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

СОВ ПАК «Плутон»

Руководство по установке и эксплуатации программного обеспечения

Листов 143

2016

АННОТАЦИЯ

Настоящий документ является руководством по установке и эксплуатации программных средств СОВ ПАК «Плутон», в том числе:

– «Сервер управления сенсорами» (далее по тексту – ПС «Сервер УС»);

– «АРМ управления сенсорами» (далее по тексту – ПС «АРМ УС»);

– «Сенсор» (далее по тексту – ПС «Сенсор»).

В документе рассмотрены назначение, условия выполнения программных средств. Приведена методика их установки, настройки и работы в программных модулях, типовые приемы работы и выдаваемые сообщения.

СОДЕРЖАНИЕ

1. УСТАНОВКА И НАСТРОЙКА ПС «СЕРВЕР УС»

1.1. Установка ПС «Сервер УС»

1.1.1. Среда установки

Установка ПС «Сервер УС» осуществляется на технические средства с установленной операционной системой Astra linux Special Edition «Смоленск» 1.5.

При установке ОС необходимо задать пароль учетной записи операционной системы «root», которая играет роль учетной записи привилегированного технологического пользователя в ПС «Сервер УС». Данная учетная запись используется только при технологических операциях по установке и диагностике ПО.

1.1.2. Установка ПС «Сервер УС»

Перед установкой необходимо выполнить следующие подготовительные операции с техническим средством (ТС), на которое устанавливается ПС «Сервер УС»:

– проверить правильность подключения клавиатуры и дисплея (KVM-панели) к ТС;

– в случае использования KVM-панели – переключить KVM-панель на взаимодействие с ТС;

– включить ТС;

– при отсутствии в составе ТС CD/DVD-привода – подключить переносной CD/DVD-привод к свободному USB-разъему ТС.

Поместить оптический диск с установочными пакетами ПС «Сервер управления сенсорами» в CD-привод.

Далее необходимо нажать на клавиатуре (KVM-панели) ТС комбинацию клавиш «Ctrl+Alt+F2» и на запрос операционной системы ввести имя и пароль привилегированного технологического пользователя «root».

Примечание – Привилегированный технологический пользователь «root» создается при установке операционной системы.

После ввода учетных данных привилегированного технологического пользователя будет предоставлен доступ к командной строке операционной системы, в которой необходимо выполнить команды:

1. Скопировать инсталляционные пакеты ПС СУС в локальный каталог /opt/debs. (см. Приложение Г. «Содержимое дистрибутива СОВ ПАК Плутон»).
2. Установить системные пакеты из репозитария Астры:
   >apt-get -y install libglib2.0 libssl-dev libboost-serialization1.55 \libboost-system1.55 libboost-thread1.55 libpq-dev libtool flex \postgresql-server-dev-9.4 postgresql-9.4 bison libdbi-dev libdbi-perl libdbd-pg-perl locales-all *qt4*
3. Установить пакеты ПС СУС:
   >cd /opt/debs/; for i in `ls -1 | egrep -v "(initsus\|deploy)"`; do dpkg -i $i >> debs.log 2>&1; done; dpkg -i initsus*.deb; dpkg -i depl*.deb
4. Настроить привязку динамических ссылок в ldconfig:
   >echo -e "/usr/local/KDAB/KDReports-1.4.0/lib\n
   /usr/local/lib\n
   /usr/lib/zo\n
   /usr/local/lib/pluto\n
   /usr/local/lib/pluto/observer" > /etc/ld.so.conf.d/sus.conf
   Ldconfig
5. Убедиться в наличие русской локализации и работоспособности сервиса БД PostgeSQL:
   >locale -a | grep "ru_RU.utf8"
   ru_RU.utf8
6. Проверить конфигурацию БД PostgeSQL:
   >service postgresql status
   9.4/main (port 5432): down
   >service postgresql start
   [ok] Starting PostgreSQL 9.4 database server: main.
7. Настроить и запустить сервис протоколирования событий:
   >chkconfig genericlogd on

>service genericlogd start

8. Сконфигурировать ПС СУС через оболочку tinyshell:

   >tinysh

   $set sus name <ИМЯ_СУС>

   $set sus postgrespassword <пароль_пользователя_PostgreSQL>

   $set sus scheduletime

   $sus commit

9. Проверить содержимое конфигурационного файла PostgreSQL:

   Пример содержимого конфигурационного файла PostgreSQL /etc/postgresql/9.4/main/pg_hba.conf:

   host sensors postgres 10.31.9.0/24 trust

   host sensors postgres 10.31.9.0/24 md5

   host sensors postgres 10.31.9.0/24 pam

10. Перезапустить PostgreSQL:

    >service postgresql restart

11. Запустить ПС СУС из оболочки tinyshell:

    >tinysh

    $sus start

12. Запустить компоненты ПС СУС через сервис:

    >service attacks-sectioning start

    >service serverp start

    >attackserver

    >sensorserver

13. Проверить работу ПС СУС:

    >netstat -lptn | egrep "(2323|6011)"

    tcp 0 0 0.0.0.0:60111 0.0.0.0:* LISTEN 26526/sensorserver

    tcp 0 0 0.0.0.0:60112 0.0.0.0:* LISTEN 26526/sensorserver

    tcp 0 0 0.0.0.0:60113 0.0.0.0:* LISTEN 26521/attackserver

    tcp 0 0 0.0.0.0:60114 0.0.0.0:* LISTEN 26521/attackserver

    tcp 0 0 0.0.0.0:2323 0.0.0.0:* LISTEN 26371/ServerConsole

>ps ax | grep attacks-sectioning

24773 pts/0 S 0:00 /bin/bash /usr/sbin/attacks-sectioning.sh

>cat /var/log/attacks-sectioning.log

BEGIN

psql:/tmp/pginithlpQ1pHSBqE:6: ЗАМЕЧАНИЕ: слияние столбца "id" с наследованным определением

CREATE TABLE

CREATE INDEX

CREATE INDEX

CREATE INDEX

CREATE INDEX

GRANT

GRANT

CREATE TABLE

GRANT

GRANT

COMMIT

14. По завершении установки необходимо перезагрузить систему командой:

reboot

Внимание! Выполнение перезагрузки после установки обязательно, в противном случае корректная настройка и запуск ПС «Сервер УС» будут невозможны.

После перезагрузки следует:

– нажать на клавиатуре (KVM-панели) ТС комбинацию клавиш «Ctrl+Alt+F2»;

– ввести рабочее имя и пароль технологического пользователя (заводская установка – «admin»/«admin»), после чего будет произведен вход в командную среду технологического пользователя, предоставляющую доступ к технологическим

возможностям ПС «Сервер УС»;

– изменить пароль технологического пользователя (правила формирования паролей определяются действующим на объекте эксплуатации порядком), для чего в командной среде технологического пользователя выполнить команду:

```
user passwd admin
```

– в ответ на запрос системы дважды ввести новый пароль;

– при необходимости создать одного или несколько дополнительных технологических пользователей, выполнив команду:

```
user add <имя_пользователя>
```

– занести учетные данные технологического пользователя(-ей) в документ учета, предусмотренный действующим на объекте эксплуатации порядком учета паролей (если предусмотрено);

– выполнить настройку программных средств согласно п. 3.1.3;

– завершить сеанс работы, для чего на клавиатуре KVM-панели нажать комбинацию клавиш «Ctrl+D».

1.1.3. Настройка ПС «Сервер УС»

Действия по настройке ПС «Сервер УС» выполняются в специальной командной среде, предоставляемой для этих целей программным средством. Процедура входа в командную среду описана в п. 3.4.

Для выполнения настройки ПС «Сервер УС» следует выполнить в командной среде команды:

```
sus stop
set sus
```

Произойдет переход в режим изменения конфигурационных параметров ПС.

Далее необходимо установить конфигурационные параметры, выполнив команды установки параметров:

```
name <имя сервера УС в иерархической модели подчинения>
sendinterface <имя сетевого интерфейса, посредством  которого
осуществляется взаимодействие с АРМ>
sendinterfaceip <IP-адрес, назначаемый сетевому интерфейсу
взаимодействия с АРМ>
sendnetmask <маска подсети, посредством  которой осуществляется
взаимодействие с АРМ>
```

```
receiveinterface <имя сетевого интерфейса, посредством  которого
осуществляется взаимодействие с сенсорами>
receiveinterfaceip <IP-адрес, назначаемый сетевому интерфейсу
взаимодействия с сенсорами>
recvnetmask <маска подсети, посредством  которой осуществляется
взаимодействие с сенсорами>
scheduletime 1
susport 2323
emailsend disable
selftestinterval <интервал автоматизированного самотестирования
СУС в мин.>
longitude <географическая долгота размещения СУС>
latitude <географическая широта размещения СУС>
postgrespassword <пароль пользователя postgres>
subnetdbusers <подсеть, для которой разрешены соединения с БД, в
формате "10.10.1.0/24">
```

Пароль пользователя postgres должен содержать более 8 символов, заглавные и строчные буквы и цифры.

Если ПС «Сервер УС» должно функционировать на подчиненном уровне иерархической модели подчинения, то следует дополнительно настроить параметры:

```
hierarchyport 2323
hierarchyserverip <IP вышестоящего сервера УС>
```

По окончании внесения изменений следует выйти из режима изменения конфигурационных параметров нажатием комбинации клавиш Ctrl+D.

Для того чтобы измененные параметры вступили в силу, необходимо применить сделанные изменения и запустить ПО, выполнив команды:

```
sus commit
sus start
```

Значения всех конфигурационных параметров ПС «Сервер УС» и примеры их задания приведены в таблице 2.

Таблица 2 – Конфигурационные параметры ПС «Сервер УС»

Параметр	Пример	Значение параметра
`name <строка>`	`name TP-SUS-1`	Символьное имя сервера УС в иерархической модели подчинения
`sendinterface <iface>`	`sendinterface eth1`	Имя сетевого интерфейса ПС «Сервер УС», посредством которого производится обмен данными с ПТК «АРМ УС»

sendinterfaceip <IP>	sendinterfaceip 10.10.1.3	IP-адрес ПС «Сервер УС», посредством которого производится обмен данными с ПТК «АРМ УС»
sendnetmask <netmask>	sendnetmask 255.255.0.0 sendnetmask 16	Маска подсети для сети передачи данных, соединяющей ПС «Сервер УС» и ПТК «АРМ УС»
receiveinterface <iface>	receiveinterface eth0	Имя сетевого интерфейса ПС «Сервер УС», посредством которого производится обмен данными с ПТК «Сенсор»
receiveinterfaceip <IP>	receiveinterfaceip 10.10.1.8	IP-адрес, назначаемый сетевому интерфейсу ПС «Сервер УС», посредством которого производится обмен данными с ПТК «Сенсор»
recvnetmask <netmask>	recvnetmask 255.255.0.0 recvnetmask 16	Маска подсети для сети передачи данных, соединяющей ПС «Сервер УС» и ПТК «Сенсор»
scheduletime <sec>	scheduletime 1	Интервал работы планировщика СУС (в сек.)
susport <port>	susport 2323	Номер TCP-порта на ПТК «Сервер УС» для обмена сообщениями о событиях информационной безопасности; стандартное значение – 2323
emailsend <enable|disable>	emailsend disable	Разрешает/запрещает использование механизма почтового оповещения
emailconfigpath <path>	emailconfigpath /path/to/file	Путь к файлу настроек механизма почтового оповещения (настройки механизма почтового оповещения задаются командами `set mail`)
emailinterval <min>	emailinterval 10	Минимальный интервал рассылки почтовых оповещений (в мин.)
selftestinterval <min>	selftestinterval 1	Интервал автоматизированного самотестирования СУС (в мин.)
longitude <degree>	longitude 56.6	Географическая долгота размещения СУС
latitude <degree>	latitude 60.1	Географическая широта размещения СУС
postgrespassword <passwd>	postgrespassword GHXg7EDz23vg	Пароль системного пользователя БД
subnetdbusers <ip>/<mask>	subnetdbusers 127.0.0.1/32	Подсеть, для которой разрешены соединения с БД

sensorRepositorySourceName <name>	sensorRepositorySourceName <name>	Имя или ip сервера БД сенсоров (стандартное значение - 127.0.0.1)
sensorRepositoryDatabaseName <dbname>	sensorRepositoryDatabaseName <dbname>	Имя БД сенсоров (стандартное значение - sensors)
sensorRepositoryUserName <username>	sensorRepositoryUserName <username>	Имя пользователя БД сенсоров (стандартное значение - postgres)
sensorRepositoryUserPassword <passwd>	sensorRepositoryUserPassword <passwd>	Пароль пользователя БД сенсоров (стандартное значение совпадает со значением параметра postgrespassword)
geoInfoSourceName <name>	geoInfoSourceName <name>	Имя или ip сервера БД геоданных (стандартное значение - 127.0.0.1)
geoInfoDatabaseName <dbname>	geoInfoDatabaseName <dbname>	Имя БД геоданных (стандартное значение - sensors)
geoInfoUserName <username>	geoInfoUserName <username>	Имя пользователя БД геоданных (стандартное значение - postgres)
geoInfoUserPassword <passwd>	geoInfoUserPassword <passwd>	Пароль пользователя БД геоданных (стандартное значение совпадает со значением параметра postgrespassword)

При наличии возможности использования механизма оповещений о критичных событиях ИБ по email следует также настроить параметры таких оповещений, для чего выполнить команды:

```
set sus emailconfigpath <путь к файлу настроек email-оповещений>
set sus emailinterval <интервал почтового оповещения в мин.>
set mail
```

Произойдет переход в режим изменения настроек отправки сообщений по email.

Далее необходимо выполнить команды установки значений настроек рассылки оповещений:

```
subject <тема письма>
sendername <имя отправителя>
expeditor <email-адрес отправителя>
recipients <email-адрес получателя 1>,<email-адрес получателя
2>,…,<email-адрес получателя N>
textmessage <постоянный текст, вставляемый в каждое письмо>
smtpserver <ip-адрес smtp-сервера>
```

```
smtpport <TCP-порт smtp-сервера>
authuser <имя пользователя для авторизации на smtp-сервере>
authpasswd <пароль пользователя для авторизации на smtp-сервере>
pathconfig <путь к файлу с настройками email-оповещений>
```

Значение параметра pathconfig должно соответствовать значению, заданному командой set sus emailconfigpath.

По окончании внесения изменений следует выйти из режима изменения настроек оповещений по email нажатием комбинации клавиш Ctrl+D и применить применить сделанные изменения, выполнив команды:

```
sus mailcommit
sus commit
```

1.2. Запуск и остановка ПС «Сервер УС»

Запуск и останов ПС «Сервер УС» выполняется в автоматическом режиме в процессе запуска и останова операционной системы.

Для запуска ПС без перезапуска ОС необходимо в специальной командной среде ПС «Сервер УС» выполнить команду (процедура входа в специальной командную среду описана в п. 3.4):

```
sus start
```

Для останова ПС без останова ОС необходимо в специальной командной среде ПС «Сервер УС» выполнить команду:

```
sus stop
```

1.3. Просмотр электронных журналов регистрации событий

По команде администратора безопасности СОВ поддерживается возможность экспорта электронных журналов в ПС «АРМ управления сенсорами», при этом каждый журнал сопровождается его контрольной суммой. По результатам экспорта журнал очищается, а первой записью нового журнала ПС «Сервер УС» производит запись об его отчуждении с указанием контрольной суммы. ПС «АРМ управления сенсорами» позволяет проводить аудит записей ЭЖР посредством графического интерфейса с поддержкой поиска, сортировки и фильтрации записей.

При настройке ПС «Сервер УС» для просмотра записей ЭЖР также может применяться специальная командная среда, предоставляющая доступ к

возможностям диагностики и настройки ПС «Сервер УС». Процедура входа в командную среду описана в п. 3.4.

Для просмотра электронных журналов ПС «Сервер УС» следует выполнить в командной среде команды:

```
show log system
show log action
show log secure
```

Чтение записей ЭЖР пользователем или иными программными средствами, кроме как путем отчуждения электронного журнала и проведения аудита с помощью ПС «АРМ управления сенсорами» или посредством специальной командной среды, не предусматривается.

1.4. Использование специальной командной среды

Для начальной настройки, проверки и восстановления работоспособности ПО ПС «Сервер УС» используется специальная командная среда, предоставляющая доступ к возможностям диагностики и настройки ПС «Сервер УС».

Список всех команд, доступных из командной среды ПС «Сервер УС», с указанием выполняемых командами действий и примерами использования приведен в приложении А к настоящему руководству.

1.4.1. Вход в командную среду ПС «Сервер УС»

Чтобы войти в командную среду ПС «Сервер УС» с локальной консоли (KVM-панели), необходимо:

– нажать на клавиатуре (KVM-панели) комбинацию клавиш «Ctrl+Alt+F2», на экране появится запрос на ввод рабочего имени и пароля пользователя;

– ввести имя и пароль технологического пользователя «admin».

Чтобы войти в командную среду ПС «Сервер УС» по сети с удаленного узла (при наличии такой возможности), необходимо на удаленном узле, функционирующем под управлением операционной системы Astra linux Special Edition «Смоленск» 1.5, выполнить команду:

```
ssh <ip-адрес изделия>
```

где в качестве параметра <ip-адрес изделия> задать ip-адрес ПС «Сервер УС». В ответ на запрос необходимо ввести имя и пароль технологического пользователя «admin».

П р и м е ч а н и е – Технологический пользователь «admin» автоматически создается при установке ПО. Пароль технологического пользователя должен быть установлен в процессе наладочных работ (настройка по умолчанию - «admin»). Также в процессе подготовки ПС «Сервер УС» к использованию могут быть заведены дополнительные учетные записи технологических пользователей.

1.4.2. Выполнение команд

Для выполнения команды можно либо набрать ее на клавиатуре полностью, либо набрать несколько первых символов команды и нажать клавишу «Tab». Если набранным первым символам соответствует несколько команд, будет выведена подсказка с возможными вариантами, после чего можно откорректировать набранную команду. Если набранным первым символам соответствует одна команда, введенное начало команды в строке ввода автоматически будет дополнено недостающими символами.

Большинство команд требует задания одного или нескольких параметров. Для просмотра списка требуемых параметров после набора команды также можно нажать клавишу «Tab» для вывода необходимых параметров команды. Если команда требует параметр, значение которого выбирается из списка, по нажатию клавиши «Tab» будет выведен список возможных значений параметра. Для вывода подсказки, поясняющей действие, выполняемое командой, необходимо после набора команды набрать на клавиатуре символ «?».

Для выполнения набранной команды следует нажать клавишу «Enter».

Команды, выполняющие логически связанные действия, логически объединяются в группы. Команды в группе начинаются с одного и того же слова или нескольких слов. Это позволяет выполнять нескольких команд одной группы, не набирая каждую из них полностью: достаточно ввести общие начальные слова для группы команд и нажать клавишу «Enter», в результате чего произойдет переход в режим выполнения команд данной группы. В этом режиме требуется вводить

только завершающую часть команд, опуская общее для группы команд начало. Для возврата из режима выполнения команд той или иной группы в режим ввода команд полностью следует нажать комбинацию клавиш «Ctrl+D».

Например, для установки параметров ПС можно последовательно выполнить команды:

```
set sus hierarchyport 2323
set sus hierarchyserverip 10.10.0.16
```

К тому же результату приведет выполнение последовательности команд (после выполнения последней команды следует нажать комбинацию клавиш «Ctrl+D»):

```
set sus
hierarchyport 2323
hierarchyserverip 10.10.0.16
```

Если выводимые в результате выполнения команды сообщения не помещаются на экране, для прокрутки экрана можно использовать комбинации клавиш «Shift+PageUp» и «Shift+PageDown».

Для повторного заполнения строки ввода ранее выполненной командой используются клавиши «↑» и «↓».

Для завершения сеанса работы в командной среде ПС «Сервер УС» следует нажать комбинацию клавиш «Ctrl+D».

1.5. Проверка программы

Для проверки основных функций ПС «Сервер УС», а также корректности его настройки, предусмотрена операция проведения самотестирования следующими способами:

– обязательное прохождение самотестирования при старте ПС «Сервер УС»;

– периодическое выполнение самотестирования ПС «Сервер УС» через заданный интервал времени (интервал задается при настройке ПС «Сервер УС»);

– выполнение самотестирования по команде оператора СОВ ПАК «Плутон», подаваемой посредством ПС «АРМ УС».

Результаты самотестирования, проводимого при запуске ПС, и периодического самотестирования фиксируются в электронном журнале

регистрации событий ПС «Сервер УС». Результаты самотестирования, выполняемого по команде оператора СОВ ПАК «Плутон», отображаются оператору в графическом интерфейсе ПС «АРМ УС», а также фиксируются в электронном журнале регистрации событий ПС «Сервер УС».

В процессе самотестирования ПС «Сервер УС» производятся следующие проверки:

1) проверка контрольной суммы дистрибутива;
2) проверка системы журналирования;
3) контроль подключения к базе данных (авторизация администратора системы обнаружения вторжений).

По результатам проверок выводятся сообщения вида:

```
Результат контроля целостности:
/usr/sbin/ServerConsole = Успех
Результат проверки журналирования = Успех
Результат контроля авторизации администратора СОВ =
Успех
```

1.6. Дополнительные возможности

Использование функций ПС «Сервер УС» оператором производится посредством ПС «АРМ УС». Действия оператора, предусмотренные для использования функций ПС «Сервер УС», описаны в руководстве пользователя ПС «АРМ УС».

При начальной настройке, проверке и восстановлении работоспособности ПС «Сервер УС» также может использоваться специальная командная среда, предоставляющая доступ к возможностям диагностики и настройки ПС «Сервер УС». Порядок входа в специальную командную среду и её использования определен в п. 3.4 настоящего руководства.

Список всех команд, доступных из командной среды ПС «Сервер УС», с указанием выполняемых командами действий и примерами использования приведен в приложении А к настоящему руководству.

Взаимодействие оператора с ПС «Сервер УС», кроме как посредством ПС «АРМ УС» или специальной командной среды, не предусматривается.

1.7. Сообщения системному администратору

При возникновении проблем в процессе функционирования ПС «Сервер УС» диагностические сообщения выводятся в три файла /var/log/logaction, /var/log/logsecure и /var/log/logsystem.

Основные сообщения представлены в Таблица 1.

Таблица 1. Диагностические сообщения

Сообщение ОС	Значение	Файл
[000363] 16330:ServerConsole	Результат контроля целостности: /usr/sbin/ServerConsole=Успех Результат проверки системы журналирования=Успех Результат контроля авторизации администратора СОВ=Успех	/var/log/logsecure
[000367] 16330:ServerConsole	Результат контроля целостности: /usr/sbin/ServerConsole=Успех Результат проверки системы журналирования=Успех Результат контроля авторизации	/var/log/logsecure

	администратора СОВ=Неудача	
[000143] 16330:ServerConsole	Получена команда самотестирования СУС	/var/log/logaction
[000162] 16330:ServerConsole	Получена команда самотестирования сенсора с УИС 5	/var/log/logaction
[000155] 16330:ServerConsole	Получена команда настройки стат. анализатора	/var/log/logaction
[000172] 16330:ServerConsole	Команда настройки стат. анализатора завершена успешно	/var/log/logaction
[000170] 16330:ServerConsole	Получена команда обновления правил на сенсоре Плутон	/var/log/logaction
[000136] 16330:ServerConsole	Получена команда очистки таблиц БД	/var/log/logaction
[000153] 16330:ServerConsole	Команда очистки таблиц БД завершена успешно	/var/log/logaction
[000198] 16254:ServerConsole	Параметры доступа к БД заданы не полностью. Запустите программу InitDB_P	/var/log/logsystem
[000082] 16254:ServerConsole	LOGCMDOPEN	/var/log/logsystem
[000239] 16272:ServerConsole	Некорректно задано время фиксации атак. Перенастройте параметры	/var/log/logsystem

	в конфигурационном файле	
[000267] 16294:ServerConsole	Некорректно задано время проверки наличия файлов атак. Перенастройте параметры в конфигурационном файле	/var/log/logsystem
[000253] 16312:ServerConsole	Некорректно задано время запуска планировщика. Перенастройте параметры в конфигурационном файле	/var/log/logsystem
[000134] 16330:ServerConsole	Оповещение по почте не подключено	/var/log/logsystem
[000099] 16330:ServerConsole	Сервер запущен	/var/log/logsystem
[000132] 16330:ServerConsole	Проверка системы журналирования	/var/log/logsystem
[000131] 16330:ServerConsole]	Соединение с СУБД восстановлено	/var/log/logsystem

2. УСТАНОВКА И НАСТРОЙКА ПС «АРМ УС»

2.1. Установка ПС «АРМ УС»

ПС «АРМ УС» работоспособно на ЭВМ с ОС Astra linux Special Edition «Смоленск» 1.5. Установку и настройку ОС Astra linux Special Edition «Смоленск» 1.5 необходимо произвести в соответствии с эксплуатационным документом на ОС.

Перед началом работы с ПС «АРМ УС» необходимо произвести установку и настройку программных модулей входящих в состав ПС «АРМ УС».

Для выполнения установки ПС «АРМ УС» следует поместить оптический диск с установочными пакетами ПС «АРМ УС» в CD/DVD-привод.

Далее необходимо нажать на клавиатуре (KVM-панели) ТС комбинацию клавиш «Ctrl+Alt+F2» и на запрос операционной системы ввести имя и пароль привилегированного технологического пользователя «root».

Примечание – Привилегированный технологический пользователь «root» создается при установке операционной системы.

После ввода учетных данных привилегированного технологического пользователя будет предоставлен доступ к командной строке операционной системы, в которой необходимо выполнить:

1. Скопировать инсталляционные пакеты ПС АРМ УС в локальный каталог /opt/debs. (см. Приложение Г. «Содержимое дистрибутива СОВ ПАК Плутон»).
2. Установить системные пакеты из репозитария Астры:
   >apt-get -y install libglib2.0 libssl-dev libboost-serialization1.55 \
   libboost-system1.55 libboost-thread1.55 libpq-dev fly* libtool flex liblzo2-dev \
   libdbi-dev libdbi-perl libdbd-pg-perl bison *qt4* locales-all libphonon-dev
3. Установить пакеты ПС АРМ УС
   >dpkg -i /opt/debs/*.deb
4. Настроить привязку динамических ссылок в ldconfig:
   >echo -e "/usr/local/KDAB/KDReports-1.4.0/lib\n
   /usr/local/lib\n
   /usr/local/lib/marble/plugins\n

/usr/lib/zo\n

/usr/local/lib/pluto\n

/usr/local/lib/pluto/observer\n

/usr/lib/x86_64-linux-gnu/qt4/plugins/designer" > /etc/ld.so.conf.d/ARM.conf

ldconfig

5. Настроить и запустить службы протоколирования событий:

   >chkconfig genericlogd on

   >service genericlogd start

6. Запустить графическую утилиту настройки ПС АРМ УС:

   >InitARM

Примечание – в случае ошибок в работе утилиты требуется удалить файл /usr/share/zo/etc/shadow.conf.

7. Запустить приложение SensorControlGUIClient:

   >export QT_GRAPHICSSYSTEM=native

   >SensorControlGUIClient

Примечание – приложение SensorControlGUIClient запускается только из под обычного пользователя (запуск из под root не допускается).

8. По завершении установки необходимо перезагрузить систему командой:

   reboot

2.2. Настройка ПС «АРМ УС»

Настройка ПС «АРМ УС» заключается в проведении следующих работ:

– настройка доступа к БД;

– регистрация сенсоров.

2.2.1. Настройка доступа к БД

Для настройки доступа к БД необходимо выполнить вход в систему под учетной записью администратора root и выполнить команду:

```
# InitARM
```

Далее в появившемся окне (рис. 1) задать параметры БД и нажать кнопку [Принять].

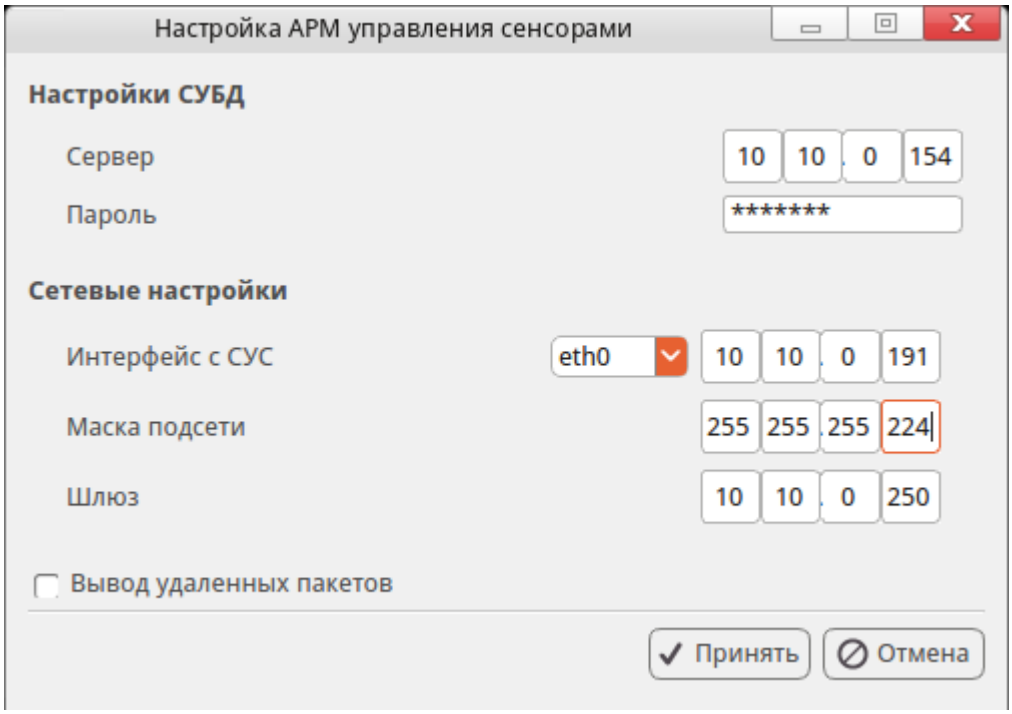


Рис. 1. Настройка доступа к БД

2.2.2. Регистрация сенсоров

Регистрация сенсоров производится с помощью ПМ «Консоль сетевого управления ПС «Сенсор». Работа с ПМ «Консоль сетевого управления ПС «Сенсор» описана ниже.

2.3. ПМ «Консоль сетевого управления ПС «Сенсор»

Для запуска ПМ «Консоль сетевого управления ПС «Сенсор» необходимо запустить терминал, ввести команду:

```
$ SensorControlGUIClient
```

После завершения ввода команды нажать клавишу **[Enter]**. В открывшемся окне (рис. 2) следует ввести имя и пароль пользователя.

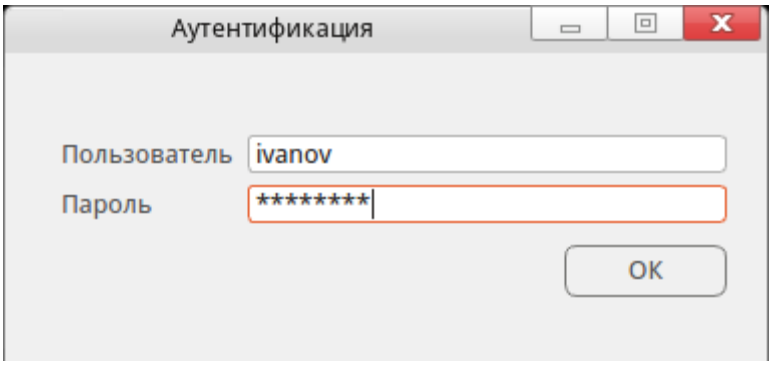


Рис. 2 – Ввод учетных данных пользователя.

После запуска программы появится главное окно системы управления сенсорами (рис. 3).

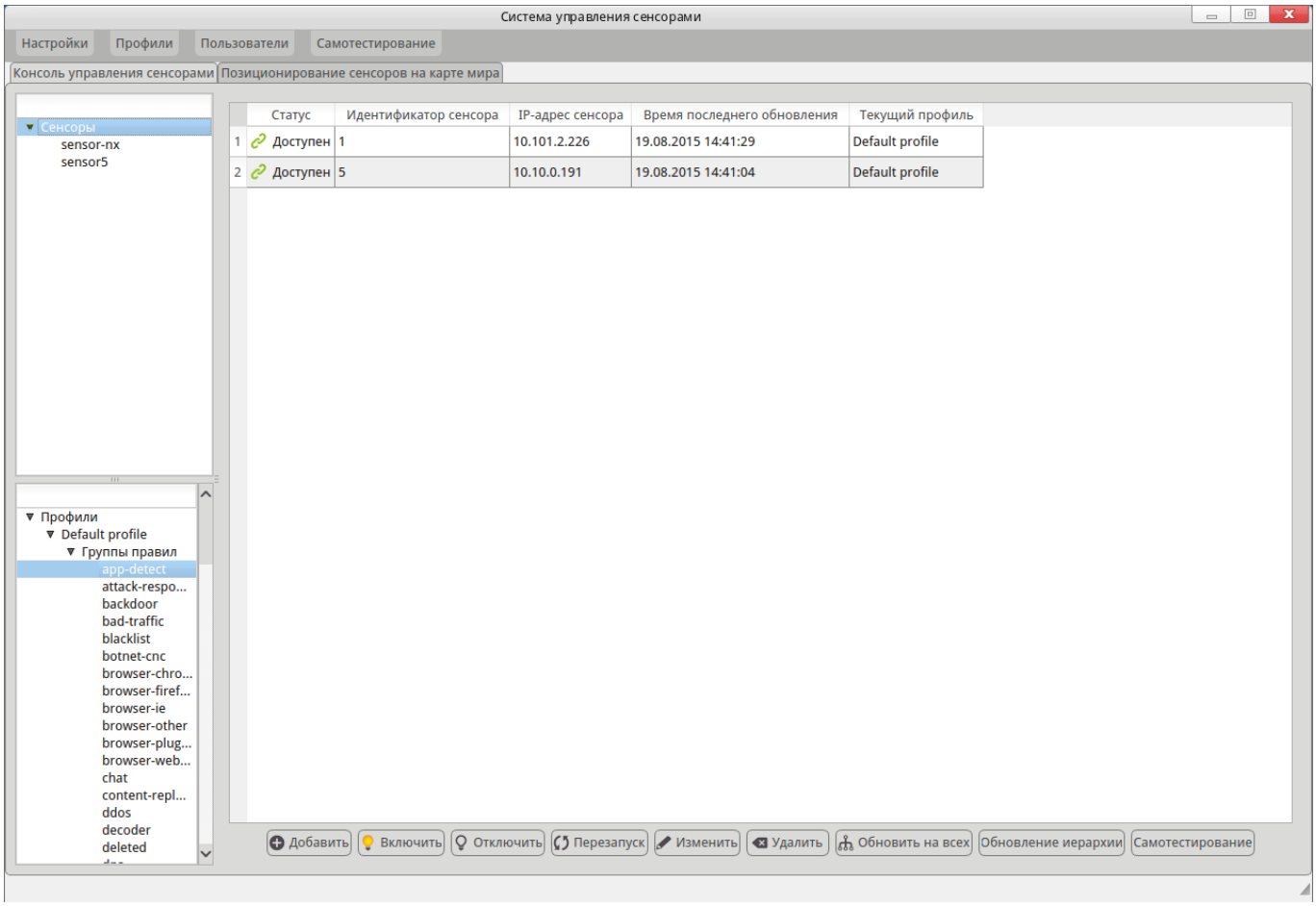


Рис. 3. Главное окно системы управления сенсорами

В главном окно системы управления сенсорами следует выделить следующие экранные области:

область «Сенсоры» - служит для вывода списка зарегистрированных сенсоров;

– область «Профили» - служит для вывода списка профилей и правил;

– основная область вывода информации.

2.3.1. Добавление субъекта федерации

Прежде чем создать новый сенсор необходимо создать субъект федерации. Для добавления менеджера субъекта федерации, в главном меню выбрать пункт «Настройки» > «Менеджер субъекта федерации» появится основное окно менеджера субъекта федерации.

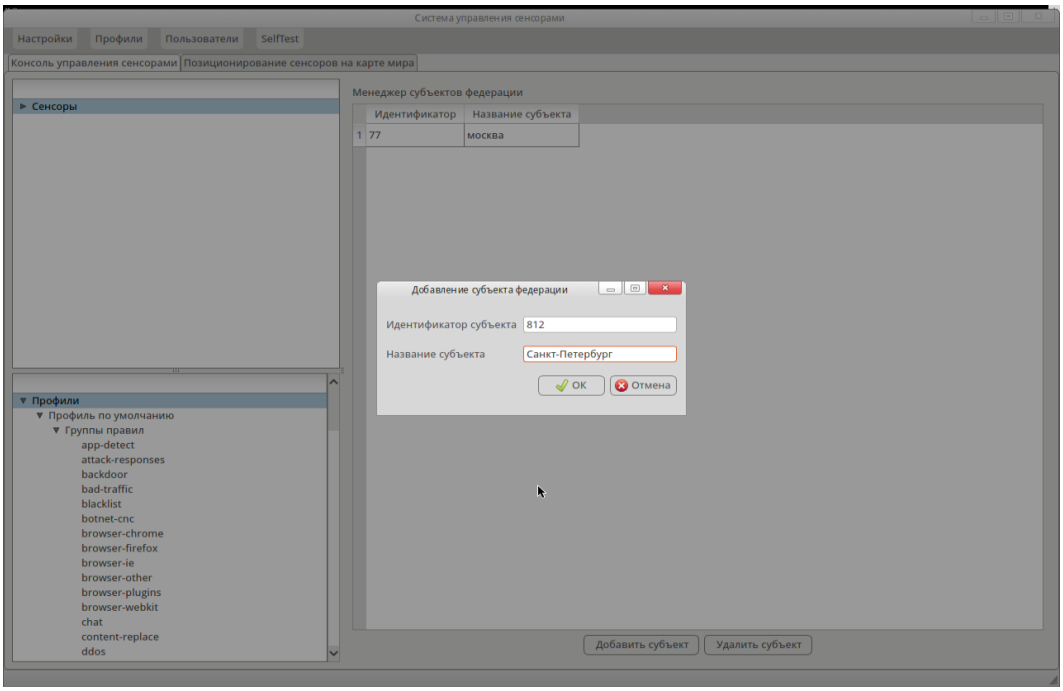


Рис. 4. Окно добавления субъекта федерации

Для добавления нового менеджера субъекта федерации необходимо нажать кнопку [`Добавить субъект`], после чего появится диалоговое окно «Добавление субъекта федерации» (рис. 4), где следует заполнить следующие поля:

– Идентификатор субъекта;

– Название субъекта.

