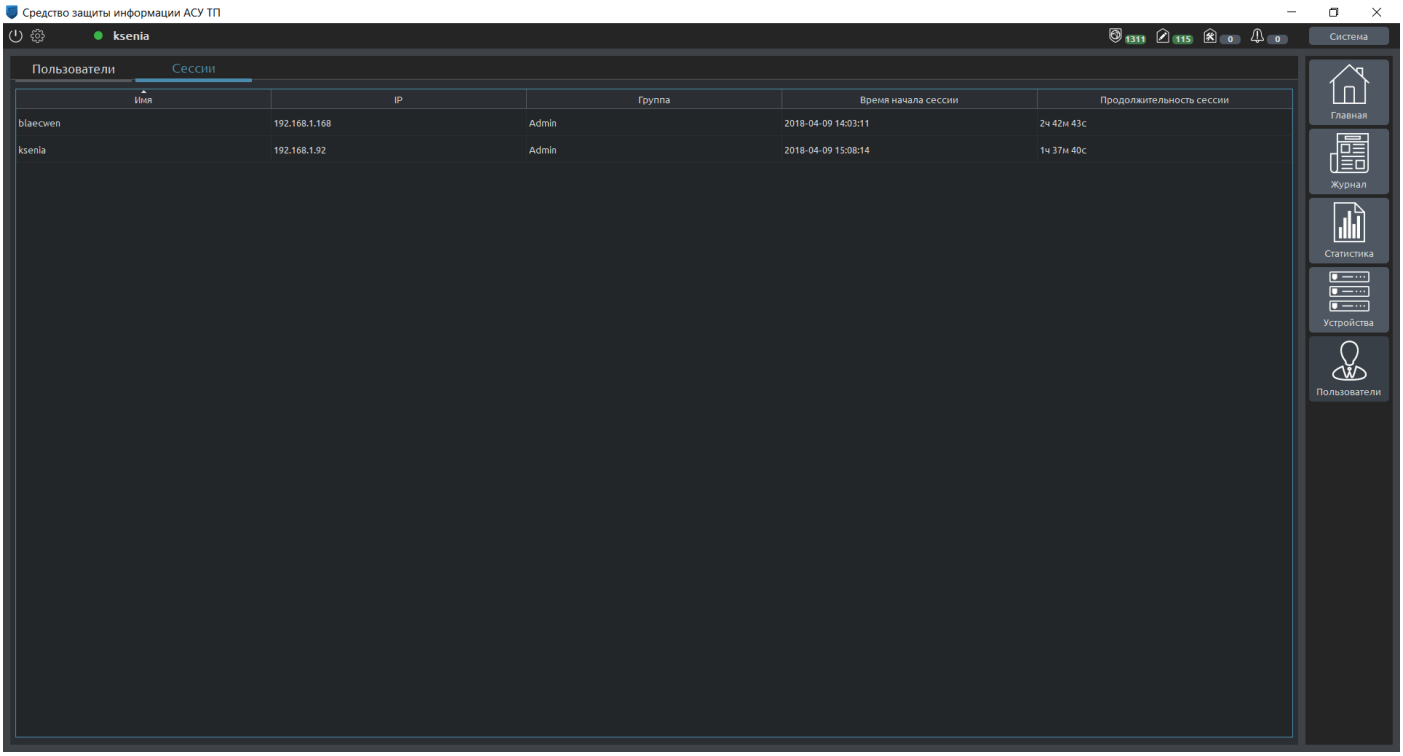


Рисунок 51. Сессии

6.6. СИСТЕМА

Окно настроек вызывается нажатием на кнопку «Система» навигационной панели и делится на 3 вкладки: «Сервер», «Обслуживание» и «Аудит и мониторинг» (Настройки).

