УТВЕРЖДЕН

МКЕЮ.00539-01 32 01-ЛУ

Программное средство обнаружения компьютерных атак

«ЗАСТАВА-IDS»

версия 1

Руководство системного программиста

МКЕЮ.00539-01 32 01

Листов 43

Подп. и дата	
Инв. № дубл.	
Взам. инв.№	
Подп. и дата	
Инв.№ подл.	

2016

Содержание

1. Введение

1.1. О средстве обнаружения компьютерных атак «ЗАСТАВА-IDS»

1.1.1. Общие сведения

Средство обнаружения компьютерных атак (СОА) «ЗАСТАВА-IDS» – это программное средство, предназначенное для обнаружения компьютерных атак на основе анализа сетевого трафика стека протоколов TCP/IP со скоростью передачи данных не менее 1 Гбит/сек сигнатурным методом. СОА «ЗАСТАВА-IDS» состоит из двух основных компонентов – сетевого сенсора (сенсор) и Центрального сервера (ЦС).

Сенсор предназначен для поиска компьютерных атак в сетевом трафике. Сенсор подключается к контролируемым каналам связи по схеме «Т-образие» (SPAN, Port mirroring и т.д.). К ЦС может быть подключено несколько сенсоров.

Основные задачи ЦС – управление подключенными сенсорами, а также сбор с них информации об обнаруженных компьютерных атаках и отображение ее администратору.

1.1.2. Архитектура и принципы функционирования

СОА «ЗАСТАВА-IDS» является распределённой системой обнаружения компьютерных атак. Она состоит из датчиков (сетевых сенсоров) и ЦС. На рисунке (см. Рисунок 1) представлена общая архитектура СОА «ЗАСТАВА-IDS».

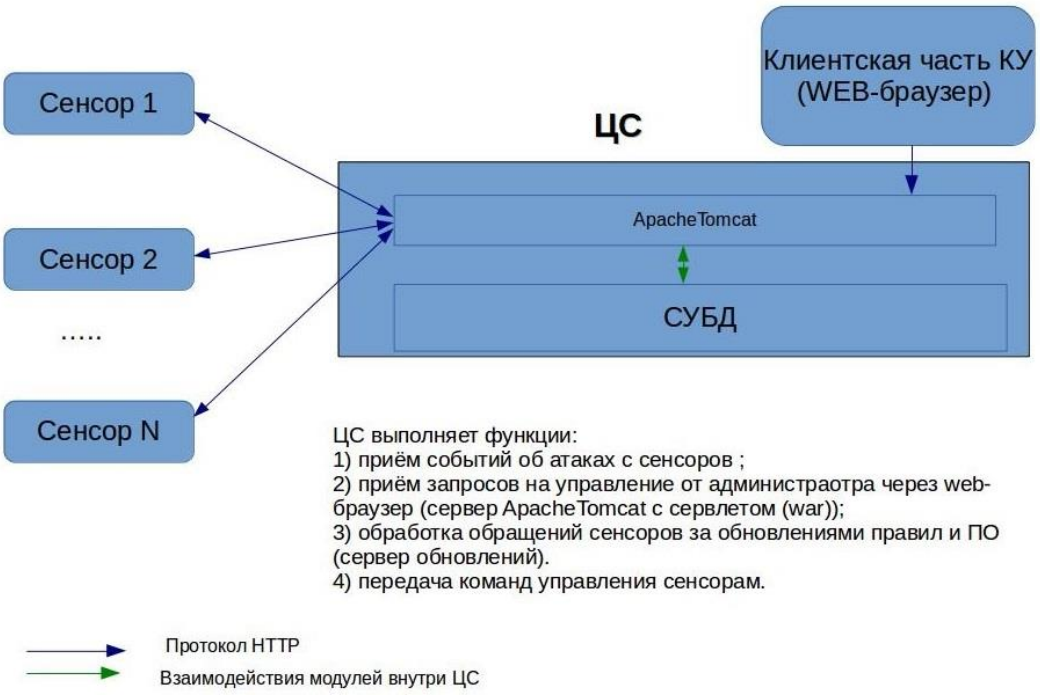

Рисунок 1 - Общая архитектура СОА «ЗАСТАВА-IDS»

В основе работы сенсора лежит сигнатурный анализ (поиск подстрок по заданным шаблонам) сетевого трафика. Для выполнения основной функции сенсора используется программное обеспечение (ПО) Snort.

ЦС построен на базе сервера приложений Apache Tomcat и системы управления базами данных (СУБД) Postgresql.

Каждый сенсор предназначен для обнаружения компьютерных атак на основе анализа сетевого трафика. Сенсор состоит из следующих компонентов:

- модуль захвата трафика (DAQ-модуль с поддержкой библиотеки PF_RING);
- сигнатурный анализатор (ПО Snort);
- модуль взаимодействия с центральным сервером.

ЦС предназначен для:

- сбора и хранения информации об обнаруженных компьютерных атаках;
- хранения настроек всех подключённых сенсоров;
- управления всеми подключёнными сенсорами.

ЦС состоит из следующих компонентов:

- СУБД Postgresql;
- сервер приложений Apache Tomcat;
- модуль приёма информации об обнаруженных компьютерных атаках;
- модуль управления;
- модуль консоли управления.

1.2. О данном документе

1.2.1. Типографские соглашения

Полужирный	**Полужирный** шрифт используется для обозначения разделов меню и кнопок графического интерфейса. Иногда полужирный шрифт используется для акцента.
Курсив	*Курсив* используется, чтобы указать строку данных, которая будет введена в поле. Курсив также может использоваться для акцента.
«Кавычки»	Текст, заключенный в кавычки, используется, чтобы указать выбор из списка в данном поле (то есть выбор из предопределенного списка в окне), окон программы, выбора из меню, а также параметров и атрибутов объектов, для обозначения разделов меню, позиций табуляции, кнопок, полей, объектов.
МАЛЫЕ ПРОПИСНЫЕ	Малые прописные используются для названий документов (стандарты, монографии, бумаги, технические и пользовательские документы по программным продуктам, интерактивные справочные системы и т.д.), а также для ссылок на разделы документов.
`Непропорциональный`	Непропорциональный шрифт используется для ссылок на системные папки и каталоги, последовательности пунктов меню, файлы и пути, и команды в интерфейсе командной строки.
<Угловые скобки>	Угловые скобки используются в описаниях параметров.

1.2.2. Как использовать данный документ

Для того чтобы узнать, как установить и подготовить к работе СОА «ЗАСТАВА-IDS», обратитесь к разделу 2 ПОДГОТОВКА К ИСПОЛЬЗОВАНИЮ.

Чтобы узнать, как конфигурировать СОА «ЗАСТАВА-IDS», обратитесь к разделу 4 ФАЙЛ КОНФИГУРАЦИИ. СОСТАВЛЕНИЕ И ПРАВКА.

Чтобы узнать, как просмотреть журналы СОА «ЗАСТАВА-IDS», настроить базу сигнатур, отдать команды сенсорам, обратитесь к разделу 3 АДМИНИСТРАТИВНАЯ КОНСОЛЬ И РАБОТА С НЕЙ.

2. Подготовка к использованию

2.1. Системные требования

2.1.1. Системные требования к сенсору

Сенсор предназначен для работы на серверных многоядерных платформах. Для выбора аппаратной платформы для сенсора необходимо руководствоваться следующими соображениями:

– один экземпляр ПО Snort обрабатывает поток данных со скоростью около 100 Мбит/с;

– один экземпляр ПО Snort полностью занимает одно ядро центрального процессора;

– при наличии большой базы сигнатур (свыше 20 000) количество потребляемой оперативной памяти одним экземпляром СОА может превышать 1,5 Гбайт;

– необходимы минимум два сетевых интерфейса достаточной пропускной способности – один рабочий, другой управляющий.

Например, для работы сенсора на каналах связи с пропускной способностью 1 Гбит/с достаточно сервера с 4 физическими ядрами (8 с гипертредингом) и ОЗУ 16 Гбит/с.

Рекомендуемые конфигурации представлены в таблицах (см. Таблица 1,

Таблица 2).

Таблица 1 – Требования для каналов с пропускной способностью не более 1 Гбит/с

Элемент	Параметры
Операционная система (ОС)	CentOS Linux 7.* x64 ALT Linux 6.* x64 ALT Linux 7.* x64
Процессор	xeon e3-1281v3 3.7GHz 4-core
Оперативная память	32 Гбайт
Привод	Привод для компакт-дисков
Сетевой адаптер	2x Gigabit adapter
Жёсткий диск	2x HDD 1 Тбайт

Таблица 2 – Требования для каналов с пропускной способностью более 1 Гбит/с

Элемент	Параметры
ОС	CentOS Linux 7.* x64 ALT Linux 6.* x64 ALT Linux 7.* x64
Процессор	xeon e5-2660v3 3.7GHz 10-core
Оперативная память	64 Гбайт
Привод	Привод для компакт-дисков
Сетевой адаптер	1x Gigabit adapter 1x 10 Gigabit adapter
Жёсткий диск	2x HDD 1Тбайт

2.1.2. Системные требования к ЦС

Аппаратная база для ЦС должна иметь достаточный объём дискового пространства для хранения журналов компьютерных атак и резервных копий СУБД (не менее 1 Тбайт). Объём ОЗУ должен быть не менее 4 Гбайт, количество ядер центрального процессора, не менее двух. Должен быть минимум один сетевой адаптер с пропускной способностью 1 Гбит/сек.

Рекомендуемая конфигурация компьютера, на котором функционирует ЦС, приведена в таблице (см. Таблица 3).

Таблица 3 – Требования к ЦС

Элемент	Параметры
ОС	CentOS Linux 7.* x64 ALT Linux 6.* x64 ALT Linux 7.* x64
Процессор	xeon e3-1281v3 3.7GHz 4-core
Оперативная память	≥ 4 Гбайт
Привод	Привод для компакт-дисков
Жесткий диск	≥ 1 Тбайт
Сетевой адаптер	1x Gigabit adapter

2.2. Установка СОА

2.2.1. Установка программного обеспечения сенсора

Ядро linux на системе, в которой производится установка, должно совпадать с ядром системы, на которой производилась сборка.

Для установки ПО сенсора надо скопировать rpm пакет sensor-1-alt1.x86_64.rpm на целевую машину и выполнить на ней от имени пользователя **root**:

```
apt-get install ./sensor-1-alt1.x86_64.rpm
```

2.2.2. Установка программного обеспечения ЦС

Для установки ПО ЦС выполнить последовательность действий:

1) Подключить сервер к сети Интернет. Установить пакеты:

```
apt-get update
apt-get install java-1.7.0-openjdk postgresql9.4-server tomcat ant tomcat-systemv
```

2) Инициализировать СУБД (в случае, если в качестве системы инициализации установлен system V)

```
/etc/init.d/postgresql initdb
/etc/init.d/postgresql start
```

Скопировать папку `DataBase` в произвольную директорию (например, `/opt`). Выполнить:

```
cd /opt/DataBase
```

```
chmod +x ./create.sh
./create.sh
```

База данных создана.

База **ids**, пользователь **idsuser** с паролем **idsuser**.

3) Скопировать war-файлы: `controlpanel.war`, `manager.war`, `receiver.war` в директорию `$CATALINA_HOME/webapps`

$CATALINA_HOME – внутренняя переменная сервера TOMCAT, по умолчанию в среде AltLinux $CATALINA_HOME=/usr/share/tomcat

4) Скопировать файлы `console_tools` и `console_tools.jar` в папку `/opt`.

5) Создать директорию `$CATALINA_HOME/conf/centralserver/`

6) Скопировать файл `centralserver.conf` в данную директорию.

7) В файле `$CATALINA_HOME/conf/catalina.properties` внести изменение:

строку:

```
shared.loader=
```

заменить на:

```
shared.loader=$CATALINA_HOME/conf/centralserver
```

8) Перезапустить сервера postgresql и tomcat:

```
/etc/init.d/postgresql restart
/etc/init.d/tomcat restart
```

9) Добавить учётную запись пользователя по умолчанию (пользователь **admin**, пароль **admin**). Для этого надо выполнить:

```
cd /opt
./console_tools --users-add-default -c  \
$CATALINA_HOME/conf/centralserver/centralserver.conf
```

где: `$CATALINA_HOME` – домашняя директория сервера Tomcat.

10) Далее подключиться к серверу при помощи web-браузера по следующему url:

http://<адрес сервера ЦС>:8080/controlpanel/faces/login.xhtml

11) В системе не установлено никаких сенсоров, и нет никаких сигнатур.

На первом этапе необходимо создать хотя бы один сенсор. Для этого надо:

- выбрать меню: **Администрирование – Сенсоры – Добавить сенсор;**
- заполнить поле **Имя сенсора**;
- в поле **Идентификатор сенсора** ввести идентификатор, который был присвоен сенсору в процессе установки;
- параметр **IP-адрес сенсора** носит информативный характер, можно оставить значение по умолчанию;

– нажать кнопку **Добавить**.

12) Установить обновления правил:

– На главной странице выбрать пункт меню **Администрирование – Правила обнаружения – Обновить правила**.

– Нажать кнопку **Обзор** и указать путь к файлу с правилами, который должен находиться на компьютере администратора, запустившего web-браузер.

Описание процедуры создания файла обновления см. в подразделе 5.2.

13) Диагностические журналы ЦС располагаются в директории `$CATALINA_HOME/logs`:

`ids_controlpanel.log` – журнал для сервлета controlpanel.war;

`ids_receiver.log` – журнал для сервлета receiver.war;

`ids_manager.log` – журнал для сервлета manager.war.

2.3. Обязательная начальная настройка программы (комплекса)

2.3.1. Начальная настройка сенсора

После установки ПО сенсора необходимо выполнить его первоначальную конфигурацию. Существует два варианта, как это можно сделать.

Вариант 1. Редактирование конфигурационного файла `/etc/sensor.conf`.

– указать слушающий интерфейс – параметр **interface**;

– указать количество экземпляров Snort – параметр **Snorts-num;**

– указать уникальный идентификатор сенсора – параметр **sensor-unique-id;**

– указать адрес ЦС – параметр **server-addr**.

Описание вышеперечисленных и прочих параметров сенсора см. в подразделе 4.1.

Вариант 2. Указанные в варианте 1 параметры можно настроить в интерактивном режиме через управляющий скрипт. Для этого в командной строке сенсора выполнить:

```
/etc/init.d/sensord init
```

Настройка параметров сборки tcp-сессий (в случае необходимости)

Сборка TCP-сессий осуществляется выборочно, по заданным критериям. За сборку отвечает специализированный препроцессор ПО Snort — **stream5_tcp**.

Например, для сборки tcp-сессий по порту сервера 12345, необходимо в конфигурационный файл `Snort.conf` добавить это порт в раздел настроек препроцессора stream5_tcp.