Для подтверждения добавления субъекта федерации нажать кнопку [`OK`], новый менеджер субъекта федерации появится в основном окне консоли.

2.3.2. Добавление и редактирование данных о сенсорах

В процессе эксплуатации (или настройки) системы СОВ ПАК «Плутон» возникает необходимость в подключении к системе новых сенсоров или редактирования настроек подключения уже работающих сенсоров.

Для добавления сенсоров необходимо выделить поле «Сенсоры» в соответствующей области и нажать кнопку [Добавить]. В открывшемся окне следует ввести данные по необходимому сенсору, по окончании ввода нажать [ОК] рис. 5.

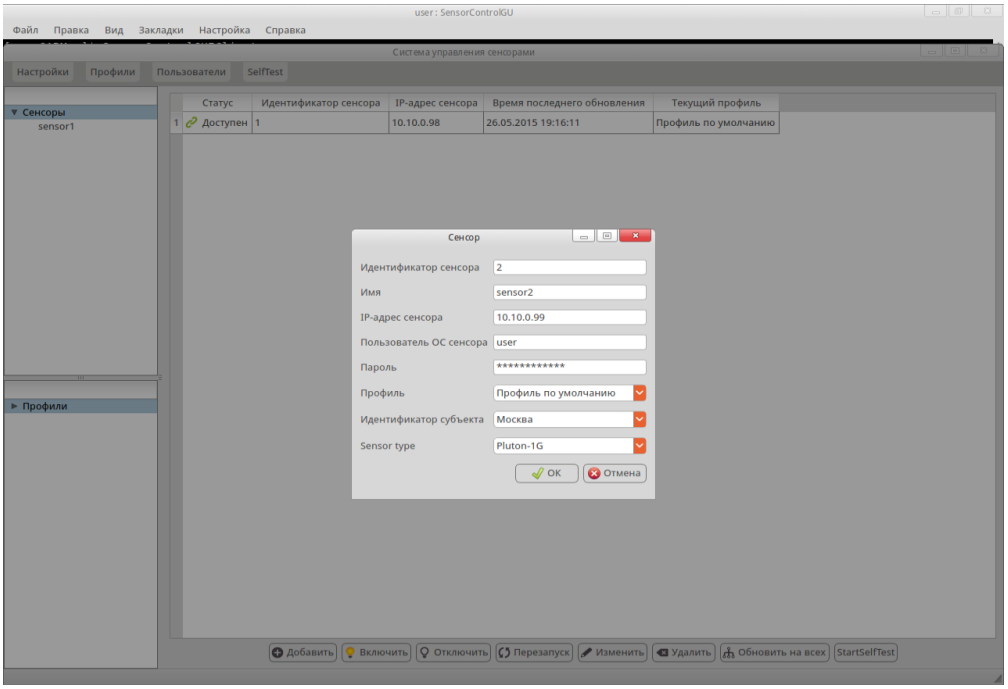


Рис. 5. Окно добавления сенсоров

При добавлении сенсоров в обязательном порядке, необходимо заполнить следующие поля:

– идентификатор сенсора – должен соответствовать идентификатору, который был установлен в подключаемом сенсоре;

– имя – должно соответствовать имени, которое было установлено в подключаемом сенсоре;

– IP-адрес сенсора – соответственно IP-адрес подключаемого сенсора;

– пользователя ОС сенсора – логин пользователя ОС на подключаемом сервере;

– пароль - пароль пользователя ОС на подключаемом сервере;

– профиль – необходимо выбрать из списка необходимый профиль, по умолчанию будет установлен «Профиль по умолчанию»;

– идентификатор субъекта – необходимо выбрать идентификатор субъекта;

– тип сенсора – необходимо выбрать нужный тип сенсора.

При успешном выполнении операции добавления сенсора он отобразиться в области отображения информации.

Примечание – следует внимательно вводить данные о сенсорах, они должны строго соответствовать тем данным, которые был введены при установке ПТК «Сенсор».

Для редактирования данных о сенсоре необходимо выделить нужный сенсор и нажать кнопку [Изменить], при этом откроется окно данных о сенсоре (рис. 5).

Панель управления сенсорами (рис. 6) позволяет выполнить следующие функции:

– кнопка [Добавить] - добавление сенсора в БД (см. п. 4.2);

– кнопки [Включить] и [Отключить] – соответственно включение и отключение сенсора;

– кнопка [Перезапуск] - перезапуск сенсора (при этом на сенсоре перезапуститься только СПО сенсора);

– кнопка [Изменить] - изменение данных по сенсору (см. п. 4.2);

– кнопка [Удалить] - удаление сенсора из БД;

– кнопка [Обновить на всех] - обновление правил на всех сенсорах одновременно (см. п. 4.3);

– кнопка [Самотестирование] - запуск самотестирования сенсора (см. п. 4.9);

– кнопка [Обновление иерархии] - запуск обновления базы решающих правил на нижестоящих серверах управления сенсорами в иерархической модели подчинения.

Рис. 6. Панель управления сенсорами

При нажатии кнопки [Обновление иерархии] необходимо выбрать профиль, содержащий решающие правила, которые будут отправлены на нижестоящие серверы управления сенсорами (рис. 7).

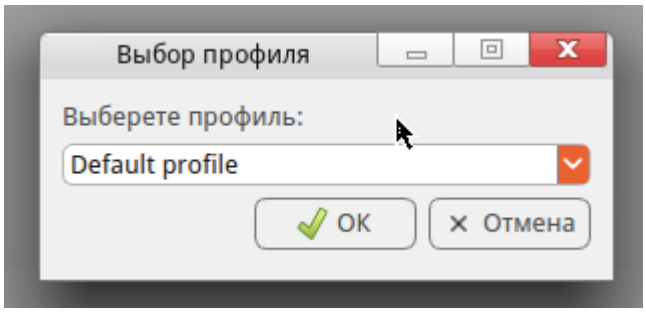


Рис. 7. Выбор профиля при обновлении базы решающих правил в иерархической структуре

2.3.3. Добавление и редактирование профилей и правил

Для организации автоматизированного обновления базы решающих правил используется понятие профилей. Профиль включает в себя определенную конфигурацию решающих правил.

Информация о профилях, содержащихся в них решающих правилах, и сведения о соответствии сенсоров и профилей хранятся в базе данных системы управления.

С помощью профилей решается задача обновления базы решающих правил на выбранных сенсорах системы обнаружения атак. Обновление базы решающих правил на сенсорах происходит путем назначения сенсору соответствующего профиля. Также имеется возможность создания профилей на базе уже существующих.

Для работы с профилями, в меню «Профили» доступны следующие пункты меню окна:

– «Добавить профиль» - создание нового профиля;

– «Загрузить новый профиль по умолчанию (из архива tar.gz)» - загрузка профиля по умолчанию;

– «Найти правило» - поиск правила;

– «Загрузить новый профиль по умолчанию (из файла)» - загрузка профиля из файла (рис. 8).

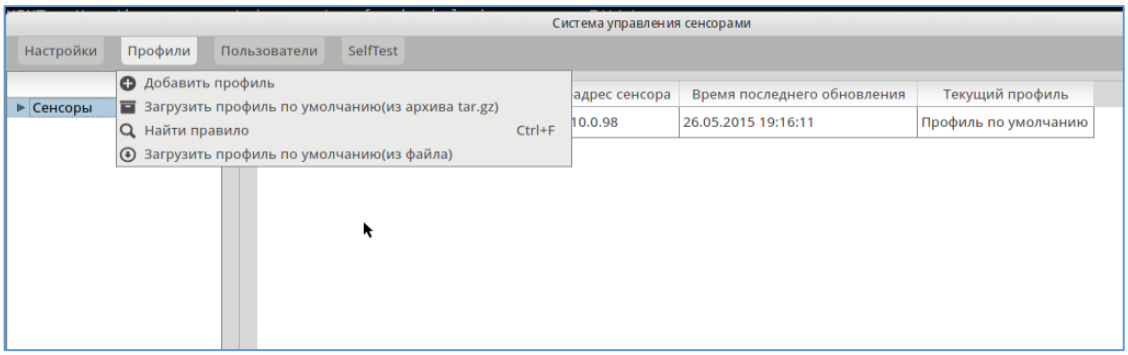


Рис. 8. Работа с профилями

Для первоначальной загрузки профиля решающих правил, в главном меню выбрать пункт «Профили» > «Загрузить новый профиль по умолчанию (из архива tar.gz)», при этом появится диалоговое окно выбора файла «Открыть файл с архивом правил». После выбора необходимого файла (с архивом правил формата совместимого с ПС «Сенсор») и нажатия кнопки [**Open**] будет проведена загрузка правил в профиль «Профиль по умолчанию». В основном окне, представлена информация о профилях и правилах, входящих в профили, с группировкой по их типам (рис. 9).

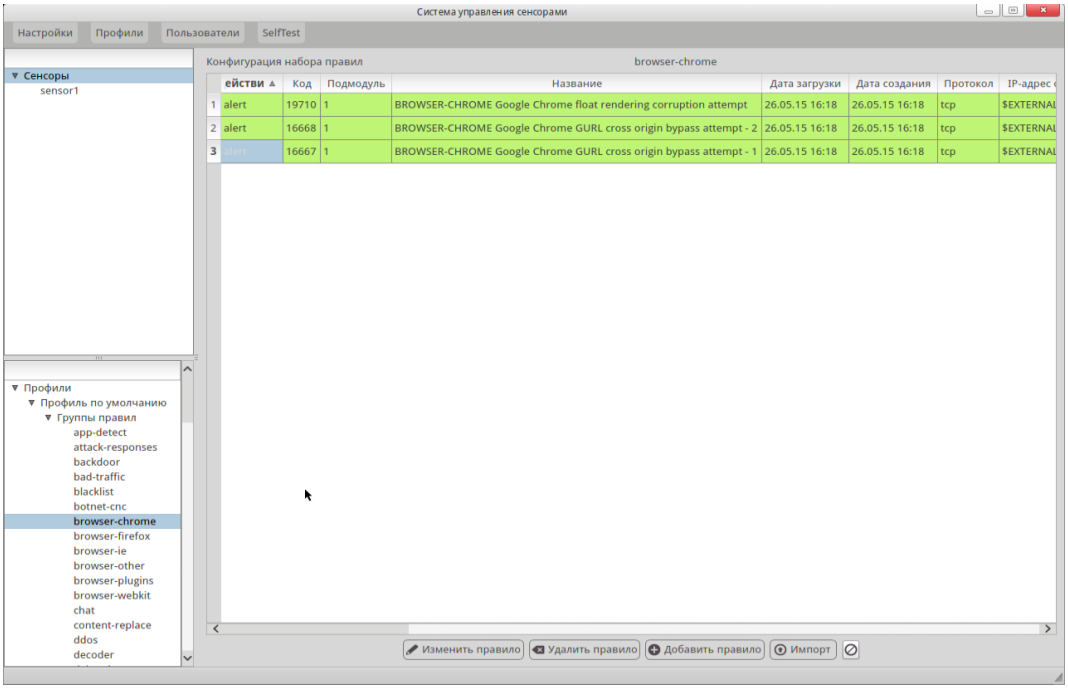


Рис. 9. Окно выбора группы правил в профиле

Выбор необходимого профиля и группы правил осуществляется в области «Профиль» (рис. 9), при этом при выборе необходимого профиля, в области

«Конфигурация набора правил» будут перечислены правила выбранной группы данного профиля. Для просмотра или изменения параметров правила необходимо выбрать соответствующее правило и нажать кнопку [Изменить правило], при этом появиться окно редактирования правила (рис. 10). В окне редактирования правила можно посмотреть и изменить параметры правила, входящие в профиль. Правила имеют следующий набор параметров:

– Имя;
– Действие;
– Протокол;
– Приоритет;
– IP-адрес отправителя;
– Порт отправителя;
– Направление;
– IP-адрес получателя;
– Порт получателя;
– Опции правила.

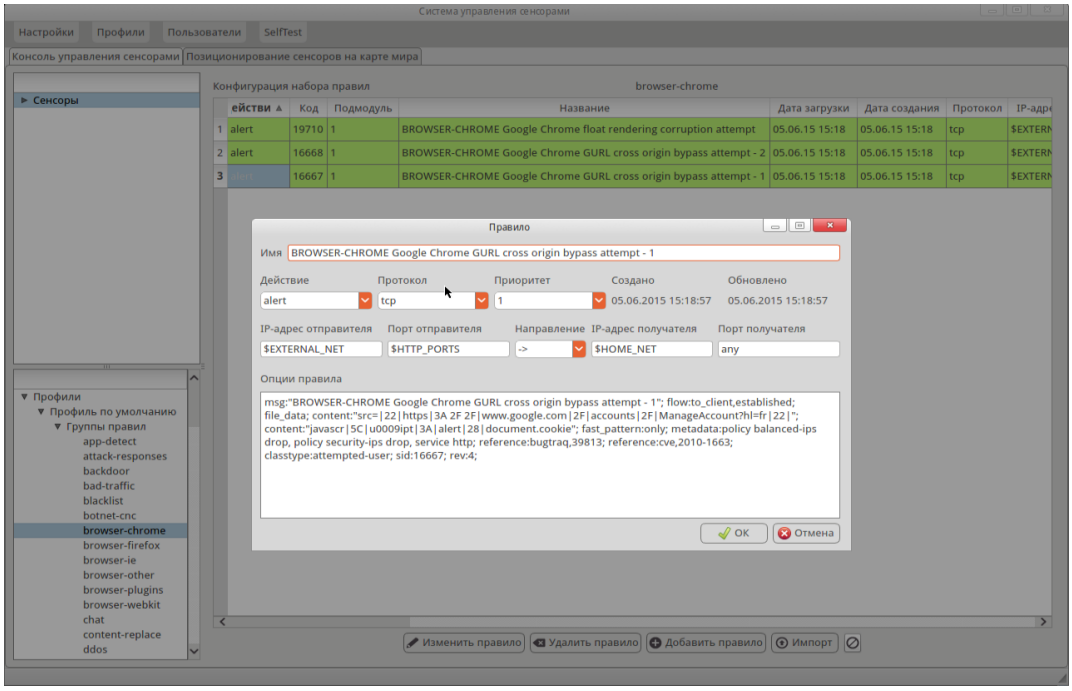


Рис. 10. Окно редактирования правила

Для сохранения изменений в правиле нажать кнопку [OK].

Для добавления новых правил в профиль необходимо нажать кнопку

[Добавить правило], появится окно «Правило», где следует заполнить соответствующие поля для нового правила (рис. 11).

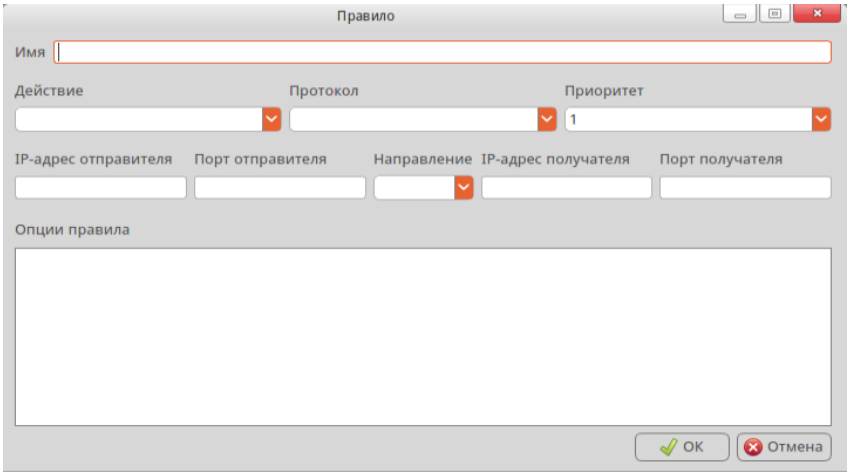


Рис. 11. Добавление правила

Для подтверждения добавления правила нажать кнопку [OK].

Для удаления правила нажать кнопку [Удалить правило].

Для массового добавления новых правил в профиль из файла необходимо нажать кнопку [Импорт], появится окно «Импорт правил из файла», после чего будет проведена загрузка правил в соответствующую группу правил. Для подтверждения добавления правила нажать кнопку [OK].

Для установки действий **«alert»/«drop»** для всех правил в выбранной группе необходимо нажать кнопку [Изменения действия] (рис. 12).

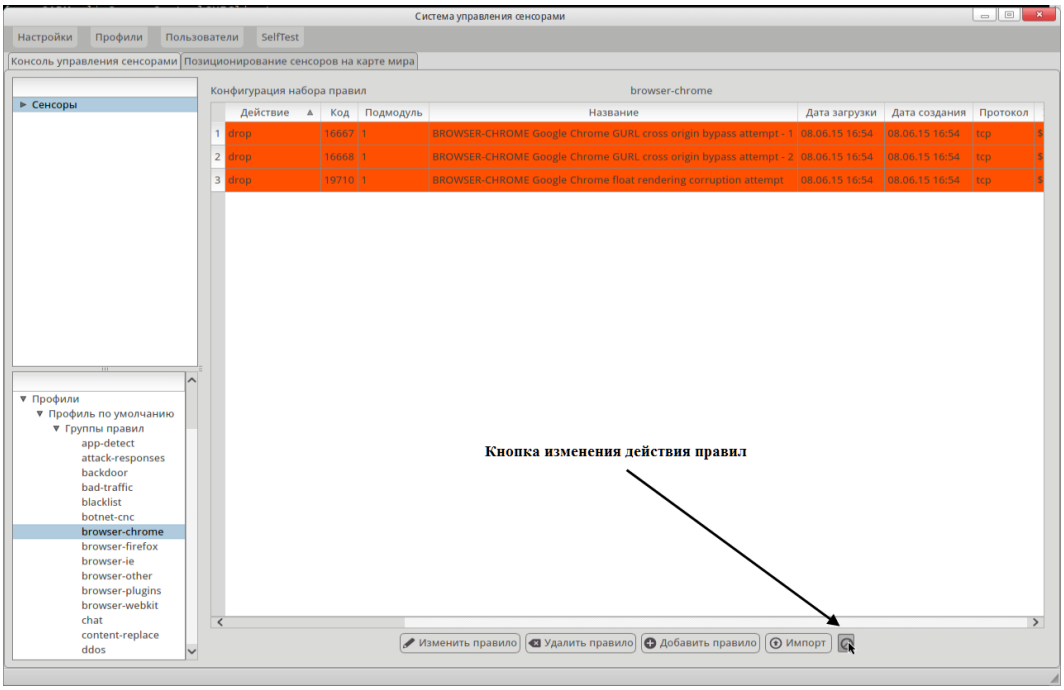


Рис. 12. Кнопка изменения действия правил

Для создания профиля, на базе существующего, необходимо выбрать в главном меню пункт «Профили» > «Добавить профиль», при этом появится окно «Профиль» (рис. 13), где следует заполнить следующие поля:

– Названия профиля;

– Описания профиля;

– Профиль на базе.

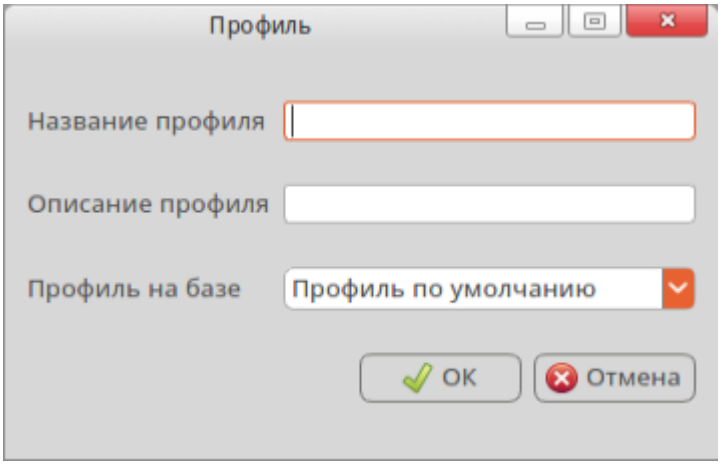


Рис. 13. Добавление профиля

При нажатии кнопки [OK] созданный профиль будет отображаться в основном

окне графической консоли сетевого управления сенсорами системы обнаружения атак.

Для поиска правила по коду и подмодулю атаки необходимо в области «Профиль» выбрать элемент древовидного списка «Группы правил» и нажать пункт меню `[Найти правило]` или выбрать его из контекстного меню (рис. 14).

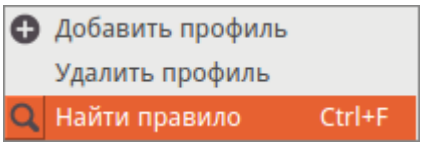


Рис. 14 . Контекстное меню области «Профиль»

В появившемся диалоге (рис. 15) указать параметры кода и подмодуля атаки и нажать кнопку `[Найти]`, для отмены поиска нажать кнопку `[Отмена]`.

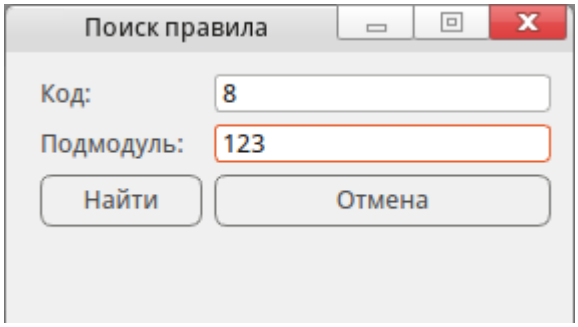


Рис. 15 Диалог поиска правила

Для назначения флагов критичности компьютерных атак для каждого конкретного сенсора необходимо выбрать в главном меню пункт «Настройки» > «Критические атаки». Появиться окно для просмотра списка атак, которые будут помечены флагом критичности.

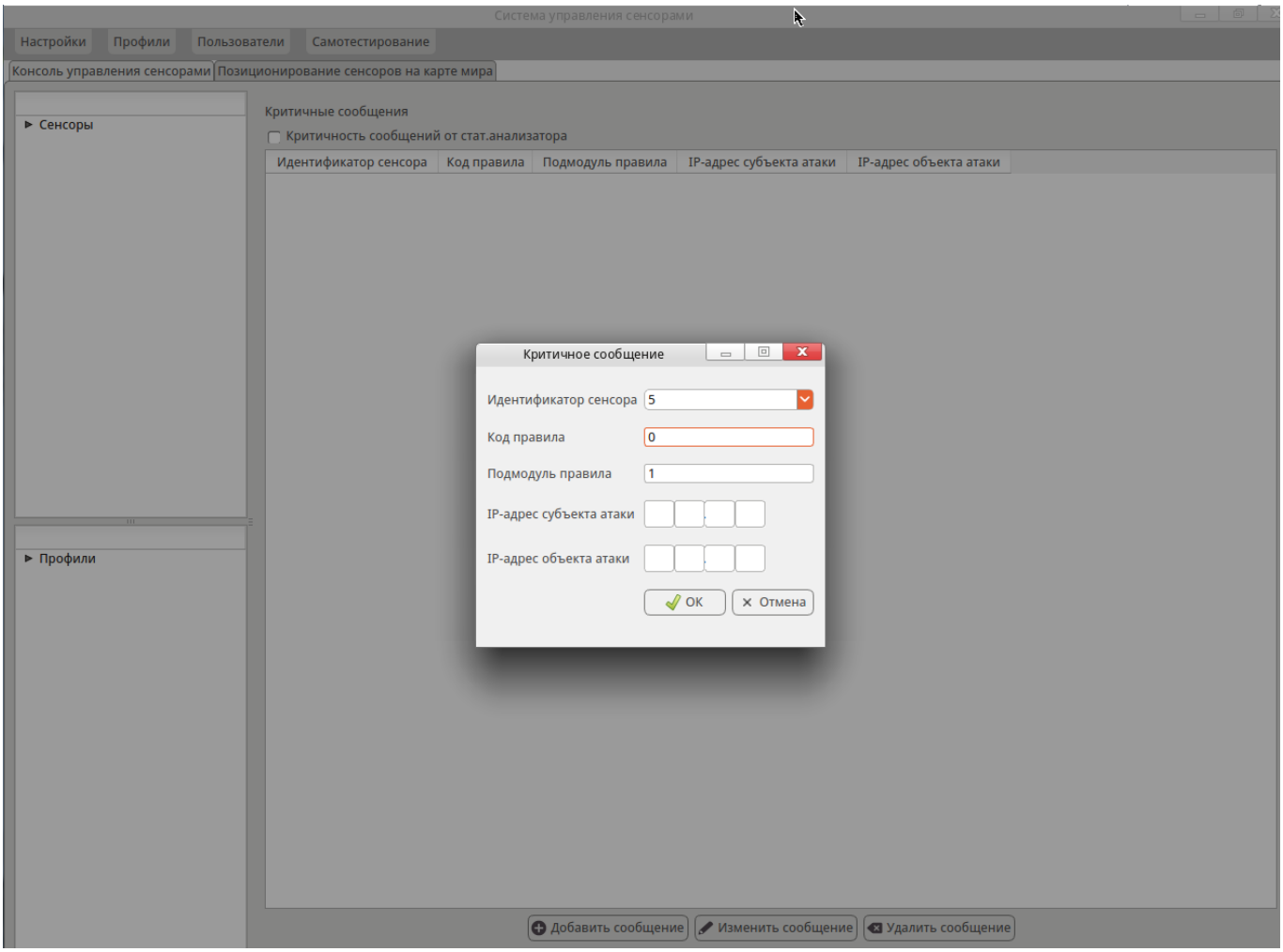


Рис. 16 Окно добавления критичных атак

Для добавления критичных атак необходимо нажать кнопку [Добавить сообщение] (рис. 16), при этом появится окно «Критичное сообщение» (рис. 17), где следует заполнить соответствующие поля:

– Идентификатор сенсора;
– Код правила;
– Подмодуль правила;
– IP-адрес субъекта атаки;
– IP-адрес объекта атаки.

Для подтверждения добавления критичной атаки нажать кнопку [OK].

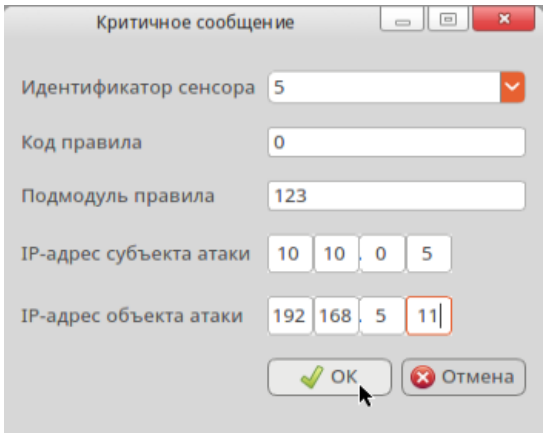


Рис. 17. Окно добавления и изменения критичных сообщений

Для изменения параметров соответствующей критической атаки необходимо выбрать ее и нажать кнопку [Изменить сообщение]. Появится окно «Критическое сообщение» (рис. 17), где можно посмотреть и изменить параметры критических атак. Для сохранения изменений в правиле нажать кнопку [OK].

Для удаления критичной атаки нажать кнопку [Удалить сообщение].

Для установки флага критичности для сообщений от статистического анализатора необходимо установить переключатель «Критичность сообщений от стат. анализатора».

2.3.4. Очистка базы данных

Для выполнения очистки базы данных необходимо выбрать в главном меню пункт «Настройка» > «Очистка БД», при этом откроется окно (рис. 18).

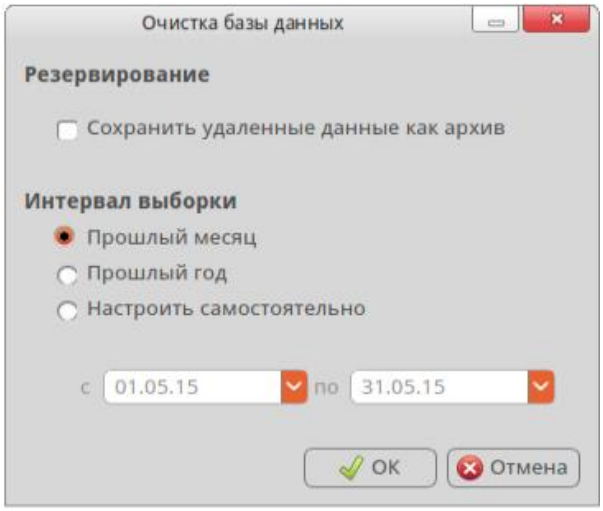


Рис. 18 Очистка БД

Необходимо задать интервал выборки для очистки, а также при необходимости выставить признак в поле «Сохранить удаленные данные как архив». По окончанию ввода данных нажать кнопку [OK].

2.3.5. Добавление новых пользователей

Для работы с учетными записями пользователей в ПС «АРМ УС» предусмотрено меню «Пользователи», которое позволяет выполнить:

– добавление новых учетных записей пользователей («Добавление пользователя»);

– редактирование учетной записи пользователей («Редактирование пользователей»);

– удаление учетной записи пользователей («Удаление пользователей»);

– добавление пользователей, прописанных на других АРМ ПС «АРМ УС» или в БД («Установка пользователей»).

Добавление пользователя

Для добавления новых пользователей необходимо выбрать в главном меню пункт «Пользователи» > «Добавление пользователя», при этом откроется диалог добавления пользователя (рис. 19).

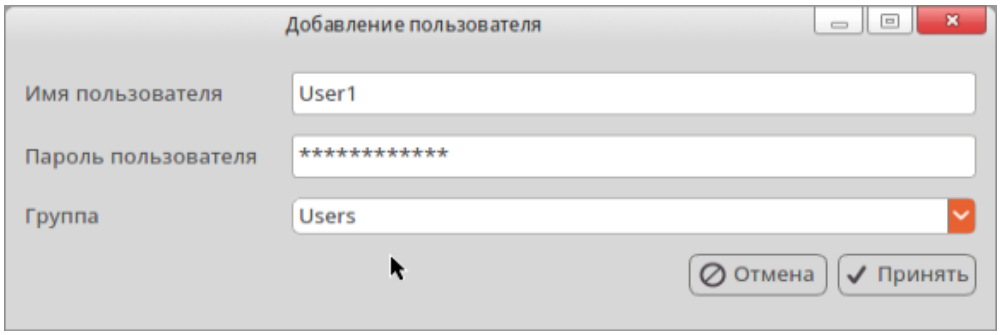


Рис. 19. Диалог добавления пользователя

При вводе данных ученой записи пользователя необходимо определить роль пользователя, для этого необходимо выбрать группу пользователя «Users» или «Admins». В следующем окне необходимо ввести пароль суперпользователя root для регистрации пользователя на АРМ (рис. 20) и нажать кнопку [Аутентификация], для отмены действий по добавлению пользователя нажмите кнопку [Отмена].

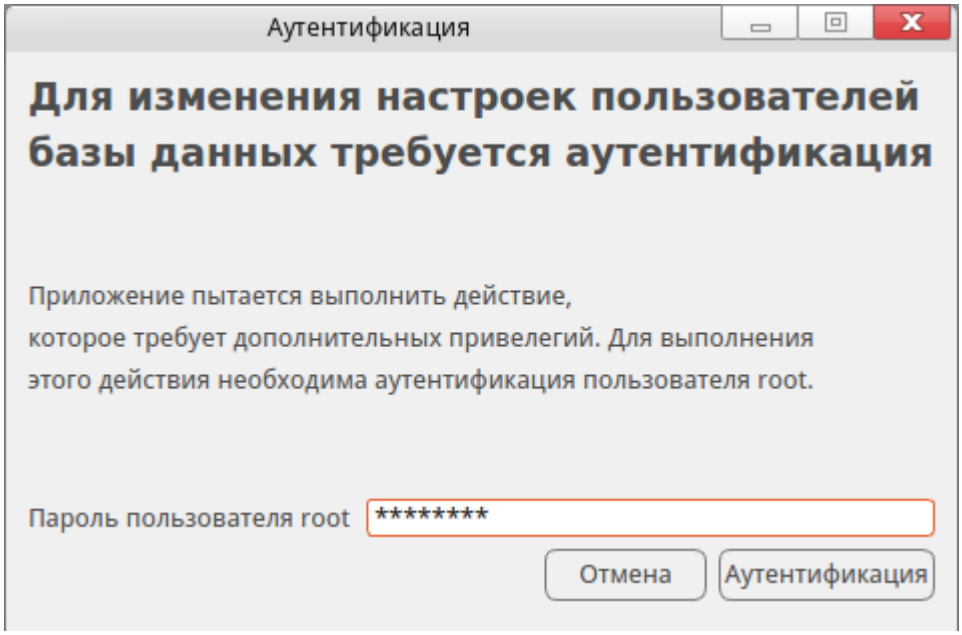


Рис. 20 Аутентификация

Редактирование пользователей

Для редактирования параметров пользователя необходимо выбрать пункт меню «Редактировать пользователей» и появившемся диалоге (рис. 21) дважды нажать на запись, которую необходимо редактировать. В диалоге редактирования (рис. 22) указать новое наименование пользователя, пароль и старый пароль пользователя. После нажатия кнопки [Принять] произвести аутентификацию суперпользователя (см. «Добавление пользователя»).

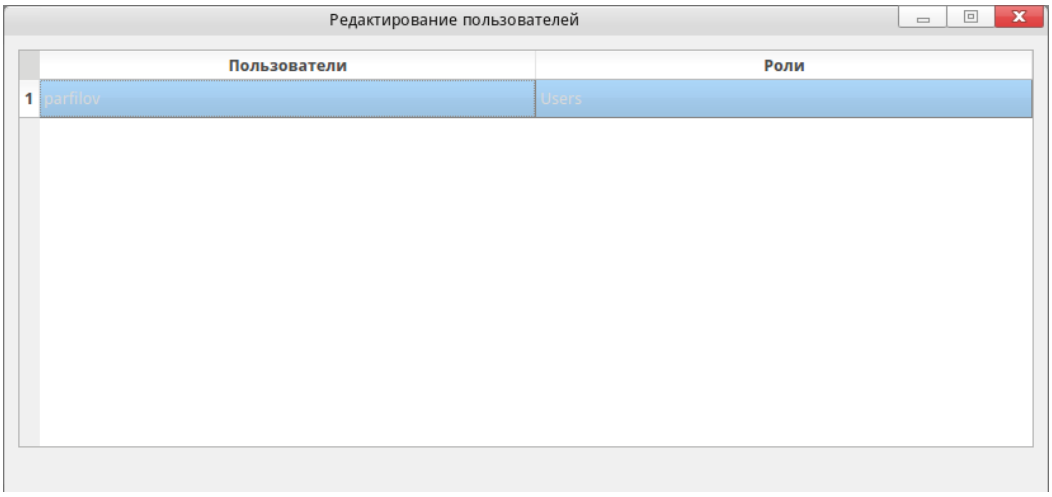


Рис. 21. Окно выбора пользователей для редактирования

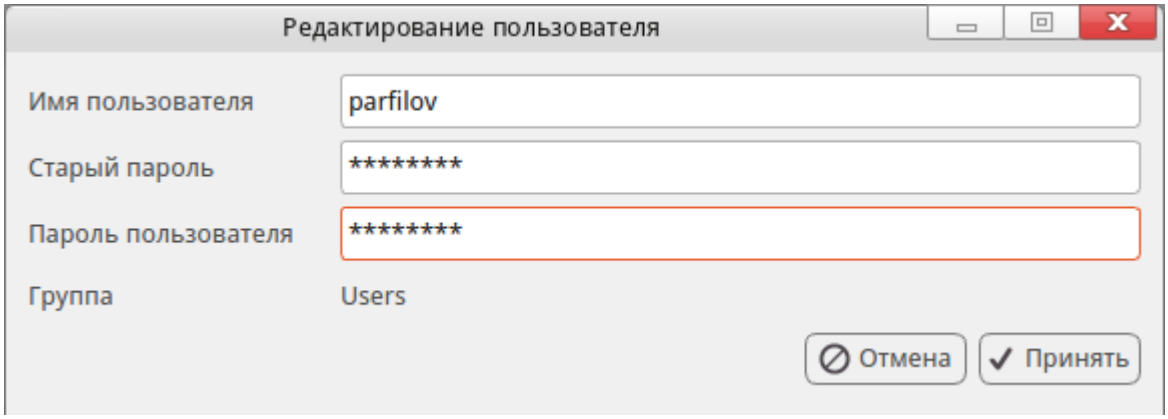


Рис. 22. Диалог редактирования пользователя

Удаление пользователей

Для удаления пользователей необходимо выбрать пункт меню «Удаление пользователей». В появившемся диалоге (рис. 23) необходимо отметить записи пользователей, которые будут удалены.