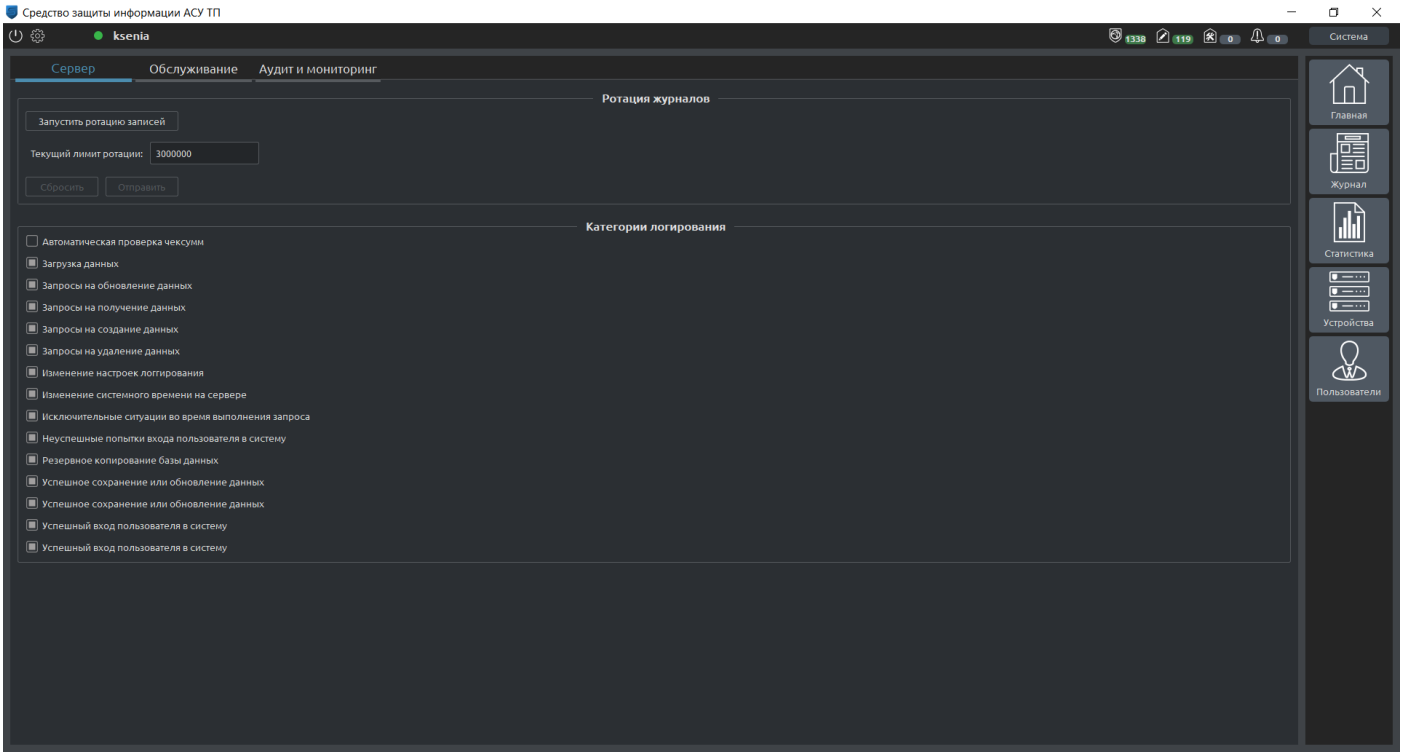


Рисунок 52. Настройки

6.6.1. СЕРВЕР

В данной вкладке (Настройки) производятся настройки сервера: лимит числа записей в журналах и типы данных для логирования в журнале «События системы»:

- автоматическая проверка контрольных сумм;
- загрузка данных;
- запросы на обновление данных;
- запросы на получение данных;
- запросы на создание данных;
- запросы на удаление данных;
- изменение системного времени на сервере;
- исключительные ситуации во время выполнения запроса;
- неуспешные попытки входа пользователя в систему;
- резервное копирование базы данных;
- успешное сохранение или обновление данных;
- успешный вход пользователя в систему.

6.6.2. «ОБСЛУЖИВАНИЕ»

Вкладка «Обслуживание» содержит в себе 3 раздела: «Настройки системного времени», «Настройки NTP», «Команды сервера» (Обслуживание).

Раздел «Настройки системного времени» позволяет настроить дату и время на сервере.

Раздел «Настройки NTP» позволяет настроить получение времени со стороннего NTP сервера и самому выступать в роли NTP сервера.

Раздел «Команды сервера» позволяет перезапустить или выключить сервер.