Это будет выглядеть следующим образом:

```
preprocessor stream5_tcp: policy windows, detect_anomalies, require_3whs 180, \
overlap_limit 10, small_segments 3 bytes 150, timeout 180, \
```

```
ports client 21 22 23 25 42 53 79 109 110 111 113 119 135 136 137\
161 445 513 514 587 593 691 1433 1521 1741 2100 3306 6070 \
ports both 80 81 311 383 443 465 563 591 593 636 901 989 992 993\
 7917 7918 7919 12345
```

Более подробное описание параметров настройки ПО Snort см. по адресу:

http://manual-Snort-org.s3-website-us-east-1.amazonaws.com/

2.3.2. Подключение сенсора

Сенсор СОА работает в пассивном режиме. Для подключения сенсора необходима точка съёма сетевого трафика, которая может быть реализована при помощи активного сетевого оборудования (маршрутизаторы и коммутаторы с функцией зеркалирования или мониторинга) либо при помощи специализированных сетевых ответвителей (TAP). Рабочий (слушающий) интерфейс сенсора должен быть подключён к такой точке. Для контроля правильности подключения можно воспользоваться утилитой **tcpdump**. Для этого в терминале сенсора выполнить:

```
tcpreplay -i [рабочий интерфейс] -n -nn -c 100
```

В результате в терминале должно отобразиться 100 пакетов сетевого трафика из контролируемой сети.

После подключения к точке съёма сетевого трафика следует проверить наличие связи с ЦС, для этого в терминале надо выполнить:

```
curl [адрес_сервера]:8080
```

В конфигурационном файле сенсора (`/etc/sensor.conf`) указать уникальный идентификатор сенсора, адрес ЦС, количество запускаемых экземпляров ПО Snort и маску процессоров.

Описание вышеперечисленных и прочих параметров сенсора см. в подразделе 4.1.

После настройки выполнить запуск сенсора:

```
/etc/init.d/sensord start
```

2.3.3. Начальная настройка ЦС

После установки программного обеспечения сенсора необходимо выполнить его первоначальную конфигурацию. Для этого в текстовом редакторе на ЦС надо открыть файл `$(catalina.home)/conf/centralserver/centralserver.conf`

- указать адрес сервера СУБД – параметр **url**;
- указать имя пользователя и пароль к СУБД – параметры **user** и **password**;
- при необходимости настроить параметры отправки сообщений на электронную почту.

Описание вышеперечисленных и прочих параметров ЦС см. в подразделе 4.2.

2.4. Проверка правильности функционирования программы (комплекса)

2.4.1. Проверка работоспособности сенсора

Выполнить проверку работоспособности сенсора можно двумя способами.

Вариант 1: через командную строку сенсора:

```
/etc/init.d/sensod status
/etc/init.d/sensod seftest
```

Вариант 2: через web-интерфейс:

- в web-браузере перейти по ссылке:
  http://<адрес сервера СОА>:8080/controlpanel/faces/login.xhtml
- в разделе **Главная** выбрать проверяемый сенсор. Подождать некоторое время. В случае работоспособности сенсора и наличия с ним связи статус должен измениться на «А»;
- выбрать пункт меню **Главная – Управление – Команда – Самотестирование**;
- результат смотреть в журнале атак (пункт **Главная – Журналы атак – Все атаки)**: должно появиться три записи о тестовых компьютерных атаках.

2.4.2. Проверка работоспособности ЦС

Чтобы проверить работоспособность ЦС следует выполнить следующие действия:

- проверить то, что запущены сервисы:

```
/etc/init.d/tomcat status
/etc/init.d/postgresql status
```

- установить связь с ЦС через web-браузер. Перейти по ссылке:

http://<адрес сервера СОА>:8080/controlpanel/faces/login.xhtml

- выполнить проверку работоспособности любого доступного сенсора (см. п. 2.4.1).

3. Административная консоль и работа с ней

3.1. Консоль управления ЦС

3.1.1. Запуск консоли

Консоль управления (КУ) СОА «ЗАСТАВА-IDS» представляет собой приложение, построенное на основе web-технологий. Для запуска КУ необходимо в web-браузере компьютера, имеющего сетевой доступ к ЦС, перейти по адресу:

http://<IP-адрес ЦС>:8080/controlpanel/faces/login.xhtml

3.1.2. Вход в систему

На рисунке (см. Рисунок 2) показана страница входа в систему. Для входа в систему необходимо ввести имя пользователя и его пароль.

По умолчанию для входа в систему используется единственный пользователь admin с паролем admin.

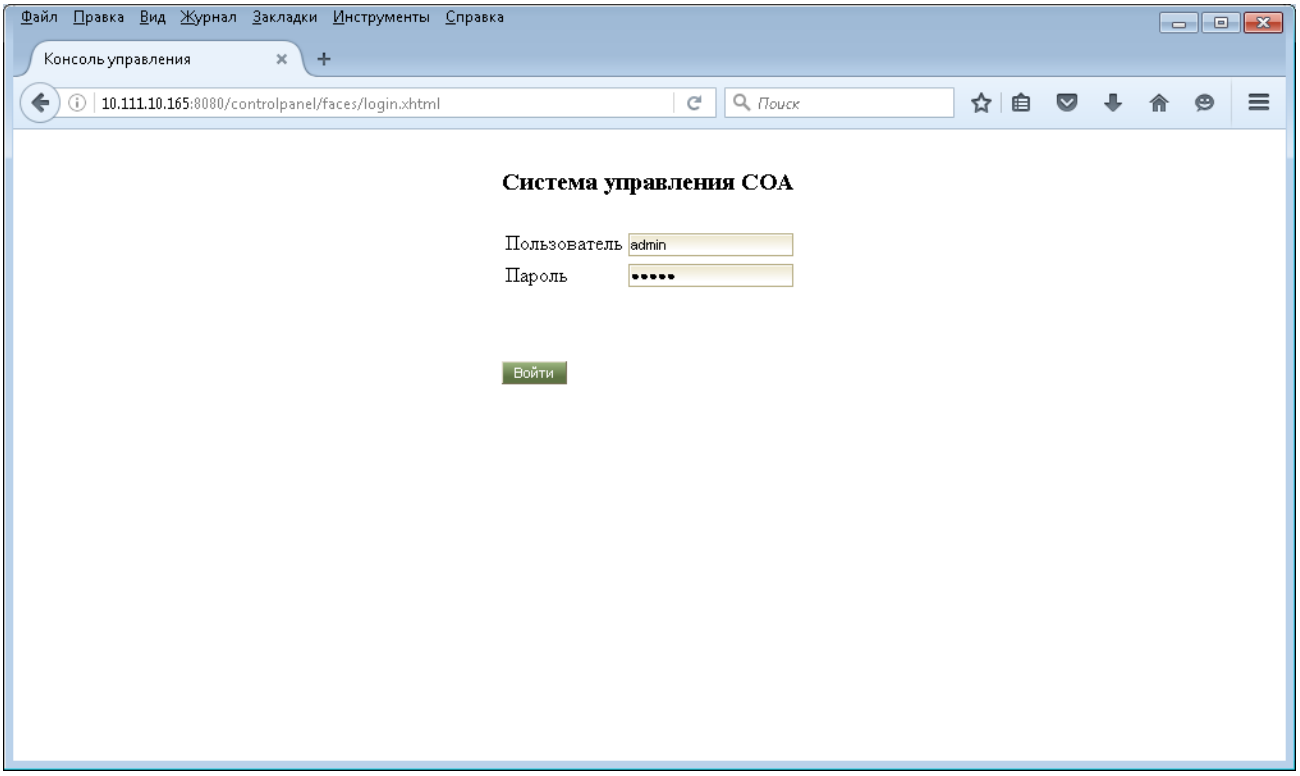

Рисунок 2 – Страница входа в систему управления СОА

3.1.3. Главное окно

Интерфейс КУ состоит из двух частей: «Главная» и «Администрирование». Каждая часть содержит все три группы элементов (см. Рисунок 3): рабочее меню (1), меню выбора (2), и рабочую область (3).

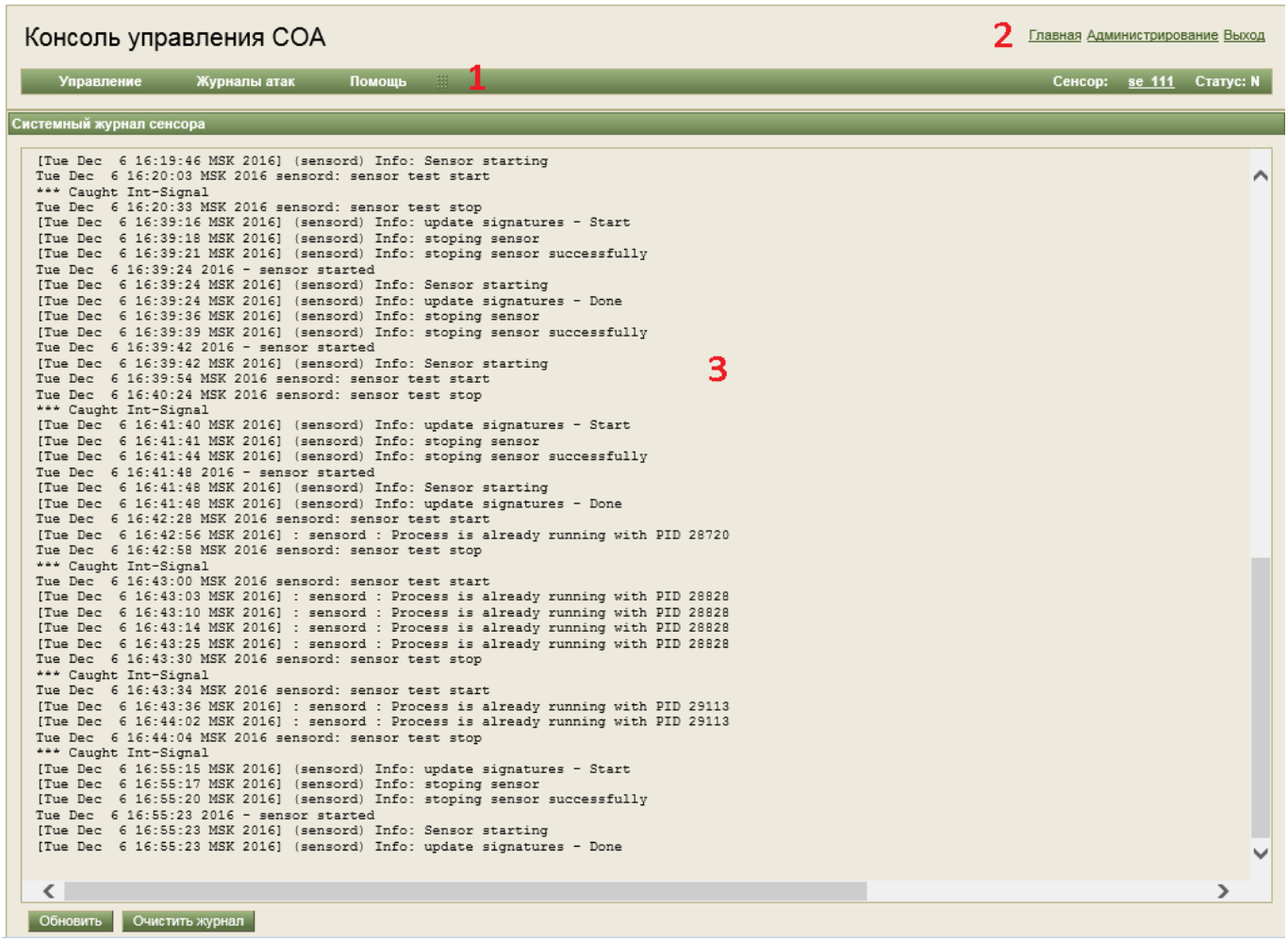

Рисунок 3 – Интерфейс КУ ЦС

3.1.4. Описание интерфейса «Главная» КУ ЦС

На рисунке (см. Рисунок 3) показан интерфейс **Главная** КУ ЦС. Рабочее меню этого интерфейса состоит из трёх меню:

– «Управление»;

– «Журналы атак»;

– «Помощь».

В правой части рабочего меню интерфейса отображается текущий выбранный сенсор.

Для выбора текущего сенсора необходимо нажать по имени сенсора, при этом произойдёт переход в интерфейс **Администрирование** на страницу с выбором сенсоров (см. Рисунок 4), а после нажатия кнопки **Выбрать** – возвращение в интерфейс **Главная**.

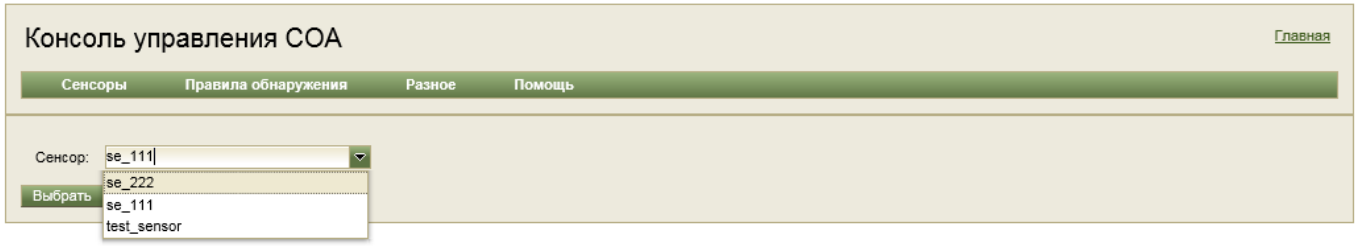

Рисунок 4 – Выбор текущего сенсора

3.1.4.1. Меню «Управление»

Меню **Управление** состоит из подменю и пунктов (см. Рисунок 5):

– «Команда»;

– «Информация»;

– «Очередь команд»;

– «Настройка сигнатур»;

– «Журналы».

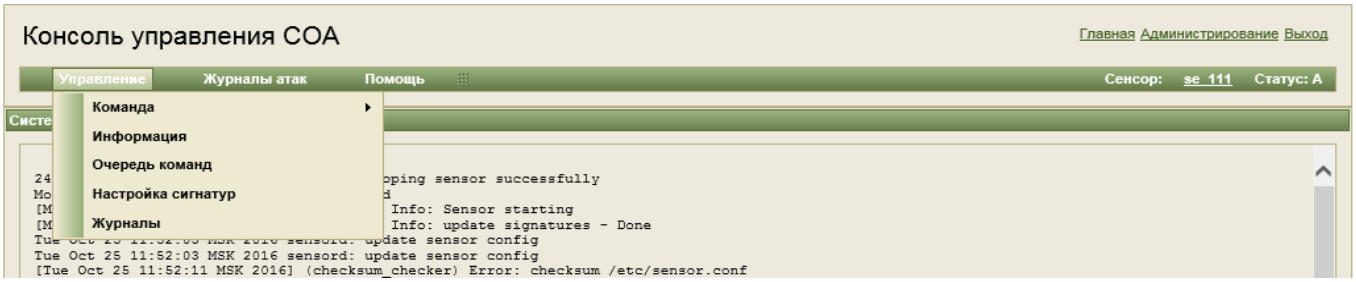

Рисунок 5 – Состав меню «Управление»

Состав подменю **Команда** отображён в таблице (см. Таблица 4).

Таблица 4 – Состав подменю «Команда»

Пункт меню	Действие
«Старт»	передать команду «Старт» текущему сенсору
«Стоп»	передать команду «Стоп» текущему сенсору
«Рестарт»	передать команду «Рестарт» текущему сенсору
«Самотестирование»	передать команду «Самотестирование» текущему сенсору
«Обновить правила»	передать команду «Обновить правила» текущему сенсору
«Обновить программное обеспечение»	передать команду «Обновить программное обеспечение» текущему сенсору
«Копировать файлы с сенсора»	передать команду «Копировать файлы с сенсора» текущему сенсору

После выполнения любой команды пользователь будет перенаправлен на страницу с отображением текущей очереди команд для сенсора (см. Рисунок 6).