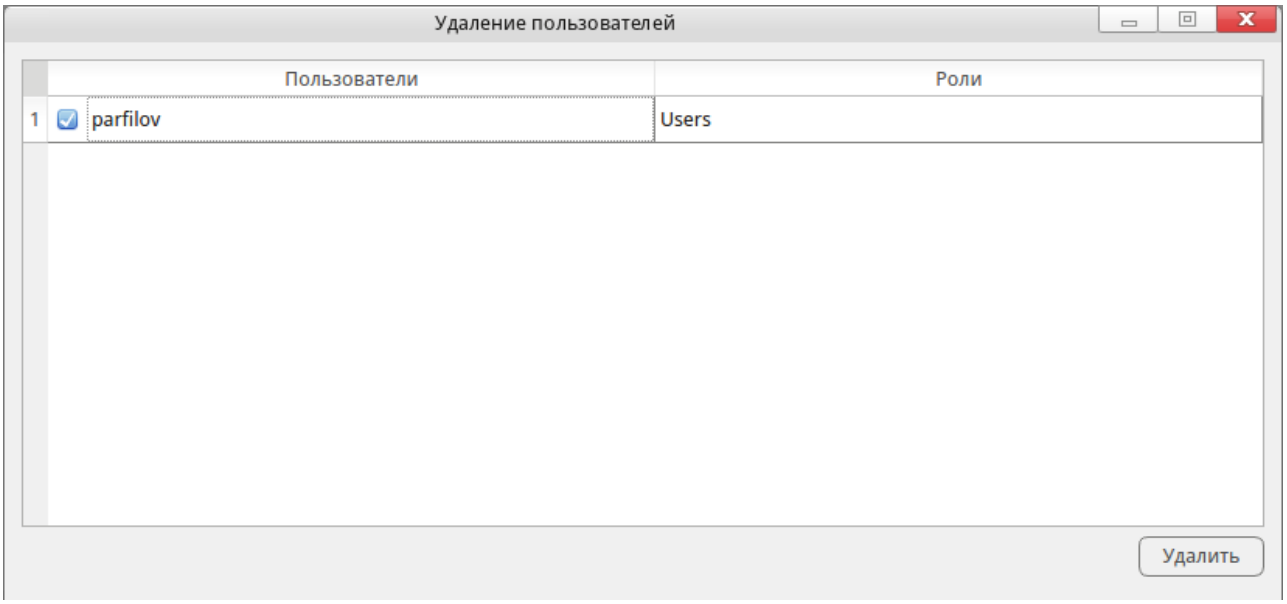


Рис. 23. Удаление пользователей

После появления диалога подтверждения удаления, для удаления нажмите кнопку [Да], для отмены удаления нажмите кнопку [Нет]. Затем необходимо провести операцию аутентификации (см. «Добавление пользователя»).

Примечание – пользователь не будет удален из базы данных, а только заблокирован (из-под данного пользователя аутентификация невозможна). При необходимости пользователя можно будет восстановить.

Установка пользователя

Для регистрации пользователя базы данных, который не установлен на ЭВМ АРМ, необходимо выбрать пункт меню «Установка пользователя». В появившемся диалоге (рис. 24) выбрать необходимого пользователя двойным кликом. В появившемся диалоге (рис. 25) задать пароль пользователя (необходимо задать существующий пароль) и нажать кнопку [Принять], для отмены нажать кнопку [Отмена]. Далее необходимо пройти операцию аутентификации (см. «Добавление пользователя»).

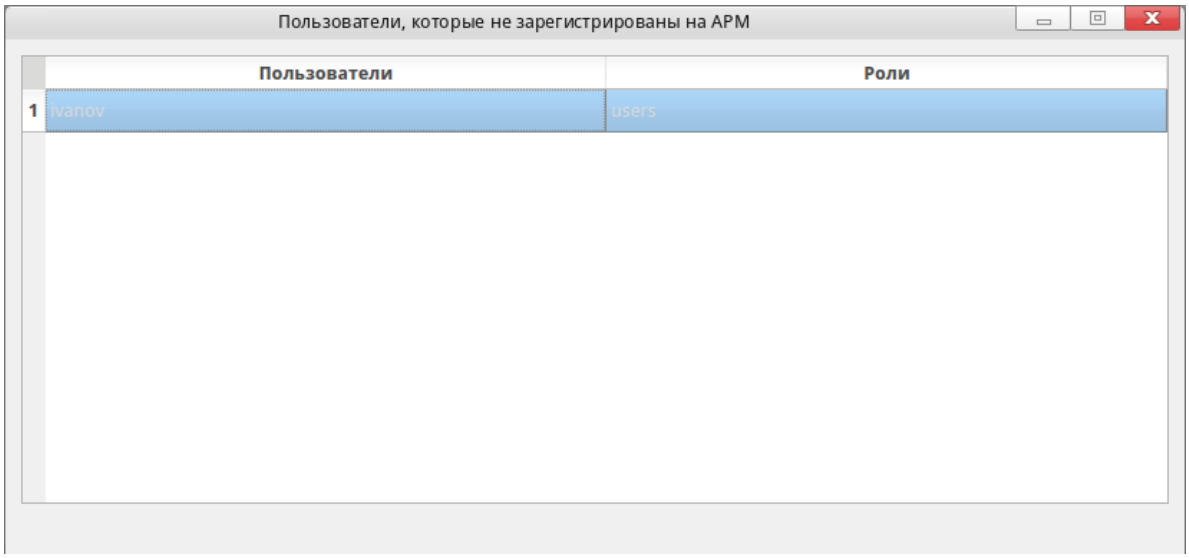


Рис. 24. Выбор незарегистрированных пользователей

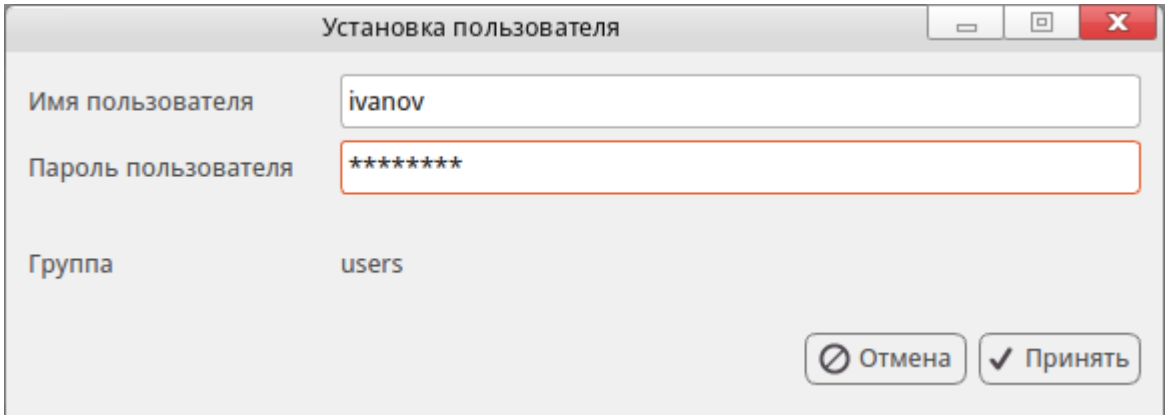


Рис. 25. Установка пользователя

2.3.6. Обновление СПО на сенсорах

Консоль сетевого управления сенсорами позволяет осуществлять обновление ПС «Сенсор». Для реализации данной возможности организуется локальное хранилище пакетов специального программного обеспечения с возможностью добавления и удаления пакетов. Данное хранилище используется для обновления специального программного обеспечения на сенсорах системы обнаружения атак.

Для создания архива в главном меню выбрать пункт «Настройки» > «Архив СПО». Появится основное окно локального хранилища специального программного обеспечения, для добавления СПО необходимо нажать кнопку [`Добавить в архив`], а для удаления из архива соответственно выделить не нужный архив СПО и

нажать кнопку [Удалить из архива]. При добавлении СПО в архив появиться окно выбора необходимого файла СПО (рис. 26).

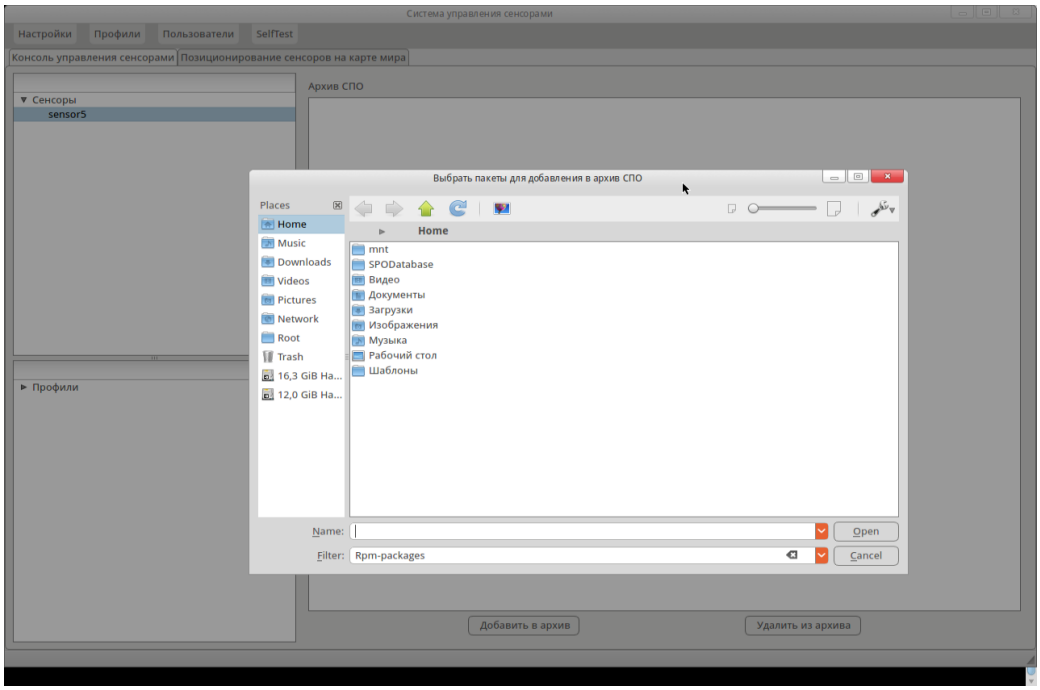


Рис. 26 Добавление СПО в архив

Для обновления СПО на сенсорах из локального хранилища или получения удаленного доступа к технологическим возможностям сенсора (командная строка операционной системы сенсора) необходимо выбрать соответствующий сенсор и нажать соответствующую кнопку, для обновления СПО на сенсоре – кнопку [Обновить СПО сенсора], а для вызова командной строки - [Командная строка ОС] (рис. 27).

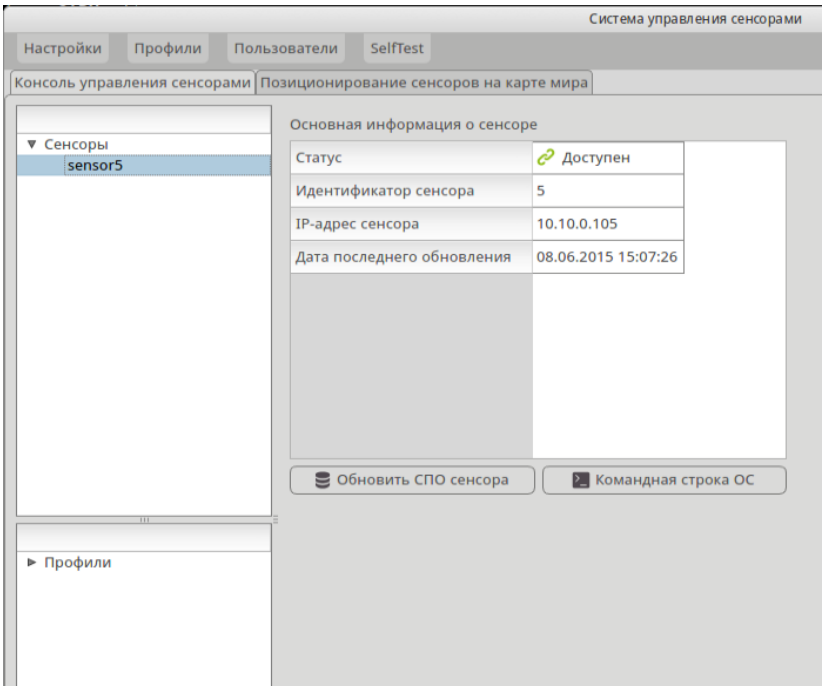


Рис. 27. Обновление СПО на сенсоре

После появлении окна с основными параметрами выбранного сенсора (рис. 28), в строке «Дата последнего обновления» будет указана дата и время последнего обновления. Для обновления сенсора необходимо нажать кнопку [`Обновить СПО сенсора`].

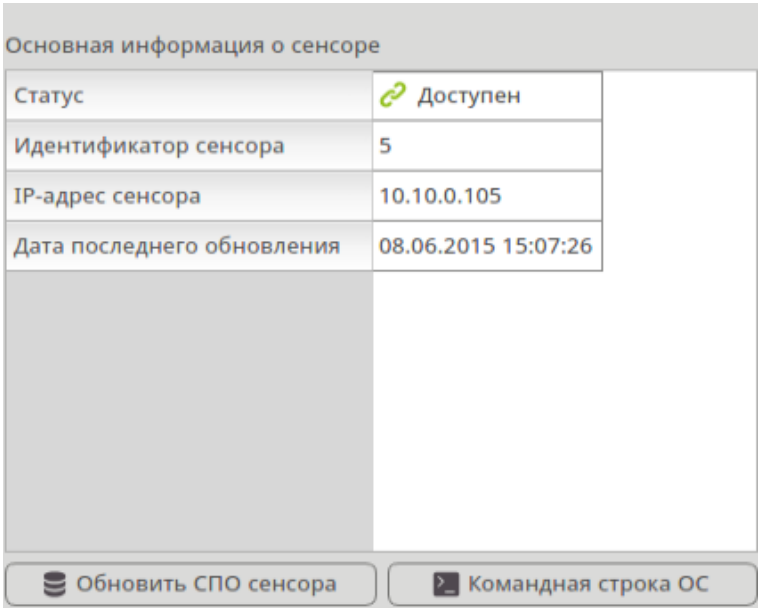


Рис. 28. Основная информация о сенсоре

При нажатии кнопки [Командная строка ОС] появится окно удаленного доступа к технологическим возможностям сенсора, т.е. командная строка управления сенсором.

2.3.7. Настройка взаимодействия с межсетевыми экранами

Для подключения и работы с межсетевыми экранами необходимо его зарегистрировать аналогично сенсору СОВ ПАК «Плутон». Для этого необходимо выделить поле «Сенсоры» в соответствующей области и нажать кнопку [Добавить]. В открывшемся окне следует ввести данные по необходимому сенсору, по окончании ввода нажать [ОК]. В поле тип сенсора выбрать «Firewall» (Рис. 29).

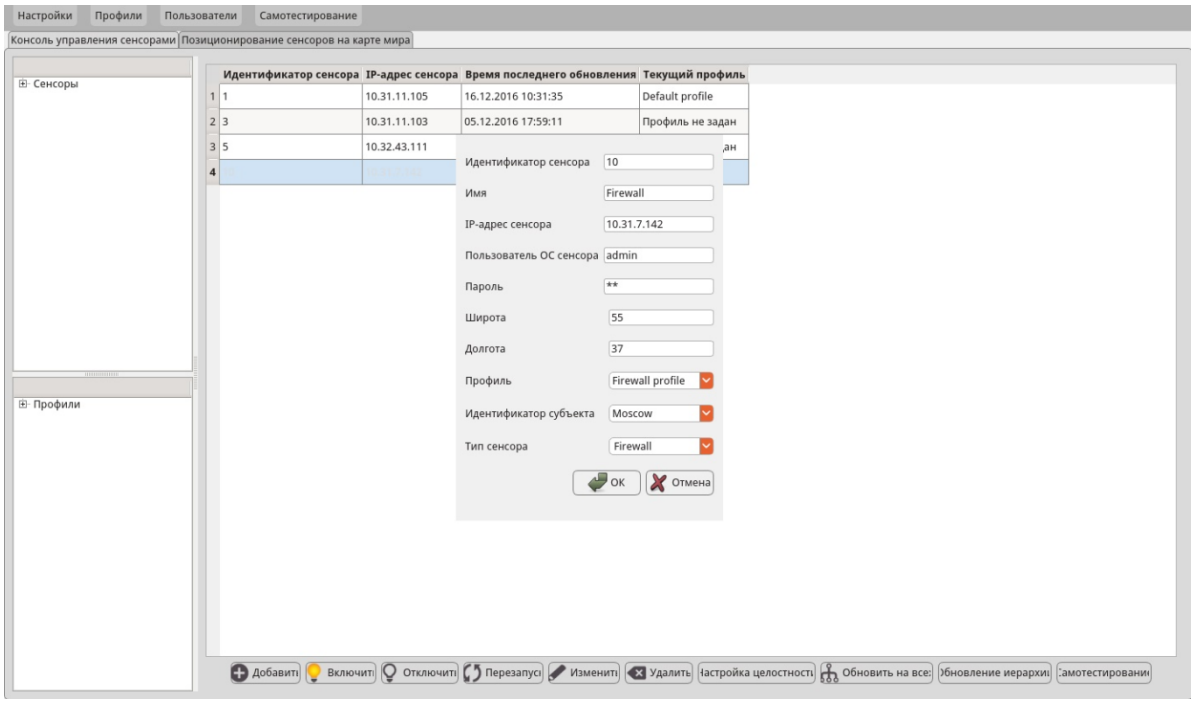


Рис. 29. Регистрация МСЭ в консоли сетевого управления ПС «Сенсоры»

Для настройки правил межсетевого экранирования, необходимо выбрать интересующее правило в профиле и нажать на кнопку «Настройка МСЭ», после чего в появившемся диалоговом окне выбрать параметры экранирования: режим, действие и время блокировки (рис. 30). В качестве режима может быть выбрано:

– «Выключен» - отсутствие блокировки;
– «Авто» - автоматическая блокировка.

В качестве действия могут быть выбраны различные параметры блокировки:

– «Блокировать по ip-источника»;
– «Блокировать по ip-источника и ip-получателя»;
– «Блокировать по ip-источника и порту получателя»;
– «Блокировать по ip-источника и ip и порту получателя».

В качестве времени действия блокировки могут быть выбраны:

– «30 минут»;
– «1 час»;
– «1 день»;
– «Постоянно».

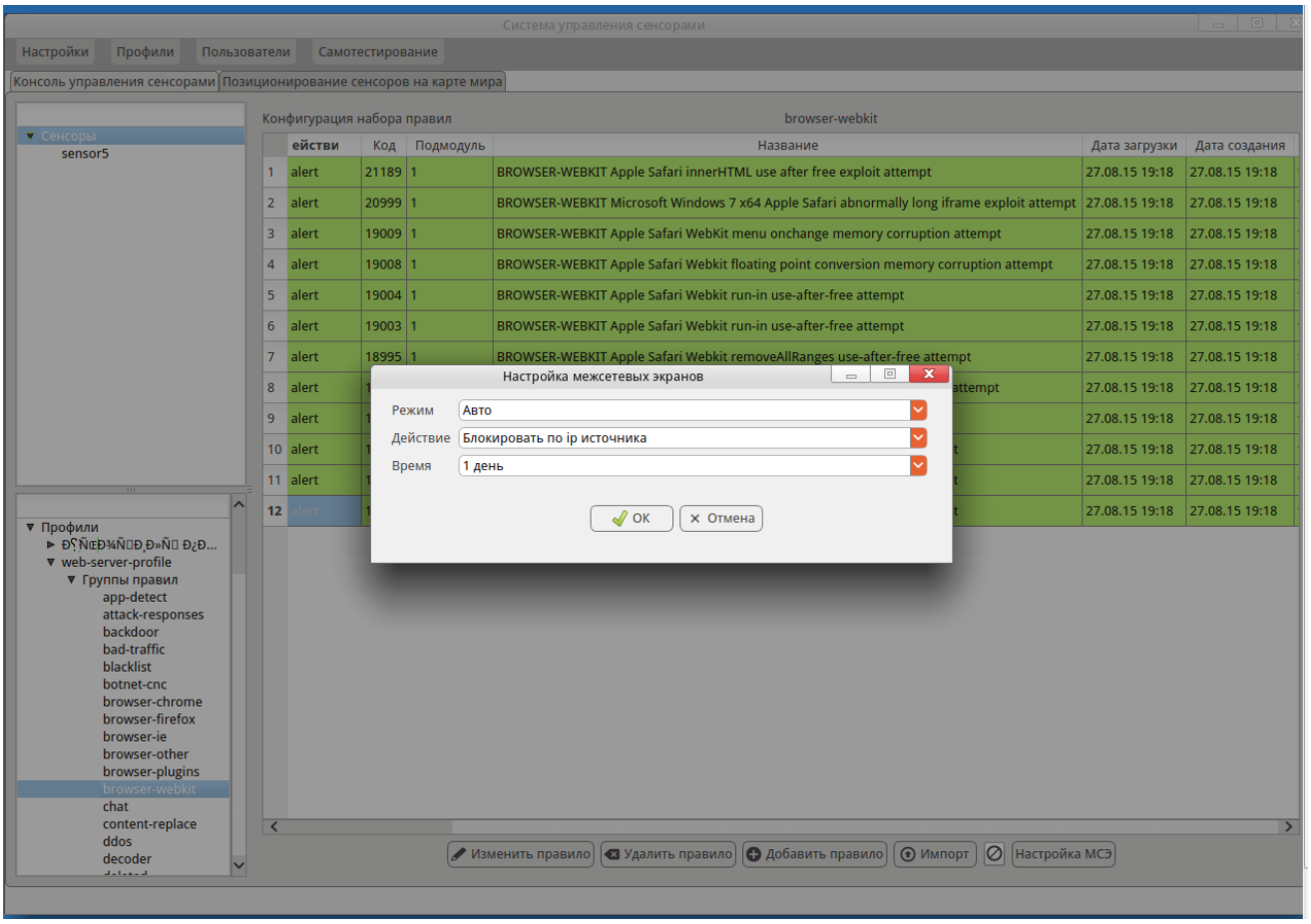


Рис. 30. Настройка параметров автоматизированной блокировки атак посредством МЭ

2.3.8. Позиционирование сенсоров на карте мира

Для привязки сенсоров к их географическому расположению на карте мира следует в главном окне ПС выбрать вкладку «Позиционирование сенсоров на карте мира» (рис. 31).

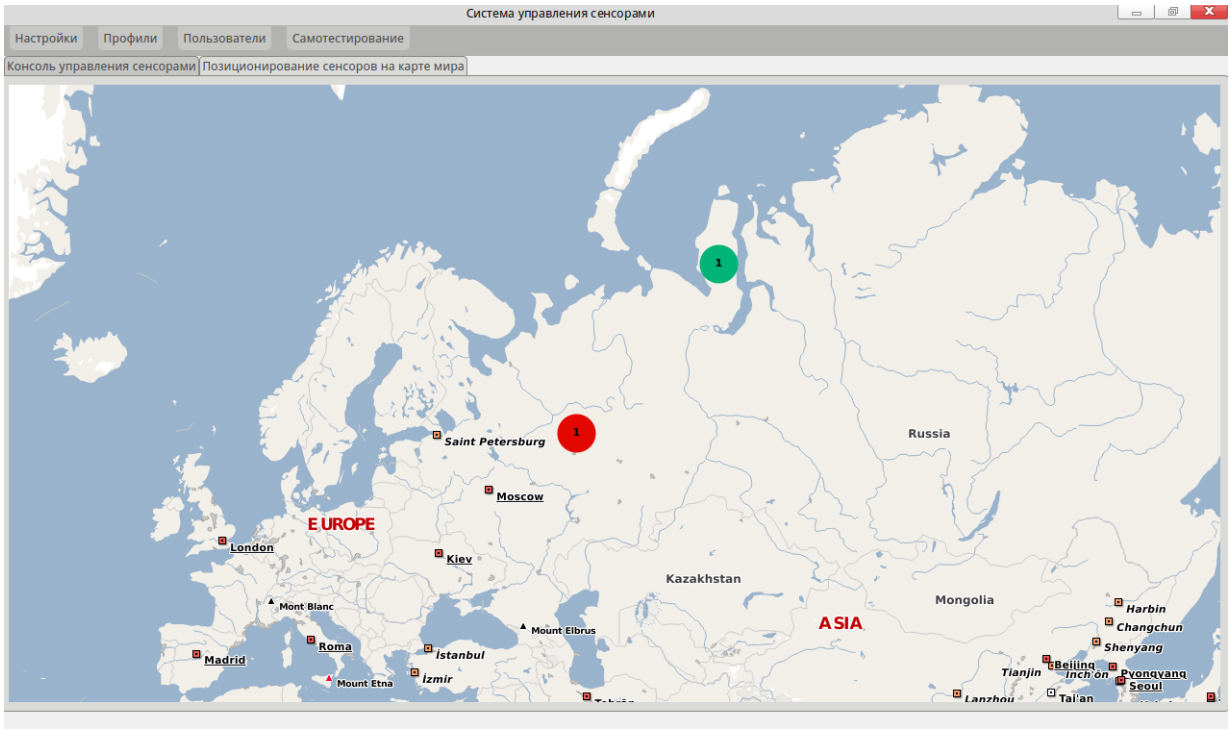


Рис. 31 Позиционирование сенсоров на карте мира

Для добавления нового сенсора на карту мира следует нажать правой кнопкой мыши в точке карты, соответствующей его местоположению. Далее в контекстном меню выбрать пункт «Добавить сенсор». В появившемся диалоге необходимо задать параметры сенсора и нажать кнопку «ОК». Поля, заполняемые при задании параметров сенсора, описаны в п.п. 4.2 настоящего руководства.

Ранее добавленные сенсоры отображаются на карте разным цветом в зависимости от их состояния (зеленый – «работает», красный - «выключен»). При наведении указателя мыши на сенсор выводится всплывающая подсказка с информацией о сенсоре, а при одинарном клике левой кнопкой мыши на нем появится контекстное меню, в котором можно выбрать действие с данным сенсором:

– «Выключить» - выключает сенсор;

– «Включить» - включает сенсор;

– «Редактировать» - вызывает диалог редактирования параметров сенсора (процедура задания параметров сенсора описана в п.п. 4.2 настоящего руководства);

– «Переместить» - включает режим изменения местоположения сенсора на карте мира;

– «Удалить» - удаляет сенсор.

После включения режима перемещения сенсора необходимо переместить указатель мыши (объект на карте следует за ним) в новую точку расположения сенсора на карте мира, после чего нажать левую кнопку мыши.

Если несколько сенсоров расположены слишком близко друг к другу при данном масштабе карты, они отображаются в виде одного группового объекта (рис. 32). Внутри группового объекта выводится число сенсоров в этом объекте, а при наведении на него указателя мыши выводится всплывающая подсказка со списком этих сенсоров.

Рис. 32 Отображение близкорасположенных сенсоров на карте мира в виде группового объекта.

Для изменения масштаба карты следует использовать колесо мыши, для перемещения отображаемой области карты следует нажать левую кнопку мыши и, не отпуская ее, переместить указатель мыши (отображаемая область карты при этом будет сдвигаться в окне), после чего отпустить кнопку мыши.

2.3.9. Выполнение самотестирования системы

Для выполнения самотестирования сервера управления сенсорами и АРМ управления сенсорами следует выбрать пункт главного меню «Самотестирование» (рис. 33).

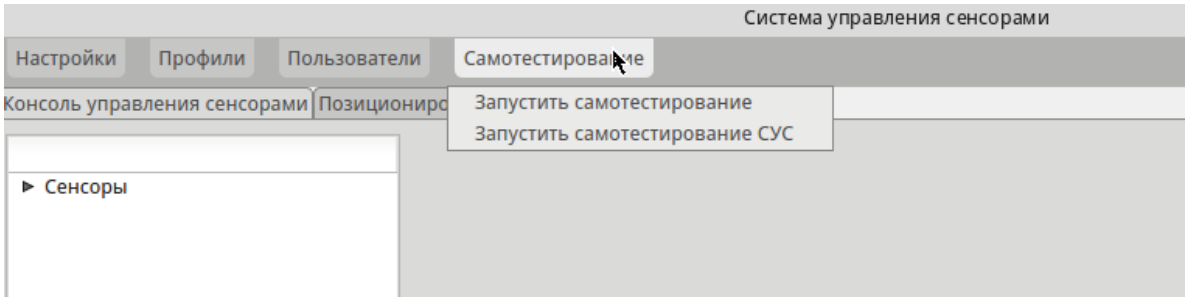


Рис. 33. Пункт меню «Самотестирование»

Для выполнения самотестирования АРМ управления сенсорами необходимо выбрать пункт «Запустить самотестирование».

Для выполнения самотестирования сервера управления сенсорами необходимо выбрать пункт «Запустить самотестирование СУС».

Для выполнения самотестирования сенсора необходимо в главном окне в области «Сенсоры» выбрать элемент «Сенсоры», в области отображения выделить сенсор и нажать кнопку «Самотестирование».

В результате выполнения соответствующей команды отображается диалог, сообщающий о результатах самотестирования (рис. 34).

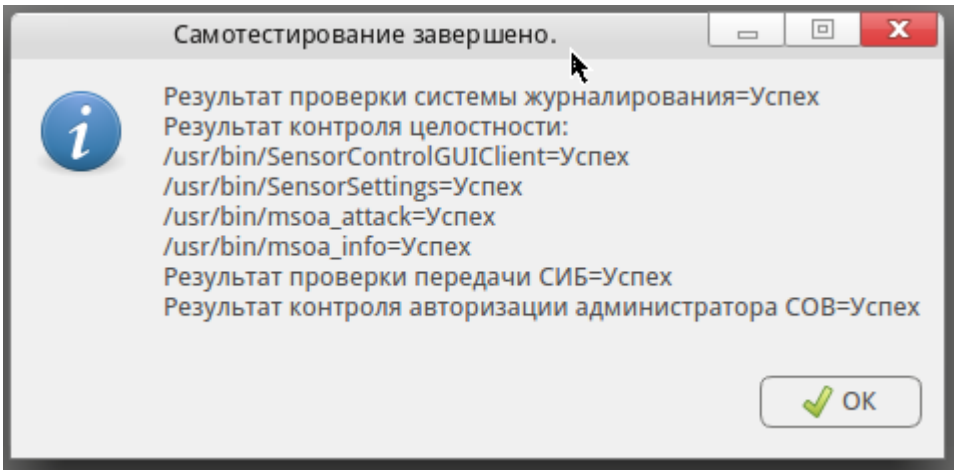


Рис. 34 Результат самотестирования

2.3.10. Настройка статистического анализатора

Для выполнения настройки статистического анализатора необходимо выбрать в главном меню пункт «Настройка» > «Статистический анализатор», при этом откроется диалог (рис. 35).

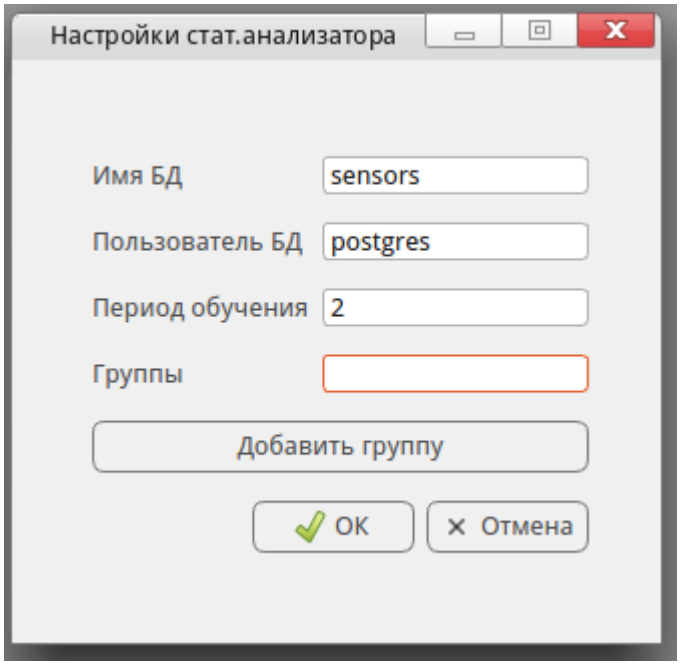


Рис. 35. Диалог настройки статистического анализатора

В данном диалоге следует задать для статистического анализатора параметры подключения к БД (имя БД и пользователя) и период обучения статистического анализатора (в часах, минимально допустимое значение – 2 часа). Затем необходимо настроить разбиение сенсоров на группы, статистика от которых агрегируется в

единый массив для целей статистического анализа. Если не задать ни одной группы, статистический анализатор не будет анализировать поступающие данные.

Для добавления группы следует нажать кнопку «Добавить группу», при этом откроется диалог настройки группы (Рис. 36).

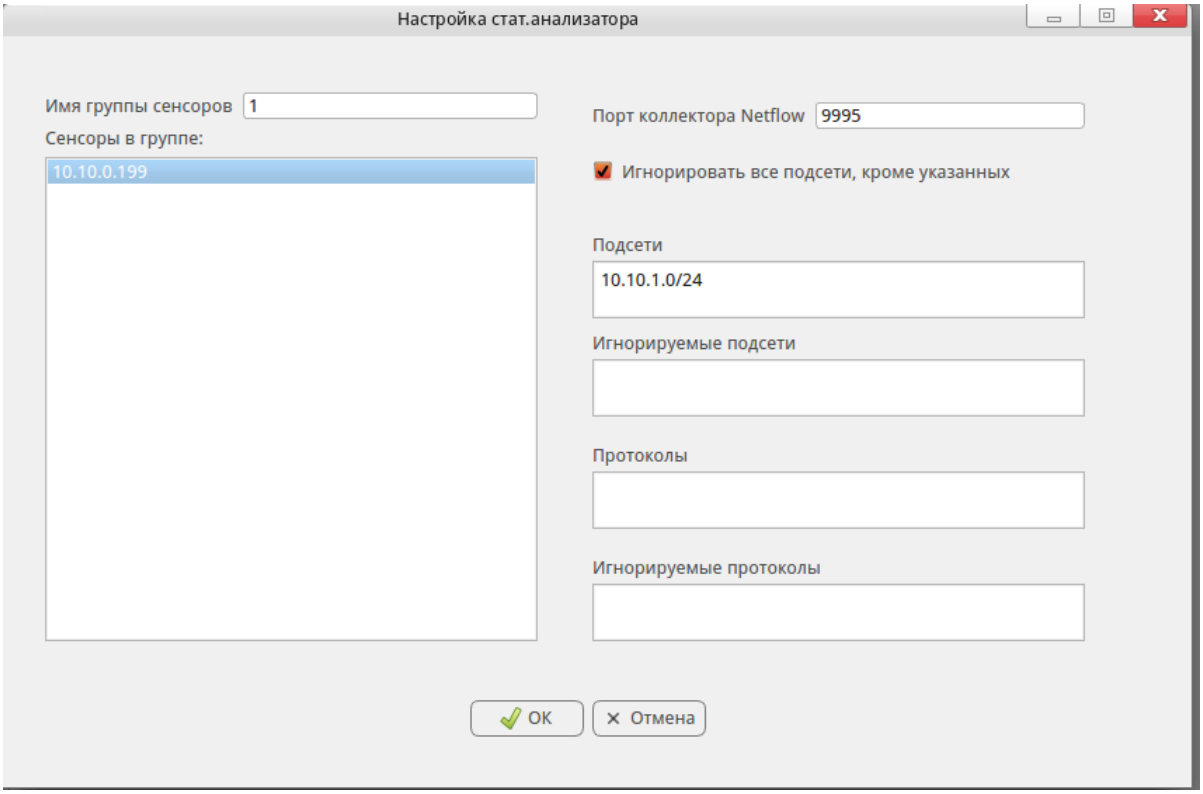


Рис. 36. Диалог добавления группы сенсоров для статистического анализатора

В данном диалоге следует в поле «Имя группы сенсоров» задать имя для группы, а в списке «Сенсоры в группе» выбрать сенсоры, включаемые в группу.

Далее в поле «Порт коллектора Netflow» необходимо указать порт, на котором статистический анализатор будет ожидать статистические данные от сенсоров. В поле «Подсети» задаются диапазоны ip-адресов контролируемых подстетей, а в поле «Игнорируемые подсети» диапазоны ip-адресов подсетей, трафик от (в) которых игнорируется при статистическом анализе. Если задан переключатель «Игнорировать все подсети, кроме указанных», то при статистическом анализе игнорируется трафик из всех подсетей, кроме указанных в поле «Подсети».

В поле «Протоколы» можно добавить нестандартные специализированные протоколы, если известно какие порты и тип протокола они используют. Протоколы

задаются в формате «<номер порта>/<тип протокола>» через запятую, например «4444/TCP,3248/UDP».

В поле «Игнорируемые протоколы» можно добавить протоколы, для которых трафик будет игнорироваться при выполнении статистического анализа. Формат поля аналогичен формату поля «Протоколы».

По окончанию ввода данных для сохранения настроек необходимо нажать кнопку [OK].

2.4. ПМ «Визуализация состояния ПС «Сенсор»

ПМ «Визуализация состояния ПС «Сенсор»» предназначен для информирования оператора о системных параметрах сенсоров в режиме реального времени и вывода статистических данных по отключениям сенсоров за заданный интервал времени.

ПМ «Визуализация состояния ПС «Сенсор»» позволяет выполнить следующие функции:

– функцию просмотра списка сенсоров с указанием их наименования, состояния и IP адреса;

– функции контроля состояния ПМ сенсора;

– функцию оценка загрузки центральных процессоров (ЦП);

– функцию просмотра загруженности оперативной памяти (ОП) и файла подкачки SWAP;

– функцию просмотра диаграммы заполнения монтируемых устройств с указанием времени последней перезагрузки;

– функцию просмотра целостности конфигурационных файлов;

– функцию получения информации о длительности отключения ПС сенсоров;

– функцию оповещения о недостатке места на монтируемых устройствах;

– функцию отображения состояния сенсоров на карте мира.