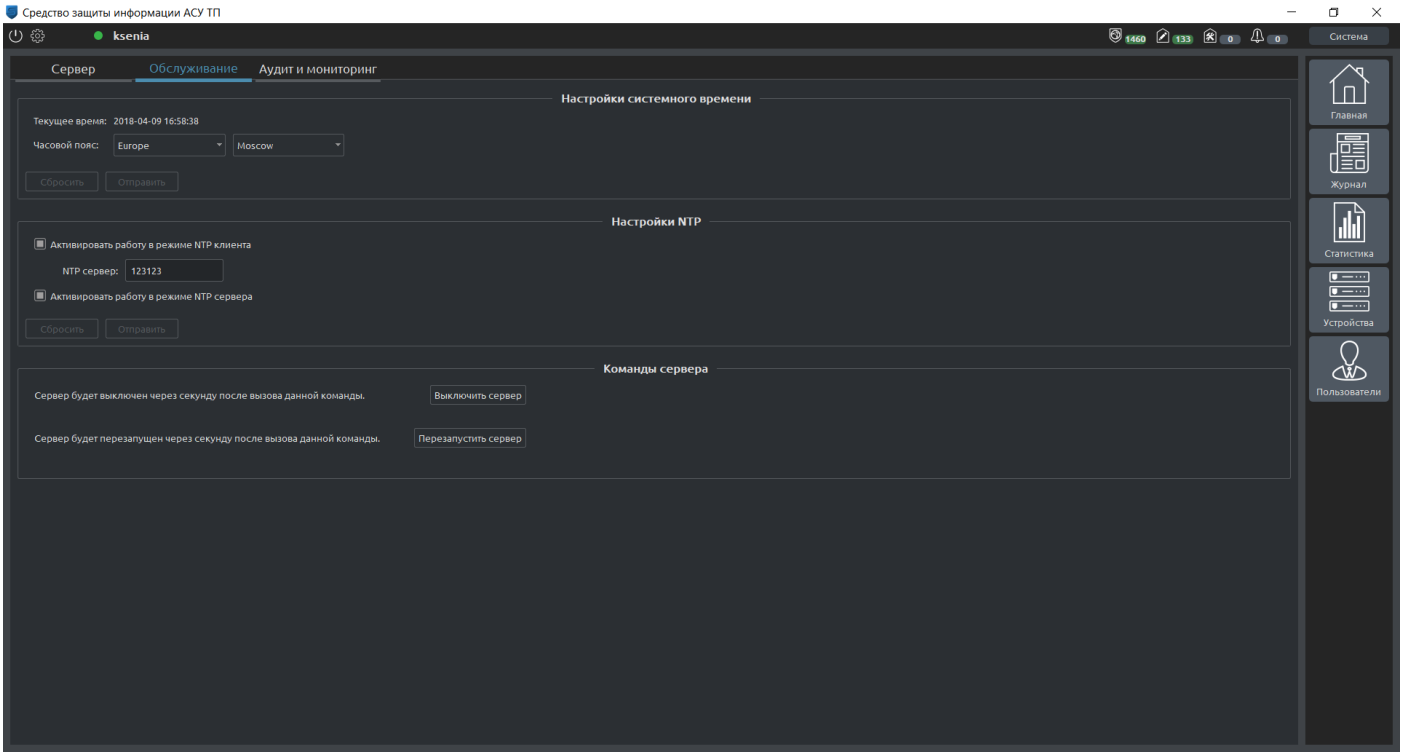


Рисунок 53. Обслуживание

6.6.3. «АУДИТ И МОНИТОРИНГ»

Во вкладке «Аудит и мониторинг» предоставляется возможность настройки подключения к почтовому серверу, настройки отправки по syslog.

Настройка подключения к почтовому серверу

Данный раздел позволяет настроить параметры для подключения к почтовому серверу для последующей отправки на него системных событий, а также включить или выключить отправку этих событий.

Настройка отправки по syslog

Данный раздел позволяет настроить параметры для подключения к серверу syslog для последующей отправки на него событий безопасности, а также включить или выключить отправку этих событий.