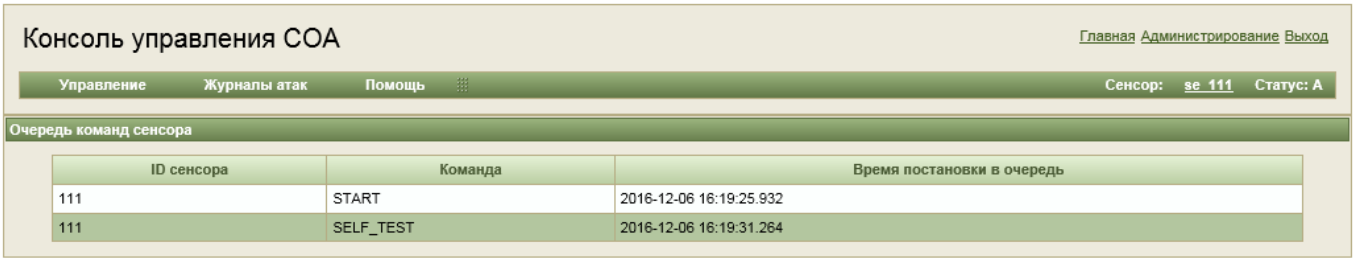

Рисунок 6 – Страница «Очередь команд сенсора»

Очередь команд отображается динамически по мере поступления/выполнения команд и также доступна через меню: **Главная — Управление — Очередь команд**.

Пункт меню «Информация»

Данный пункт меню открывает страницу **Параметры сенсора**, которая отображает системную информацию о текущем сенсоре (см. Рисунок 7).

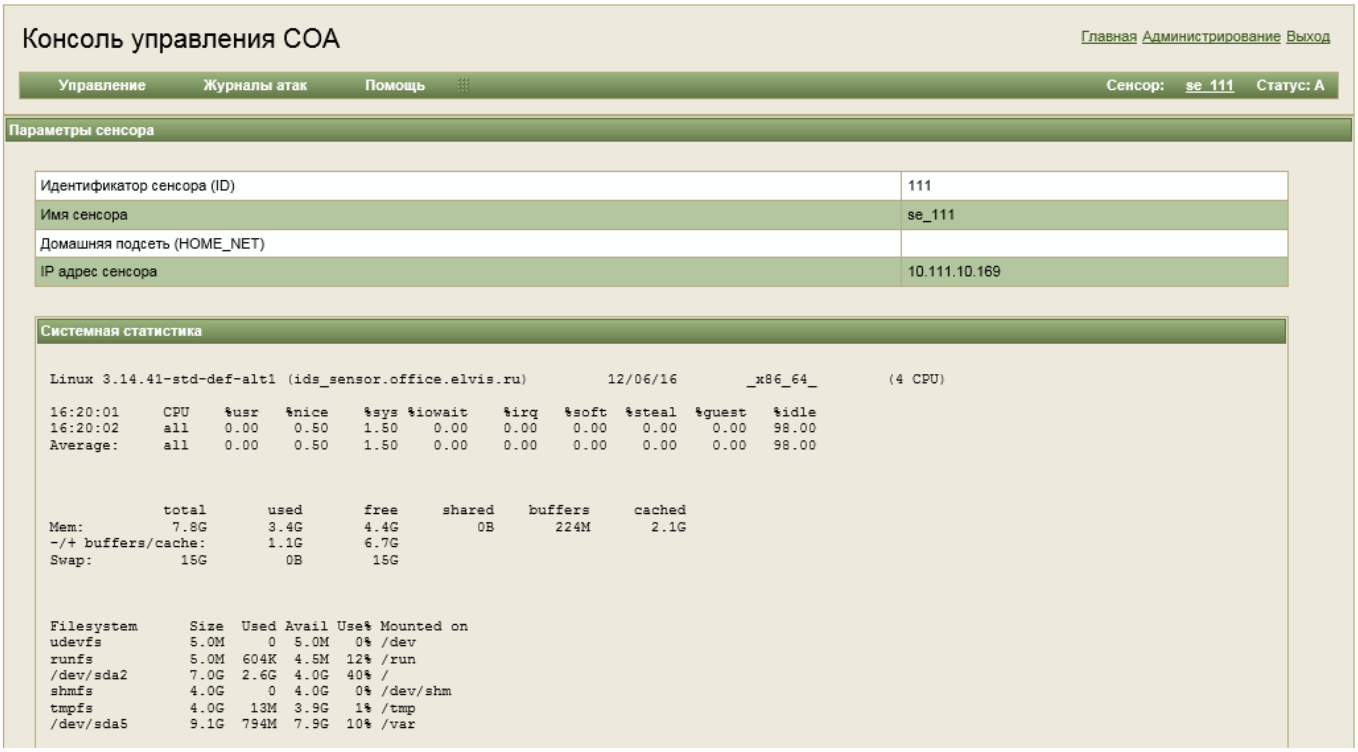

Рисунок 7 – Страница «Параметры сенсора»

Пункт меню «Настройка сигнатур»

Данный пункт меню открывает страницу **Настройка сигнатур**, где отображается информация о сигнатурах для текущего сенсора (см. Рисунок 8).

На данной странице производится настройка сигнатур для текущего выбранного сенсора. Управления сигнатурами заключается в их активировании/деактивировании для выбранного класса (активированная сигнатура — сигнатура, которая загружается в сенсор).

	Каждая сигнатура относится к определённому классу атак. Класс задаётся в параметре сигнатуры «classtype». Если класс сигнатуры не задан, то сигнатура автоматически входит в класс «unknown».
	Описание классов загружается в систему вместе с обновлением сигнатур и содержится в файле обновления `etc/classification.config`.

Для просмотра полного описания сигнатуры следует нажать на интересующей сигнатуре в поле **Сигнатура**. Результат показан на рисунке (см. Рисунок 9).

После внесения изменений в текущем классе сигнатур следует нажать кнопку **Сохранить изменения**, прежде чем выбрать другой класс в выпадающем списке **Класс**.

После внесения всех изменений в сигнатуры следует выполнить их запись на сенсор. Для этого выполнить команду для сенсора через меню: **Управление – Команда – Обновить правила**.

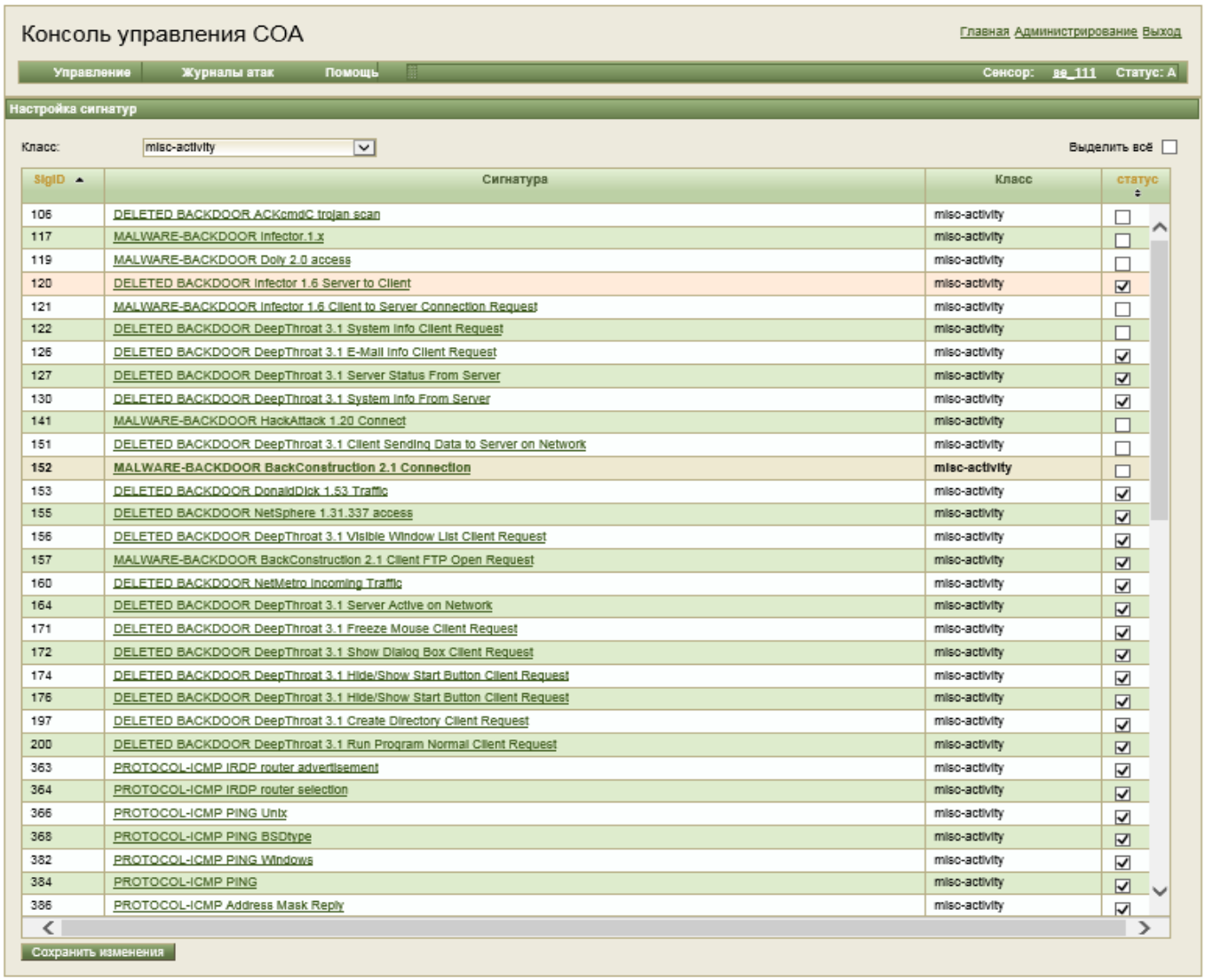

Рисунок 8 – Страница «Настройка сигнатур»

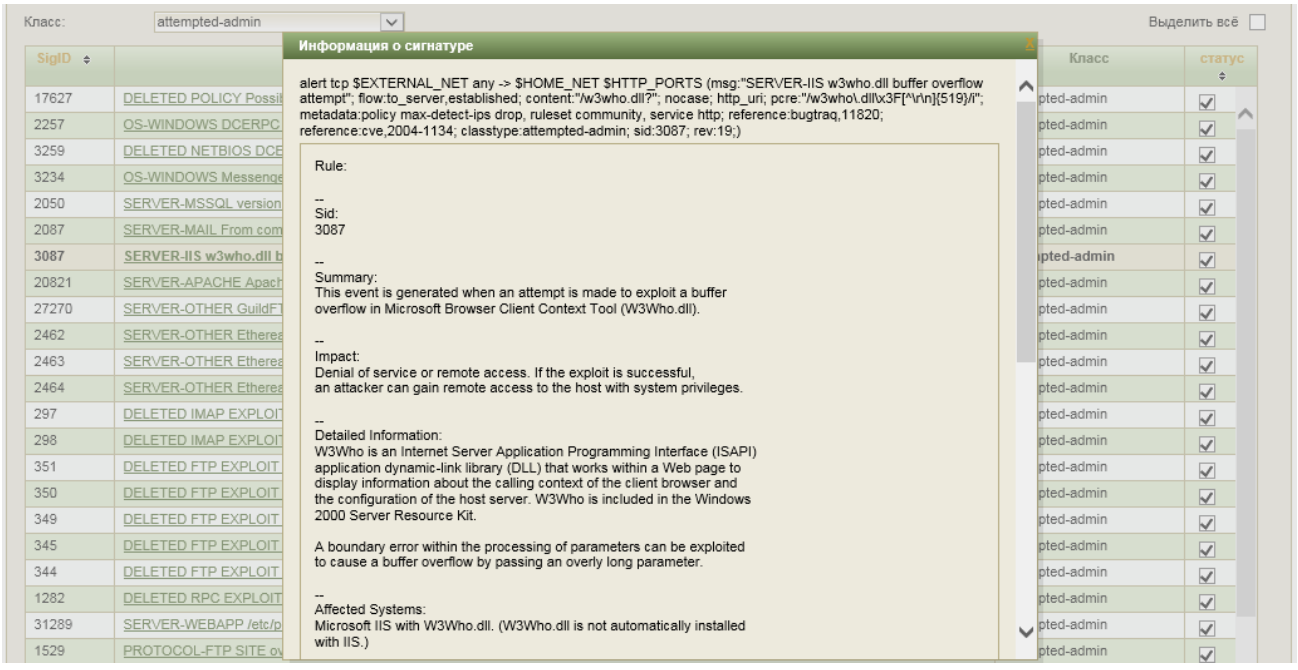

Рисунок 9 – Окно «Информация о сигнатуре»

Пункт меню «Журналы»

Данный пункт меню открывает страницу, которая отображает системные журналы текущего сенсора (см. Рисунок 10).

Размер отображаемого журнала ограничен и содержит последний 1000 записей в журнале. Полный журнал хранится только на сенсоре. Его максимальный размер 10 Мбайт, в случае превышения файл создаётся заново.

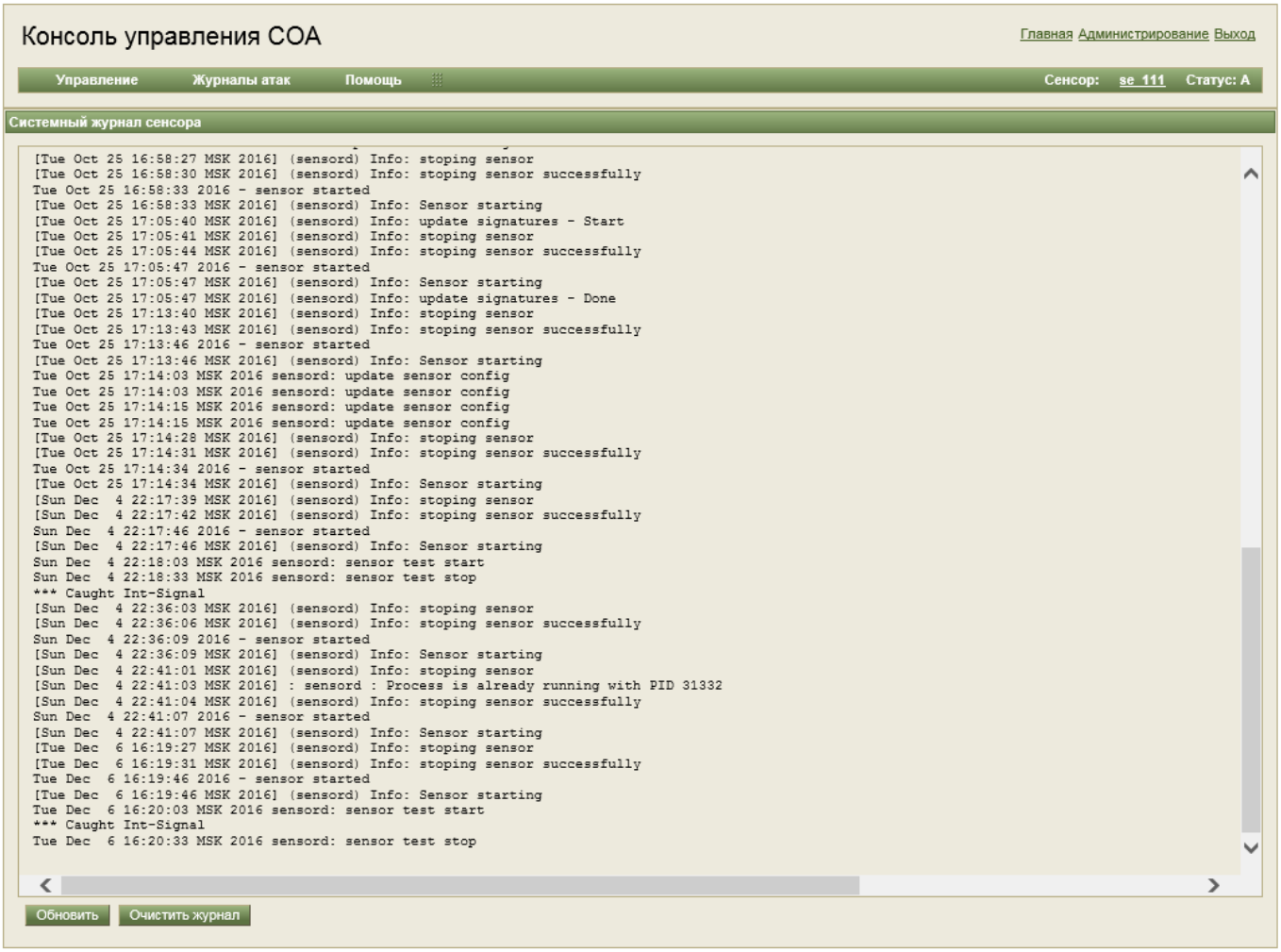

Рисунок 10 – Страница «Системный журнал сенсора»

3.1.4.2. Меню «Журналы атак»

Меню **Журналы атак** состоит из пунктов:

- «Все атаки»;
- «ТОП 10 атак»;
- «ТОП 20 атак»;
- «Последние 100 атак»;
- «Последние 1000 атак»;
- «Фильтр атак».