Для запуска ПМ «Визуализация состояния ПС «Сенсор» необходимо запустить терминал, ввести команду:

$ msoa_info

Далее и нажать клавишу **[Enter]**. После запуска программы появится основное окно (рис. 37), которое отображает список сенсоров с указанием их наименования, состояния и IP адреса.

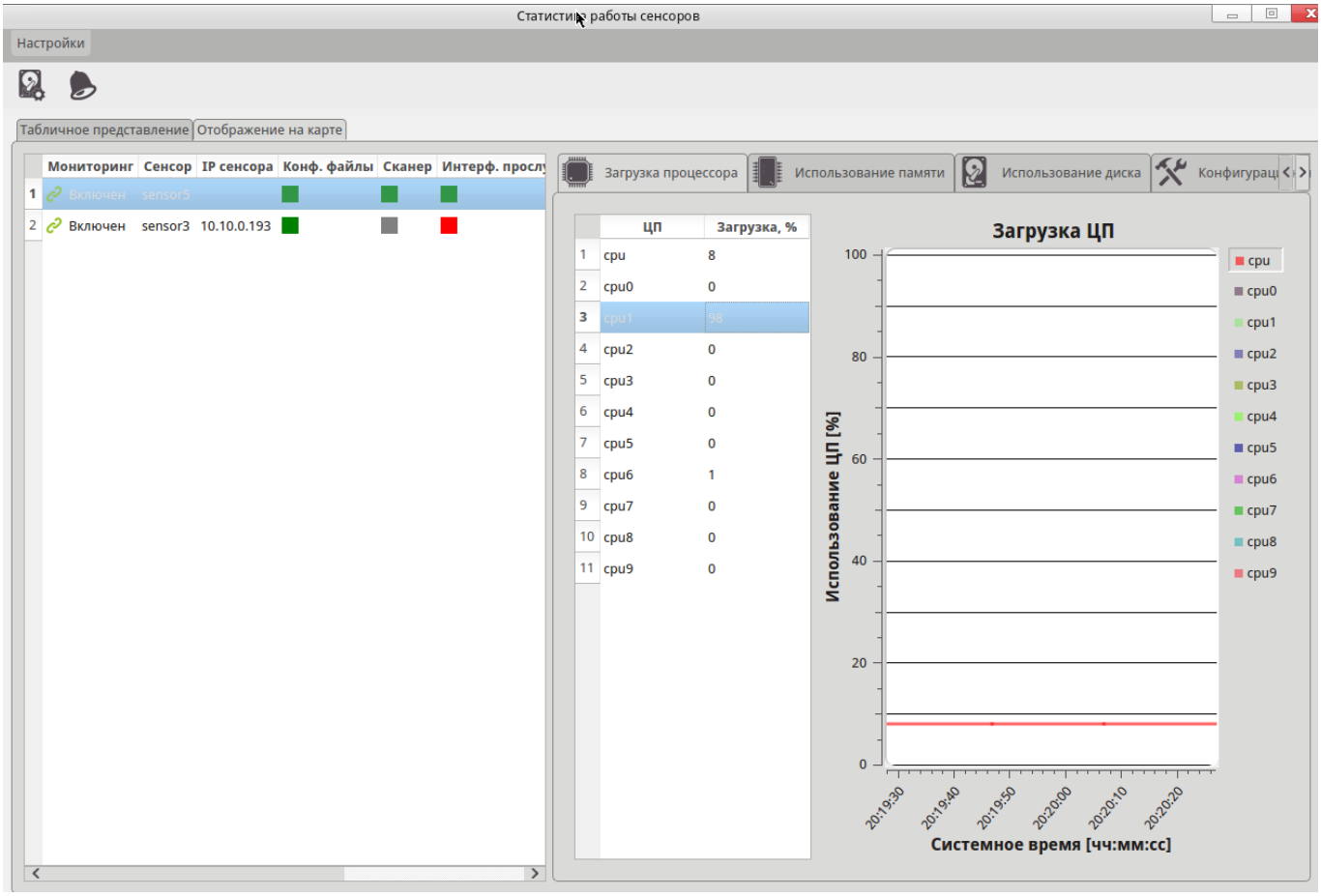


Рис. 37. Основное окно статистики работы сенсоров

2.4.1. Контроль состояния ПМ сенсор

Функция контроля состояния ПМ сенсора выводит в поле «Мониторинг» (см. рис. 37) следующие состояния активности ПМ сенсора:

– зеленая иконка – ПМ работает;

– красная иконка – ПМ не работает.

Поле «Сканер» отражает состояние работоспособности ПМ обнаружения атак:

– зеленый квадрат – ПМ функционирует;

– серый квадрат – ПМ отключено.

Поле «Конф. файлы» отражает состояние целостности конфигурационных файлов:

– зеленый квадрат – целостность не нарушена;

– красный квадрат – нарушена целостность.

Поле «Интерф. прослуш.» отражает состояние интерфейса сканера:

– зеленый квадрат – передача исследуемого трафика включена;

– красный квадрат – нарушена передача исследуемого трафика.

Поле «Причина отключения» отражает причину отключения ПМ сенсоров:

– «сенсор» – отключен сенсором;

– «сервер управления сенсорами» – отключен сервером управления сенсорами.

2.4.2. Функция оценки загрузки ЦП

Функция оценки загрузки ЦП позволяет вывести в виде графика загрузку ЦП в различные моменты времени (рис. 38).

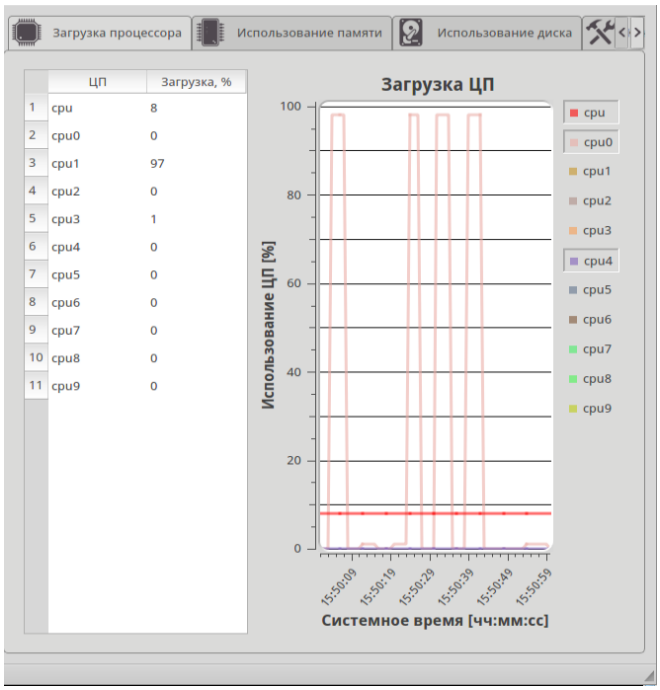


Рис. 38 Загрузка ЦП

2.4.3. Функция просмотра загруженности ОП и файла подкачки SWAP

Функция просмотра загруженности ОП и файла подкачки SWAP позволяет вывести в виде графика загруженность ОП и файла подкачки SWAP в различные моменты времени (рис. 39).

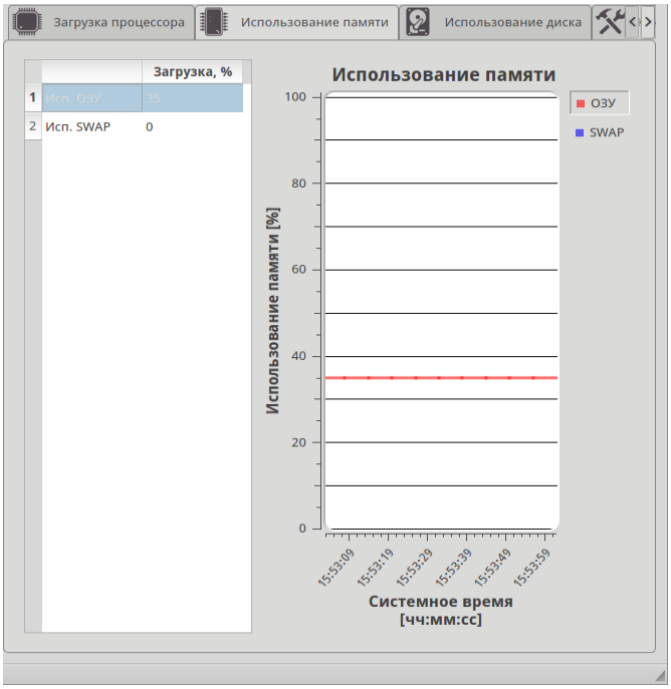


Рис. 39 Загруженность ОП и файла подкачки SWAP

2.4.4. Функция просмотра диаграммы заполнения монтируемых устройств

Функция позволяет просматривать диаграмму заполнения монтируемых устройств с указанием времени последней перезагрузки (рис. 40).

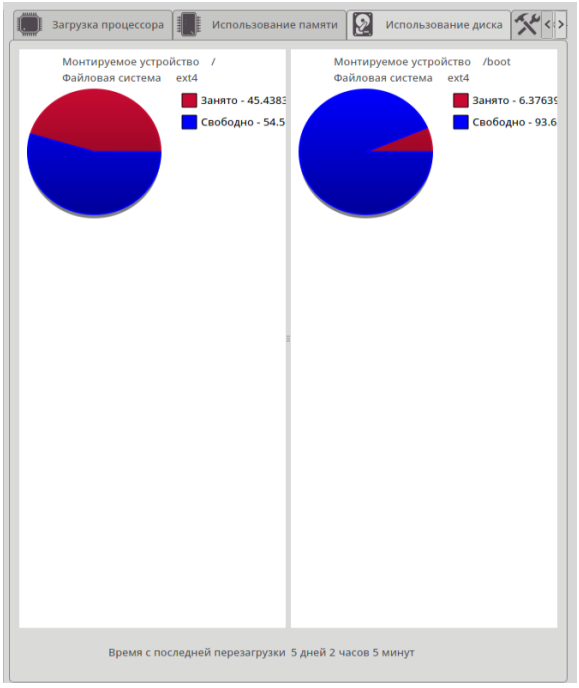


Рис. 40. Круговая диаграмма состояния монтируемых устройств

2.4.5. Функция просмотра целостности конфигурационных файлов

Функция позволяет просматривать целостность конфигурационных файлов. Во вкладке «Конфигурационные файлы» отражается информация по всем файлам правил и конфигурации (рис. 41):

– зеленый квадрат – целостность не нарушена;

– красный квадрат – нарушена целостность).

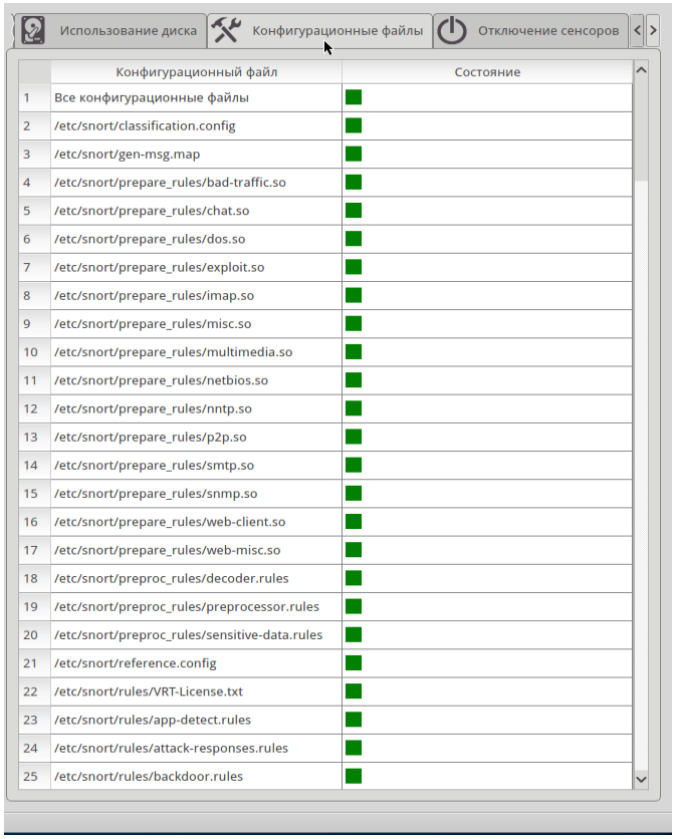


Рис. 41 Целостность конфигурационных файлов

2.4.6. Функция получения информации о длительности отключения ПС сенсоров

Функция позволяет получать информацию о длительности отключения ПС сенсоров. Во вкладке «Отключение сенсоров» пользователь может получать интервал времени отключения, включения и длительности отключения сенсоров (рис. 42). Для получения необходимой выборки можно задать следующие параметры:

– задать демоны – состояние сенсоров (сбор статистики) или сканер атак;

– задать сенсор;

– задать интервал выборки фактов отключения и включения сенсоров.

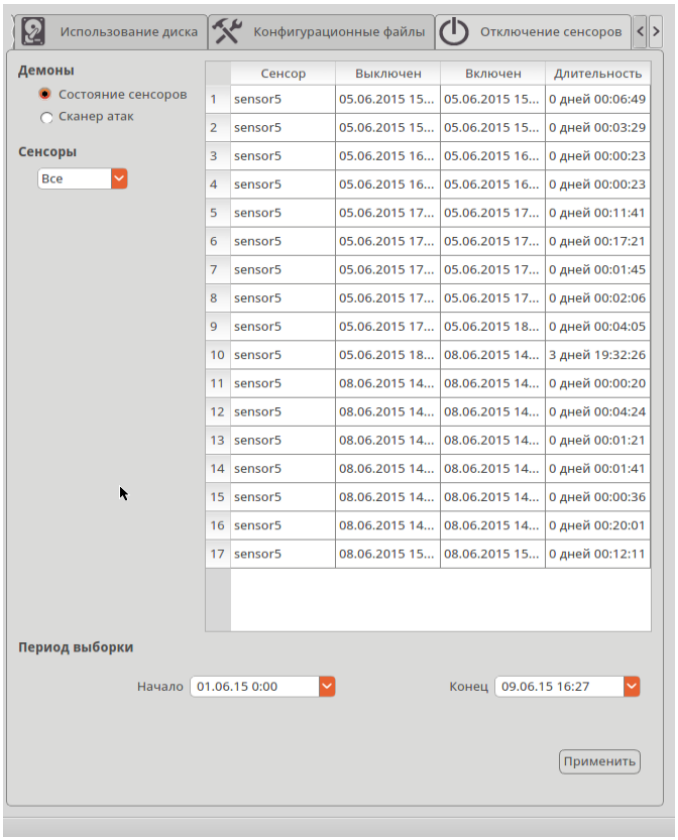


Рис. 42. Просмотр отключения сенсоров

2.4.7. Функция оповещения о недостатке места на монтируемых устройствах

Для настройки механизма оповещения о недостатке места на монтируемых устройствах необходимо выбрать пункт меню «Настройки» > «Минимальный объем свободного места на устройстве». В появившемся диалоге (рис. 43) необходимо установить процент остатка свободного места на диске, при котором будет производиться звуковое и визуальное оповещение, а также устройства, для которых будет производиться отслеживание. По умолчанию, устанавливается оповещение для корневого каталога («/») и для устройства для хранения временных файлов атак («/var»). Процент остатка свободного места на монтируемом устройстве, по умолчанию, равен 10%.

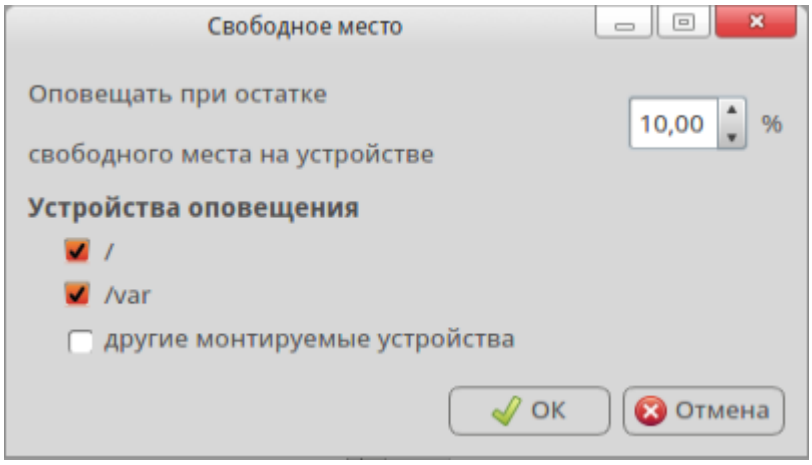


Рис. 43. Окно настройки оповещения

Для включения или отключения звукового оповещения о недостатке места на монтируемых устройствах необходимо выбрать пункт меню «Настройки» > «Звуковое оповещение» (рис. 44) и выбрать необходимое действие.

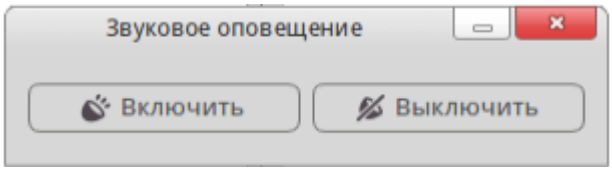


Рис. 44 Включение\выключение звукового оповещения

2.4.8. Функция отображения состояния сенсоров на карте мира

Для перехода в режим отображения состояния сенсоров на карте мира необходимо выбрать вкладку «Отображение на карте» (рис. 45).

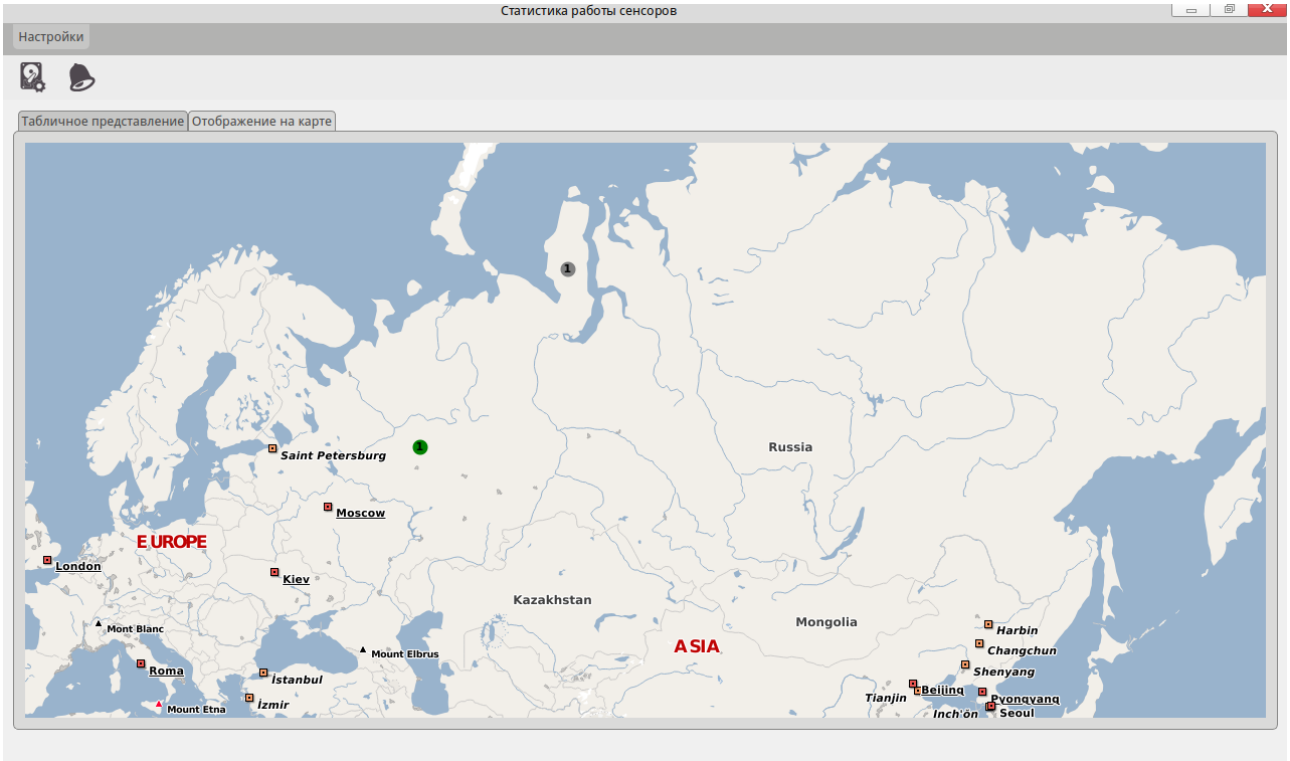


Рис. 45 Отображение состояния сенсоров на карте мира

Состояние сенсора на карте мира отображается различным цветом:

– зеленый – «работает»;

– красный – «остановлен»;

– серый – «нет связи с сенсором».

При наведении указателя мыши на сенсор выводится всплывающая подсказка с информацией о сенсоре. Для изменения масштаба карты следует использовать колесо мыши, для перемещения отображаемой области карты следует нажать левую кнопку мыши и, не отпуская ее, переместить указатель мыши (отображаемая область карты при этом будет сдвигаться в окне), после чего отпустить кнопку мыши.

2.5. ПМ «Утилита задания ресурсов сенсорам»

Для запуска утилиты необходимо в главном меню выбрать «Другие» > «Утилита задания ресурсов сенсорам». После запуска утилиты появится основное окно (рис. 46). В основном окне содержится «Имя сенсора» и уникальный идентификатор сенсора - «УИС». Для добавления ресурса для сенсора, необходимо указать сенсор и выбрать пункт меню «Ресурсы» > «Добавить ресурс» или выбрать

соответствующую кнопку панели инструментов. Если сенсор не выбран, появится окно предупреждения (рис. 47).

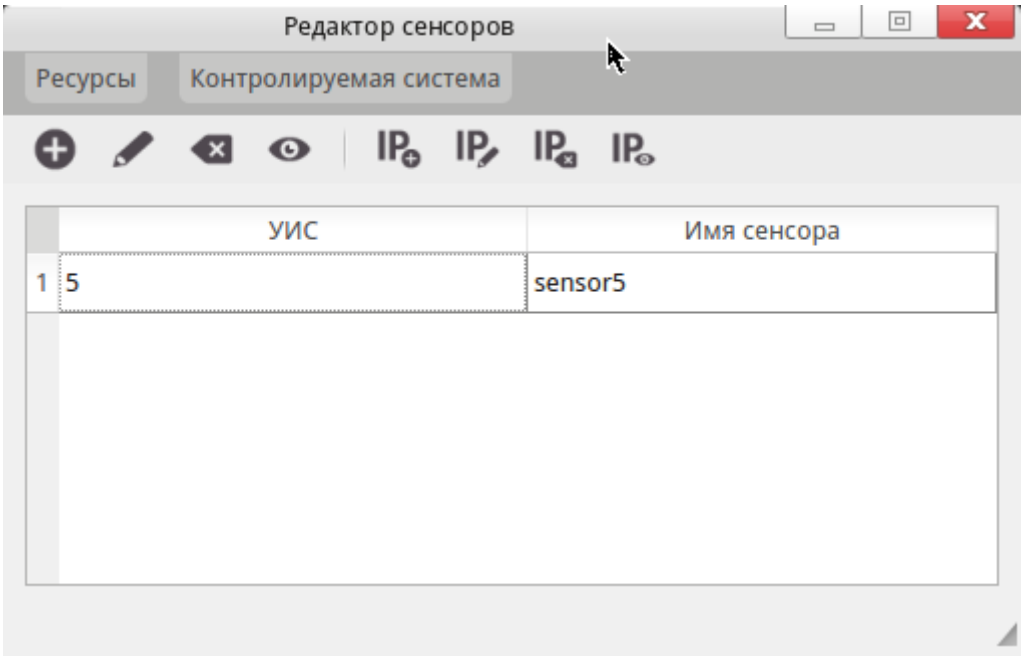


Рис. 46. Главное окно

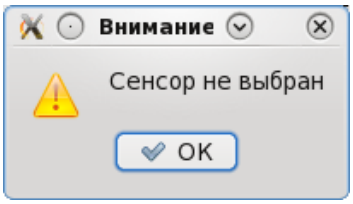


Рис. 47. Предупреждающее сообщение

В диалоге «Добавление ресурса» (рис. 48), необходимо указать доменное имя ресурса и IP адрес. Если IP-адрес не задан, при нажатии на кнопку «Принять», появится окно предупреждения (рис. 49).

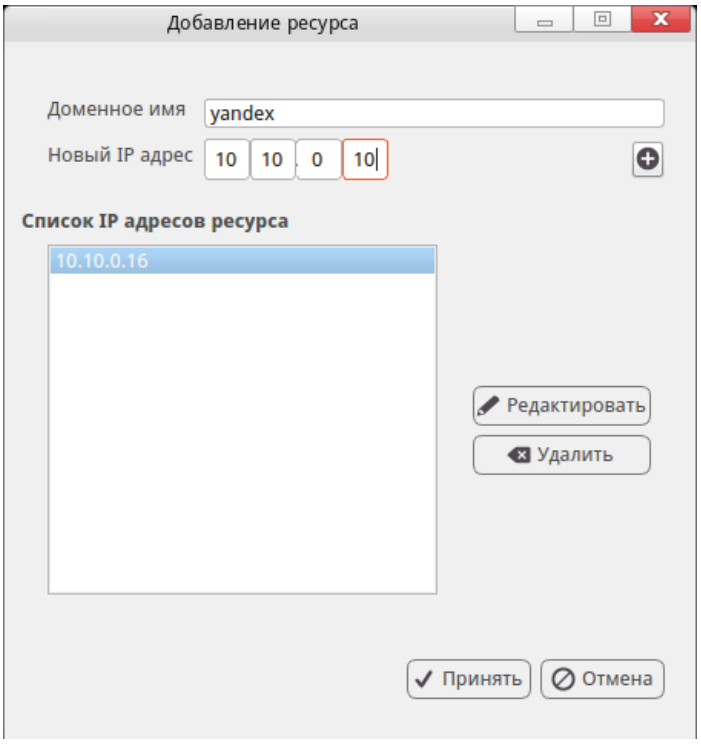


Рис. 48. Диалог добавления ресурса

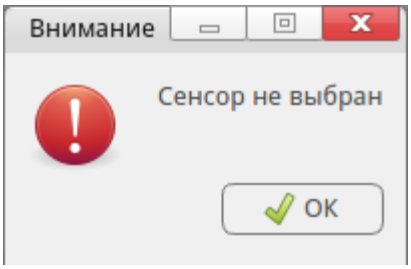


Рис. 49. Предупреждающее сообщение

При добавлении ресурса с существующим именем появится предупреждающее сообщение (рис. 50).

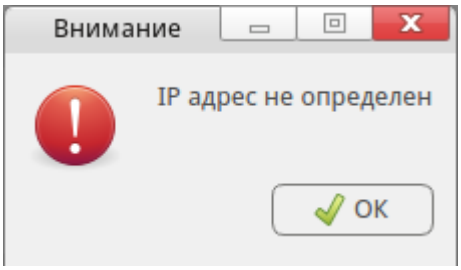


Рис. 50. Предупреждающее сообщение

При добавлении для ресурса IP-адреса, который уже зарегистрирован за данным ресурсом, появится предупреждающее сообщение (рис. 51).

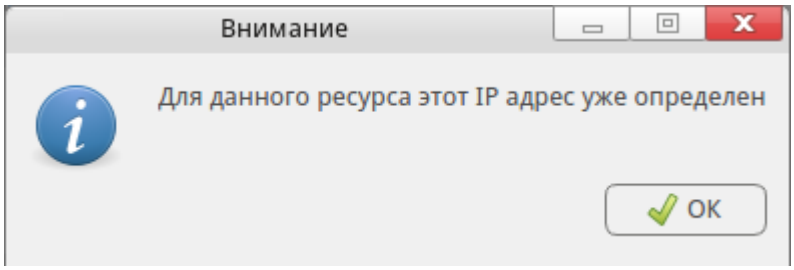


Рис. 51. Предупреждающее сообщение

Для редактирования IP адреса ресурса необходимо выделить его из списка IP-адресов ресурса и нажать кнопку «Редактировать». В диалоге «Редактирование IP» (рис. 52) в поле IP-адреса указать новый адрес. Изменив IP-адрес, нажать кнопку «ОК»

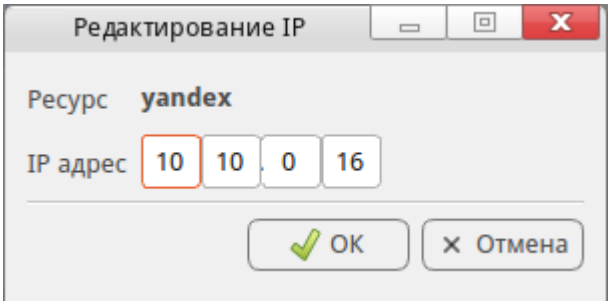


Рис. 52 Окно редактирования IP-адреса

Для редактирования ресурсов, зарегистрированных за сенсором в главном окне (рис. 46) указать сенсор и выбрать пункт меню «Ресурсы» > «Редактировать ресурсы» или соответствующую кнопку панели инструментов. В диалоге «Редактирование ресурсов» отображается список доменных имен ресурсов, зарегистрированных за сенсором (рис. 53). Для вывода окна редактирования конкретного ресурса необходимо дважды нажать на соответствующую строку списка.

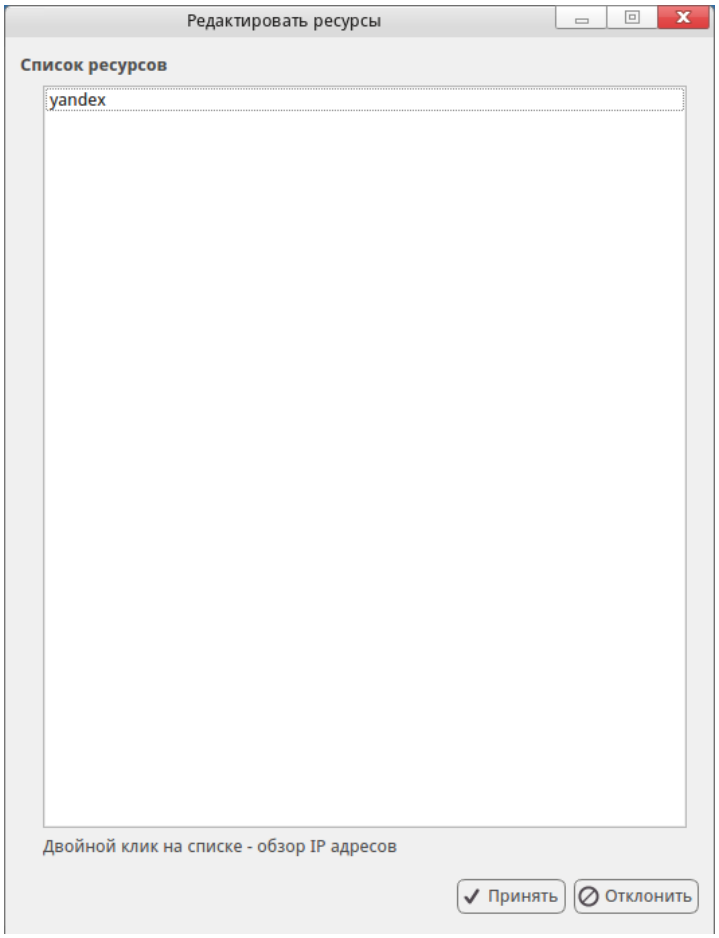


Рис. 53 Список ресурсов

В диалоге «Редактирование ресурса» (рис. 54) для редактирования IP-адреса ресурса необходимо выбрать соответствующий IP-адрес и нажать кнопку «Редактировать». Дальнейшие действия аналогичны действиям, указанным в разделе добавления ресурса.

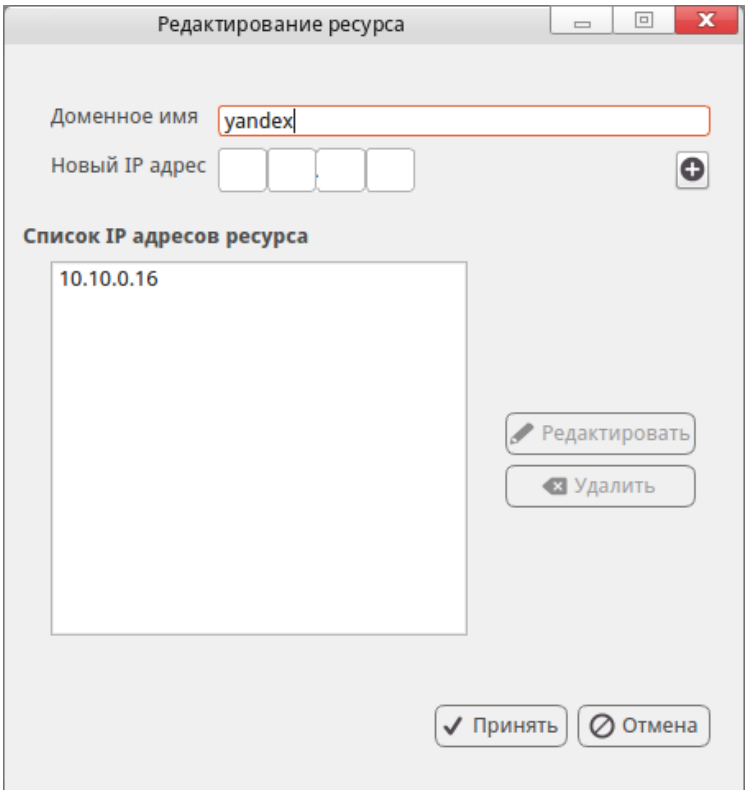


Рис. 54 Диалог «Редактирование ресурса»

Для удаления ресурсов, зарегистрированных за сенсором в главном окне программы (рис. 46) указать нужный сенсор и выбрать пункт меню «Ресурсы» > «Удалить ресурсы» или соответствующую кнопку панели инструментов. В диалоге «Удаления ресурсов» (рис. 55) отметить ресурсы, которые необходимо удалить, и нажать кнопку [Принять].

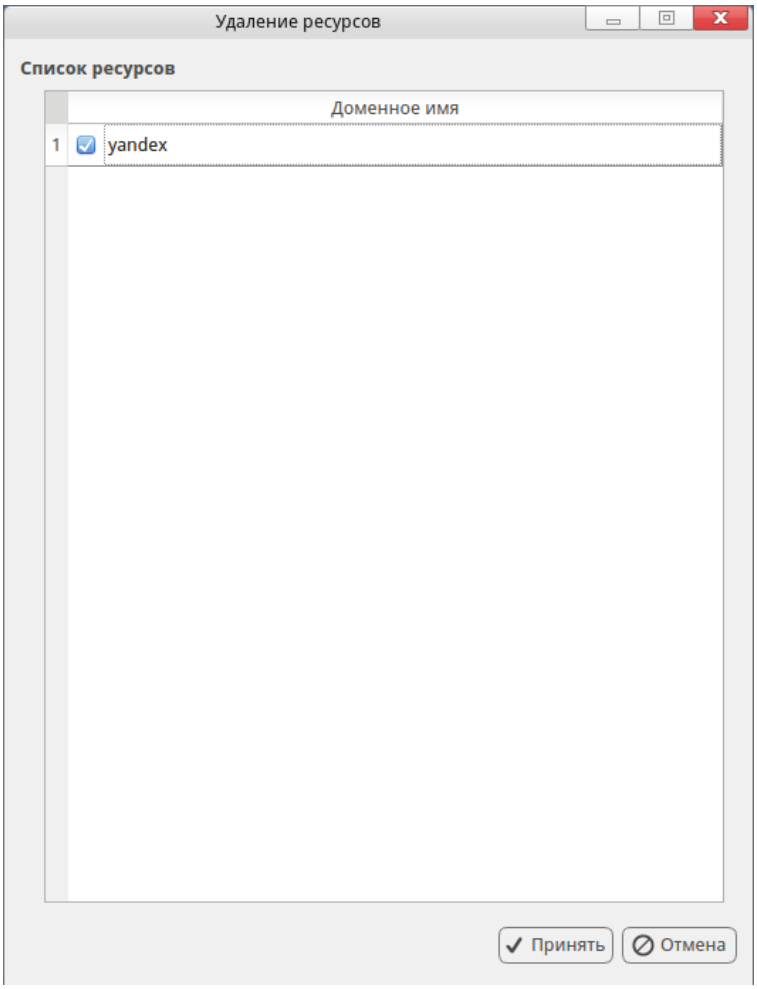


Рис. 55 Диалог удаления ресурсов сенсора

В появившемся предупреждающем сообщении подтвердить операцию удаления (рис. 56).

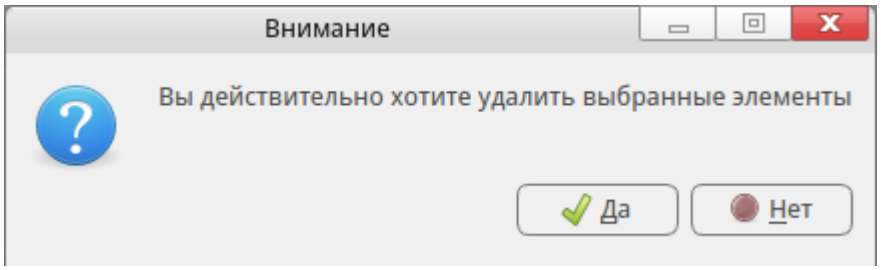


Рис. 56 Сообщение подтверждения удаления

Для просмотра параметров ресурсов, зарегистрированных за сенсором, без их редактирования необходимо выбрать пункт меню в главном окне программы (рис. 46) указать нужный сенсор и выбрать пункт меню «Ресурсы» > «Обзор ресурсов» или соответствующую кнопку панели инструментов (рис. 57).