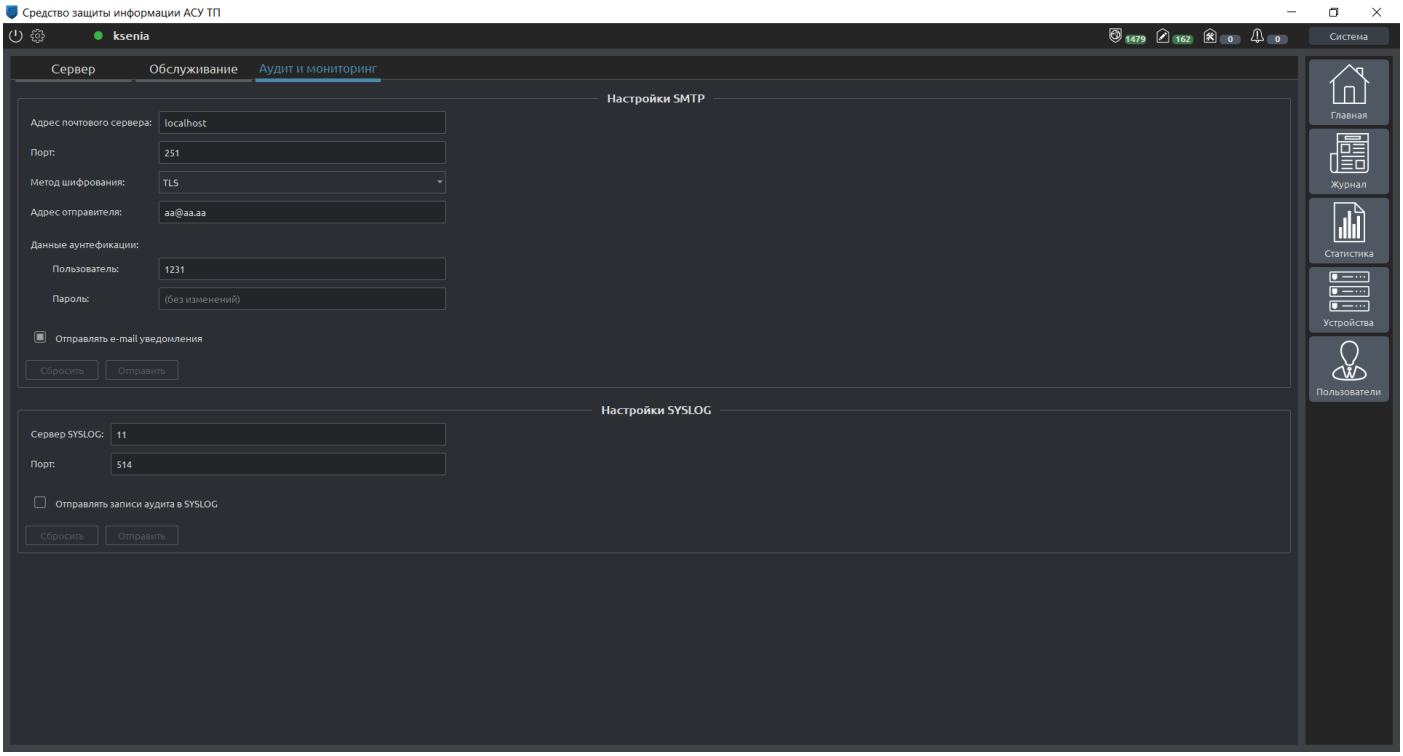


Рисунок 54. Аудит и мониторинг

[2] Компьютерная атака – целенаправленное несанкционированное воздействие на информацию, на ресурс автоматизированной информационной системы или получение несанкционированного доступа к ним с применением программных или программно-аппаратных средств.
[3] При развертывании системы начинается процесс формирование таблицы соответствия MAC-адресов и IP-адресов. При изменении MAC-адреса для какого либо IP-адреса выдается оповещение об атаке ARP-Spoofing.

7. ПОЯСНЕНИЯ ПО ИСПОЛЬЗОВАНИЮ ПОЛЬЗОВАТЕЛЬСКОГО ФУНКЦИОНАЛА

7.1. СОВМЕСТНОЕ ИСПОЛЬЗОВАНИЕ ПАК «АРКАН-М» И ПАК «АРКАН-К»

Описанное в данном руководстве ПО позволяет унифицировано управлять как ПАК «Аркан-М», так и ПАК «Аркан-К». В случае управления одним устройством ПАК «Аркан-М», программное обеспечения подключается к данному устройству для его управления. Если используется ПАК «Аркан-К», то возможно подключение нескольких устройств ПАК «Аркан-М» к одному серверу ПАК «Аркан-К». Кнопка «Система» будет предназначена для настройки к тому ПАК, к которому произведено подключение.