Пункты меню «Все атаки», «Последние 100 атак» и «Последние 1000 атак»

На рисунке (см. Рисунок 11) показано типовое окно, отображающее информацию о зафиксированных компьютерных атаках. В рабочем окне отображается последние 5000 записей о компьютерных атаках для пункта меню **Все атаки**. Записи отображаются постранично.

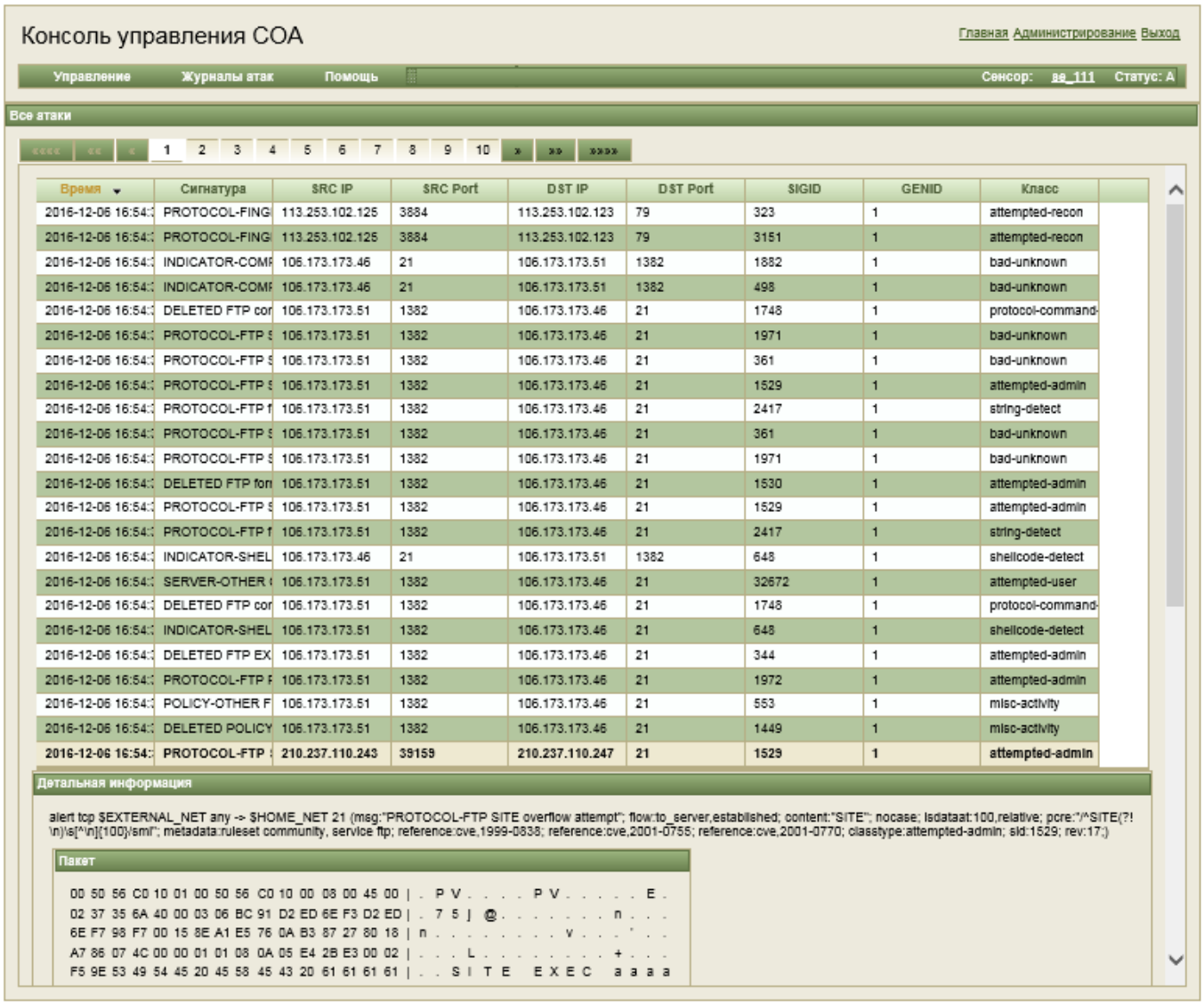

Рисунок 11 – Страница журнала атак «Все атаки»

Рабочая область (см. Рисунок 12) состоит из панели переключения страниц (1), информации о зафиксированных компьютерных атаках (2) и детальной информации о выбранной компьютерной атаке (3).

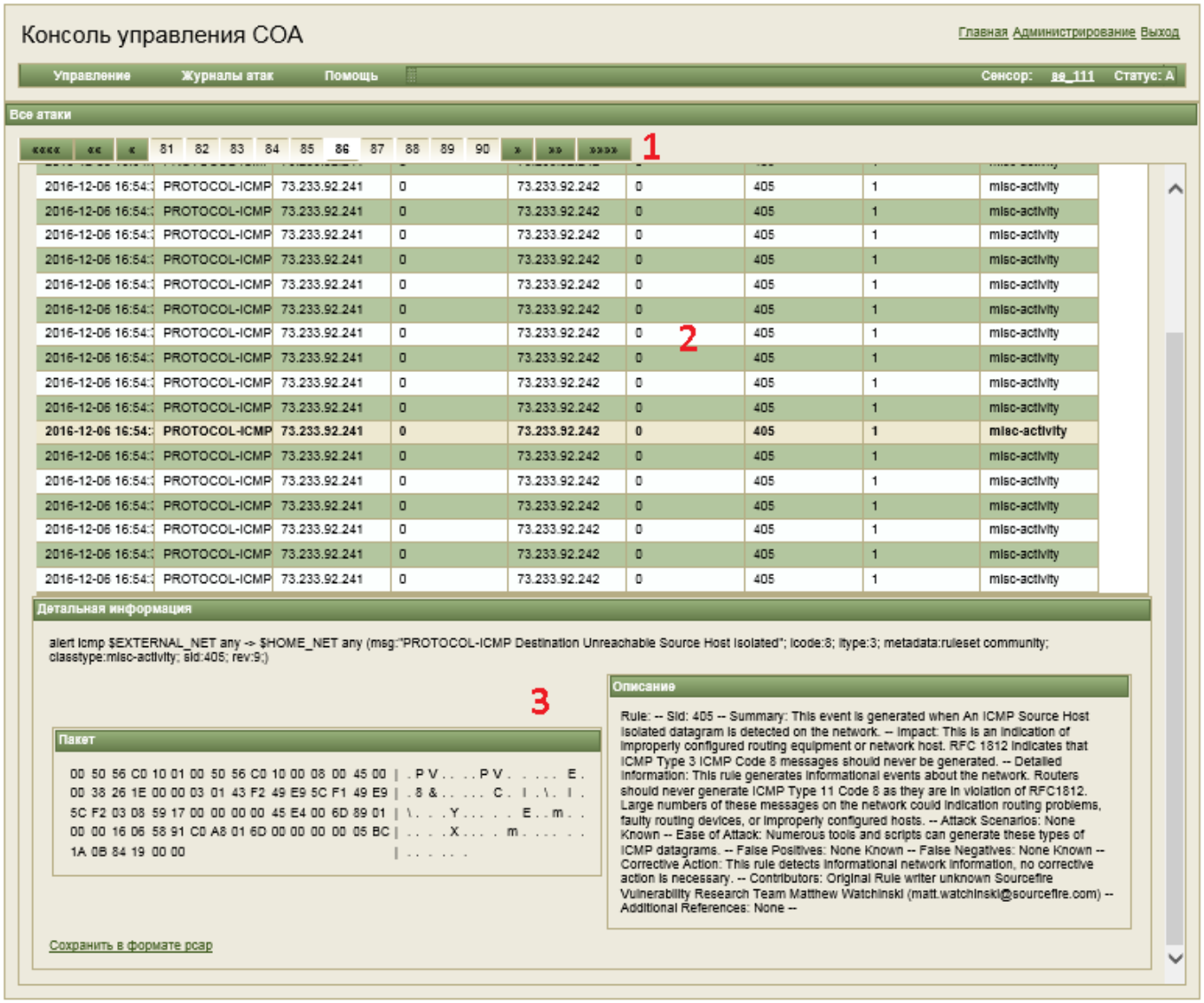

Рисунок 12 – Рабочая область журнала атак

Компьютерные атаки отображаются в виде таблицы. Описание столбцов таблицы приведено в таблице (см. Таблица 5).

Таблица 5 – Параметры зафиксированных в журнале атак

Столбец	Значение	Примечание
Время	Время обнаружения атаки	По данному полю возможна сортировка.
Сигнатура	Короткое описание сигнатуры	
SRC IP	IP-адрес источника атаки	
SRC Port	tcp или udp порт источника атаки	
DST IP	IP-адрес объекта атаки	
DST Port	tcp или udp порт атакуемого объекта	
SIGID	Идентификатор сигнатуры	
GENID	Идентификатор препроцессора Snort	
Класс	Класс, к которому относится данная компьютерная атака.	

В области с детальным описанием выбранной компьютерной атаки (Рисунок 12, **3)** отображается текстовое представление сигнатуры (верхняя часть области), сетевой пакет в 16-ричном виде, в котором сигнатура была обнаружена (присутствует не для всех атак) (левая часть области) и текстовое описание сигнатуры (если было загружено для сигнатуры) (правая часть области).

Пункты меню «ТОП 10 атак», «ТОП 20 атак»

На рисунке (см. Рисунок 13) показана типовая страница, отображающая сводную информацию о зафиксированных компьютерных атаках.

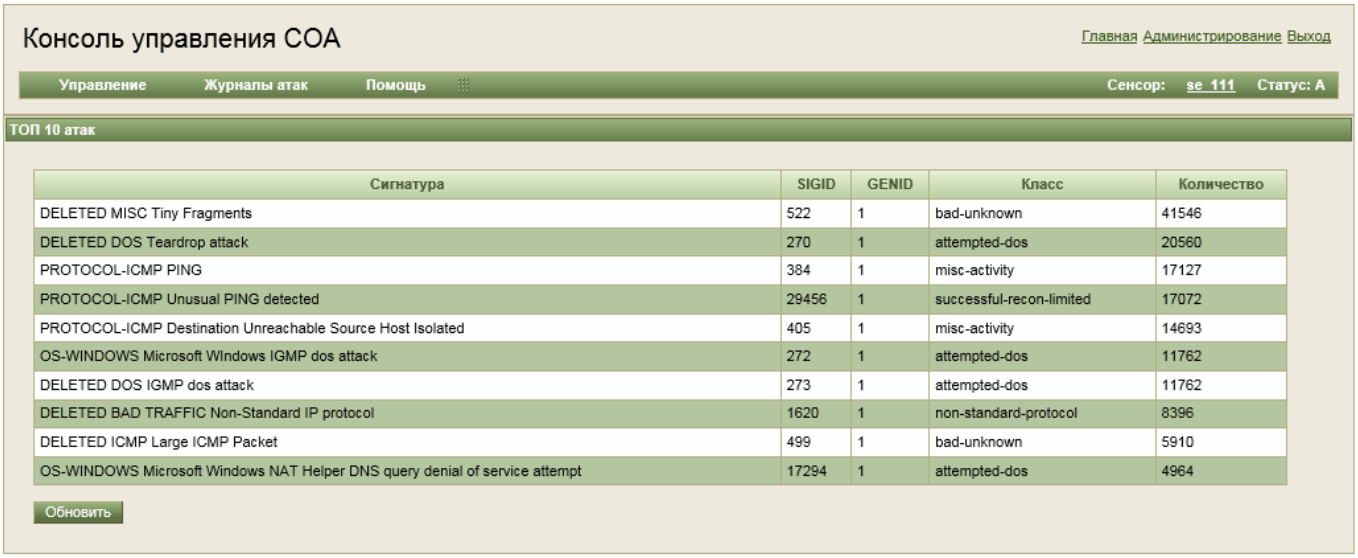

Рисунок 13 – Страница «ТОП 10 атак»

В данном окне отображаются наиболее часто встречающиеся атаки за всё время работы.

Пункт меню «Фильтр атак»

Данная команда предназначена для задания различных фильтров записей в журнале атак (см. Рисунок 14). Описания и примеры фильтров перечислены в таблице (см. Таблица 6).