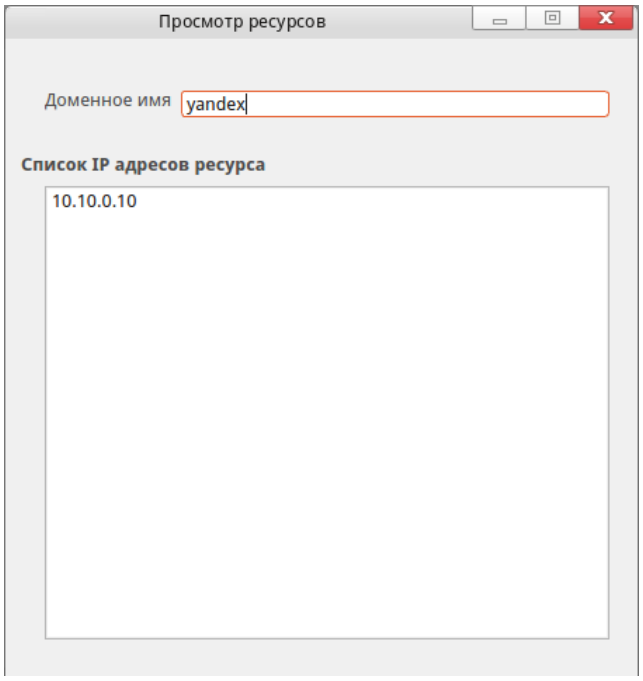


Рис. 57. Просмотр ресурсов

Для добавления контролируемой системы (КС) в главном окне (рис. 46) необходимо указать сенсор, выбрать пункт меню «Контролируемые системы» > «Добавить контролируемую систему» или соответствующую кнопку панели инструментов. В появившемся диалоге (Рис. 58) указать наименование системы и в поле «Список диапазонов» нажать кнопку [`Добавить`].

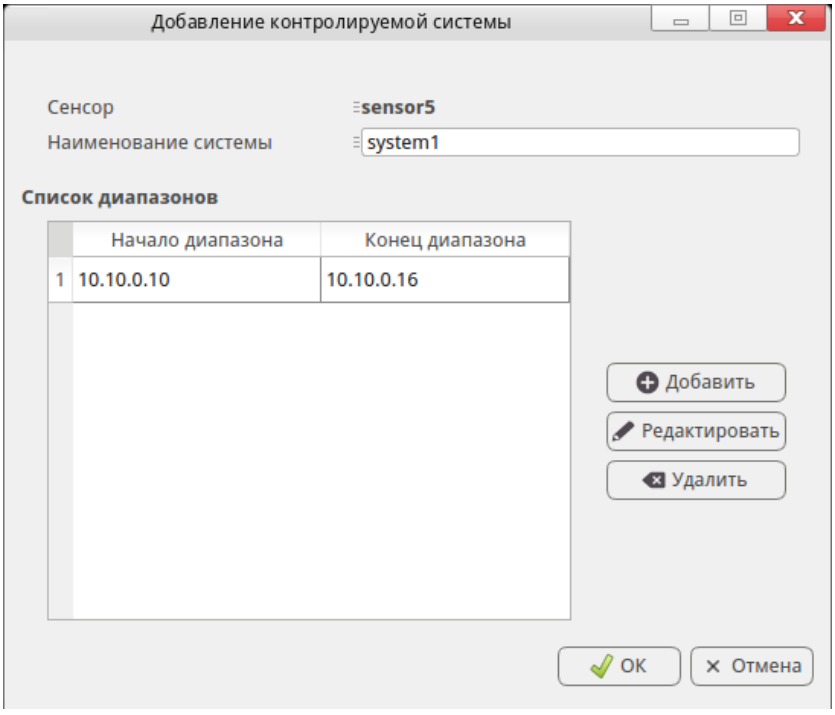


Рис. 58. Диалог добавления контролируемой системы

В диалоге «Добавление диапазона IP адресов» (рис. 59) указать начальное и конечное значение диапазона и нажать кнопку [OK].

.

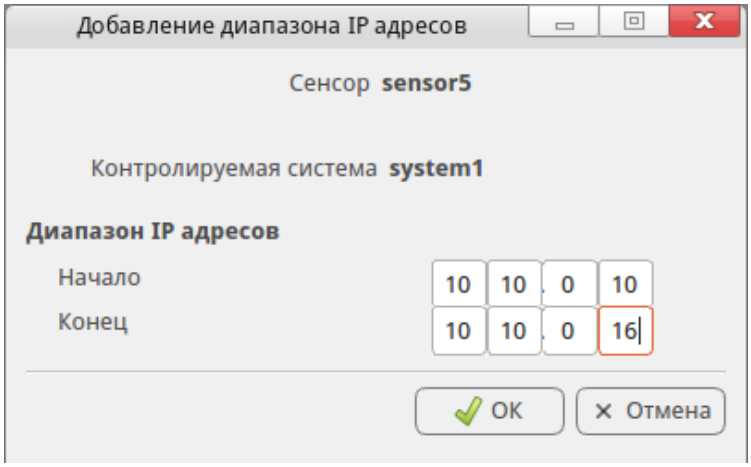


Рис. 59 Диалог добавления диапазона адресов

Для редактирования существующих контролируемых систем необходимо в главном окне (рис. 46) указать сенсор и выбрать пункт меню «Контролируемая система» > «Редактировать контролируемые системы» или соответствующую кнопку панели инструментов. В появившемся диалоге (рис. 60) отметить интересуемую КС и дважды нажать на строке левой клавишей мыши.

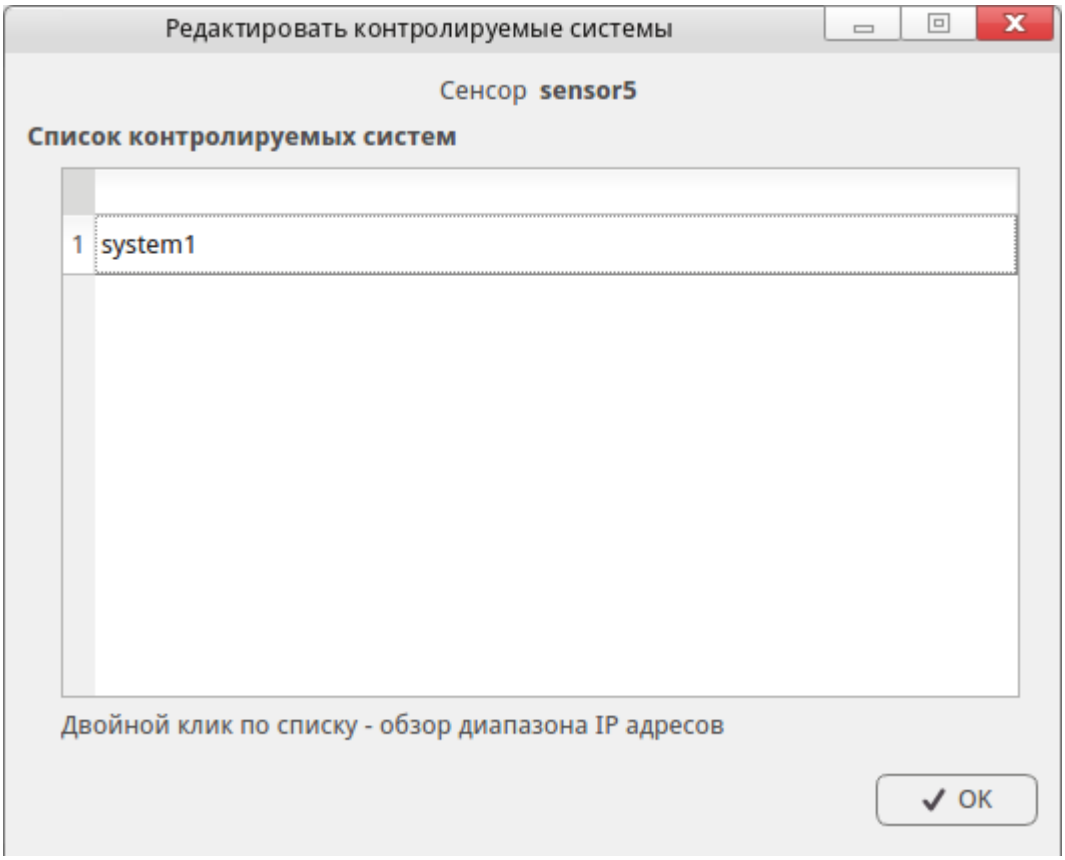


Рис. 60. Список зарегистрированных КС

В диалоге «Редактирование контролируемых систем» (рис. 61) операции с диапазонами IP адресов аналогичны операциям при добавлении КС.

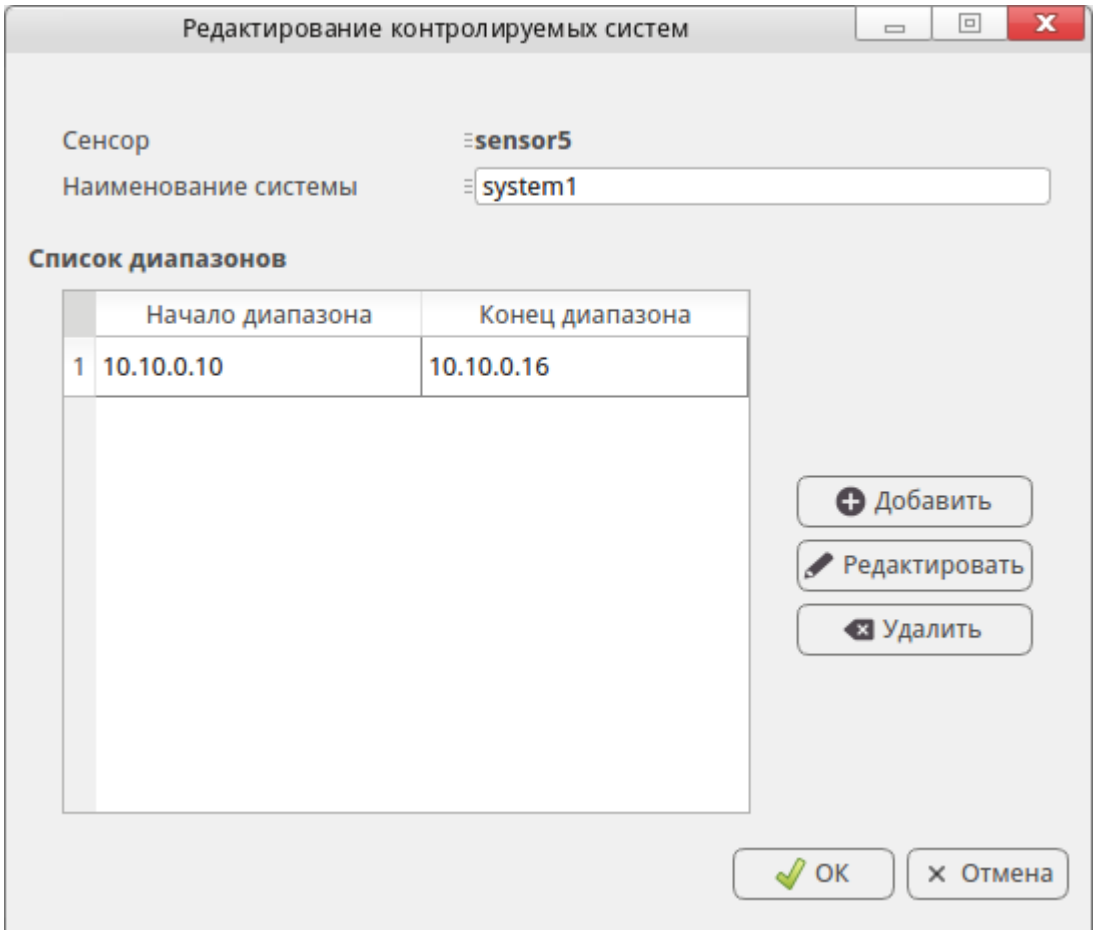


Рис. 61. Редактирование КС

Для удаления КС необходимо в главном окне (рис. 46) указать сенсор и выбрать пункт меню «Контролируемые системы» > «Удалить контролируемые системы» или выбрать соответствующую кнопку панели инструментов. В диалоге «Удаление контролируемых систем» (рис. 62) отметить подлежащие удалению КС и нажать кнопку [OK]. В появившемся предупреждающем сообщении подтвердить операцию удаления.

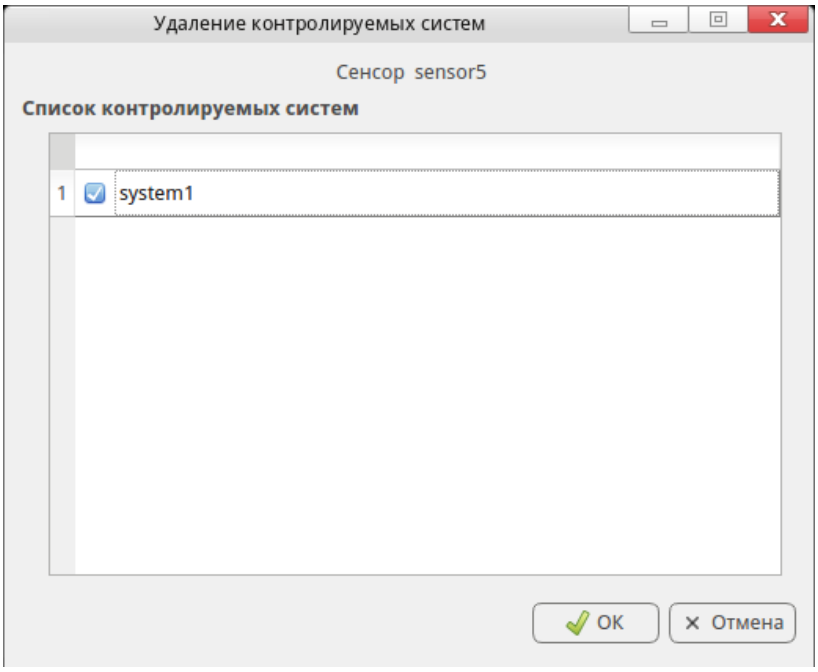


Рис. 62. Диалог удаления КС

Для просмотра контролируемых систем, зарегистрированных за сенсором, без их редактирования необходимо в главном окне (рис. 46) указать сенсор и выбрать пункт меню «Контролируемая система» > «Обзор контролируемых систем» или соответствующую кнопку панели инструментов (рис. 63).

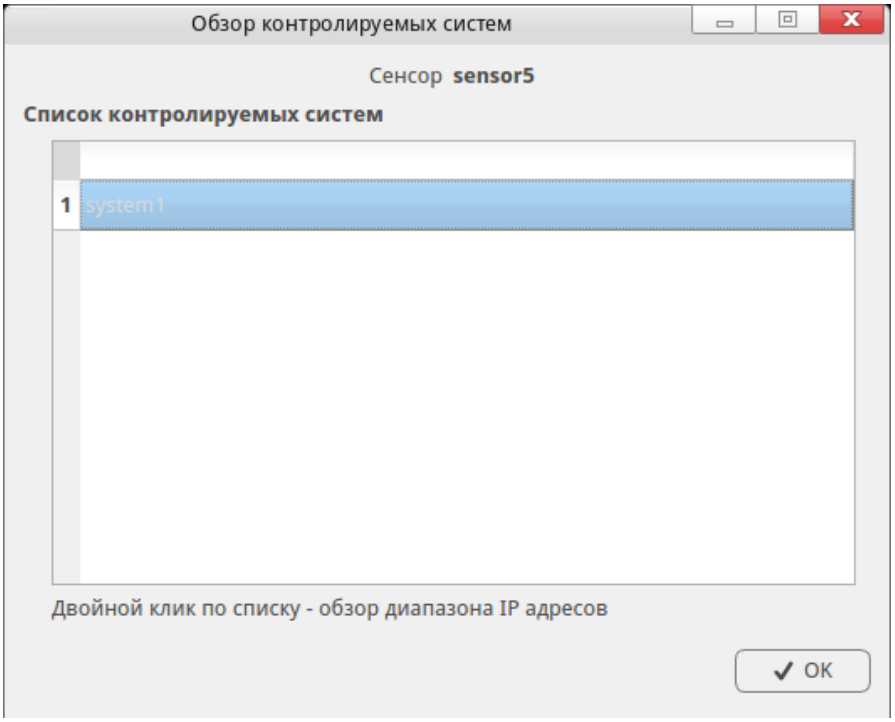


Рис. 63. Обзор контролируемых систем

Для просмотра списка диапазонов IP-адресов, зарегистрированных за контролируемой системой необходимо дважды кликнуть левой клавишей мыши по

выбранной контролируемой системе. В диалоге (рис. 64) отображается список диапазонов IP-адресов с указанием IP-адресов начала и конца диапазона.

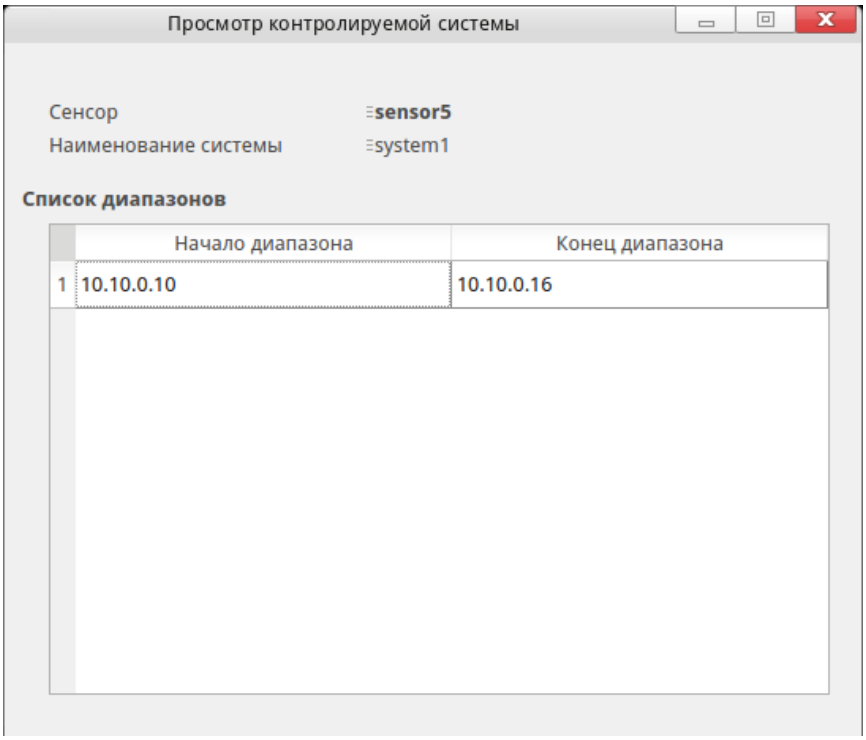


Рис. 64. Просмотр диапазонов IP адресов контролируемой системы

2.6. ПМ «Визуализации статистики компьютерных атак»

2.6.1. Запуск ПМ «Визуализации статистики компьютерных атак»

Для запуска ПМ «Визуализация статистики компьютерных атак» необходимо запустить терминал, ввести команду **msoa_attack** и нажать клавишу **[Enter]**. После запуска программы появится основное окно, вкладка «Критические атаки» (рис. 65).

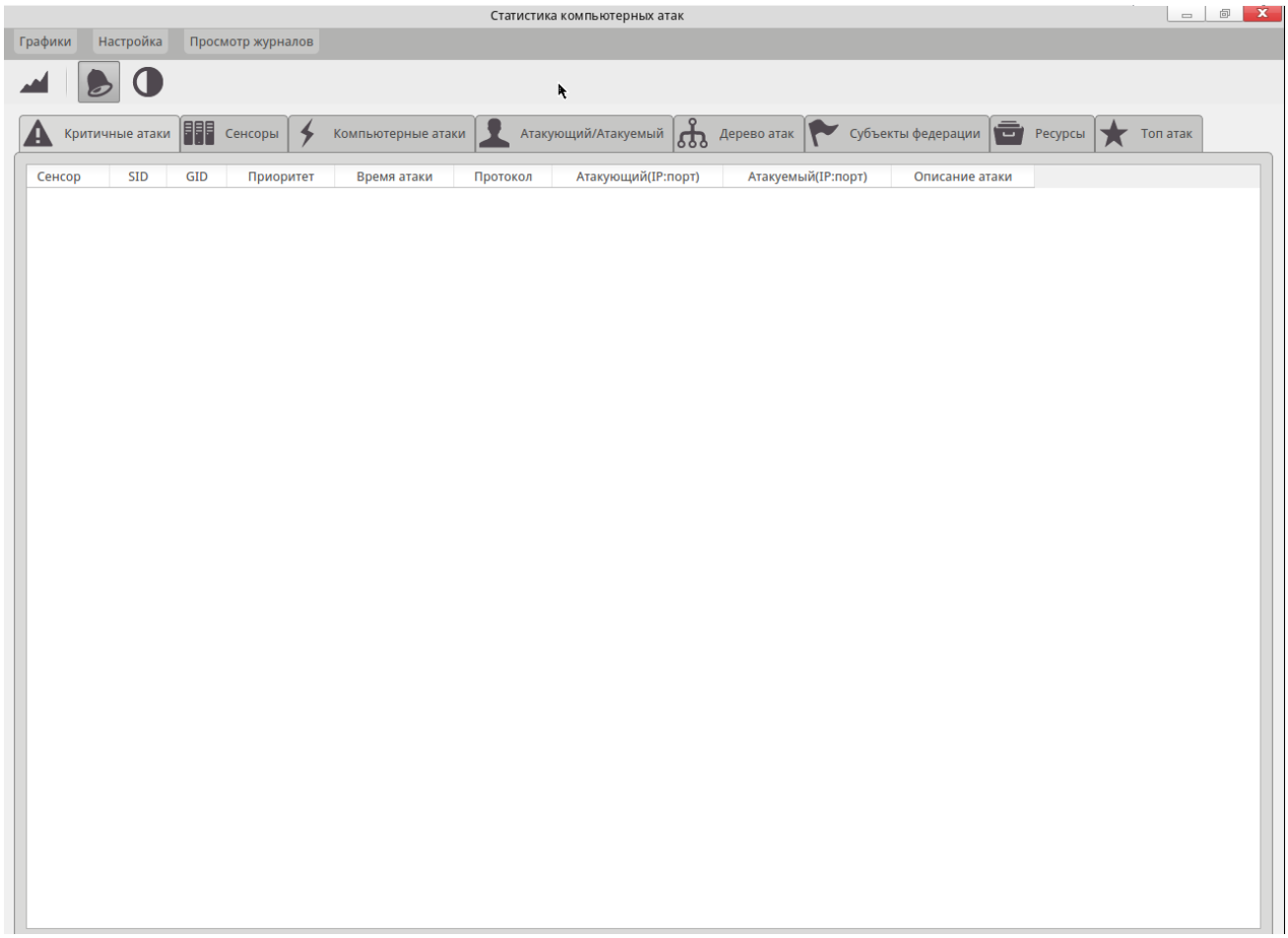


Рис. 65. Главное окно программы

ПМ «Визуализация статистики компьютерных атак» может выполнять следующий набор действий:

1) получать информацию о динамике обнаружения КА с учетом заданных параметров фильтрации и интервала обновления статистики;
2) строить статистические выкладки оценки компьютерных атак с заданными параметрами фильтрации;
3) формировать отчетные документы по полученной статистике.

2.6.2. Получение статистической информации о КА

Для получения статистической информации о КА в реальном масштабе времени необходимо настроить использование гистограмм и нажать кнопку «Динамическая статистика»  или в меню «Графики» —> «Динамическая статистика».

2.6.2.1. Настройка параметров фильтрации.

Для установки параметров фильтрации для графика реального времени необходимо нажать кнопку  «Настройки» на боковой панели инструментов. В появившемся диалоге «Настройки» (рис. 66), следует заполнить следующие параметры:

– Сенсор;
– Приоритет;
– Дополнительные параметры.

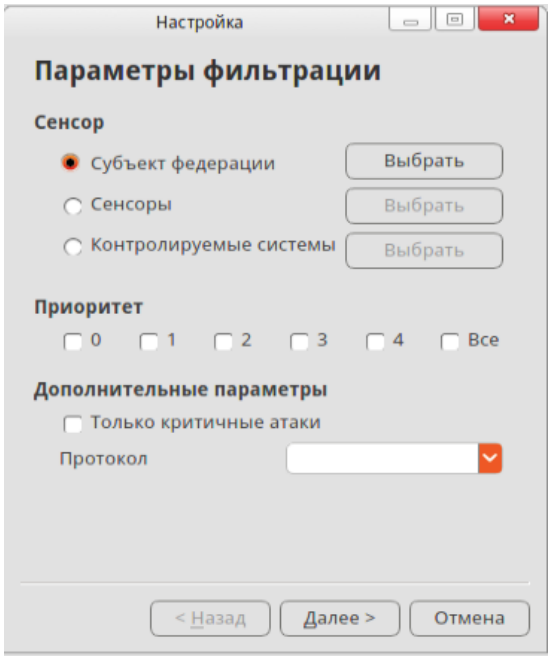


Рис. 66. Окно «Параметры фильтрации»

Настройка субъекта федерации в параметрах фильтрации

Для выбора субъекта федерации необходимо выбрать пункт «Субъект федерации» и нажать кнопку «Выбрать» при этом появиться диалог выбора субъекта федерации (рис. 67).

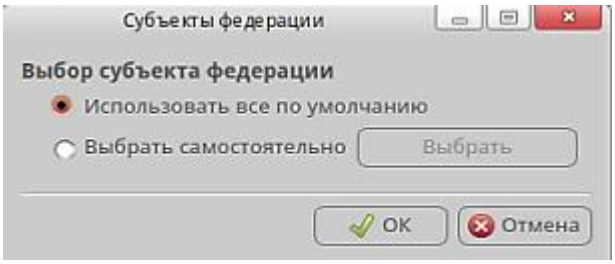


Рис. 67. Диалог «Субъекты федерации»

Пользователь может выбрать все субъекты федерации, используя пункт «Использовать все по умолчанию», или выбрать самостоятельно список субъектов, для этого выбрать пункт «Выбрать самостоятельно» и нажать кнопку «Выбрать».

При самостоятельном выборе субъекта федерации появится диалоговое окно, в котором необходимо выбрать нужные названия субъектов с помощью галочек. Для сохранения настроек фильтрации необходимо нажать кнопку «ОК», для отмены изменений нажать кнопку «Отмена».

Настройка сенсоров в параметрах фильтрации

При выборе пункта фильтрации «Сенсоры» и нажатии кнопки «Выбрать» появится диалог выбора сенсоров фиксации КА (рис. 68).

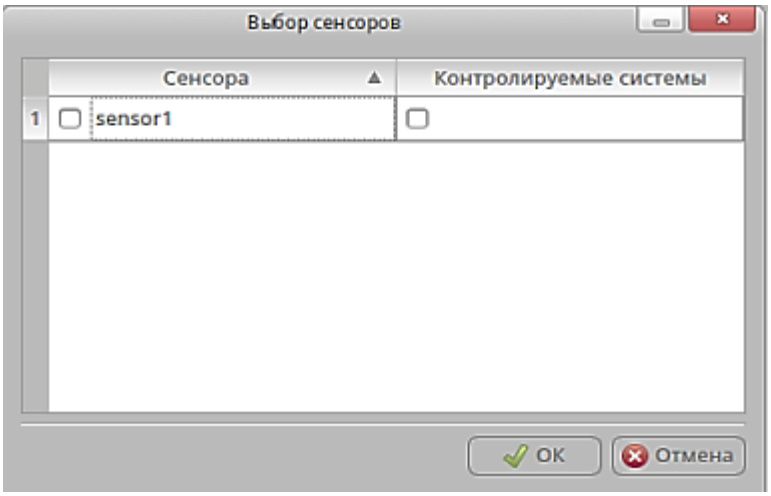


Рис. 68. Диалог выбора отдельных сенсоров

В появившемся диалоге установить галочки перед названиями требуемых сенсоров и контролируемых систем. При отметке контролируемых систем (КС) сенсора появляется диалог выбора контролируемых систем (рис. 69). Пользователь может выбрать все КС сенсора, используя пункт «Использовать все по умолчанию»,

или выбрать самостоятельно список КС, выбрав пункт «Выбрать самостоятельно» и нажав кнопку «Выбрать».

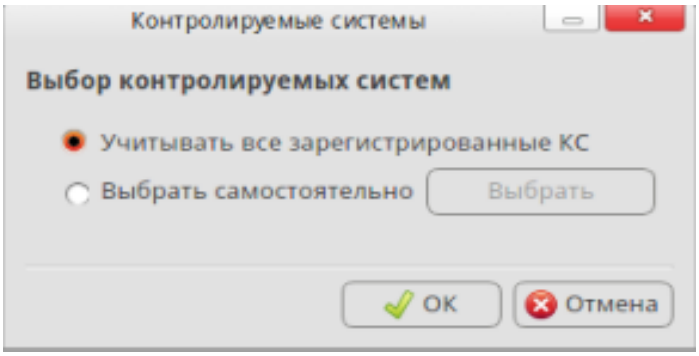


Рис. 69. Диалог «Контролируемые системы»

При самостоятельном выборе контролируемых систем, после нажатия кнопки «Выбрать», появится диалоговое окно (рис. 70) в котором пользователь устанавливает галочки перед названиями необходимых систем. Для сохранения настроек фильтрации необходимо нажать кнопку «ОК», для отмены изменений нажать кнопку «Отмена».

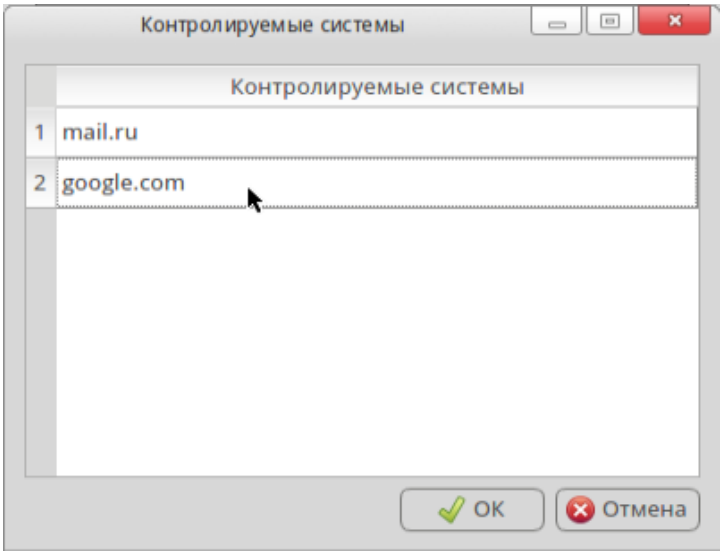


Рис. 70. Диалог выбора отдельных КС для выбранного сенсора

Настройка контролируемые систем в параметрах фильтрации

При выборе пункта фильтрации «Контролируемые системы» и нажатии кнопки «Выбрать» появится диалог выбора всех зарегистрированных КС (рис. 70). Для выбора КС необходимо выделить строку с его содержимым путем однократного

нажатия левой клавиши мыши на строке КС. Для сохранения настроек необходимо нажать кнопку «ОК», для отмены фильтрации кнопку «Отмена».

2.6.2.2. Отображение статистической информации о КА в различных представлениях.

После окончания выбора параметров фильтрации необходимо нажать кнопку «Далее». В появившемся окне (рис. 71) необходимо выбрать форму вывода статистики, доступную в трех вариантах:

– гистограмма;
– круговая диаграмма;
– карта.

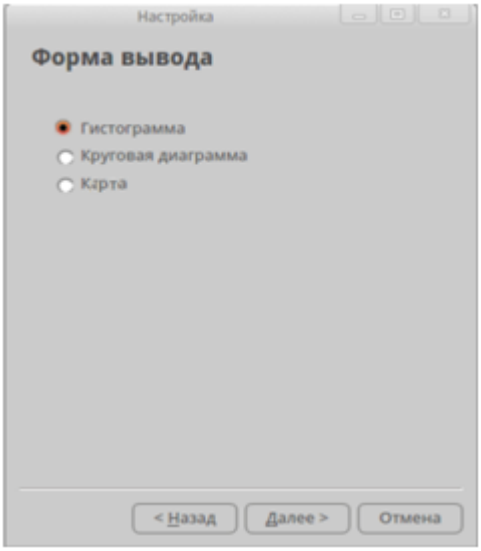


Рис. 71. Диалог выбора формы вывода статистики

При выборе пункта «Гистограмма» откроется окно, в котором необходимо выбрать цвет графика и количество выводимых столбцов (рис. 72). После установки параметров вывода гистограммы необходимо нажать кнопку «Далее».

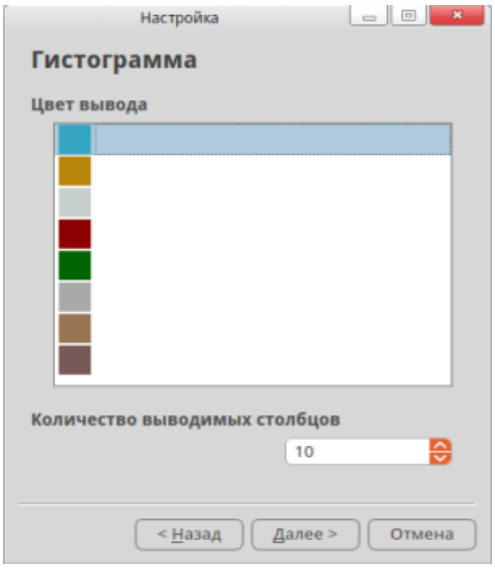


Рис. 72. Диалог настройки гистограммы

При выборе пункта «Круговая диаграмма» откроется окно, в котором необходимо выбрать параметры группирования компьютерных атак (рис. 73).

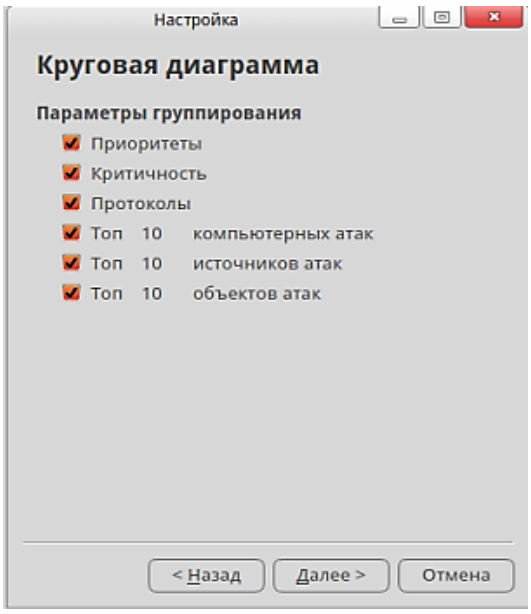


Рис. 73. Диалог настроек круговой диаграммы

После установки параметров вывода круговой диаграммы необходимо нажать кнопку «Далее».

В открывшемся окне необходимо настроить интервал обновления диаграммы. Для этого необходимо выбрать один из предложенных вариантов интервала обновления или задать требуемый интервал вручную, и нажать кнопку «Завершить».

Для запуска статистики в режиме реального времени с заданными параметрами необходимо нажать кнопку  на боковой панели инструментов, появится окно вывода статистики (рис. 74).