7.2. НАСТРОЙКА ФИЛЬТРАЦИИ НА ПРИКЛАДНОМ УРОВНЕ

Для настройки фильтрации на прикладном уровне используется пункт меню «Настройки L7» в настройках конкретного устройства защиты (ПАК «Аркан-М») (описано в разделе «Настройки безопасности»). Для пользователя доступно добавление правил для фильтрации по каждому промышленному протоколу из перечня. Для каждого протокола доступны следующие поля для редактирования:

- название правила;
- действие, которое необходимо произвести с пакетом данных;
- сообщение, которое должно быть выдано при обнаружении;
- адрес источника (от которого рассматривается дальнейшее действие правила);
- адрес назначения (от которого рассматривается дальнейшее действие правила);
- поля, зависящие от конкретного протокола (пример для протокола Modbus TCP отражен на рисунке Пример задания правил фильтрации для протоколов прикладного уровня)

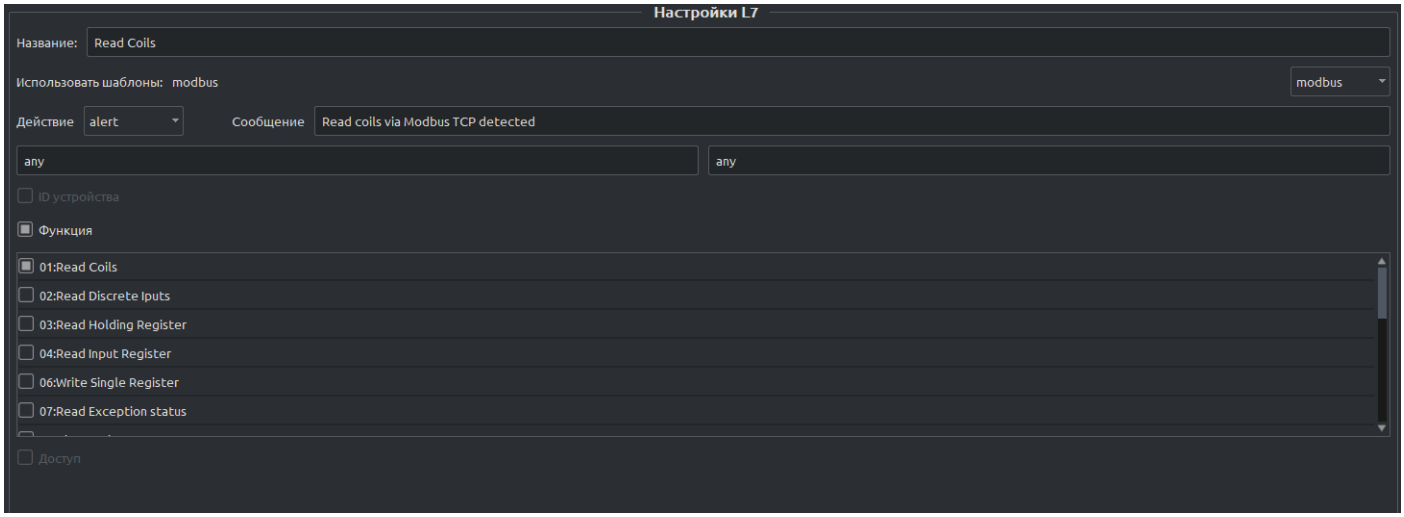


Рисунок 55. Пример задания правил фильтрации для протоколов прикладного уровня

7.3. УПРАВЛЕНИЕ ИНЦИДЕНТАМИ

Управление инцидентами может осуществляться путем управления посредством пункта меню «Настройка инцидентов» (раздел Настройка инциденов). Каждый выявленный инцидент отображается в данном меню. Инциденты автоматически агрегируются по трем полям: устройство, которое зафиксировало инцидент, IP адрес источника, вызвавшего исходное событие и MAC адрес устройства, вызвавшего исходное событие. Для управления инцидента предоставляется возможность регулировки состояния. Для конкретной группы инцидентов можно выбрать одно из трех состояний:

- «Уведомлять» – принадлежащие данной группе инциденты отображаются. В случае нового зафиксированного события будет выведено уведомление (Рисунок 23), если не включена опция, отключающая уведомления.
- «Игнорировать» – принадлежащие данной группе инциденты не отображаются, уведомление не выводится.
- «Решено» – принадлежащие данной группе инциденты не отображаются. В случае нового зафиксированного события данной группы будет выведено уведомление, а группа перейдёт в состояние «Уведомлять». В соответствии с правилами обработки инцидентов ИБ, после обнаружения инцидента (новый инцидент появляется в состоянии «Уведомлять») инцидент должен быть переведен либо в состояние «Решено» (если данный инцидент решен), либо «Игнорировать» (если данный инцидент связан с выявлением нормальной работы сети, а пользователь не желает получать новые уведомления о данном инциденте).

Обнаружение инцидентов связана с работой индикаторов состояния на окне «Главная» (Главная). Если выявлен новый инцидент, то индикатор поменяет свое состояние и будет отображено количество инцидентов на главном экране. В случае перевода всех инцидентов, относящихся к данному индикатору в состояние «Решено» или «Игнорировать», индикатор

вернется в исходное состояние.

7.4. ОБНОВЛЕНИЕ БАЗЫ РЕШАЮЩИХ ПРАВИЛ

Обновление базы решающих правил возможно без подключения к сети Интернет. Обновления сигнатур предоставляется Заказчикам в режиме поддержки или по договорной основе. Процесс обновления описан в разделе 6.4.4 «Настройки безопасности» в подразделе «Общие настройки».

7.5. ДОБАВЛЕНИЕ НОВЫХ УСТРОЙСТВ ПАК «АРКАН-М» В СИСТЕМУ

Если используется ПАК «Аркан-К», то он может управлять несколькими устройствами «Аркан-М». Каждое устройство «Аркан-М» может быть размещено в любом сегменте сети, но подключаемое устройство защиты (ПАК «Аркан-М») не должно быть за NAT (при этом сам сервер (ПАК «Аркан-К» может находиться за NAT). Добавление новых устройств для управления описано в разделе 6.4 Устройства.

7.6. ИНТЕГРАЦИЯ С SIEM

Интеграция с SIEM может быть настроена посредством протокола Syslog. Все события, зафиксированные системой отправляются по протоколу Syslog в соответствии с настройками. Настройка описана в разделе «Аудит и мониторинг».

7.7. ИЗМЕНЕНИЕ РЕЖИМА РАБОТЫ (МОНИТОРИНГА И БЛОКИРОВАНИЯ)

ПАК «Аркан-М» может работать в двух режимах:

- режиме мониторинга (обнаружения вторжений), при котором устройство работает как система обнаружения вторжений (СОВ);
- режиме межсетевого экрана (блокирования), при котором устройство работает как система межсетевого экранирования (МЭ).

Для настройки в режиме мониторинга должен быть настроен по крайней мере один сетевой интерфейс в режиме «Span». Для работы в режиме блокирования по крайней мере два интерфейса в режиме «Inline». Процедура настройки интерфейсов описана в разделе «Настройки устройства».

При необходимости могут быть настроены и смешанные режимы работы – некоторые интерфейсы могут работать в режиме «Span», некоторые в режиме «Inline».

7.8. ОГРАНИЧЕНИЕ ДОСТУПА ПО ИМЕНИ ПОЛЬЗОВАТЕЛЯ

Комплекс имеет возможность блокирования доступа пользователя к сети на основе имени пользователя. Для использования данной функции, ПАК «Аркан-М» должен работать в режиме блокирования, а на каждый ПК, доступ которого к сети должен быть ограничен, устанавливается ПО АРМ ИБ ПК «Аркан». При регистрации пользователя, у которого в настройках отмечено право на «Доступ к сети» будет активировано правило, которое разрешит сетевой обмен. Более подробно см. в разделе «Пользователи».

7.9. ВЫЯВЛЕНИЕ ИНФОРМАЦИОННЫХ АТАК

Выявление информационных атак производится автоматически на основе:

- встроенных алгоритмов;
- базы решающих правил;
- правил межсетевого экранирования.

Все алгоритмы функционируют независимо от режима работы (мониторинг или блокирование). Правила межсетевого экранирования в режиме мониторинга работают как правила информационных потоков в организации.