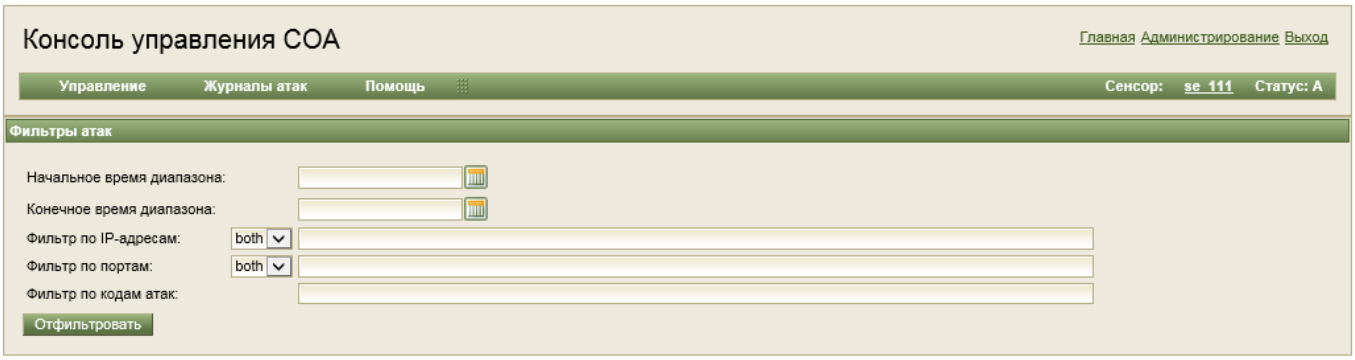

Рисунок 14 – Страница «Фильтры атак»

Таблица 6 – Фильтры журнала компьютерных атак

Название фильтра	Описание фильтра	Пример
Начальное время диапазона	Задаётся через специальную форму календаря. Для выбора времени нажать кнопку **Apply** 	апр 7, 2016 12:00
Конечное время диапазона	см. выше.	апр 10, 2016 18:00
Фильтр по IP-адреса	Состоит из двух частей: выпадающий список и текстовое поле. Первая часть указывает условия фильтрации IP-адресов: both – «Порт должен быть в поле SRCPORT или DSTPORT» src – « Порт должен быть в поле SRCPORT» dst – «Порт должен быть в поле DSTPORT» Вторая часть описывает искомые адреса, указываемые через запятую. Допустимы следующие форматы ввода IP-адресов: «IP» – одиночный IP-адрес в формате «XXX.XXX.XXX.XXX» «IP1-IP2» — диапазон IP-адресов «IP/mask» -диапазон IP-адресов по маске.	В выпадающем списке: «dst». В текстовом поле: 10.0.4.3, 10.4.2.1, 123.123.123.45-123.123.123.254, 192.168.1.1/24
Фильтр по портам	Состоит из двух частей: выпадающий список и текстовое поле. Первая часть указывает условия фильтрации IP-адресов: both – «Порт должен быть в поле SRCPORT или DSTPORT» src – « Порт должен быть в поле SRCPORT» dst – «Порт должен быть в поле DSTPORT» Вторая часть описывает искомые порты, указываемые через запятую. Допустимы следующие форматы ввода портов: «port» – одиночный порт «port1-port2» — диапазон портов.	В выпадающем списке: «dst». В текстовом поле: 12336, 12467, 1-1024
Фильтр по кодам атак	Через запятую указываются искомые коды атак.	1394,10543,123

3.1.4.3. Меню «Помощь»

Пункт меню «О сигнатуре»

Данная страница предоставляет доступ к справочной системе по загруженным сигнатурам (см. Рисунок 15).

Для просмотра информации о сигнатуре следует ввести код сигнатуры в поля **Код сигнатуры (sid)** (идентификатор сигнатуры) и **Код сигнатуры (gid)** (идентификатор модуля обнаружения Snort).

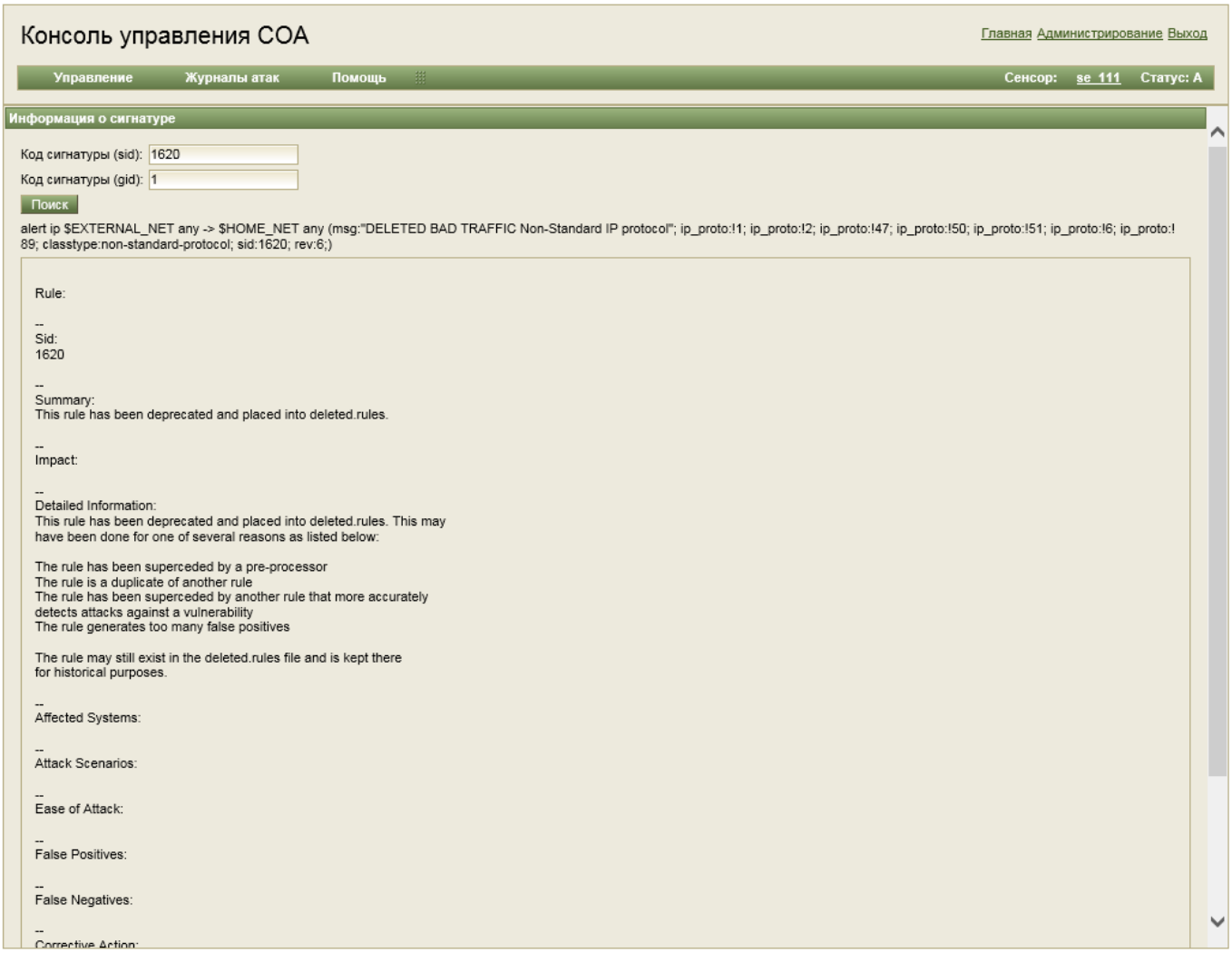

Рисунок 15 – Страница «Информация о сигнатуре»

3.1.5. Описание интерфейса «Администрирование» КУ ЦС

На рисунке (см. Рисунок 4) показано рабочее меню интерфейса **Администрирование**. Оно состоит из следующих меню:

– «Сенсоры»;

– «Правила обнаружения»;

– «Разное».

3.1.5.1. Меню «Сенсоры»

На рисунке (см. Рисунок 16) показан состав меню **Сенсоры**.

Рисунок 16 – Состав меню «Сенсоры»

Пункт меню «Список сенсоров»

Данный пункт меню открывает страницу, которая отображает все подключённые сенсоры в одном окне. Данное представление автоматически обновляется. Таким образом, возможно осуществлять постоянный мониторинг состояния подключённых сенсоров.

На рисунке (см. Рисунок 17) показано типовое окно данного пункта. В таблице (см. Таблица 7) приведены пояснения по каждому столбцу таблицы списка сенсоров.

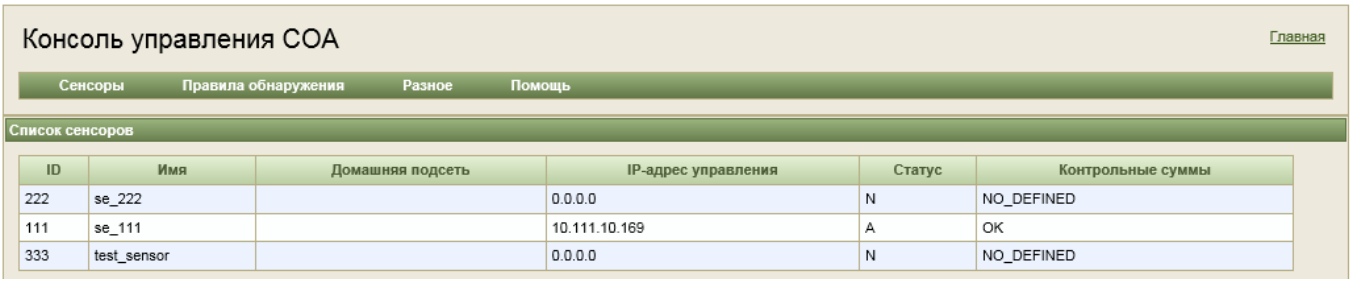

Рисунок 17 – Страница «Список сенсоров»

Таблица 7 – Описание полей таблицы отображения состояния сенсоров

Имя поля	Описание	Примечание
Id	Идентификатор сенсора	
Имя	Имя сенсора	
Домашняя подсеть	Информационное поле, содержащее адреса, контролируемых сенсором подсетей.	
IP-адрес управления	Информационное поле — адрес интерфейса управления (если есть) сенсора.	
Статус	Статус работы сенсора.	A — сенсор работает. N — сенсор не работает.
Контрольные суммы	Результат проверки контрольных сумм заданных файлов.	OK — контрольные суммы соответствуют заданным. ERROR – контрольные суммы не соответствуют заданным (подробности см. в журнале сенсора). NOT_DEFINED – для сенсора не заданы контрольные суммы.

Пункт меню «Добавить сенсор»

Позволяет добавить новые сенсоры в КУ ЦС.

На рисунке (см. Рисунок 18) показано типовая страница добавления сенсора.

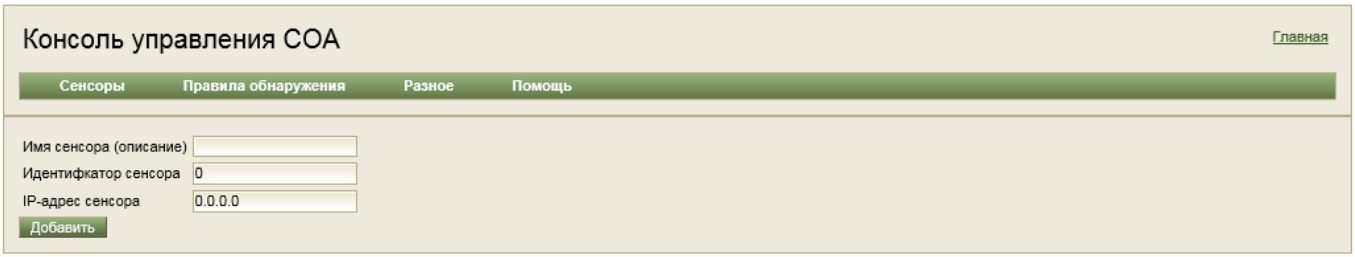

Рисунок 18 – Страница «Добавить сенсор»

В таблице (см. Таблица 8) приведено описание полей ввода данной страницы.

Таблица 8 – Поля ввода страницы «Добавить сенсор»

Имя поля	Значение	Формат	Примечание
Имя сенсора (описание)	Задаётся имя сенсора, которое будет отображаться в КУ.	Текстовый формат. Ограничения на количество символов нет.	Необходимо ограничить количество вводимых символов.
Идентификатор сенсора	Идентификатор подключаемого сенсора (см. параметр sensor-unique-id в подразделе 4.1)	Числовое целочисленное значение.	Должно точно совпадать с полем sensor-unique-id в настройках сетевого сенсора.
IP-адрес	IP-адрес сетевого сенсора.	Текстовое представление IP-адреса. Не выполняется проверка корректности ввода.	Не обязательный параметр. Используется для информации.

Пункт меню «Удалить сенсор»

Данный пункт меню позволяет удалить сенсор из КУ ЦС.

На рисунке показана (см. Рисунок 19) типовая страница данного пункта.

При удалении сенсора все данные этого сенсора о компьютерных атаках, его настройки и журналы будут удалены.

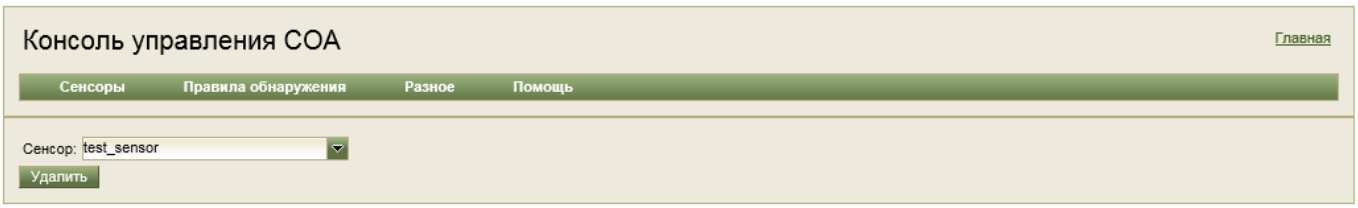

Рисунок 19 – Страница «Удалить сенсор»

Пункт меню «Настройки сенсора»

На данной странице предоставляется возможность произвести настройку сенсора.

На рисунке (см. Рисунок 20) показан типовой вид данной страницы.