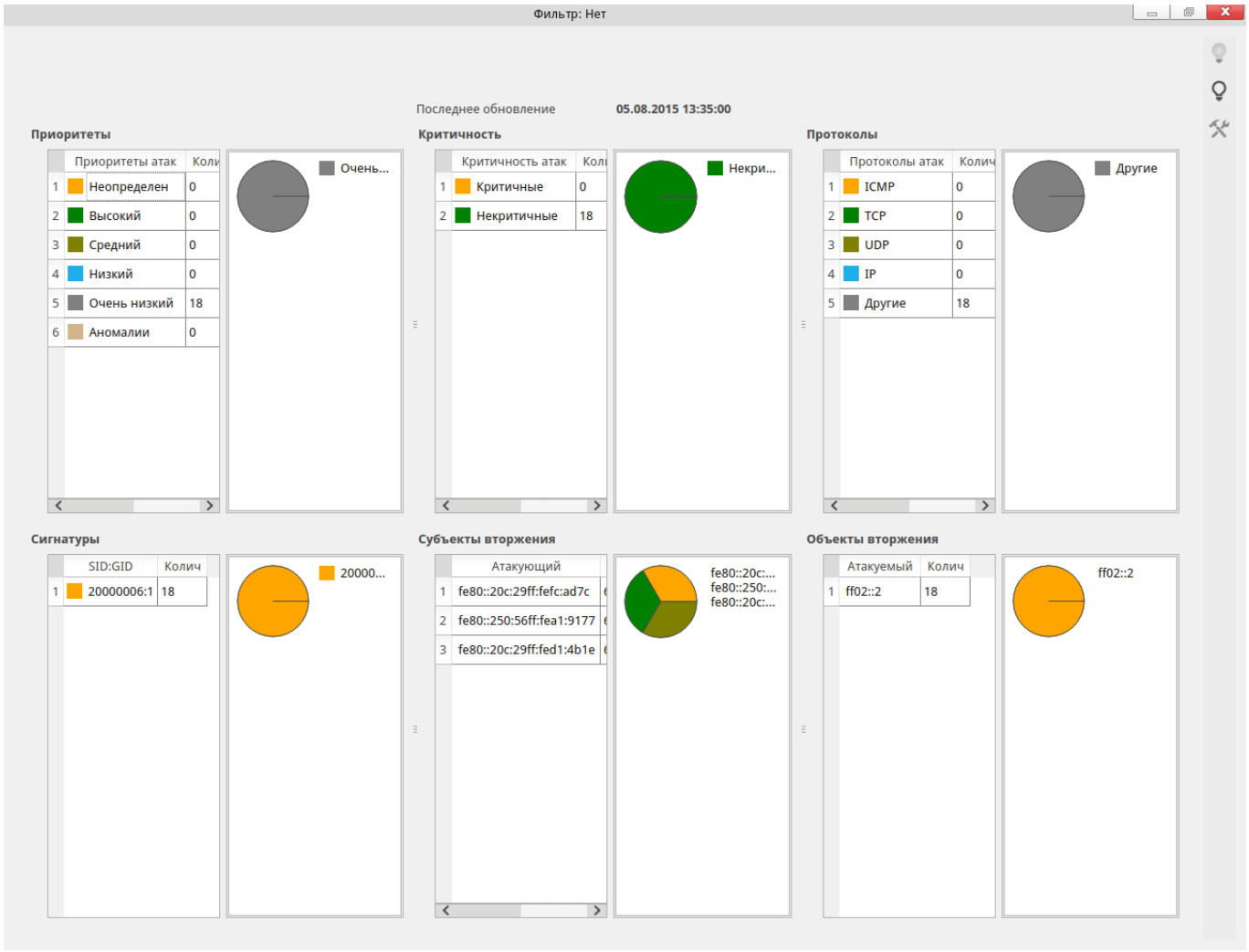
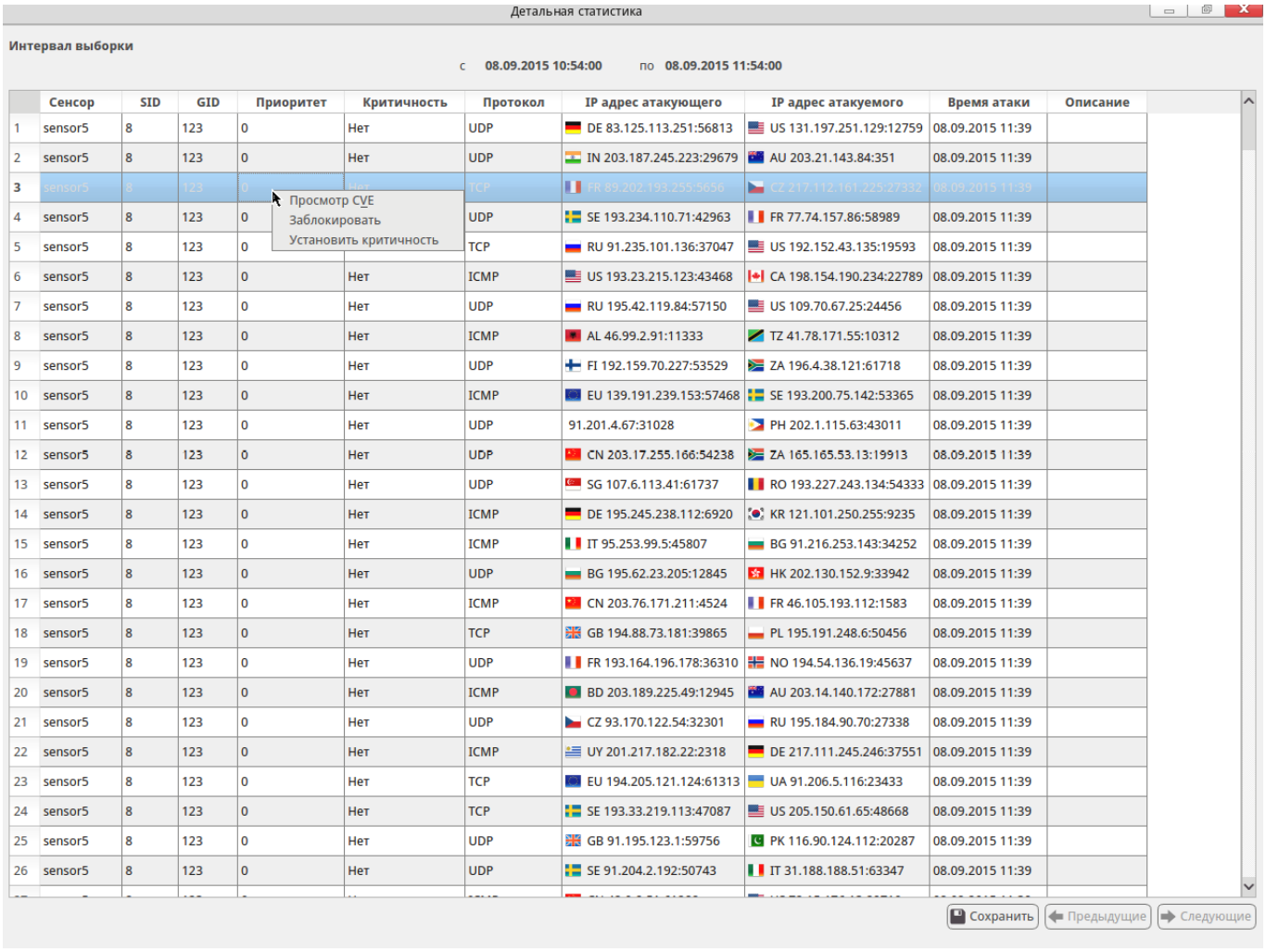


Рис. 74. Окно статистики в виде круговой диаграммы

Для вывода детальной информации (рис. 75) по атакам необходимо нажать интересующую колонку диаграммы.



	Сенсор	SID	GID	Приоритет	Критичность	Протокол	IP адрес атакующего	IP адрес атакуемого	Время атаки	Описание
1	sensor5	8	123	0	Нет	UDP	DE 83.125.113.251:56813	US 131.197.251.129:12759	08.09.2015 11:39	
2	sensor5	8	123	0	Нет	UDP	IN 203.187.245.223:29679	AU 203.21.143.84:351	08.09.2015 11:39	
3	sensor5	8	123	0	Нет	TCP	FR 89.202.193.255:5656	CZ 217.112.161.225:27332	08.09.2015 11:39	
4	sensor5	8	123	0	Нет	UDP	SE 193.234.110.71:42963	FR 77.74.157.86:58989	08.09.2015 11:39	
5	sensor5	8	123	0	Нет	TCP	RU 91.235.101.136:37047	US 192.152.43.135:19593	08.09.2015 11:39	
6	sensor5	8	123	0	Нет	ICMP	US 193.23.215.123:43468	CA 198.154.190.234:22789	08.09.2015 11:39	
7	sensor5	8	123	0	Нет	UDP	RU 195.42.119.84:57150	US 109.70.67.25:24456	08.09.2015 11:39	
8	sensor5	8	123	0	Нет	ICMP	AL 46.99.2.91:11333	TZ 41.78.171.55:10312	08.09.2015 11:39	
9	sensor5	8	123	0	Нет	UDP	FI 192.159.70.227:53529	ZA 196.4.38.121:61718	08.09.2015 11:39	
10	sensor5	8	123	0	Нет	ICMP	EU 139.191.239.153:57468	SE 193.200.75.142:53365	08.09.2015 11:39	
11	sensor5	8	123	0	Нет	UDP	91.201.4.67:31028	PH 202.1.115.63:43011	08.09.2015 11:39	
12	sensor5	8	123	0	Нет	UDP	CN 203.17.255.166:54238	ZA 165.165.53.13:19913	08.09.2015 11:39	
13	sensor5	8	123	0	Нет	UDP	SG 107.6.113.41:61737	RO 193.227.243.134:54333	08.09.2015 11:39	
14	sensor5	8	123	0	Нет	ICMP	DE 195.245.238.112:6920	KR 121.101.250.255:9235	08.09.2015 11:39	
15	sensor5	8	123	0	Нет	ICMP	IT 95.253.99.5:45807	BG 91.216.253.143:34252	08.09.2015 11:39	
16	sensor5	8	123	0	Нет	UDP	BG 195.62.23.205:12845	HK 202.130.152.9:33942	08.09.2015 11:39	
17	sensor5	8	123	0	Нет	ICMP	CN 203.76.171.211:4524	FR 46.105.193.112:1583	08.09.2015 11:39	
18	sensor5	8	123	0	Нет	TCP	GB 194.88.73.181:39865	PL 195.191.248.6:50456	08.09.2015 11:39	
19	sensor5	8	123	0	Нет	UDP	FR 193.164.196.178:36310	NO 194.54.136.19:45637	08.09.2015 11:39	
20	sensor5	8	123	0	Нет	ICMP	BD 203.189.225.49:12945	AU 203.14.140.172:27881	08.09.2015 11:39	
21	sensor5	8	123	0	Нет	UDP	CZ 93.170.122.54:32301	RU 195.184.90.70:27338	08.09.2015 11:39	
22	sensor5	8	123	0	Нет	ICMP	UY 201.217.182.22:2318	DE 217.111.245.246:37551	08.09.2015 11:39	
23	sensor5	8	123	0	Нет	TCP	EU 194.205.121.124:61313	UA 91.206.5.116:23433	08.09.2015 11:39	
24	sensor5	8	123	0	Нет	TCP	SE 193.33.219.113:47087	US 205.150.61.65:48668	08.09.2015 11:39	
25	sensor5	8	123	0	Нет	UDP	GB 91.195.123.1:59756	PK 116.90.124.112:20287	08.09.2015 11:39	
26	sensor5	8	123	0	Нет	UDP	SE 91.204.2.192:50743	IT 31.188.188.51:63347	08.09.2015 11:39	

Рис. 75. Окно детальной статистики

Для просмотра содержимого атаки необходимо двойным нажатием выделить интересующую строку таблицы (рис. 76).

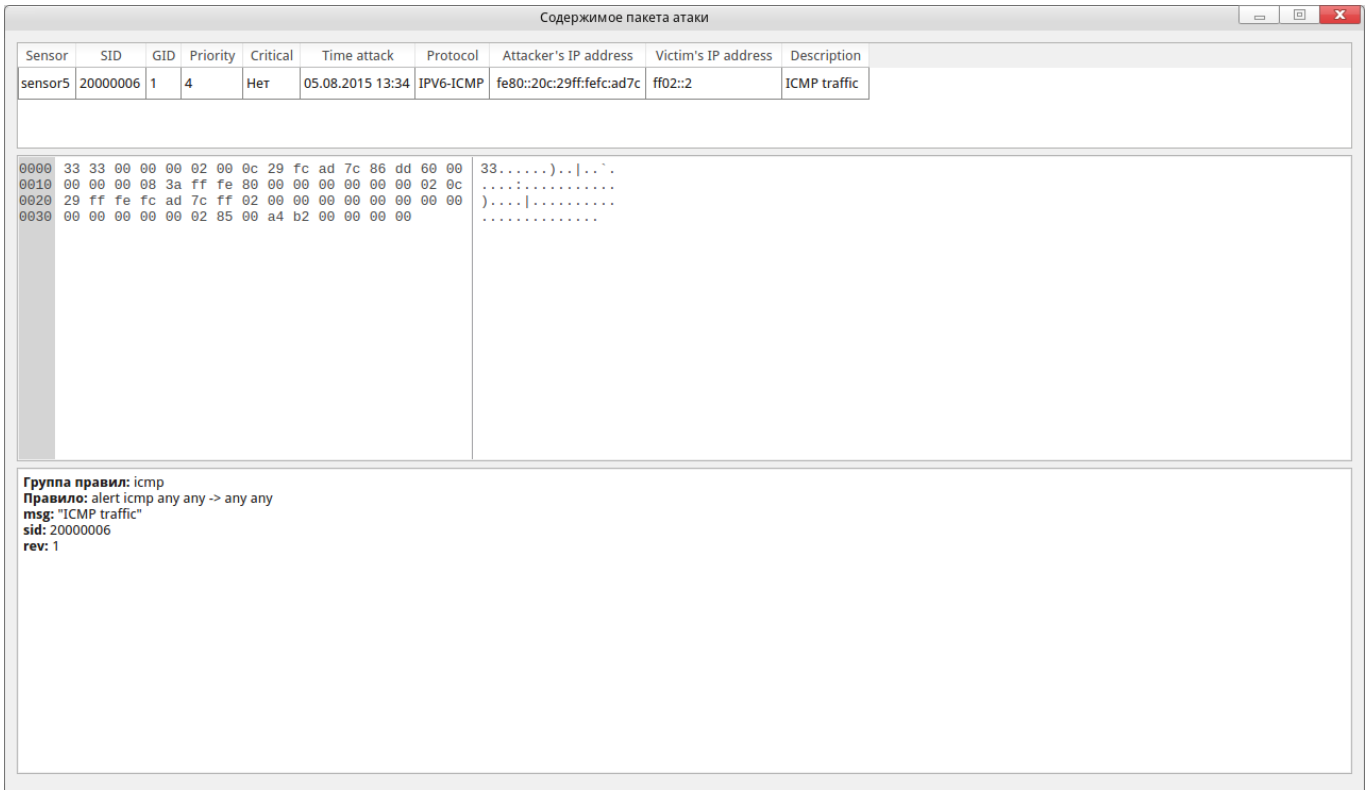


Рис. 76. Окно «Содержимое пакета атаки»

При правом клике на строке атаки в окне детальной статистики откроется контекстное меню, в котором можно выбрать пункты:

– «Просмотр CVE» - позволяет просмотреть описание известной компьютерной атаки, если оно есть (рис. 77);

– «Заблокировать» - позволяет задать правило блокировки атаки для межсетевого экрана;

– «Установить критичность» - позволяет задать флаг критичности для данной атаки.

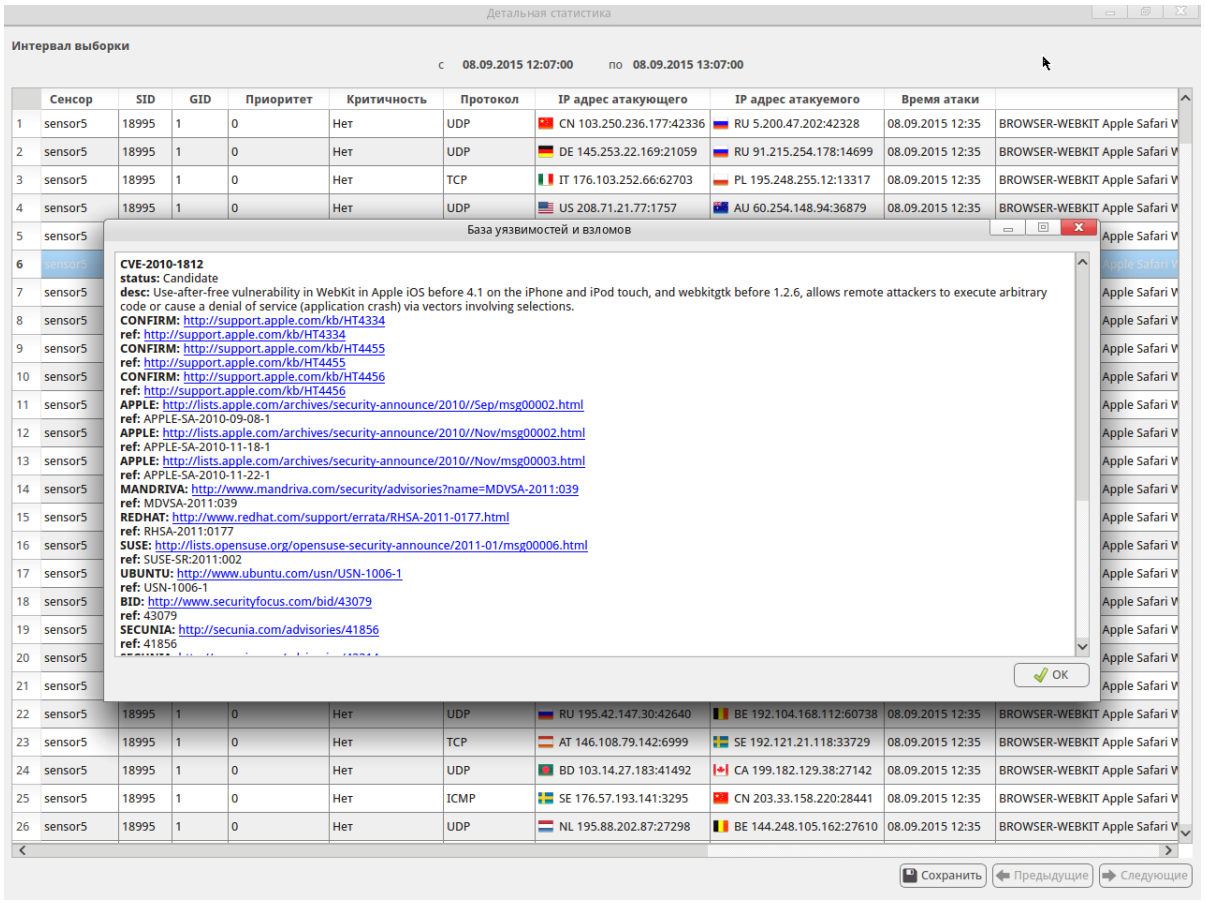


Рис. 77. Описание КА из базы CVE

При выборе пункта «Заблокировать» в появившемся диалоговом окне (рис. 78) следует выбрать параметры экранирования: действие и время блокировки, после чего нажать кнопку «ОК».

В качестве действия могут быть выбраны различные параметры блокировки:

– «Блокировать по ip-источника»;
– «Блокировать по ip-источника и ip-получателя»;
– «Блокировать по ip-источника и порту получателя»;
– «Блокировать по ip-источника и ip и порту получателя».

В качестве времени действия блокировки могут быть выбраны:

– «30 минут»;
– «1 час»;
– «1 день»;
– «Постоянно».

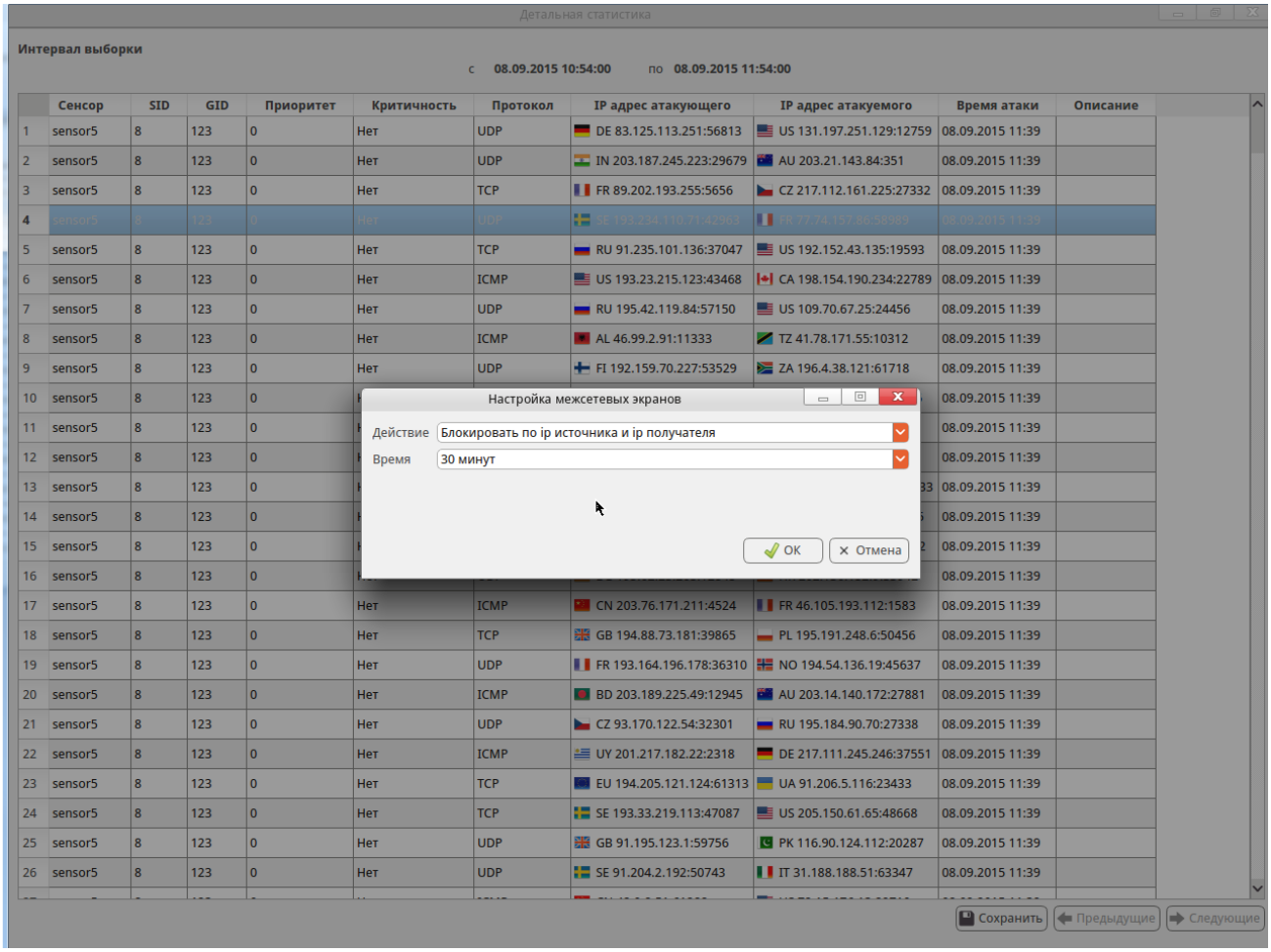
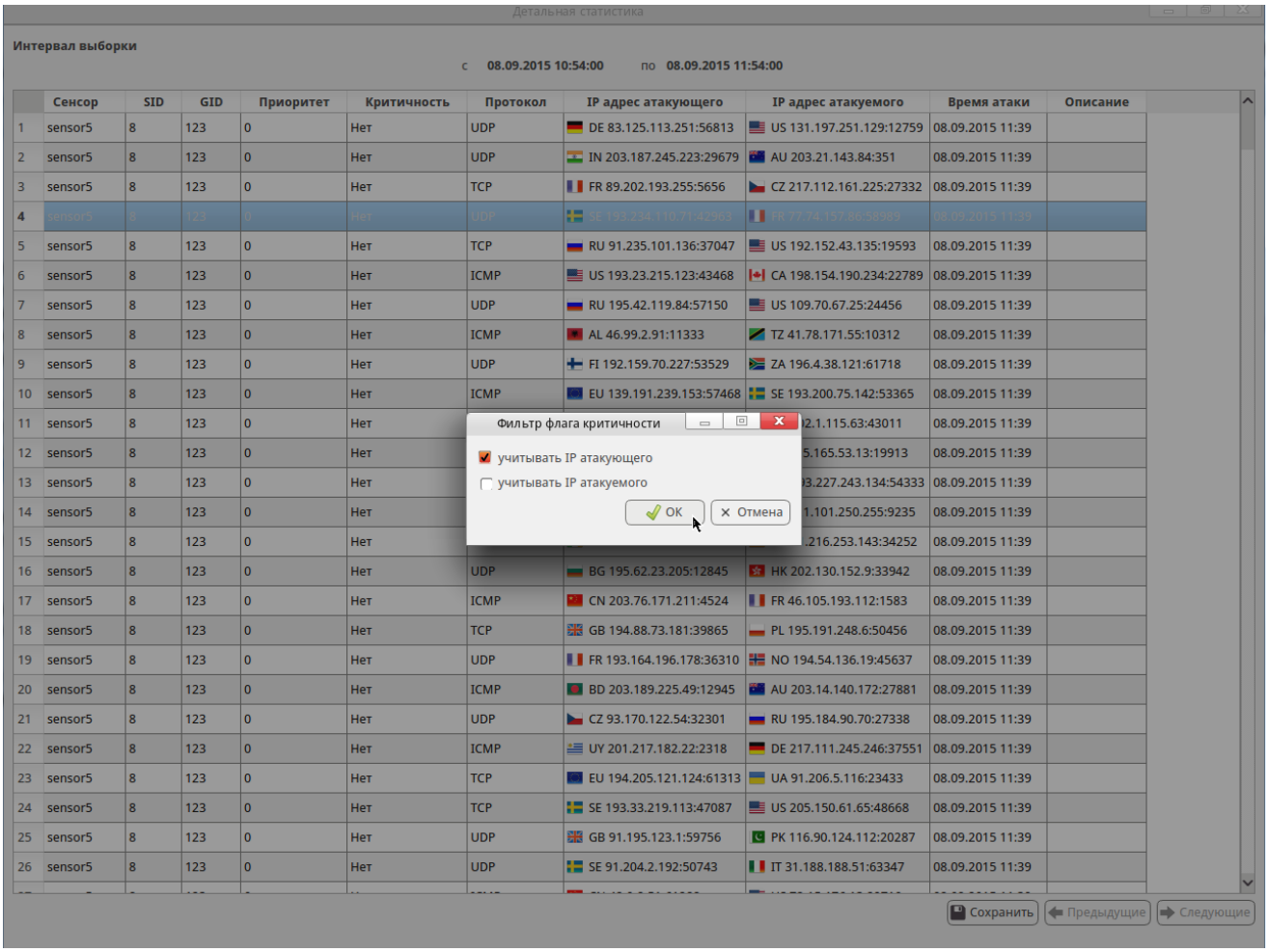


Рис. 78. Блокировка атаки путем задания правила межсетевого экранирования

При выборе пункта «Установить критичность» в появившемся диалоговом окне (рис. 79) следует переключателями выбрать, будет ли флаг критичности устанавливаться для данной атаки только при совпадении ip-адреса атакующего или атакуемого с указанными в таблице, после чего нажать кнопку «ОК».



	Сенсор	SID	GID	Приоритет	Критичность	Протокол	IP адрес атакующего	IP адрес атакуемого	Время атаки	Описание
1	sensor5	8	123	0	Нет	UDP	DE 83.125.113.251:56813	US 131.197.251.129:12759	08.09.2015 11:39	
2	sensor5	8	123	0	Нет	UDP	IN 203.187.245.223:29679	AU 203.21.143.84:351	08.09.2015 11:39	
3	sensor5	8	123	0	Нет	TCP	FR 89.202.193.255:5656	CZ 217.112.161.225:27332	08.09.2015 11:39	
4	sensor5	8	123	0	Нет	UDP	SE 193.234.110.71:42963	FR 77.74.157.86:58989	08.09.2015 11:39	
5	sensor5	8	123	0	Нет	TCP	RU 91.235.101.136:37047	US 192.152.43.135:19593	08.09.2015 11:39	
6	sensor5	8	123	0	Нет	ICMP	US 193.23.215.123:43468	CA 198.154.190.234:22789	08.09.2015 11:39	
7	sensor5	8	123	0	Нет	UDP	RU 195.42.119.84:57150	US 109.70.67.25:24456	08.09.2015 11:39	
8	sensor5	8	123	0	Нет	ICMP	AL 46.99.2.91:11333	TZ 41.78.171.55:10312	08.09.2015 11:39	
9	sensor5	8	123	0	Нет	UDP	FI 192.159.70.227:53529	ZA 196.4.38.121:61718	08.09.2015 11:39	
10	sensor5	8	123	0	Нет	ICMP	EU 139.191.239.153:57468	SE 193.200.75.142:53365	08.09.2015 11:39	
11	sensor5	8	123	0	Нет				08.09.2015 11:39	
12	sensor5	8	123	0	Нет				08.09.2015 11:39	
13	sensor5	8	123	0	Нет				08.09.2015 11:39	
14	sensor5	8	123	0	Нет				08.09.2015 11:39	
15	sensor5	8	123	0	Нет				08.09.2015 11:39	
16	sensor5	8	123	0	Нет	UDP	BG 195.62.23.205:12845	HK 202.130.152.9:33942	08.09.2015 11:39	
17	sensor5	8	123	0	Нет	ICMP	CN 203.76.171.211:4524	FR 46.105.193.112:1583	08.09.2015 11:39	
18	sensor5	8	123	0	Нет	TCP	GB 194.88.73.181:39865	PL 195.191.248.6:50456	08.09.2015 11:39	
19	sensor5	8	123	0	Нет	UDP	FR 193.164.196.178:36310	NO 194.54.136.19:45637	08.09.2015 11:39	
20	sensor5	8	123	0	Нет	ICMP	BD 203.189.225.49:12945	AU 203.14.140.172:27881	08.09.2015 11:39	
21	sensor5	8	123	0	Нет	UDP	CZ 93.170.122.54:32301	RU 195.184.90.70:27338	08.09.2015 11:39	
22	sensor5	8	123	0	Нет	ICMP	UY 201.217.182.22:2318	DE 217.111.245.246:37551	08.09.2015 11:39	
23	sensor5	8	123	0	Нет	TCP	EU 194.205.121.124:61313	UA 91.206.5.116:23433	08.09.2015 11:39	
24	sensor5	8	123	0	Нет	TCP	SE 193.33.219.113:47087	US 205.150.61.65:48668	08.09.2015 11:39	
25	sensor5	8	123	0	Нет	UDP	GB 91.195.123.1:59756	PK 116.90.124.112:20287	08.09.2015 11:39	
26	sensor5	8	123	0	Нет	UDP	SE 91.204.2.192:50743	IT 31.188.188.51:63347	08.09.2015 11:39	

Рис. 79. Установка флага критичности КА

Для прекращения сбора динамической статистики необходимо нажать кнопку на боковой панели инструментов.

При выборе формы отображения статистики в реальном времени на карте мира откроется окно (см. рис. 80), в котором для каждой страны в реальном времени отображается количество атак, направленных в данную страну и из данной страны.

Для изменения масштаба карты следует использовать колесо мыши, для перемещения отображаемой области карты следует нажать левую кнопку мыши и, не отпуская ее, переместить указатель мыши (отображаемая область карты при этом будет сдвигаться в окне), после чего отпустить кнопку мыши.

Для запуска статистики в режиме реального времени с заданными параметрами необходимо нажать кнопку на боковой панели инструментов, а для

прекращения сбора динамической статистики необходимо нажать кнопку  на боковой панели инструментов.

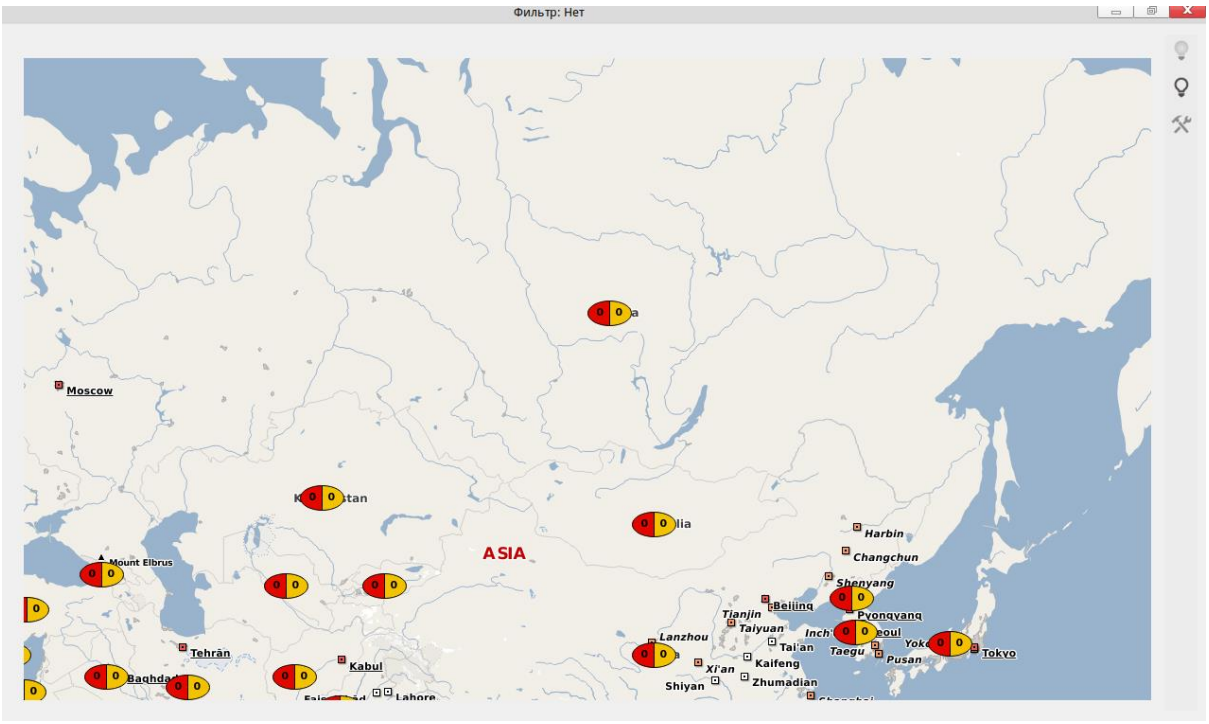


Рис. 80. Статистика по компьютерным атакам в режиме реального времени

2.6.3. Вкладка «Сенсоры»

Диалог «Сенсоры» предназначен для получения статистической информации по КА за выбранный период времени по конкретным сенсорам. Информация может быть представлена в виде гистограммы, в табличном виде или в виде сводной таблицы.

При выборе вкладки «Сенсоры» (рис. 81), следует установить следующие параметры:

– выбрать интересующие сенсоры;
– форму вывода;
– указать при необходимости направление атак;
– период выборки;
– интервал построения гистограммы (минута, час, сутки, неделя).

Для сохранения настроек нажать кнопку «Применить».

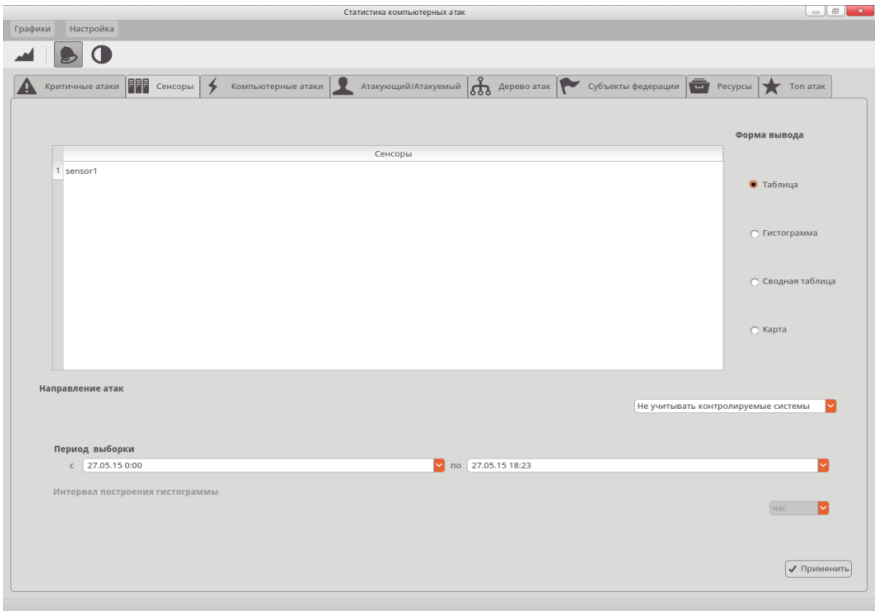
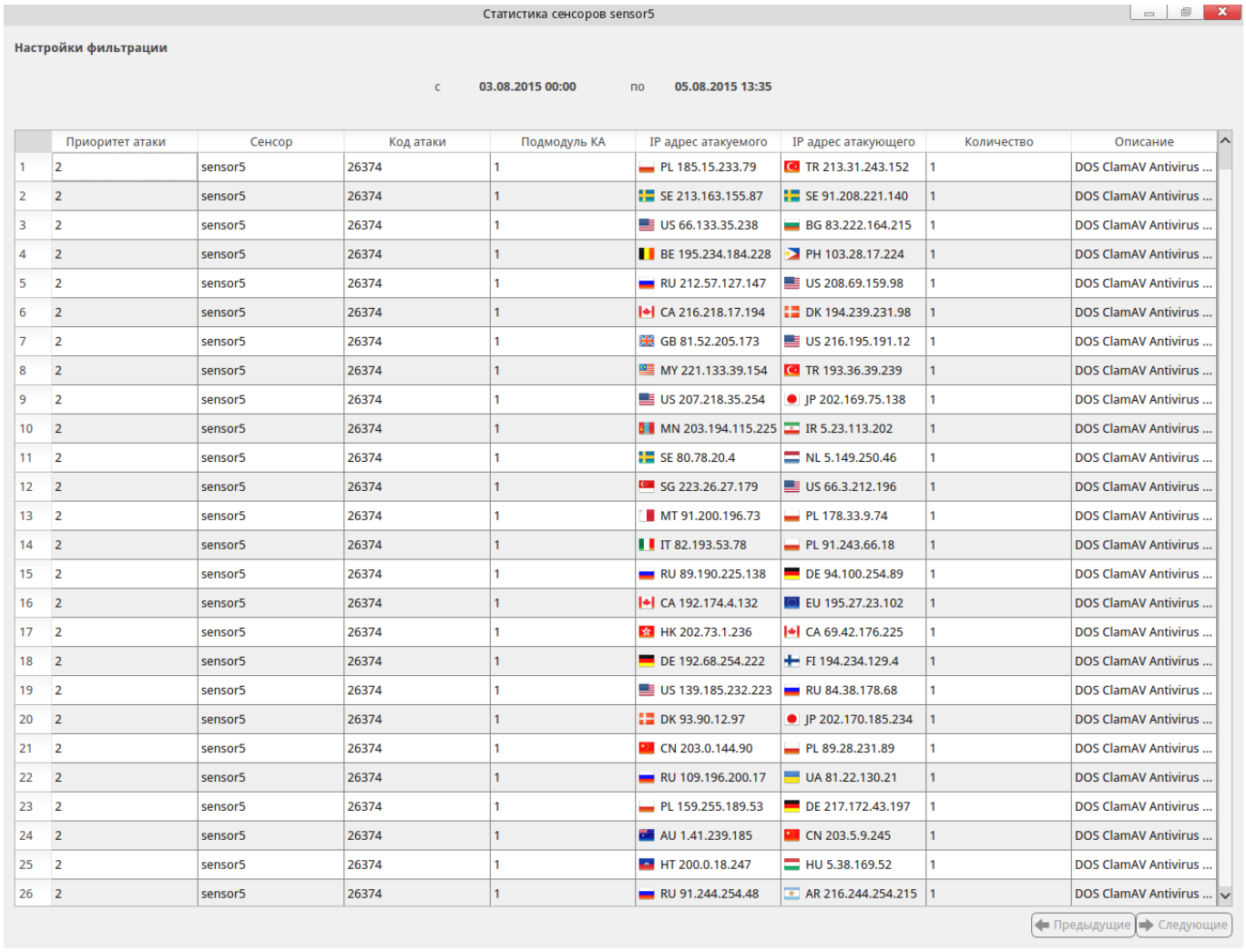


Рис. 81. Вкладка «Сенсоры»

При этом в зависимости от выбора способа вывода информации она будет выдана в виде таблицы (рис. 82), гистограммы (рис. 83), сводного отчета (рис. 84) или на карте мира (рис. 85).