7.10. СЕГМЕНТАЦИЯ СЕТИ

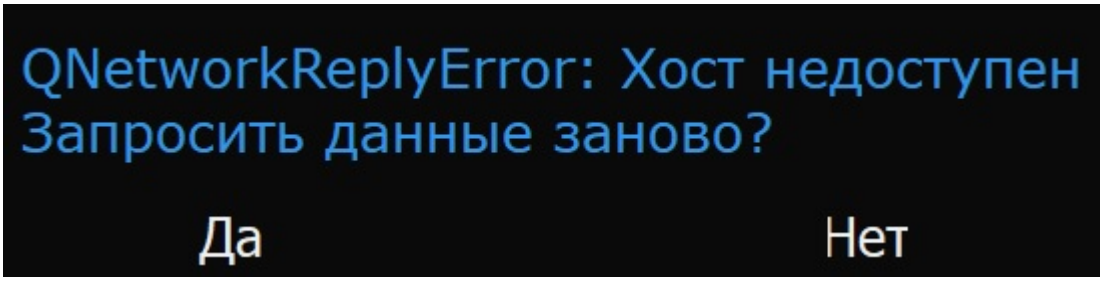
С помощью функции настройки мостов (раздел «Настройки устройства») может быть настроена сегментация сети. Каждая группа интерфейсов, объединенная в один мост, функционирует как обособленный коммутатор.

8. СООБЩЕНИЯ ОПЕРАТОРУ

8.1. ИНФОРМАЦИОННЫЕ СООБЩЕНИЯ

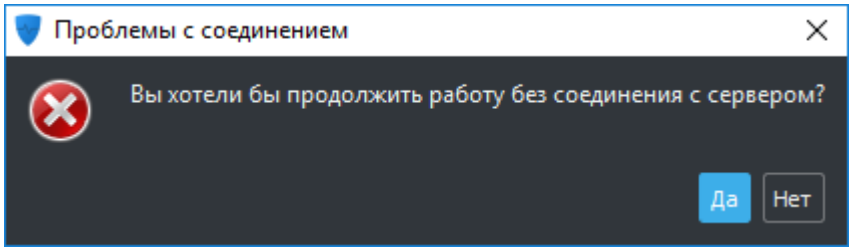
В ходе работы «ПО АРМ ИБ ПК «Аркан»» оператора все системные сообщения и сообщения об ошибках выдаются во всплывающих окнах.

8.1.1. ОШИБКА «ХОСТ НЕДОСТУПЕН»



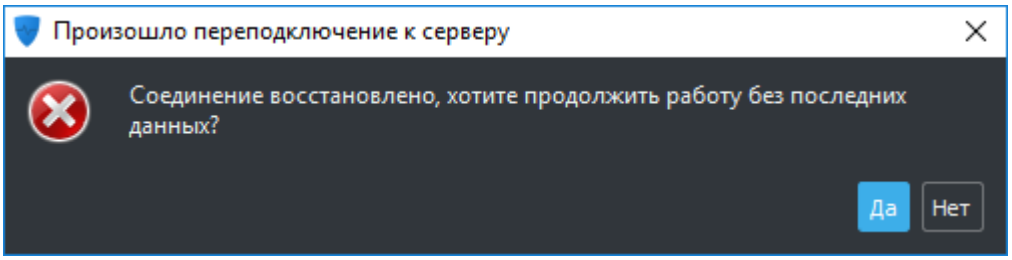
возникает в том случае если был отправлен запрос на сервер, но ответ не был получен.

8.1.2. ПРОБЛЕМЫ С СОЕДИНЕНИЕМ



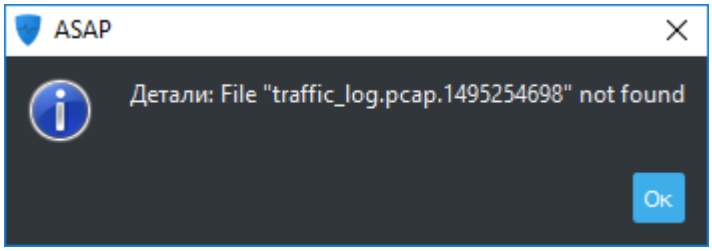
возникает в случае отсутствия соединения с сервером. Для продолжения работы с приложение в режиме «офлайн» необходимо нажать кнопку «Да», в случае нажатия кнопки «Нет», приложение закончит работу.