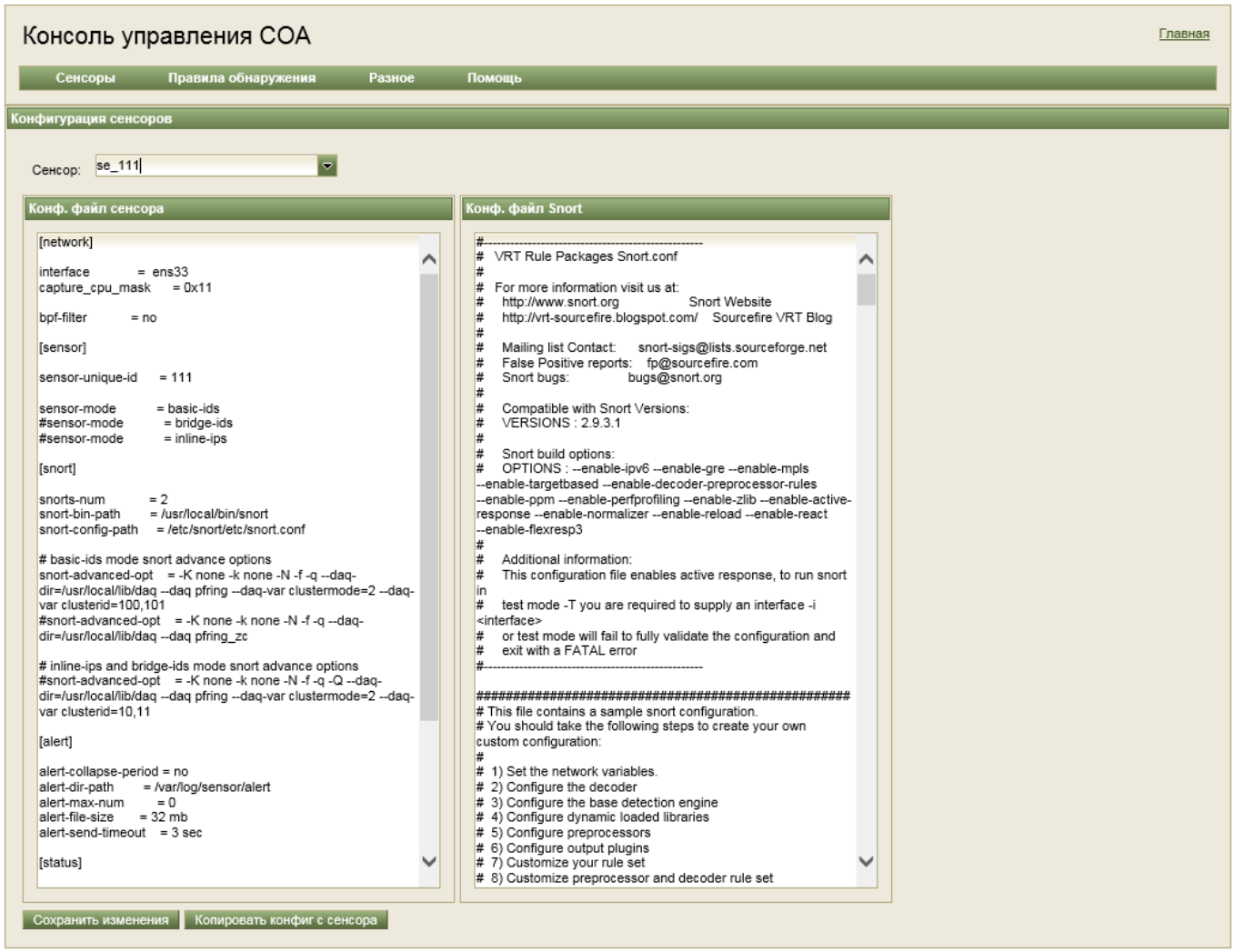

Рисунок 20 – Страница «Конфигурация сенсора»

Особенности сохранения настроек сенсора

При добавлении сенсора в КУ он должен автоматически передать свои конфигурационные данные на ЦС. В случае если этого по каким-либо причинам не произошло, его конфигурация на ЦС будет пустой. В этом случае необходимо вручную послать команду, для этого в данном разделе надо выбрать сенсор, и нажать кнопку **Копировать конфиг. с сенсора**. Команда будет выполнена в отложенном режиме, поэтому сразу после её выполнения настройки сенсора не отобразятся. Кроме того, если сенсор в настоящее время недоступен, его конфигурация будет получена только после его подключения.

Поле **Конф. файл сенсора** позволяет редактировать настройки сенсора (см. описание конфигурационного файла сенсора (sensor.conf) в подразделе 4.1).

Поле **Конф. файл Snort** позволяет редактировать настройки анализатор Snort (см. описание конфигурационного файла сенсора (Snort.conf) в подразделе 4.1).

После внесения изменений в текст конфигурации следует нажать кнопку **Сохранить изменения**.

Пункт меню «Контрольные суммы»

На рисунке (см. Рисунок 21) показана типовая страница задания и изменения контрольных сумм файлов.

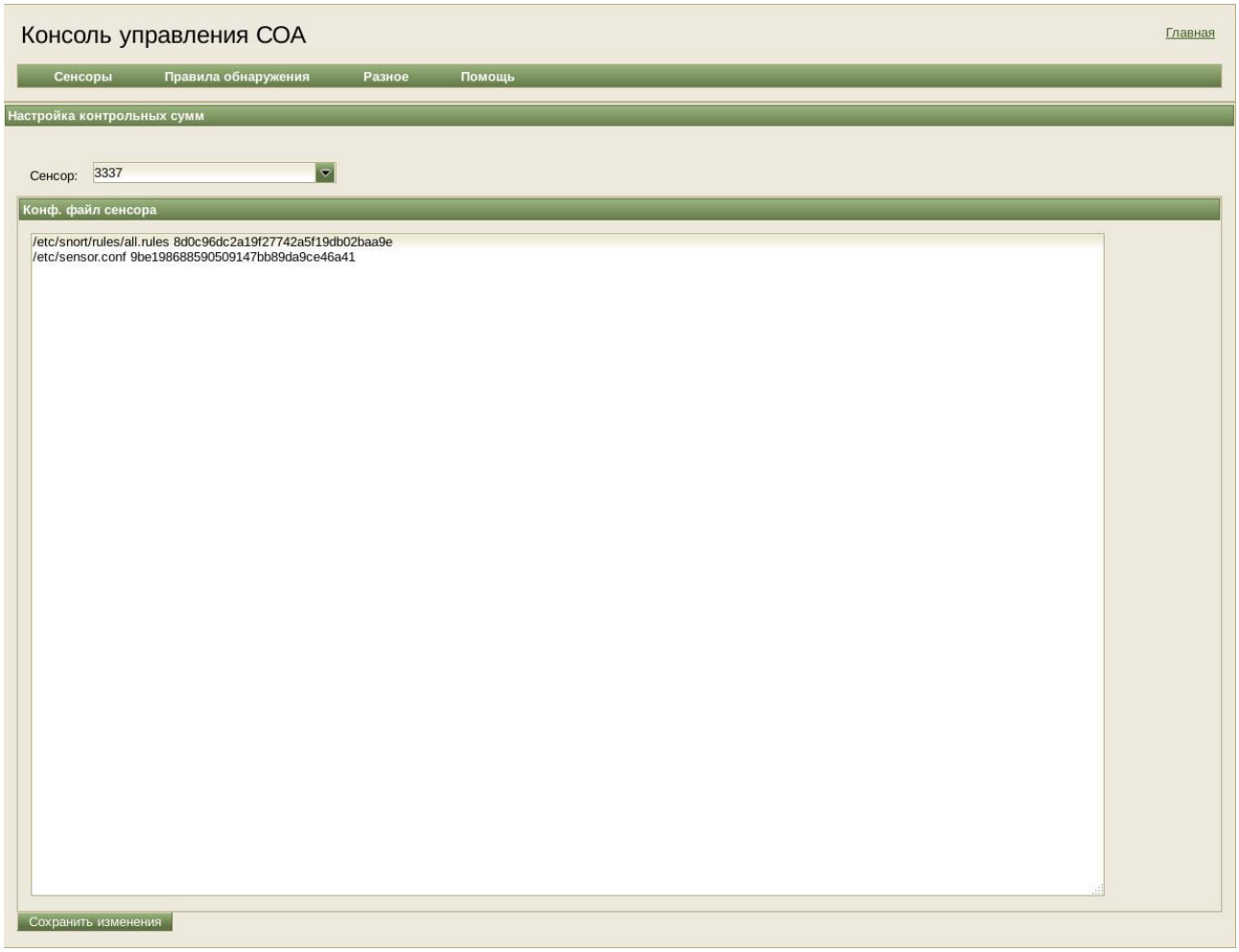

Рисунок 21 – Страница «Настройка контрольных сумм».

Для задания контрольных сумм для файлов сенсора следует:

- выбрать данное меню;
- выбрать необходимый сенсор при помощи выпадающего списка **Сенсор**;
- отредактировать текстовое поле с описанием контрольных сумм для файлов;

Список контрольных сумм представляет собой записи формата:

<имя_файла> <контрольная сумма>

На каждой строке одна запись о файле.

Пример:

```
/etc/Snort/rules/all.rules 8d0c96dc2a19f27742a5f19db02baa9e
/etc/sensor.conf 9be198688590509147bb89da9ce46a41
```

- после завершения редактирования нажать кнопку **Сохранить изменения**.

Пункт меню «Обновление сенсоров»

На рисунке (см. Рисунок 22) показано типовое окно данного пункта.

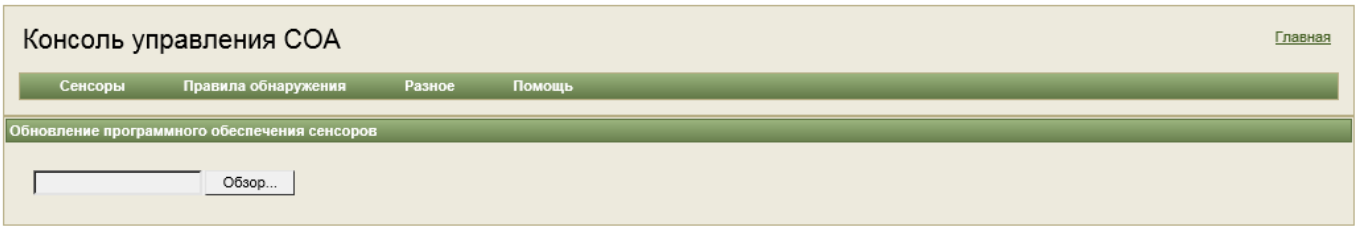

Рисунок 22 – Страница «Обновление ПО сенсоров»

На данной странице предоставляется возможность централизованного обновления ПО всех сенсоров. Подробнее о процедуре обновления см. подраздел 5.2.

3.1.5.2. Меню «Правила обнаружения»

Меню **Правила обнаружения** состоит из подменю:

«Обновить правила»;

«Добавить сигнатуру».

Пункт меню «Обновить правила»

Данный пункт открывает страницу **Обновление сигнатур** (см. Рисунок 23), которая позволяет обновить правила обнаружения (сигнатуры) компьютерных атак в системе.

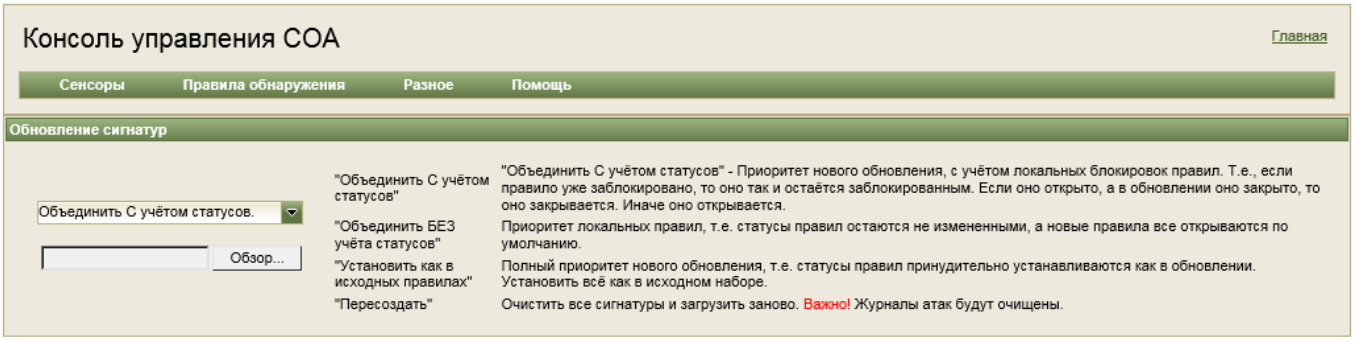

Рисунок 23 – Страница «Обновление сигнатур»

Для выполнения обновления базы правил обнаружения нужно выбрать файл с обновлениями. Как его подготовить, см. подраздел 5.1.

Доступные режимы обновления приведены в таблице (см. Таблица 9).

Таблица 9 – Режимы обновления правил обнаружения

Режим обновления	Описание
Объединить С учётом статусов	Приоритет нового обновления, с учётом локальных деактиваций правил. Т.е., если правило неактивно, то оно так и остаётся неактивным. Если оно активно, а в обновлении оно неактивно, то оно деактивируется. Иначе оно активируется.
Объединить БЕЗ учёта статусов	Приоритет локальных правил, т.е. статусы правил остаются неизменёнными, а новые правила все активируются по умолчанию.
Установить как в исходных правилах	Полный приоритет нового обновления, т.е. статусы правил принудительно устанавливаются как в обновлении. Установить всё как в исходном наборе.
Пересоздать	Очистить все сигнатуры и загрузить заново. **Важно!** Журналы атак будут очищены.

Пункт меню «Добавить сигнатуру»

Данный пункт позволяет вручную добавить новое правило обнаружения (сигнатуру) компьютерных атак в системе (см. Рисунок 24).

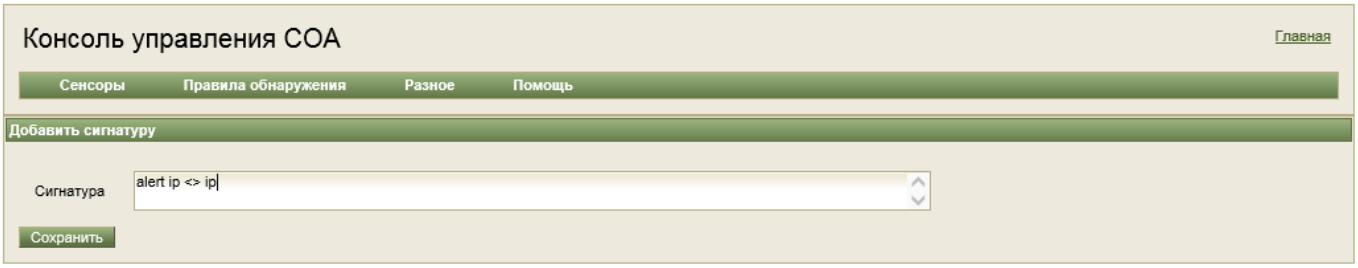

Рисунок 24 – Страница «Добавить сигнатуру»

3.1.5.3. Меню «Разное»

На рисунке (см. Рисунок 25) показан состав меню **Разное.**

Рисунок 25 – Состав меню «Разное»

Пункт меню «Выйти»

Данный пункт позволяет осуществить выход из консоли управления.

Пункт меню «Пользователь»

Данный пункт открывает страницу **Данные пользователя** (см. Рисунок 26) позволяет сменить пароль пользователя. Пароль должен иметь длину как минимум 6 символов, должен содержать хотя бы одну цифру, одну прописную и одну строчную буквы, один спец символ (@#$%^&+=). Пароль не должен содержать пробелы.

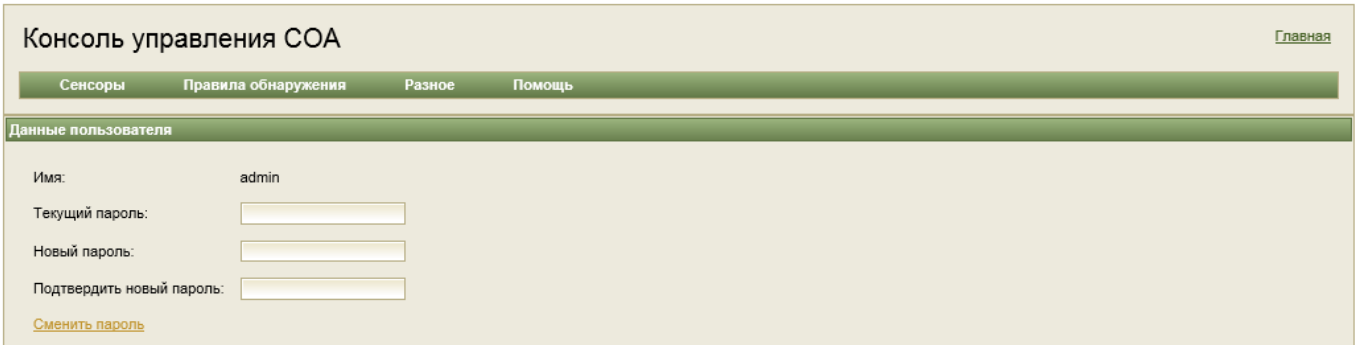

Рисунок 26 – Страница «Данные пользователя»

Пункт меню «Настройка Email»

На данной странице (см. Рисунок 27) можно указать настройки отправки электронных почтовых сообщений об обнаруженных компьютерных атаках.