	Приоритет атаки	Сенсор	Код атаки	Подмодуль КА	IP адрес атакуемого	IP адрес атакующего	Количество	Описание
1	2	sensor5	26374	1	PL 185.15.233.79	TR 213.31.243.152	1	DOS ClamAV Antivirus ...
2	2	sensor5	26374	1	SE 213.163.155.87	SE 91.208.221.140	1	DOS ClamAV Antivirus ...
3	2	sensor5	26374	1	US 66.133.35.238	BG 83.222.164.215	1	DOS ClamAV Antivirus ...
4	2	sensor5	26374	1	BE 195.234.184.228	PH 103.28.17.224	1	DOS ClamAV Antivirus ...
5	2	sensor5	26374	1	RU 212.57.127.147	US 208.69.159.98	1	DOS ClamAV Antivirus ...
6	2	sensor5	26374	1	CA 216.218.17.194	DK 194.239.231.98	1	DOS ClamAV Antivirus ...
7	2	sensor5	26374	1	GB 81.52.205.173	US 216.195.191.12	1	DOS ClamAV Antivirus ...
8	2	sensor5	26374	1	MY 221.133.39.154	TR 193.36.39.239	1	DOS ClamAV Antivirus ...
9	2	sensor5	26374	1	US 207.218.35.254	JP 202.169.75.138	1	DOS ClamAV Antivirus ...
10	2	sensor5	26374	1	MN 203.194.115.225	IR 5.23.113.202	1	DOS ClamAV Antivirus ...
11	2	sensor5	26374	1	SE 80.78.20.4	NL 5.149.250.46	1	DOS ClamAV Antivirus ...
12	2	sensor5	26374	1	SG 223.26.27.179	US 66.3.212.196	1	DOS ClamAV Antivirus ...
13	2	sensor5	26374	1	MT 91.200.196.73	PL 178.33.9.74	1	DOS ClamAV Antivirus ...
14	2	sensor5	26374	1	IT 82.193.53.78	PL 91.243.66.18	1	DOS ClamAV Antivirus ...
15	2	sensor5	26374	1	RU 89.190.225.138	DE 94.100.254.89	1	DOS ClamAV Antivirus ...
16	2	sensor5	26374	1	CA 192.174.4.132	EU 195.27.23.102	1	DOS ClamAV Antivirus ...
17	2	sensor5	26374	1	HK 202.73.1.236	CA 69.42.176.225	1	DOS ClamAV Antivirus ...
18	2	sensor5	26374	1	DE 192.68.254.222	FI 194.234.129.4	1	DOS ClamAV Antivirus ...
19	2	sensor5	26374	1	US 139.185.232.223	RU 84.38.178.68	1	DOS ClamAV Antivirus ...
20	2	sensor5	26374	1	DK 93.90.12.97	JP 202.170.185.234	1	DOS ClamAV Antivirus ...
21	2	sensor5	26374	1	CN 203.0.144.90	PL 89.28.231.89	1	DOS ClamAV Antivirus ...
22	2	sensor5	26374	1	RU 109.196.200.17	UA 81.22.130.21	1	DOS ClamAV Antivirus ...
23	2	sensor5	26374	1	PL 159.255.189.53	DE 217.172.43.197	1	DOS ClamAV Antivirus ...
24	2	sensor5	26374	1	AU 1.41.239.185	CN 203.5.9.245	1	DOS ClamAV Antivirus ...
25	2	sensor5	26374	1	HT 200.0.18.247	HU 5.38.169.52	1	DOS ClamAV Antivirus ...
26	2	sensor5	26374	1	RU 91.244.254.48	AR 216.244.254.215	1	DOS ClamAV Antivirus ...

Рис. 82. Представление информации в табличном виде

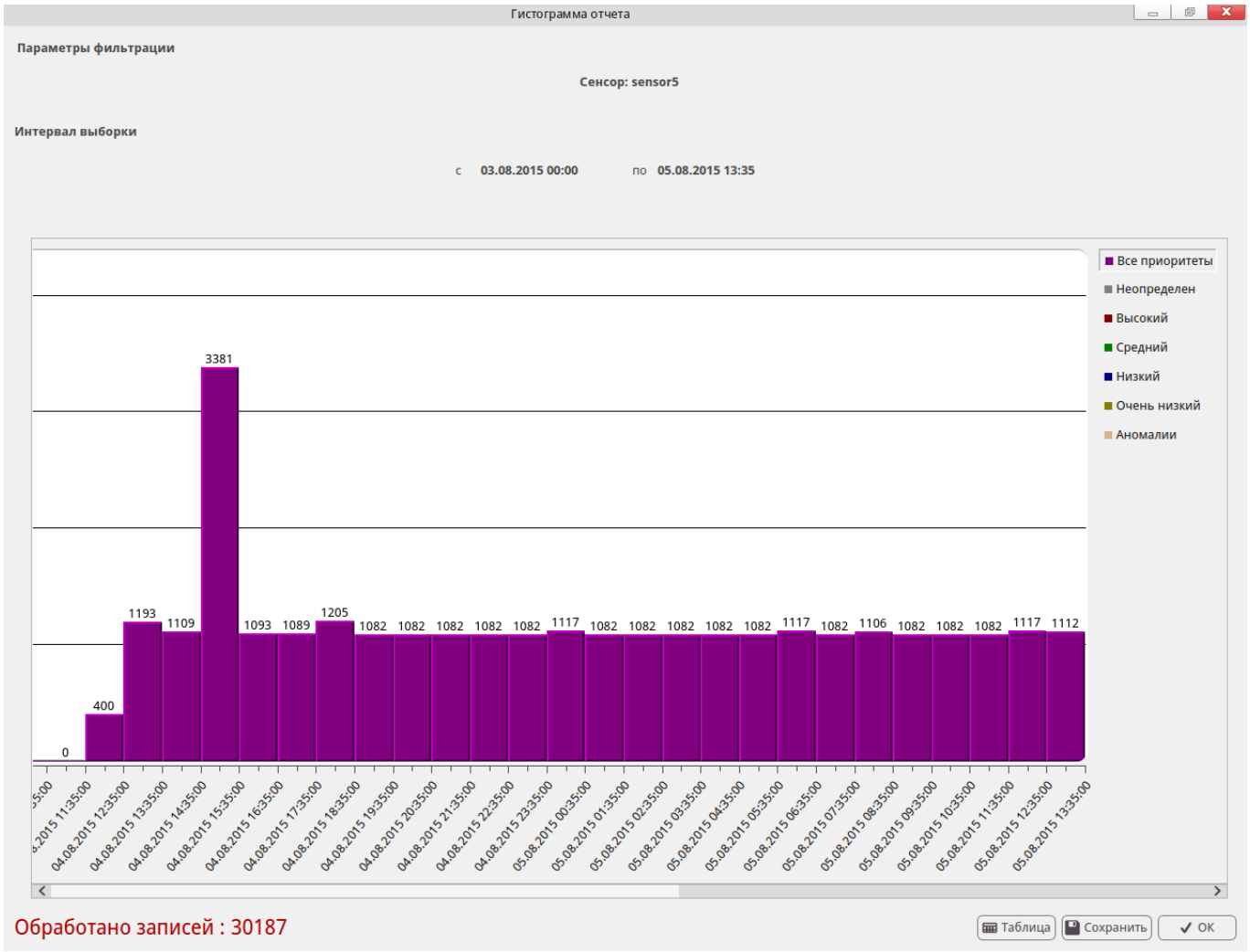


Рис. 83. Представление информации в виде гистограммы

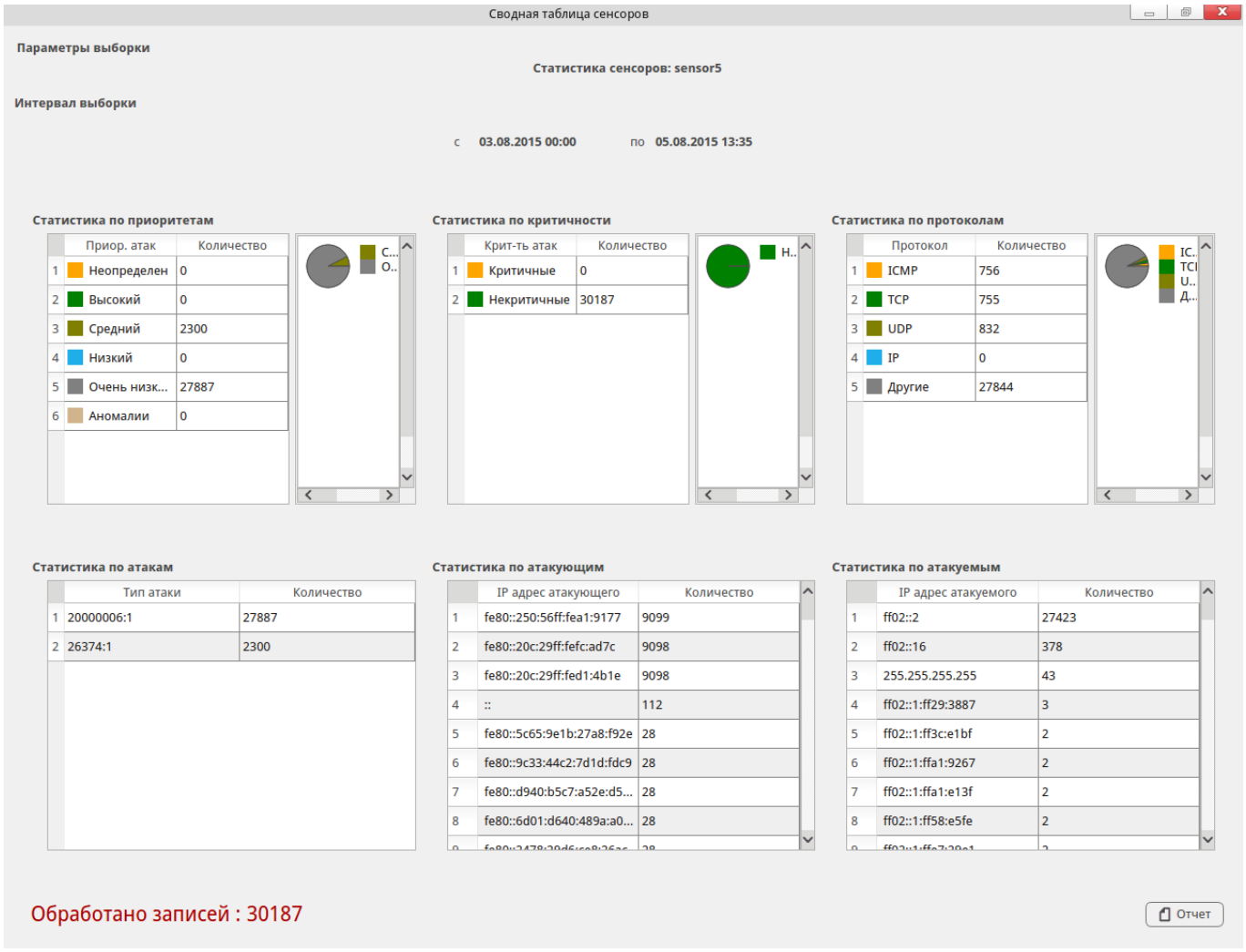


Рис. 84. Сводный отчет КА по сенсорам

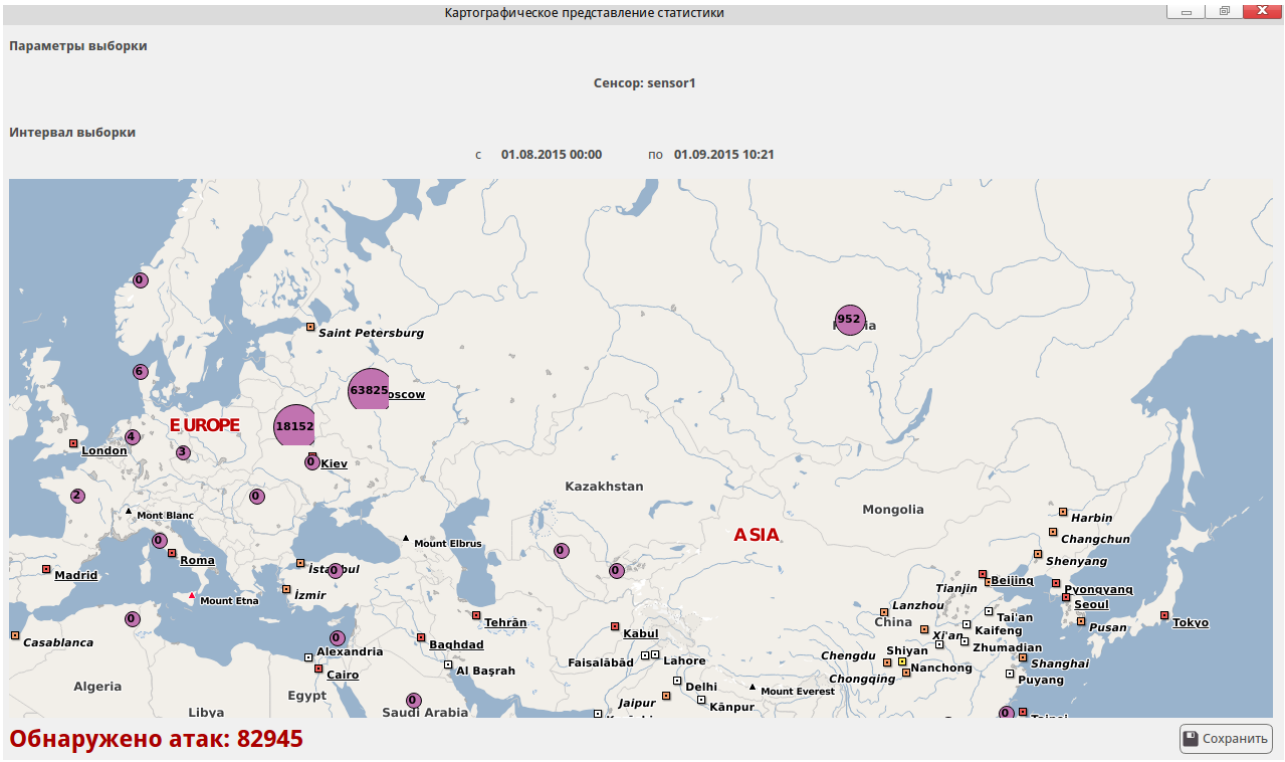


Рис. 85. Визуализация статистики по КА на карте мира

При двойном нажатии на строку табличной формы вывода, выводится детальная статистика компьютерных атак (рис. 75), а по правому клику для КА через контекстное меню доступны команды «Просмотр CVE» и «Заблокировать», описанные ранее.

Для просмотра значений гистограммы необходимо нажать кнопку «Таблица». В появившемся окне можно просмотреть данные по каждому приоритету. При необходимости сохранить данные, нажать кнопку «Сохранить».

Форма вывода «Сводная таблица» содержит сводные отчеты по следующим статистикам:

– Приоритеты;
– Критичность;
– Протоколы;
– Коды атак;
– Субъекты атаки;
– Объекты атаки.

Пользователь может вывести отчет по общей статистике при нажатии кнопки «Отчет».

Для сохранения отчета нажмите кнопку «Сохранить».

При выборе формы вывода «Карта» откроется окно отображения статистики по зарегистрированным КА на карте мира (рис. 85). На карте отображается распределение количества КА, соответствующих заданным критериям отбора, по странам – источникам этих атак. Для каждой страны выводится количество зафиксированных атак, источники которых находятся в этой стране.

Для изменения масштаба карты следует использовать колесо мыши, для перемещения отображаемой области карты следует нажать левую кнопку мыши и, не отпуская ее, переместить указатель мыши (отображаемая область карты при этом будет сдвигаться в окне), после чего отпустить кнопку мыши.

2.6.4. Вкладка «Атакующий\Атакуемый»

Вкладка «Атакующий\Атакуемый» (рис. 86) предназначена для получения статистической информации по КА за выбранный период времени по конкретным IP-адресам источников атак. Информация в зависимости от выбора может быть представлена в следующем виде:

– гистограммы;
– таблицы;
– отображена на карте.

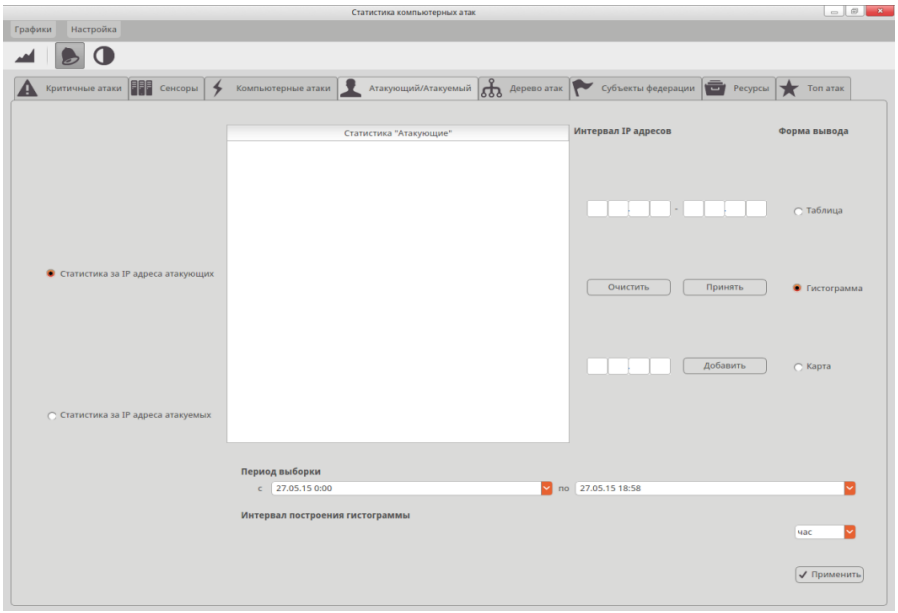


Рис. 86. Вкладка «Атакующий\Атакуемый»

Для вывода зафиксированных IP-адресов атакующих хостов за данный период выборки требуется установить переключатель «Статистика за IP-адреса атакующих», а в разделе «Интервал IP адресов» – указать начальный и конечный IP адрес возможного источника угрозы. После нажатия кнопки «Принять» выбранный диапазон попадет в область «Статистика «Атакующие»». С использованием поля «Добавить», можно внести отдельную запись в виде IP адреса атакующего. Далее следует выбрать форму вывода «Таблица», «Гистограмма» или «Карта». При построении данных можно выбрать группу IP адресов из списка «Статистика «Атакующие». Также следует заполнить интервал для гистограммы (час, сутки, неделя, месяц, год).

Далее нажать кнопку «Применить», в зависимости от формы вывода статистика будет представлена в выбранном ранее варианте.

Для получения статистической информации по КА за выбранный период времени по конкретным IP-адресам атакуемых ЭВМ следует установить переключатель «Статистика за IP-адреса атакуемых». Информация в зависимости от выбора может быть представлена в следующем виде:

– гистограммы;
– таблицы;
– отображена на карте.

Для вывода зафиксированных IP-адресов атакуемых хостов за данный период выборки требуется в разделе «Интервал IP адресов», указать начальный и конечный IP адрес атакуемых ЭВМ. После нажатия кнопки «Принять» выбранный диапазон попадет в область «Статистика «Атакуемые»». С использованием поля «Добавить», можно внести отдельную запись в виде IP адреса атакуемого. Далее следует выбрать форму вывода «Таблица», «Гистограмма» или «Карта». При построении данных можно выбрать группу IP адресов из списка «Статистика «Атакуемые»». Также следует заполнить интервал для гистограммы (час, сутки, неделя, месяц, год).

Далее нажать кнопку «Применить», в зависимости от формы вывода статистика будет представлена в выбранном ранее варианте. При выводе в табличном виде для КА через контекстное меню доступны команды «Просмотр CVE» и «Заблокировать», описанные ранее.

2.6.5. Вкладка «Компьютерные атаки»

Вкладка «Компьютерные атаки» (рис. 87) предназначена для получения статистической информации по КА за выбранный период времени по конкретному коду и подмодулю кода атаки, представленной в виде гистограммы.

Для вывода КА за установленный период времени необходимо установить данный период в области «Период выборки», установить при необходимости параметр фильтрации и нажать кнопку «Вывести список». В «Списке компьютерных атак», будет выведен результат, включающий:

– Код атаки;

– Подмодуль атаки;

– Описание атаки.

В данном списке можно выбрать только одну КА. Также необходимо заполнить интервал для гистограммы (час, сутки, неделя, месяц, год).

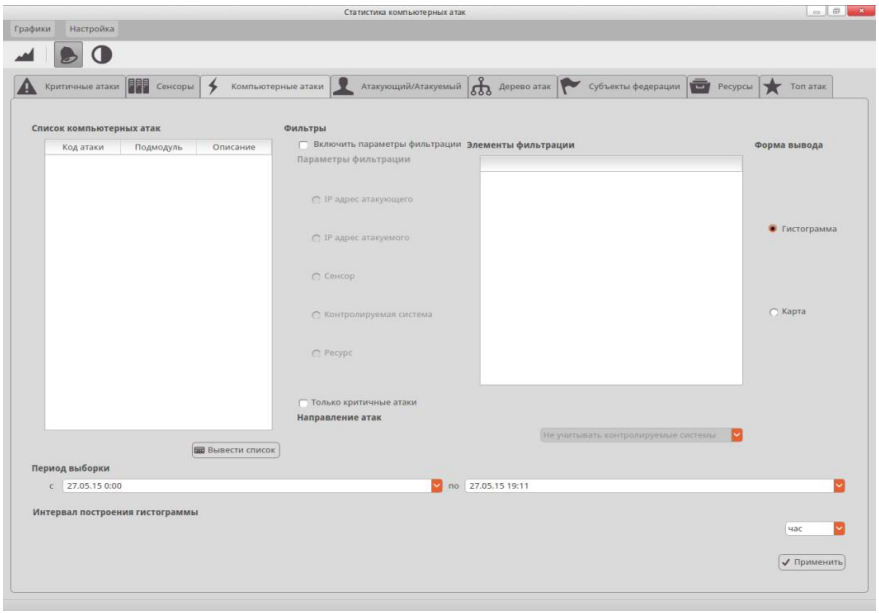


Рис. 87. Вкладка «Компьютерные атаки»

При нажатии кнопки «Применить» появится гистограмма отчета. При необходимости сохранить гистограмму необходимо нажать кнопку «Сохранить».

Для просмотра значений гистограммы необходимо нажать кнопку «Таблица». В появившемся диалоге (рис. 88) можно просмотреть данные по каждому приоритету. При необходимости сохранить данные, нажать кнопку «Сохранить».

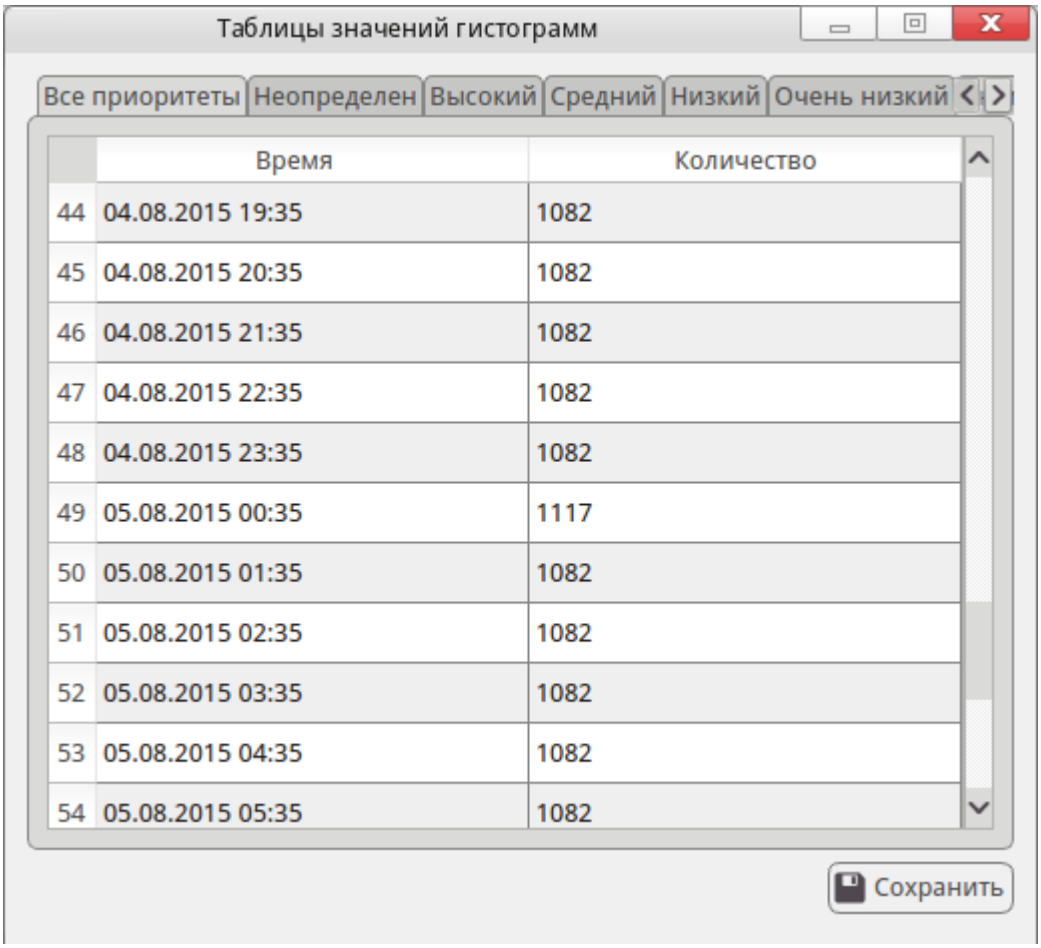


Рис. 88. Таблица значений гистограмм по приоритетам атак

2.6.6. Вкладка «Дерево атак»

Вкладка «Дерево атак» (рис. 89) предназначена для получения статистической информации по КА за выбранный период времени с учетом выбранных параметров фильтрации, представленной в виде древовидной структуры (рис. 90).

Оператору необходимо выбрать параметры по первичному группированию КА в области «Вариант первоначального группирования»:

– код атаки;

– объект атаки;

– субъект атаки.

При необходимости пользователь может указать параметры фильтрации.

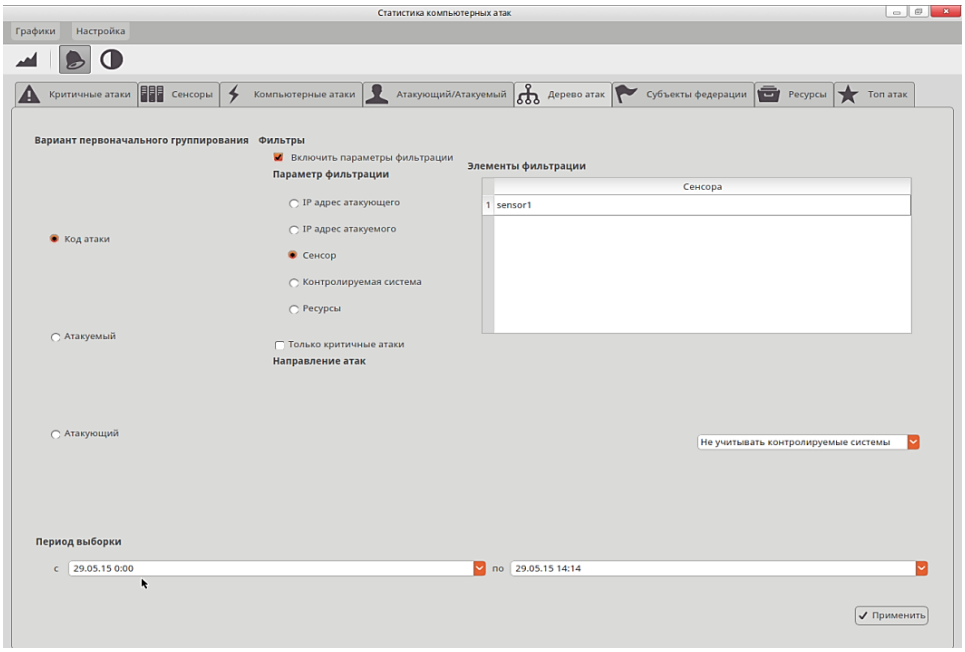


Рис. 89. Дерево атак

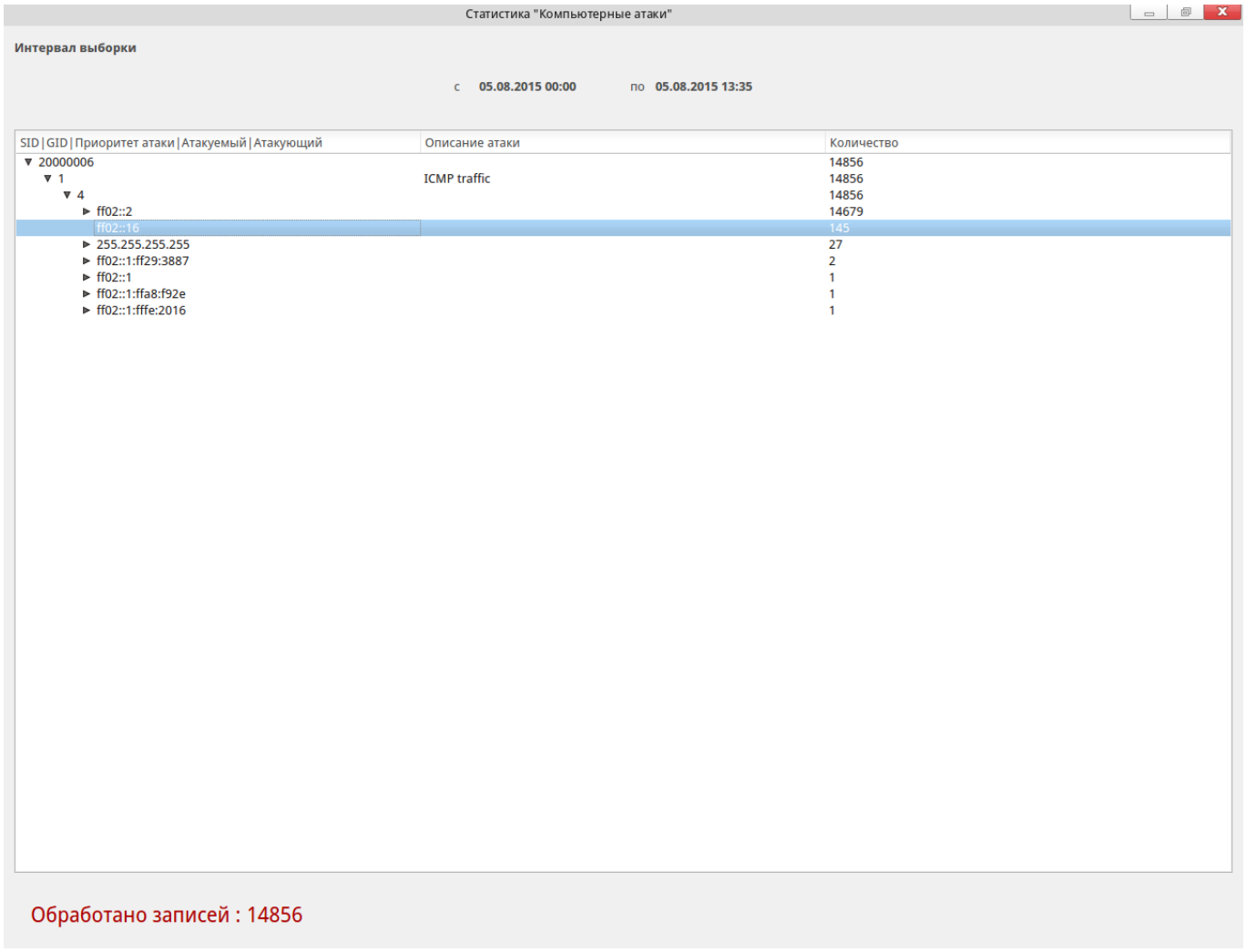


Рис. 90. Статистика КА с группировкой по коду атаки

2.6.7. Вкладка «Ресурсы»

Диалог «Ресурсы» (рис. 91) предназначен для получения статистической информации по КА за выбранный период времени по выбранному ресурсу, представленной в табличном виде.

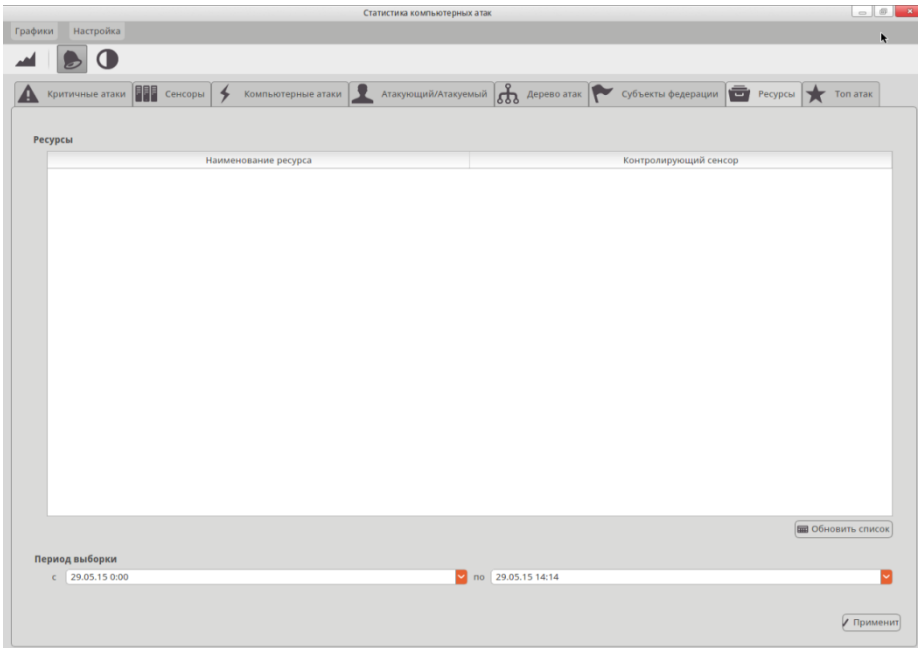


Рис. 91. Вкладка «Ресурсы»

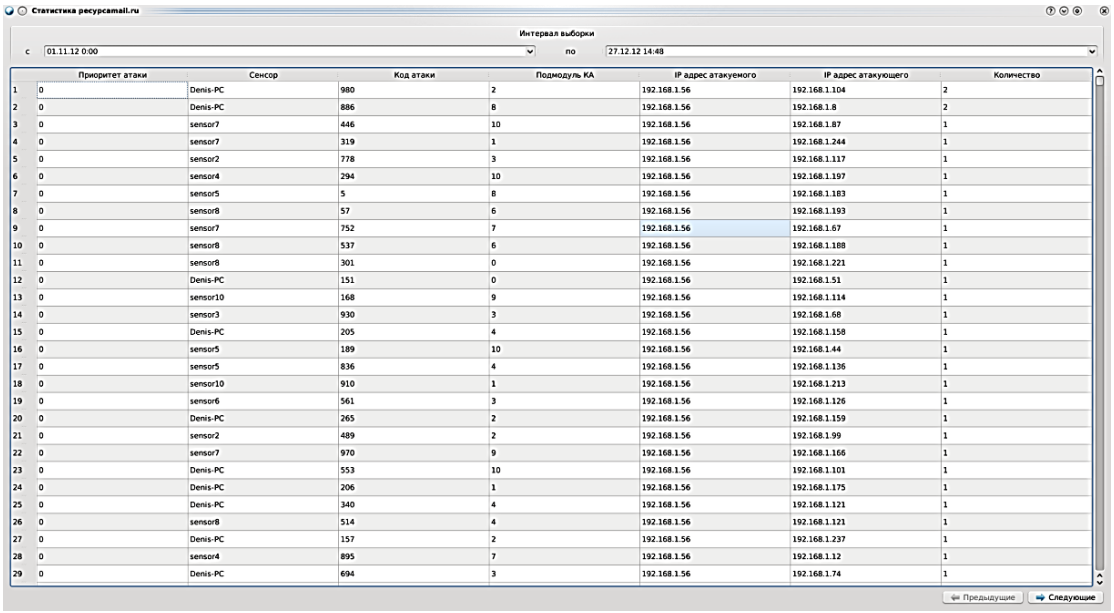
Для вывода списка зарегистрированных ресурсов оператору необходимо нажать кнопку «Вывести список». Дождаться вывода списка ресурсов, который представлен в следующем виде:

– идентификатор ресурса;

– имя ресурса;

– сенсор, на котором зарегистрирован ресурс.