8.1.3. ПРОИЗОШЛО ПЕРЕПОДКЛЮЧЕНИЕ К СЕРВЕРУ



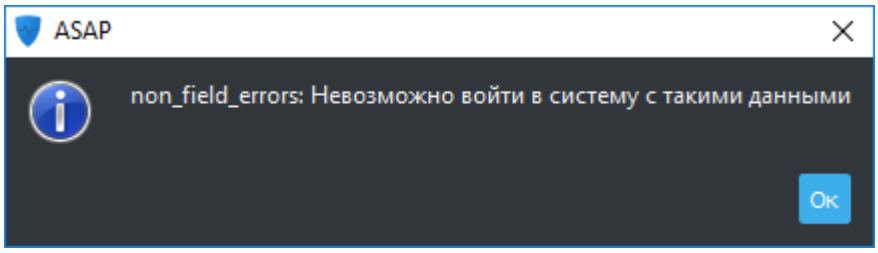
появляется в случае, если подключение к серверу было восстановлено до ответа на диалоговое окно из п. [cap_612]

8.1.4. ОТСУТСТВИЕ ФАЙЛА ЗАПИСИ ТРАФИКА



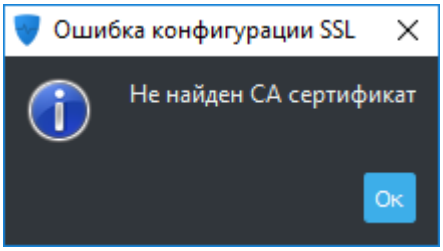
возникает, когда система не нашла путь сохранения записи трафика.

8.1.5. ОШИБКА «НЕВОЗМОЖНО ВОЙТИ В СИСТЕМУ С ТАКИМИ ДАННЫМИ»



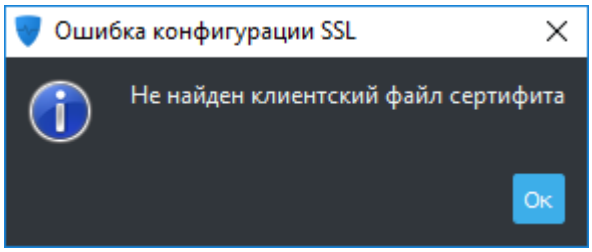
возникает, когда неправильно введен логин пользователя.

8.1.6. ОШИБКА КОНФИГУРАЦИИ SSL 1



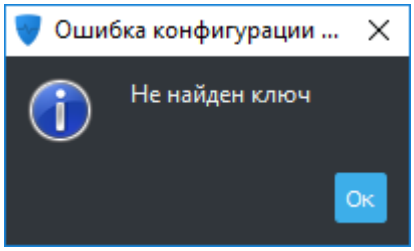
возникает, если не найден сертификат CA в настройках подключения при входе в систему.

8.1.7. ОШИБКА КОНФИГУРАЦИИ SSL 2



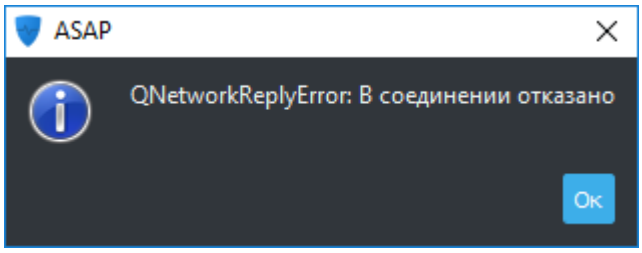
возникает, когда не найден клиентский файл сертификата в настройках подключения при входе в систему.

8.1.8. ОШИБКА КОНФИГУРАЦИИ SSL 3



возникает, если не найден ключ в настройках подключения при входе в систему.

8.1.9. ОШИБКА «В СОЕДИНЕНИИ ОТКАЗАНО»



возникает, если неверно указан адрес или порт сервера.

9. ВЕРСИЯ ДОКУМЕНТА

Версия	Дата	Автор	Правки
0.0.1	10.05.2019	Пантелеев Александр	10.05.2019