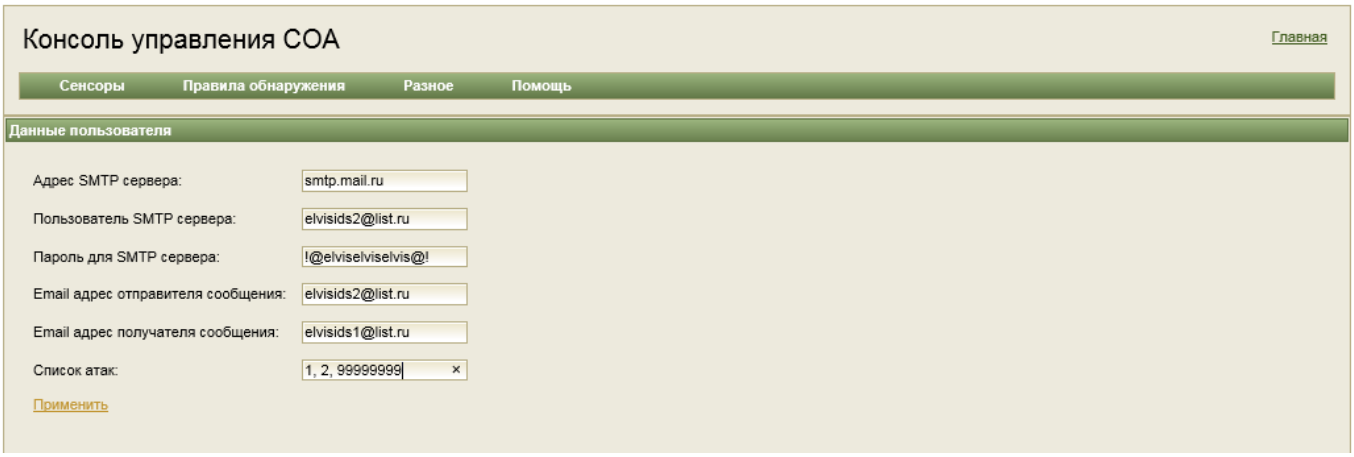

Рисунок 27 – Страница настройки E-mail

В таблице (см. Таблица 10) приведены описания полей.

Таблица 10 – Поля настройки E-mail

Поле	Описание
Адрес SMTP сервера	Имя SMTP сервера, используемого для отправки информации о фиксировании заданных компьютерных атак. По умолчанию: smtp.mail.ru
Пользователь SMTP сервера	Имя пользователя SMTP сервера. По умолчанию: elvisids1@list.ru
Пароль для SMTP сервера	Пароль для SMTP сервера. По умолчанию: !@elviselviselvis@!
Email адрес отправителя сообщения	Адрес почтового ящика отправителя почтовых сообщений. По умолчанию: elvisids1@list.ru
Email адрес получателя сообщения	Адрес почтового ящика получателя почтовых сообщений. По умолчанию: elvisids2@list.ru
Список атак	Задаёт приоритеты и коды атак, информация о которых должна отсылаться через электронную почту. Формат: через запятую перечисляются коды атак в формате attakid, а также коды приоритетов атак. Приоритеты атак соответствуют классам сигнатур (см. файл classification.config в дистрибутиве ПО Snort или в архиве обновления правил обнаружения атак). Первые 10 кодов атак зарезервированы под приоритеты, таким образом, атаки должны иметь код, начиная с 11. Пример: *email_alerts — 1,2,3,9999999*, что соответствует всем атакам с приоритетами 1, 2 и 3 и атаке с кодом 9999999.

Подменю «Журналы сервера»

Подменю позволяет получить доступ к журналам следующих модулей ЦС:

- консоль управления (controlpanel);
- загрузчик (receiver);
- управление (manager).

На рисунке (см. Рисунок 28) показан состав данного подменю.

На рисунке (см. Рисунок 29) показана страница журнала КУ.

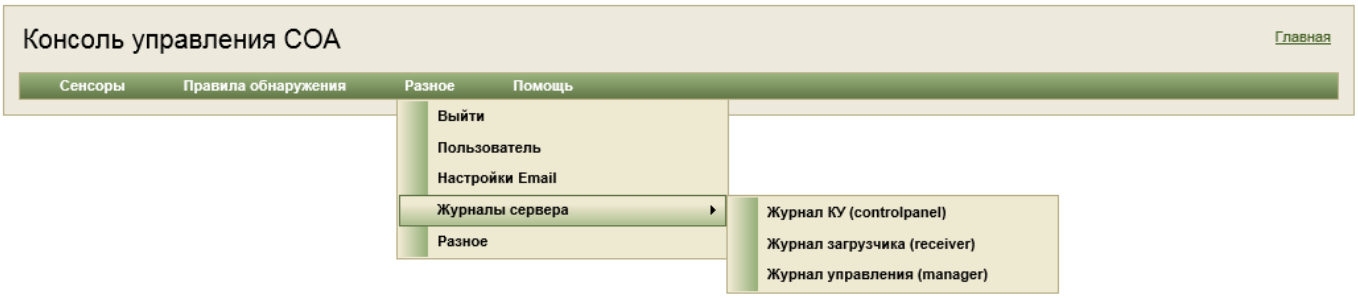

Рисунок 28 – Подменю «Журналы сервера»

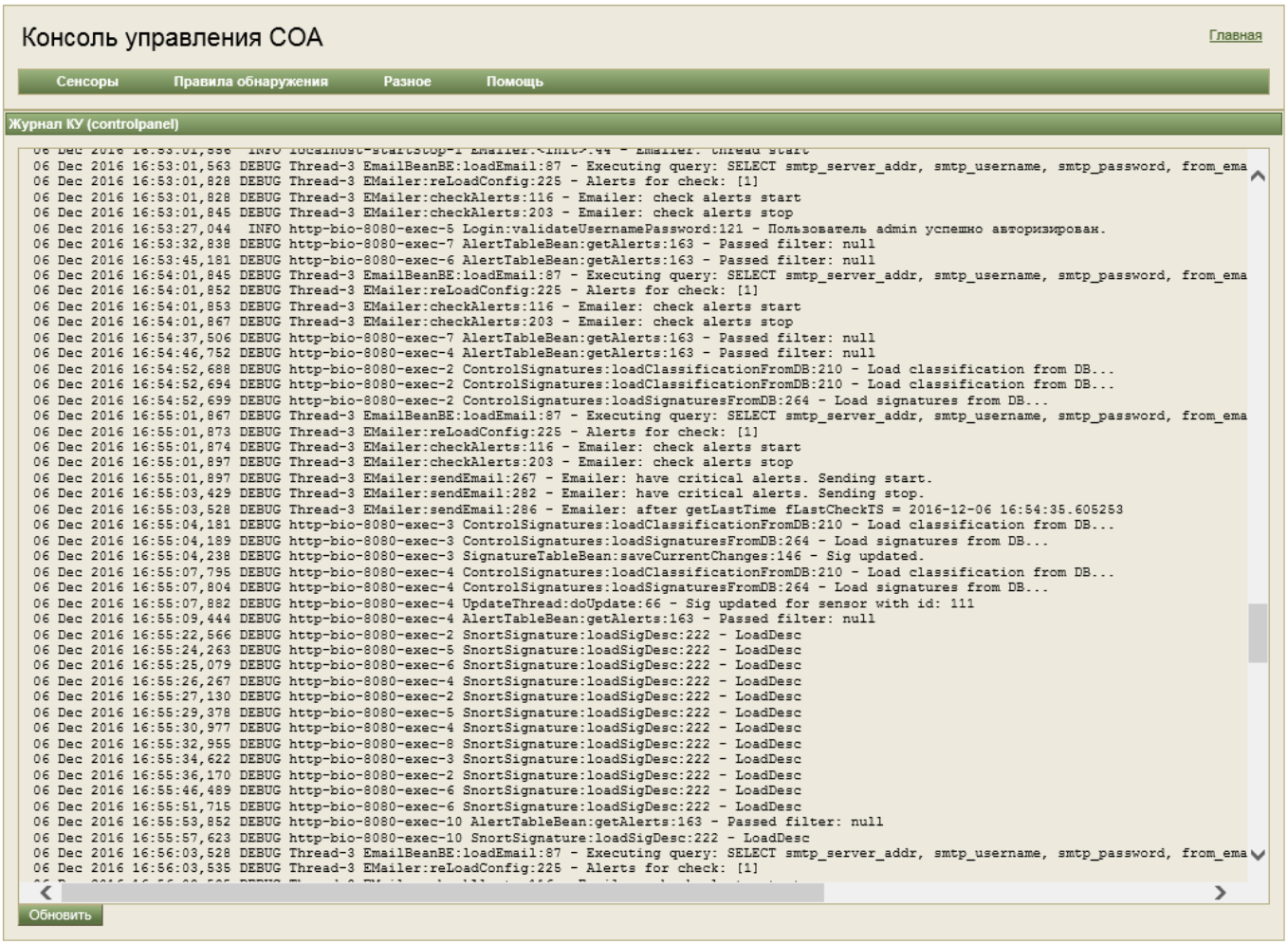

Рисунок 29 – Страница «Журнал КУ»

Подменю «Разное»

Подменю **Разное** состоит из следующих команд (см. Рисунок 30):

– «Очистить журнал атак» – удалить все данные об атаках для всех сенсорах;

– «Экспорт журнала атак в CSV формате» – сохранение всех атак для всех сенсоров в формате CSV;

– «Экспорт в ГЦМ» – сохранение атак в формате взаимодействия с Главным Центром Мониторинга (ГЦМ) (см. Рисунок 31).

Идентификатор сенсора – номер сенсора для экспорта компьютерных атак. Если в данном поле установлено значение «0», то экспортируются атаки для всех сенсоров.

Начальное время диапазонов, конечное время диапазонов — временной диапазон для экспорта.

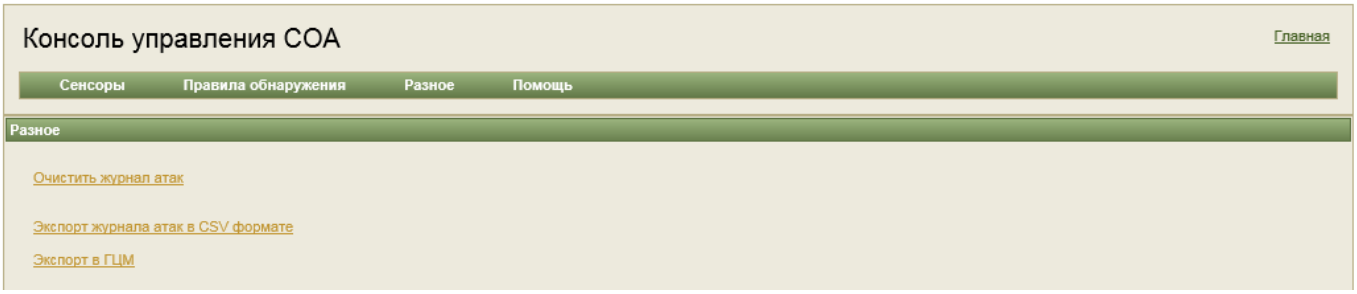

Рисунок 30 – Страница подменю «Разное»

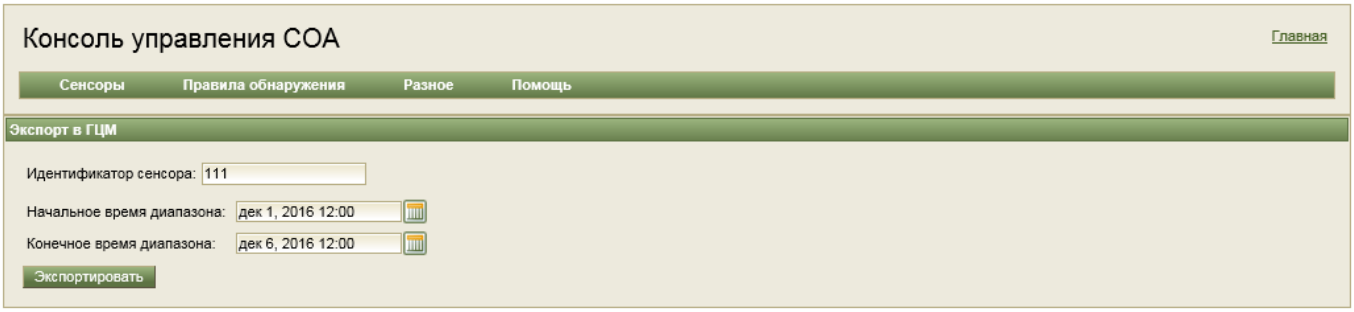

Рисунок 31 – Страница «Экспорт в ГЦМ»

3.1.6. Утилита командной строки console_tools

Данная утилита запускается из командной строки ЦС командой:

```
./console_tools <опции>
```

При запуске без указания опций утилита выводит список доступных опций:

```
--alert-all SENSORID          : Print all alerts for sensor SENSORID.
 --clear-tables           : Clean alert and signatures tables.          (default: false)
 --sensor-add ID:ADDR:HOMENET:DESC   : Add sensor.
 --sensor-change-sig-status       : Change status of sig with
 SENSORID:ALERTID:GENID:STATUS      ALERTID:GENID to STATUS (0 or 1) for
                sensor SENSORID. If SENSORID=0,  change default status
 --sensor-cmd SENSORID:CMD       : Send cmd to sensor.Available CMD:
                start, stop, restart, updatesigs, updatesoft, selftest.
 --sensor-cmd-clear SENSORID      : Clear all commands for sensor
                SENSORID. If SENSORID=0, then clear all commands from queue.
 --sensor-cmd-print SENSORID      : Print all commands for sensor
                SENSORID. If SENSORID=0, then print all commands in queue.
 --sensor-del SENSORID         : Delete sensor.
 --sensor-list            : List sensors. (default: false)
 --sensor-log SENSORID         : Print logs for sensor SENSORID.
 --sig-add SIGRULE          : Add signature to default signature set.
 --sig-count              : Count signatures. (default: false)
 --sig-del ALERTID:GENID        : Delete signature.
```

```
--sig-load-sigs SNORT_DIRECTORY    : Load and update sig in DB from Snort directory.
--sig-print ALERTID:GENID          : Print signature.
--sig-print-for-sensor ALERTID:GENID: SENSORID : Print signature for sensor SENSORID.
--sig-save-all FILE_NAME           : Save sigs from DB to file.
-c FILENAME                        : path to config file
```

3.2. Локальная консоль управления сенсора

Каждый сенсор имеет возможность локального управления. Управление выполняется через специализированный скрипт **sensord**. Для выполнения административных действий с сенсором необходимо выполнить команду вида:

```
/etc/init.d/sensord <команда>
```

В таблице (см. Таблица 11) показаны все команды управления, предоставляемые данным скриптом.

Таблица 11 – Команды управления сенсором

Команда	Функция
start	Запуск сенсора
stop	Остановка сенсора
status	Информация о текущем состоянии сенсора
restart|reload|condrestart	Перезапуск сенсора
selftest	Инициализация процедуры самотестирования
init	Первоначальная настройка сенсора
update-sig	Инициализация процедуры принудительного обновления базы сигнатур с ЦС.
upgrade	Инициализация процедуры принудительного обновления программного обеспечения с ЦС.
update-cfg	Инициализация процедуры принудительного обновления конфигурационных файлов сенсора с ЦС.
send-cfg	Инициализация процедуры принудительного обновления конфигурационных файлов в ЦС с сенсора.

4. Файл конфигурации. Составление и правка

4.1. Конфигурационный файл сенсора

4.1.1. Настройки сенсора

Файл конфигурации сенсора располагается в `/etc/sensor.conf`. После установки он заполняется типовой конфигурацией, для его изменения можно использовать текстовый редактор или скрипт начальной инициализации (`/etc/init.d/sensord init`).

Файл конфигурации состоит из групп параметров следующего вида:

[название группы параметров]

параметр_1 = значение_параметра_1

параметр_2 = значение_параметра_2

Описание параметров:

Группа [network]

interface — параметр задающий название интерфейсов, на которых будет происходить захват анализируемого трафика, если слушающих интерфейсов несколько, то они указываются через запятую.

примеры:

interface = enp0s3
interface = eth1, eth2

capture_cpu_mask — параметр привязывает запускаемые процессы Snort к определенным ядрам CPU.

Экземпляр Snort может быть привязан к ядру, если в двоичном представлении capture_cpu_mask разряд, совпадающий с номером ядра, равен 1.

примеры:

capture_cpu_mask = 0x01

Двоичное представление: 0001

привяжется к первому ядру

capture_cpu_mask = 0x0f

Двоичное представление: 1111

Экземпляры Snort привяжутся к первым 4 ядрам

capture_cpu_mask = 0x09

Двоичное представление: 1001

Экземпляры Snort привяжутся к 1 и 4 ядру

capture_cpu_mask = 0x44

Двоичное представление: 101100

Экземпляры Snort привяжутся к 3,4 и 6 ядру

Количество запускаемых экземпляров Snort не должно превышать количество используемых ядер. Если количество экземпляров Snort меньше чем возможное количество используемых ядер, то экземпляры Snort привяжутся к первым возможным ядрам. Пример:
capture_cpu_mask = 0x44
Snorts-num = 2
Двоичное представление: 101100
Экземпляры Snort привяжутся к 3-му и 4-му ядрам.

bpf-filter — пакетный фильтр Беркли (подробное описание можно прочитать на сайте `http://biot.com/capstats/bpf.html`).

пример:

bpf-filter = no

не использовать фильтр

bpf-filter = host 192.168.2.12

отслеживать только пакеты, в которых присутствует IP-адрес 192.168.2.12.

Группа [sensor]

sensor-unique-id — Задает идентификатор сенсора. У двух сенсоров подключенных к одному серверу не может быть одинаковые идентификаторы.

пример:

sensor-unique-id = 55

sensor-mode — режим работы, возможен один из вариантов:

basic-ids

– СОА при подключении по Т-образной схеме (зеркалирующий трафик);

bridge-ids

– СОА при подключении в разрыв без блокировки пакетов;

inline-ips

– СОА при подключении в разрыв с блокировкой пакетов.

пример:

sensor-mode = basic-ids

Группа [Snort]

Snorts-num — количество запускаемых экземпляров ПО Snort.

пример:

Snorts-num = 2

Snort-bin-path — путь к бинарному исполняемому файлу Snort

пример:

Snort-bin-path = /usr/local/bin/Snort

Snort-config-path путь к конфигурационному файлу Snort

пример:

Snort-config-path = /etc/Snort/etc/Snort.conf

Snort-advanced-opt — дополнительные опции для запуска Snort

пример:

Snort-advanced-opt = -K none -k none -N -f -q --daq-dir=/usr/local/lib/daq --daq pfring --daq-var clustermode=2 --daq-var clusterid=100

Группа [alert]

alert-collapse-period — время, за которое одинаковые сообщения об атаках будут объединены, если «no», то объединения не происходит.

пример:

alert-collapse-period = no

alert-dir-path — путь к рабочей папке для хранения файлов с информацией об обнаруженных атаках

пример:

alert-dir-path = /var/log/sensor/alert

alert-max-num — максимальное количество сообщений об атаках в одном файле, если «0», то максимум определяется размером файла с информацией об обнаруженных атаках

пример:

alert-max-num = 0

alert-file-size — максимальный размер файла с информацией об обнаруженных атаках

пример:

alert-file-size = 32 mb

alert-send-timeout — периодичность отправки файлов с сообщениями об атаках на сервер

пример:

alert-send-timeout = 3 sec

Группа [status]

status-dir-path — путь к рабочей папке для хранения файлов с информацией о статусе сенсора

пример:

status-dir-path = /var/log/sensor/status

status-send-timeout — периодичность отправки файлов с сообщениями о статусе на сервер, если значение «no», то не отправлять

пример:

status-send-timeout = no

Группа [disk]

disk-min-space — минимальный размер свободного дискового пространства, по исчерпанию

которого старые сообщения об атаках будут удаляться.

пример:

disk-min-space = 5 gb

Группа [server]

server-addr — URL сервера

пример:

server-addr = http://192.168.25.131:8080/receiver/ReceiverISP?type=isp

4.1.2. Настройки ПО Snort

Файл конфигурации ПО Snort по умолчанию располагается в `/etc/Snort/etc/Snort.conf`. После установки он заполняется типовой конфигурацией, для его изменения можно использовать текстовый редактор.

Для базового конфигурирования сенсора необходимо указать защищаемые подсети:

```
# Setup the network addresses you are protecting
ipvar HOME_NET [192.168.100.1/24,123.45.6.1/26]
```

Подробнее про настройку ПО Snort см. руководство по адресу:

http://manual-Snort-org.s3-website-us-east-1.amazonaws.com/

4.2. Конфигурационный файл ЦС

Файл конфигурации ЦС может располагаться в следующих местах на диске (указаны в порядке выбора):

```
${catalina.home}/conf/centralserver/centralserver.conf
/etc/centralserver.conf
/etc/sensor.conf
```

После установки он заполняется типовой конфигурацией, для его изменения можно использовать текстовый редактор.

Файл конфигурации состоит из групп параметров следующего вида:

[название группы параметров]

параметр_1 = значение_параметра_1

параметр_2 = значение_параметра_2

Описание полей:

Группа [manager]

`driver` – параметр, указывающий тип СУБД в формате jdbc-драйвера. По умолчанию имеет значение *org.postgresql.Driver*, что соответствует СУБД Postgresql.

`url` – параметр, указывающий тип адрес и имя СУБД в формате jdbc-драйвера: jdbc:postgresql://<IP-адрес>/<имя БД>. Например, *jdbc:postgresql://127.0.0.1/ids*.

`user` – имя пользователя СУБД. По умолчанию: *idsuser*.

`password` – пароль пользователя СУБД. По умолчанию: *idsuser*.

`bad-file-log-dir` – директория, в которую перемещаются фалы с атаками, которые по каким-либо причинам не смогли загрузиться в СУБД. По умолчанию: */var/log/tomcat/badlog*

`upload-dir` – директория, в которой временно хранятся файлы, полученные от сенсоров. По умолчанию: */var/log/tomcat/receiver*

`isp-check-period` – период опроса директории upload-dir загрузчиком данных в СУБД в секундах. По умолчанию: *10*

`update-sig-dir` – директория, хранящая файлы с правилами для сенсоров. По умолчанию: */var/log/tomcat/controlpanel*

`sig-file-name` – имя файла, в котором будут храниться правила (сигнатуры) для сенсора. Именно этот файл будет передаваться каждому сенсору в виде обновлений правил обнаружений.

#Настройки для почты

`smtp_server` – задаёт имя SMTP сервера, используемого для отправки информации о фиксировании заданных компьютерных атак. По умолчанию: *smtp.mail.ru*

`smtp_user` – задаёт имя пользователя SMTP сервера. По умолчанию: *elvisids1@list.ru*

`smtp_pass` – задаёт имя пользователя SMTP сервера. По умолчанию: *!@elviselviselvis@!*

`from_email` – задаёт адрес почтового ящика отправителя почтовых сообщений. По умолчанию: *elvisids1@list.ru*

`to_email` – задаёт адрес почтового ящика получателя почтовых сообщений. По умолчанию: *elvisids2@list.ru*

`email_alerts` – задаёт приоритеты и коды атак, информация о которых должна отсылаться через электронную почту.

Формат: через запятую перечисляются коды атак в формате attakid, а также коды приоритетов атак. Приоритеты атак соответствуют классам сигнатур (см. файл classification.config в дистрибутиве ПО Snort или в архиве обновления правил обнаружения атак).

По умолчанию: 1,2,3, что соответствует все атаки с приоритетами 1, 2 и 3.

Первые 10 кодов зарезервированы под приоритеты, таким образом, атаки должны иметь код, начиная с 11.

Пример:

email_alerts — 1,2,3,9999999

`chk_period` – параметр задаёт период опроса СУБД на наличие новых атак, удовлетворяющих условию «email_alerts».

5. Мероприятия по текущему обслуживанию программы (комплекса)

СОА «ЗАСТАВА-IDS» требует выполнения следующих регулярных мероприятий:

1) Обновление правил обнаружения компьютерных атак.
2) Обновление ПО.
3) Создание резервной копии СУБД ЦС.

5.1. Обновление правил обнаружения компьютерных атак

Автоматизированная подготовка файла с правилами

– В ОС ALTLinux выполнить:

```
apt-get install wget
```

Создание нового файла с правилами обнаружения может выполняться на любом компьютере под управлением ОС Linux с установленной утилитой wget.

– подключить компьютер к сети Интернет;

– скопировать из дистрибутива папку /Server/rules;

– выполнить скрипт в папке /Server/rules:

```
./prepare_rules_update.sh
```

Описание файла с правилами обнаружения компьютерных атак

Файл с правилами обнаружения атак является архивом в формате tar.gz. Далее описывается структура архива.

1) **Директория doc/signatures**

Директория содержит файлы с описанием сигнатур в текстовом виде. Имя каждого файла формируется в следующем виде:

<код_атаки>.txt либо <код_модуля_Snort>-<код_атаки>.txt

Например, описание атаки с кодом 1000 должно находиться в файле: 1000.txt

Требований к формату текстового файла не предъявляется.

2) **Директория etc/ (используется для загрузки информации о классах)**

Директория содержит конфигурационные файлы ПО Snort.

Файл etc/classification.config (описывает классы компьютерных атак)

Файл etc/reference.config

Файл etc/sid-msg.map

Файл etc/Snort.conf

Файл etc/threshold.conf

Файл etc/unicode.map

3) **Директория rules**

Директория содержит файлы с сигнатурами в формате ПО Snort. Все файлы с расширением .rules рассматриваются в качестве источника сигнатур. Данные файлы должны быть в текстовом

формате. Из них формируется общее обновление правил для сенсора.

4) **Директория preproc_rules**

Директория по умолчанию входит в состав архива набора сигнатур Snort, содержит дополнительные файлы с сигнатурами, не используется в работе сенсора.

Файл decoder.rules

Файл preprocessor.rules

Файл sensitive-data.rules

5) **Директория so_rules**

Директория по умолчанию входит в состав архива набора сигнатур Snort, содержит дополнительные файлы с сигнатурами, не используется в работе сенсора.

Директория precompiled

Директория src

Файл browser-ie.rules

<прочие файлы .rules>.

После запуска скрипта будет сгенерирован файл-архив tar.gz с обновлением правил.

5.2. Обновление ПО сенсора

Обновление ПО сенсора представляет собой архив tar.gz. Имя архива задано жёстко: `updatesensor.tgz`. Данный архив необходимо распространить на все подключенные сенсоры через меню **Администрирование – Сенсоры – Обновление сенсоров** в КУ (см. п. 3.1.5.1), для этого достаточно нажать кнопку **Обзор** и выбрать файл `updatesensor.tgz`.

5.3. Создание резервной копии СУБД ЦС

Резервная копия СУБД ЦС создаётся средствами СУБД PostgreSql. Для этого необходимо получить доступ к терминалу ЦС. Далее необходимо выполнить:

```
pg_dump -d ids -U idsuser > [имя_файла_резервной копии]
```

Для восстановления из резервной копии необходимо в терминале ЦС надо выполнить:

```
psql ids < [имя_файла_резервной копии]
```

6. Оптимизация работы программы (комплекса)

Производительность СОА «ЗАСТАВА-IDS» зависит в основном от следующих факторов:

- оптимизация настройки;
- оптимизация базы сигнатур.

Оптимизация настройки сенсора заключается в правильном определении количества запускаемых экземпляров ПО Snort. Каждый экземпляр должен соответствовать одному ядру центрального процессора сервера. Для работы ОС необходимо оставить 1 - 2 ядра. Также ПО Snort потребляет до 1,5 Гбайт оперативной памяти (для количества правил обнаружения около 20 000), что необходимо учесть при конфигурировании.

Оптимизация базы сигнатур заключается в отключении правил, не актуальных для контролируемой сети.

7. Аварийные ситуации и способы их устранения

В таблице (см. Таблица 12) перечислены типичные аварийные ситуации СОА «ЗАСТАВА-IDS» и действия по их устранению.

Таблица 12 – Аварийные ситуации и способы их устранения

Аварийная ситуация	Способ устранения
Сенсор не работает. Сенсор запущен, но в КУ статус сенсора «N».	1. Убедиться в том, что сенсор доступен по сети. Для этого при помощи ssh установить соединение с сенсором. На сенсоре выполнить curl http://<адрес ЦС>:8080 В случае если соединение не установлено – проверить сетевые настройки сенсора и сетевого оборудования. В случае если соединение установлено: 2. Убедиться в том, что уникальный идентификатор сенсора совпадает с уникальным идентификатором сенсора в КУ. 3. Перезапустить сенсор при помощи КУ. Если сенсор не работает, 4. Вручную перезапустить сенсор.
Сенсор не запускается.	Проверить правильность настроек в конфигурационных файлах, в частности, правильность указания сетевых интерфейсов.
Сенсор работает. Атаки не регистрируются.	В настройках сенсора проверить параметр HOME_NET (см. файл Snort.conf), который должен совпадать с диапазоном адресов контролируемой сети. Проверить правильность подключения сенсора к контролируемой сети. Для этого на сетевом сенсоре отключить сенсор и при помощи утилиты tcpdump выполнить выборочный съём сетевого трафика на рабочих сетевых интерфейсах. Если сетевой трафик на интерфейсе отсутствует, проверить подключение сетевого сенсора.
Сенсор не работает.	Перезапустить сенсор через КУ.

ЦС не работает.	Убедиться в том, что есть сетевая связь с ЦС.
	На ЦС убедиться в том, что процесс tomcat присутствует. Перезапустить процесс:
	`/etc/init.d/tomcate restart`
	На ЦС убедиться в том, что процесс postgresql присутствует. Перезапустить процесс:
	`/etc/init.d/postgresql restart`

Перечень принятых терминов и сокращений

АО	Акционерное общество
ГЦМ	Главный центр мониторинга системы «СОПКА» ФСБ России
КУ	Консоль управления
ОЗУ	Оперативное запоминающее устройство
ОС	Операционная система
ПО	Программное обеспечение
Сенсор	Сетевой сенсор
СОА	Средство обнаружения атак
СУБД	Система управления базами данных
ФСБ России	Федеральная служба безопасности
ЦС	Центральный сервер

Лист регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (страниц) в документе	Номер документа	Входящий номер сопроводительного документа и дата	Подпись	Дата
	изме–ненных	заме–ненных	новых	изъя–тых					