Для получения результирующей таблицы необходимо нажать кнопку «Применить». Результат представлен на рис. 92.



	Приоритет атаки	Сенсор	Код атаки	Подмодуль КА	IP адрес атакуемого	IP адрес атакующего	Количество
1	0	Denis-PC	980	2	192.168.1.56	192.168.1.104	2
2	0	Denis-PC	886	8	192.168.1.56	192.168.1.8	2
3	0	sensor7	446	10	192.168.1.56	192.168.1.87	1
4	0	sensor7	319	1	192.168.1.56	192.168.1.244	1
5	0	sensor2	778	3	192.168.1.56	192.168.1.117	1
6	0	sensor4	294	10	192.168.1.56	192.168.1.197	1
7	0	sensor5	5	8	192.168.1.56	192.168.1.183	1
8	0	sensor8	57	6	192.168.1.56	192.168.1.193	1
9	0	sensor7	752	7	192.168.1.56	192.168.1.67	1
10	0	sensor8	537	6	192.168.1.56	192.168.1.188	1
11	0	sensor8	301	0	192.168.1.56	192.168.1.221	1
12	0	Denis-PC	151	0	192.168.1.56	192.168.1.51	1
13	0	sensor10	168	9	192.168.1.56	192.168.1.114	1
14	0	sensor3	930	3	192.168.1.56	192.168.1.68	1
15	0	Denis-PC	205	4	192.168.1.56	192.168.1.158	1
16	0	sensor5	189	10	192.168.1.56	192.168.1.44	1
17	0	sensor5	836	4	192.168.1.56	192.168.1.136	1
18	0	sensor10	910	1	192.168.1.56	192.168.1.213	1
19	0	sensor6	561	3	192.168.1.56	192.168.1.126	1
20	0	Denis-PC	265	2	192.168.1.56	192.168.1.159	1
21	0	sensor2	489	2	192.168.1.56	192.168.1.99	1
22	0	sensor7	970	9	192.168.1.56	192.168.1.166	1
23	0	Denis-PC	553	10	192.168.1.56	192.168.1.101	1
24	0	Denis-PC	206	1	192.168.1.56	192.168.1.175	1
25	0	Denis-PC	340	4	192.168.1.56	192.168.1.121	1
26	0	sensor8	514	4	192.168.1.56	192.168.1.121	1
27	0	Denis-PC	157	2	192.168.1.56	192.168.1.237	1
28	0	sensor4	895	7	192.168.1.56	192.168.1.12	1
29	0	Denis-PC	694	3	192.168.1.56	192.168.1.74	1

Рис. 92. Табличное представление статистики ресурсов

Детальную информацию по каждой строке таблицы можно получить двойным нажатием на соответствующей строке. Если результат запроса превышает 5000 записей, для перехода между страницами доступны навигационные кнопки «Следующие» и «Предыдущие».

2.6.8. Вкладка «Субъекты федерации»

Вкладка «Субъекты федерации» (рис. 93) предназначена для получения статистической информации по КА за выбранный период времени по всем сенсорам, зарегистрированным в данном субъекте федерации, представленной в табличном виде.

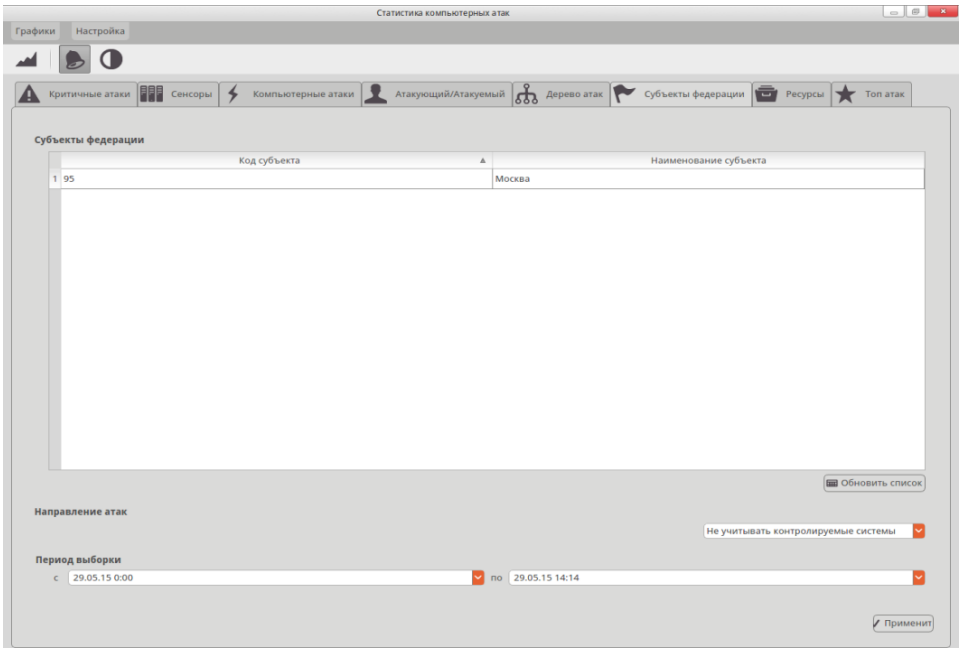


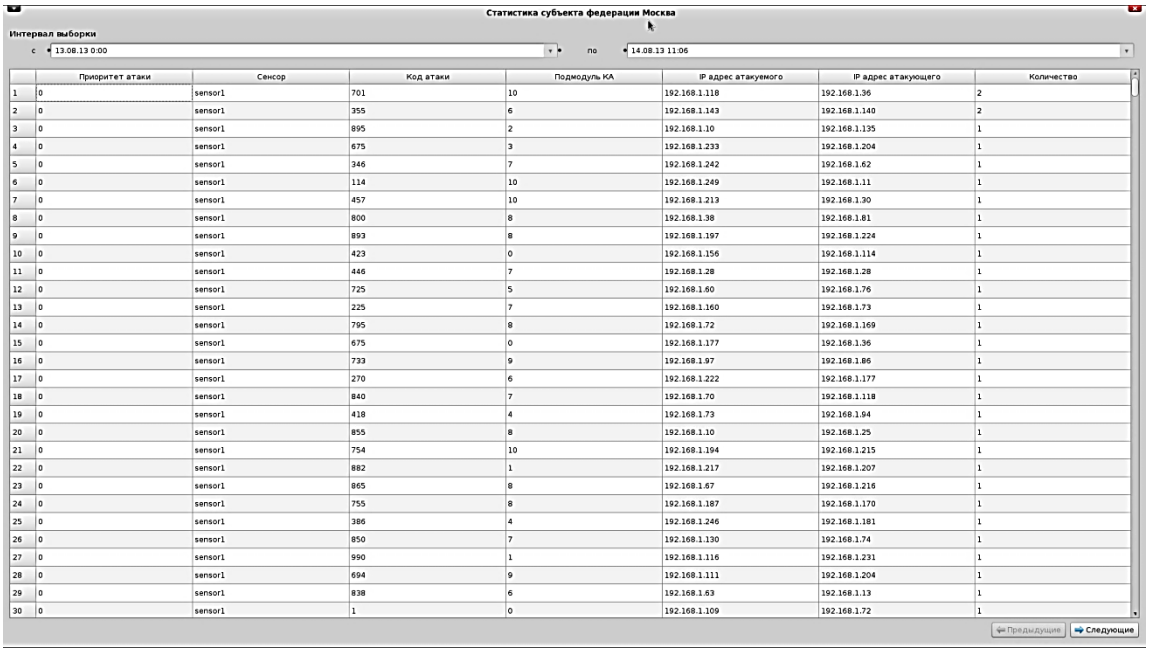
Рис. 93. Вкладка «Субъекты федерации»

Для обновления списка зарегистрированных субъектов федерации необходимо нажать кнопку «Обновить список». Список выводиться в следующем виде:

– идентификатор субъекта федерации;

– название субъекта.

Детальную информацию по каждой строке таблицы можно получить двойным нажатием на соответствующей строке. Если результат запроса превышает 5000 записей, для перехода между страницами доступны навигационные кнопки «Следующие» и «Предыдущие» рис. 94. Через контекстное меню доступны команды «Просмотр CVE» и «Заблокировать», описанные ранее.



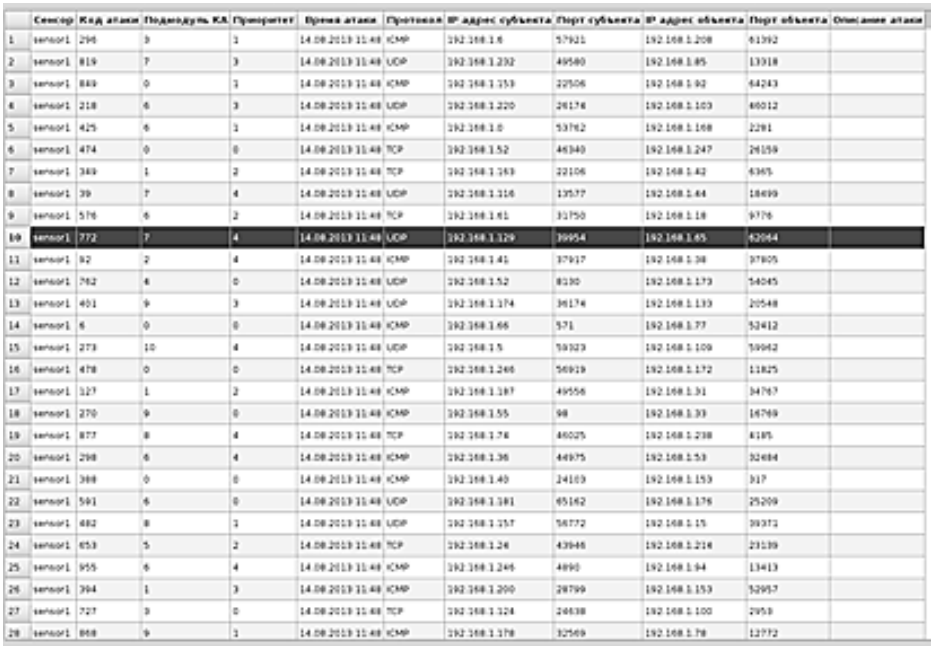
	Приоритет атаки	Сенсор	Код атаки	Подмодуль КА	IP адрес атакуемого	IP адрес атакующего	Количество
1	0	sensor1	701	10	192.168.1.118	192.168.1.36	2
2	0	sensor1	355	6	192.168.1.143	192.168.1.140	2
3	0	sensor1	895	2	192.168.1.10	192.168.1.135	1
4	0	sensor1	675	3	192.168.1.233	192.168.1.204	1
5	0	sensor1	346	7	192.168.1.242	192.168.1.62	1
6	0	sensor1	114	10	192.168.1.249	192.168.1.11	1
7	0	sensor1	457	10	192.168.1.213	192.168.1.30	1
8	0	sensor1	800	8	192.168.1.38	192.168.1.81	1
9	0	sensor1	893	8	192.168.1.197	192.168.1.224	1
10	0	sensor1	423	0	192.168.1.156	192.168.1.114	1
11	0	sensor1	446	7	192.168.1.28	192.168.1.28	1
12	0	sensor1	725	5	192.168.1.60	192.168.1.76	1
13	0	sensor1	225	7	192.168.1.160	192.168.1.73	1
14	0	sensor1	795	8	192.168.1.72	192.168.1.169	1
15	0	sensor1	675	0	192.168.1.177	192.168.1.36	1
16	0	sensor1	733	9	192.168.1.97	192.168.1.86	1
17	0	sensor1	270	6	192.168.1.222	192.168.1.177	1
18	0	sensor1	840	7	192.168.1.70	192.168.1.118	1
19	0	sensor1	418	4	192.168.1.73	192.168.1.94	1
20	0	sensor1	855	8	192.168.1.10	192.168.1.25	1
21	0	sensor1	754	10	192.168.1.194	192.168.1.215	1
22	0	sensor1	882	1	192.168.1.217	192.168.1.207	1
23	0	sensor1	865	8	192.168.1.67	192.168.1.216	1
24	0	sensor1	755	8	192.168.1.187	192.168.1.170	1
25	0	sensor1	386	4	192.168.1.246	192.168.1.181	1
26	0	sensor1	850	7	192.168.1.130	192.168.1.74	1
27	0	sensor1	990	1	192.168.1.116	192.168.1.231	1
28	0	sensor1	694	9	192.168.1.111	192.168.1.204	1
29	0	sensor1	838	6	192.168.1.63	192.168.1.13	1
30	0	sensor1	1	0	192.168.1.109	192.168.1.72	1

Рис. 94. Табличное представление статистики субъекта федерации

2.6.9. Получение информации о «критичных атаках»

Получение информации о «критичных атаках» в масштабе времени близком к реальному, необходимо в основном окне приложения выбрать вкладку «Критичные атаки» (рис. 95). В таблице будут выведены следующие параметры:

– Сенсор;
– Код атаки;
– Подмодуль кода атаки;
– Приоритет;
– Время атаки;
– Протокол;
– IP адрес субъекта;
– Порт субъекта;
– IP адрес объекта;
– Порт объекта;
– Описание атаки.



	Сенсор	Код атаки	Подозрительность КА	Приоритет	Время атаки	Протокол	IP адрес субъекта	Порт субъекта	IP адрес объекта	Порт объекта	Описание атаки
1	sensor1	296	3	1	14.08.2019 11:48	ICMP	192.168.1.6	57921	192.168.1.208	61392	
2	sensor1	819	7	3	14.08.2019 11:48	UDP	192.168.1.232	49580	192.168.1.85	13318	
3	sensor1	849	0	1	14.08.2019 11:48	ICMP	192.168.1.153	32506	192.168.1.92	64243	
4	sensor1	218	6	3	14.08.2019 11:48	UDP	192.168.1.220	26176	192.168.1.103	46012	
5	sensor1	425	6	1	14.08.2019 11:48	ICMP	192.168.1.0	53762	192.168.1.168	2291	
6	sensor1	474	0	0	14.08.2019 11:48	TCP	192.168.1.52	46340	192.168.1.247	24159	
7	sensor1	389	1	2	14.08.2019 11:48	TCP	192.168.1.163	22106	192.168.1.42	6365	
8	sensor1	39	7	4	14.08.2019 11:48	UDP	192.168.1.116	13577	192.168.1.44	18499	
9	sensor1	576	6	2	14.08.2019 11:48	TCP	192.168.1.61	31750	192.168.1.18	9776	
10	sensor1	772	7	4	14.08.2019 11:48	UDP	192.168.1.129	39954	192.168.1.65	62064	
11	sensor1	92	2	4	14.08.2019 11:48	ICMP	192.168.1.41	37917	192.168.1.38	37805	
12	sensor1	762	6	0	14.08.2019 11:48	UDP	192.168.1.52	8130	192.168.1.173	54045	
13	sensor1	401	9	3	14.08.2019 11:48	UDP	192.168.1.174	36174	192.168.1.133	20548	
14	sensor1	6	0	0	14.08.2019 11:48	ICMP	192.168.1.66	571	192.168.1.77	52412	
15	sensor1	273	10	4	14.08.2019 11:48	UDP	192.168.1.5	59323	192.168.1.109	59962	
16	sensor1	478	0	0	14.08.2019 11:48	TCP	192.168.1.246	56919	192.168.1.172	11825	
17	sensor1	127	1	2	14.08.2019 11:48	ICMP	192.168.1.187	49556	192.168.1.31	34767	
18	sensor1	270	9	0	14.08.2019 11:48	ICMP	192.168.1.55	98	192.168.1.33	16749	
19	sensor1	877	8	4	14.08.2019 11:48	TCP	192.168.1.76	46025	192.168.1.238	6185	
20	sensor1	298	6	4	14.08.2019 11:48	ICMP	192.168.1.36	44975	192.168.1.53	32484	
21	sensor1	388	0	0	14.08.2019 11:48	ICMP	192.168.1.40	24103	192.168.1.153	317	
22	sensor1	591	6	0	14.08.2019 11:48	UDP	192.168.1.181	65162	192.168.1.176	25209	
23	sensor1	682	8	1	14.08.2019 11:48	UDP	192.168.1.157	56772	192.168.1.15	39371	
24	sensor1	653	5	2	14.08.2019 11:48	TCP	192.168.1.24	43946	192.168.1.214	23139	
25	sensor1	955	6	4	14.08.2019 11:48	ICMP	192.168.1.245	4890	192.168.1.94	13413	
26	sensor1	394	1	3	14.08.2019 11:48	ICMP	192.168.1.200	28799	192.168.1.153	52957	
27	sensor1	727	3	0	14.08.2019 11:48	TCP	192.168.1.124	24638	192.168.1.100	2959	
28	sensor1	868	9	1	14.08.2019 11:48	ICMP	192.168.1.178	32569	192.168.1.78	12772	

Рис. 95. Вкладка «Критичные атаки»

Окно «Критичные атаки» обновляется каждую минуту. Если будут обнаружены критичные атаки, выдается звуковой сигнал. Звуковой сигнал по умолчанию включен. Для отключения звукового сигнала, следует выбрать пункт меню «Настройка»>«Звуковое оповещение» или соответствующую кнопку панели инструментов  .

2.6.10. Вкладка «Топ атак»

Вкладка «Топ атак» предназначена для информирования оператора о наиболее часто встречающихся участниках инцидента с КА.

Оператор при выборе вкладки «Топ атак» может получить информацию по следующим статистикам (рис. 96):

– наиболее активные источники атак;

– наиболее атакуемые IP-адреса;

– наиболее часто встречающиеся компьютерные атаки.

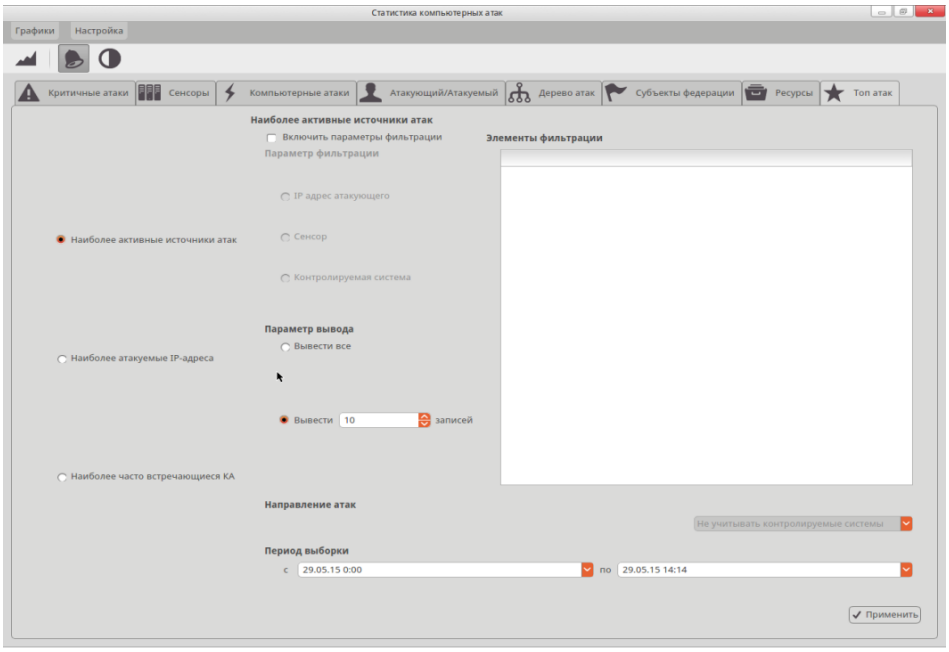


Рис. 96. Вкладка «Топ атак»

Наиболее активные источники атак

Для поиска наиболее активных источников атак пользователь, при необходимости, может установить параметр фильтрации. В списке «Параметры фильтрации» необходимо выбрать нужный параметр фильтрации, указать период выборки, и нажать кнопку «Применить». Результатом исполнения запроса является диалог статистики наиболее активных источников атак (рис. 97). При нажатии двойным щелчком мыши по строке в таблице, появится диалог детальной статистики.

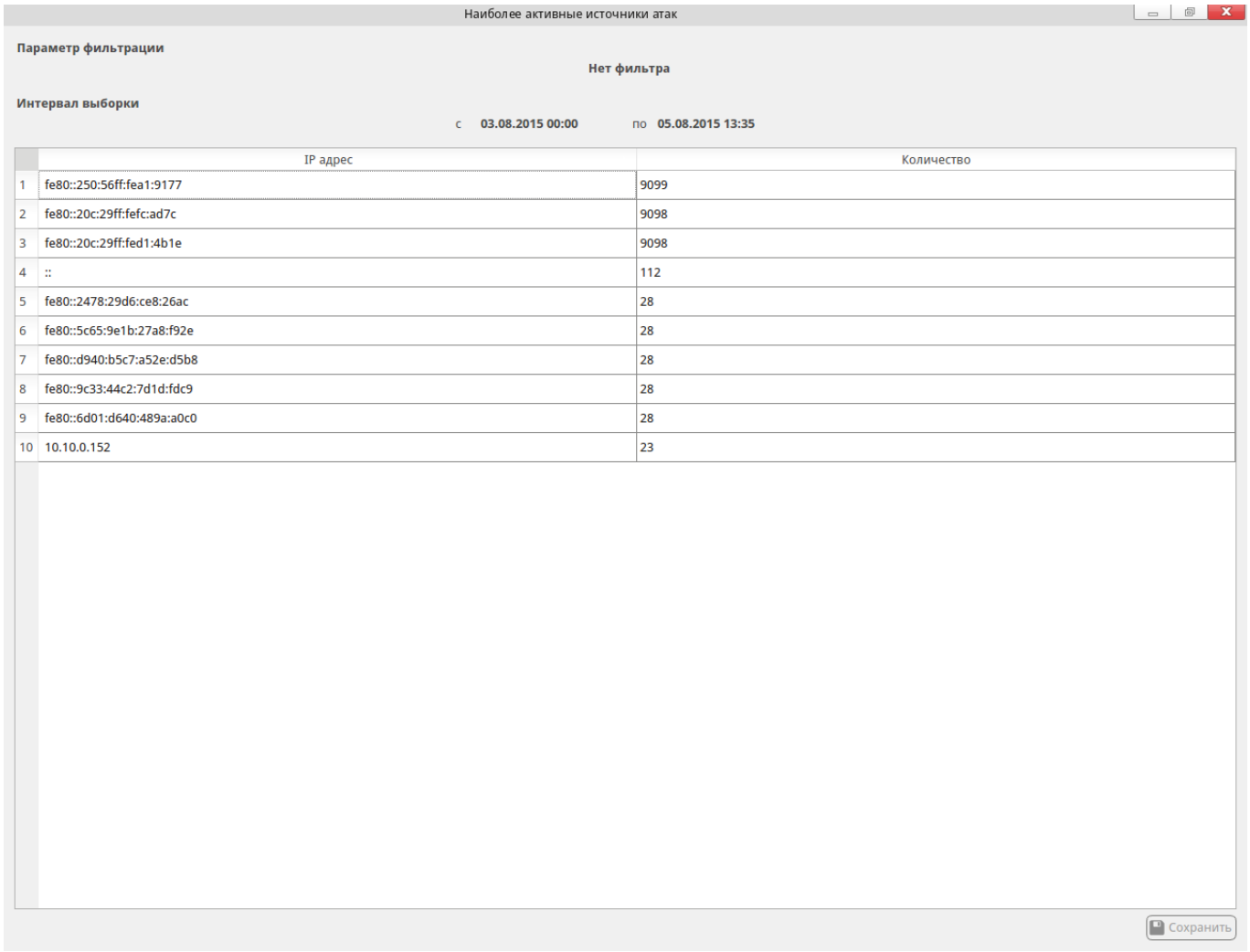


Рис. 97. Наиболее активные источники атак

Статистику по наиболее активным источникам атак можно сохранить в виде отчетного документа в формате RTF-файла, нажав кнопку «Сохранить».

Наиболее атакуемые IP-адреса

Диалог «Наиболее атакуемые IP-адреса» (рис. 98) предназначен для вывода сводной статистики по наиболее атакуемым объектам КА.

Для поиска наиболее часто атакуемых IP-адресов пользователь при необходимости может установить параметр фильтрации. В списке «Параметры фильтрации» необходимо выбрать нужный параметр фильтрации, указать период выборки, и нажать кнопку «Применить». Результатом исполнения запроса является диалог статистики наиболее часто атакуемых IP-адресов (рис. 99). При двойном щелчке по строке отчета, появится диалог детальной статистики. Для сохранения отчета в текстовом документе оператор должен нажать кнопку «Сохранить».

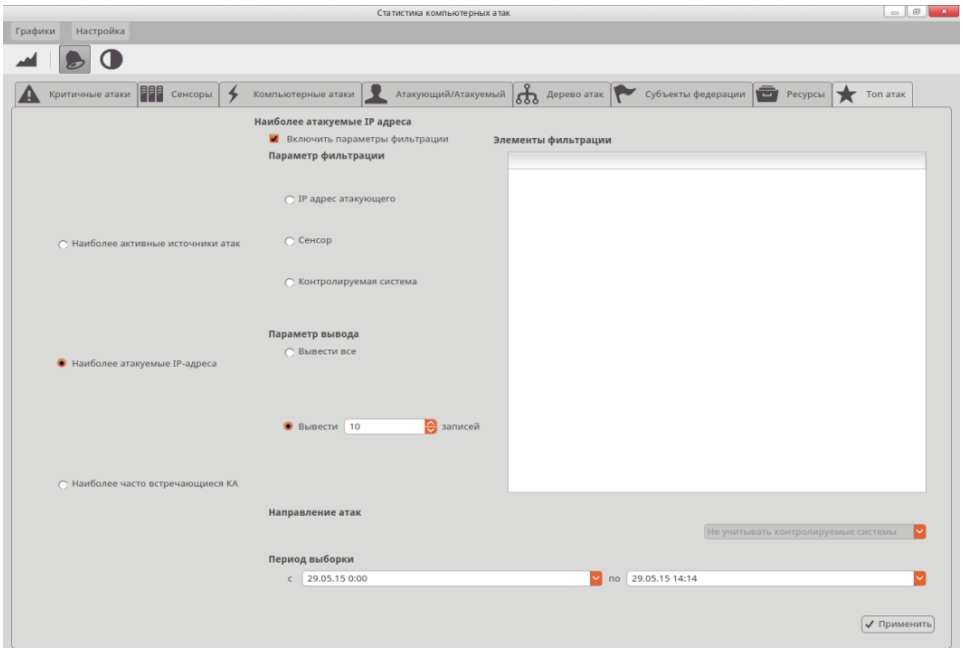


Рис. 98. Диалог «Наиболее атакуемые IP-адреса»

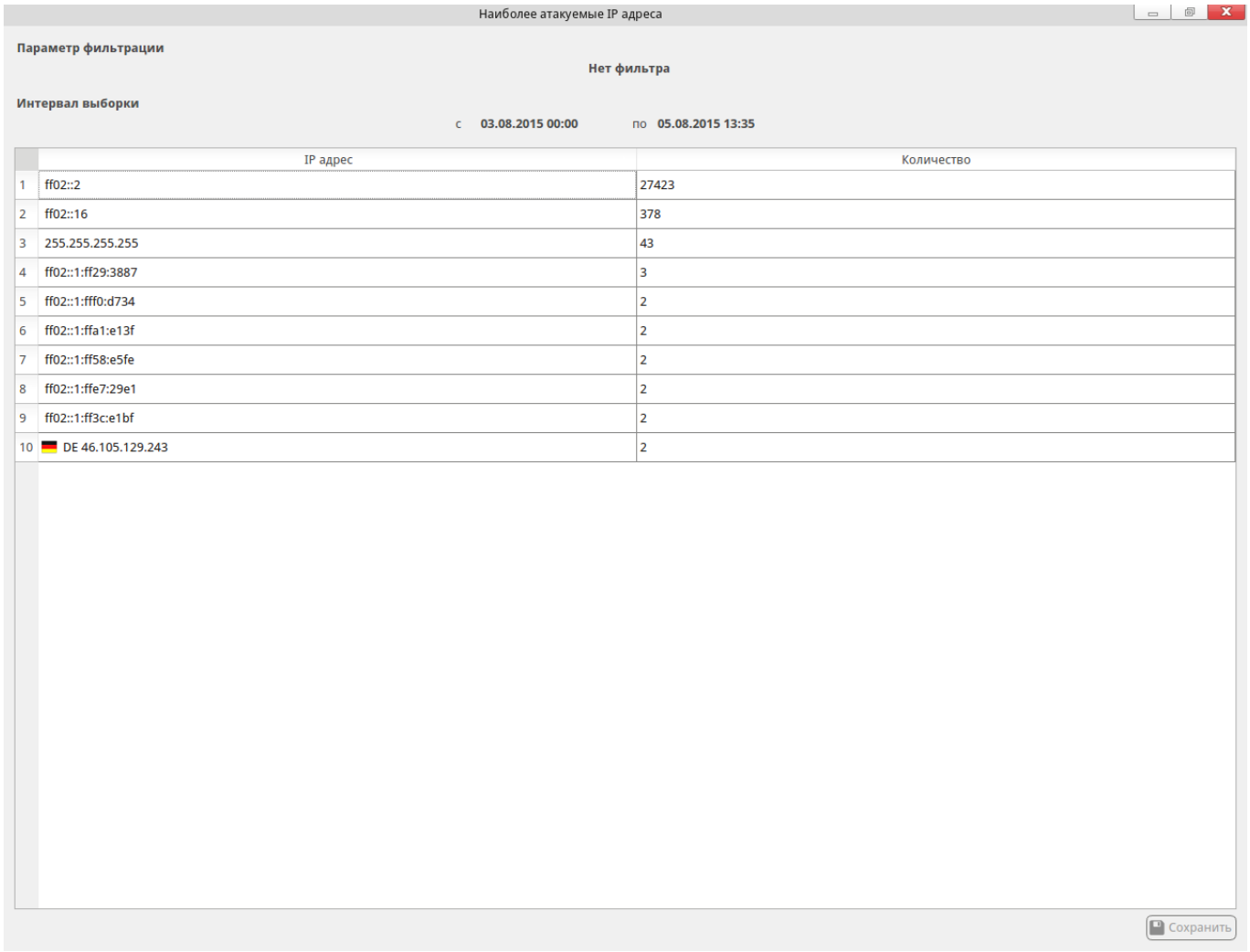


Рис. 99. Наиболее часто атакуемые адреса

Наиболее часто встречающиеся КА

Диалог «Наиболее часто встречающиеся КА» (рис. 100) предназначен для вывода сводной статистики по КА с учетом фильтрации. В качестве параметра фильтрации может выступать, IP-адрес объекта/субъекта атаки, сенсор, доменное имя ресурса или контролируемая система, зарегистрированные в БД.

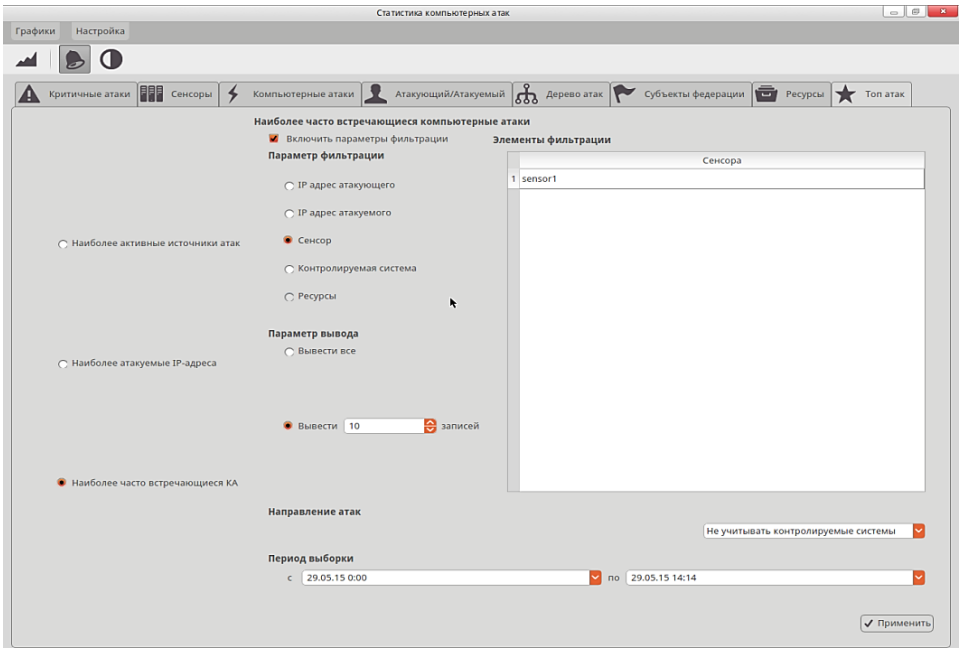


Рис. 100. Диалог «Наиболее часто встречающиеся КА»

Результатом исполнения запроса будет диалог (рис. 101), статистика в котором разделена по приоритетам. Для сохранения отчета в текстовом документе оператор должен нажать кнопку «Сохранить».

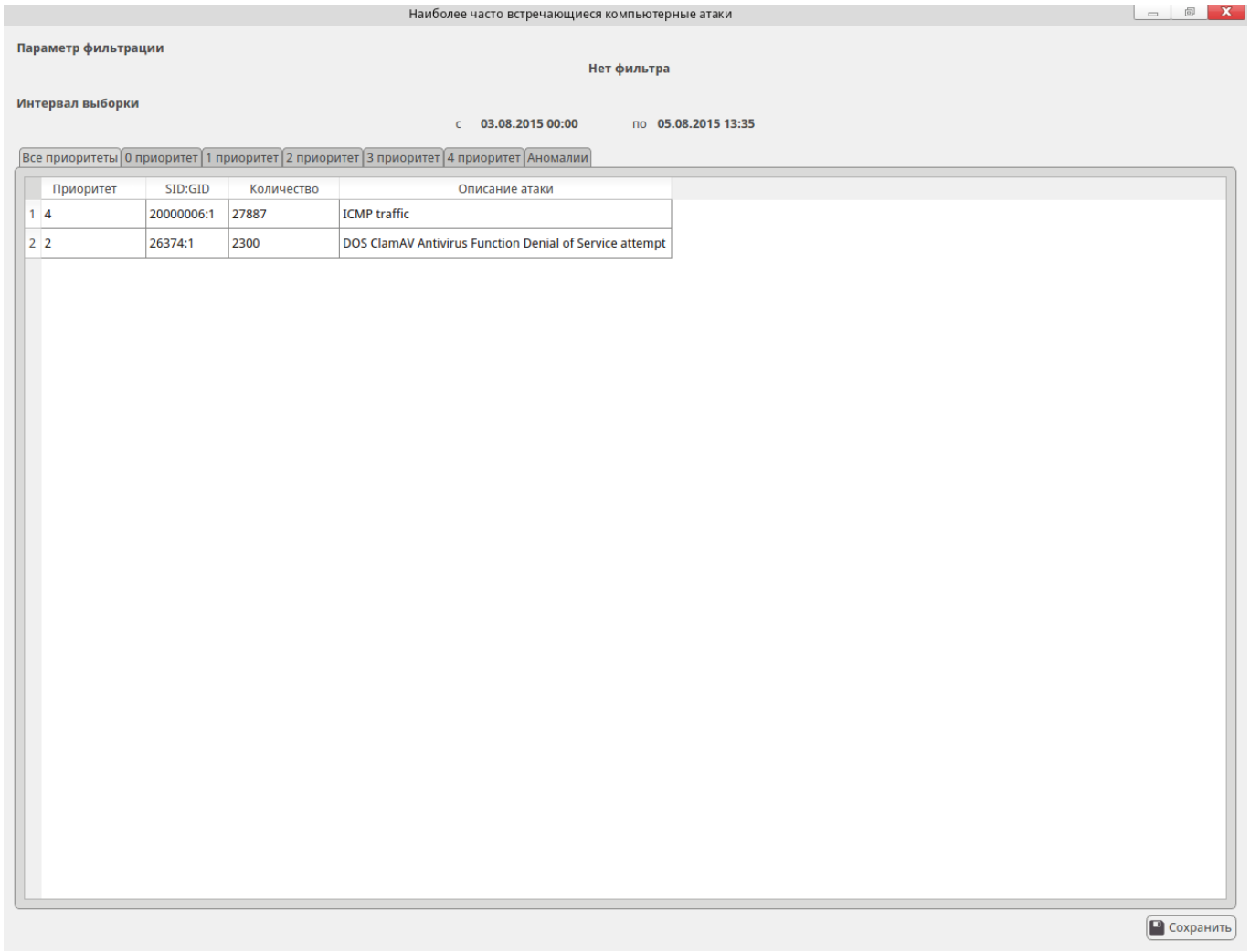


Рис. 101. Статистика наиболее часто встречающиеся компьютерные атаки

2.6.11. Настройка использования гистограмм

Для гистограмм, используемых для построения статистических графиков, имеются следующие ограничения для периода выборки:

– Для интервала построения минута – 3 часа;

– Для интервала построения час – 9 дней;

– Для интервала построения сутки – 180 дней.

Для задания собственных временных пределов необходимо выбрать пункт меню «Настройки» > «Пределы периодов выборки» или соответствующую кнопку панели инструментов. В появившемся диалоге (рис. 33) необходимо установить собственные пределы для гистограммы.

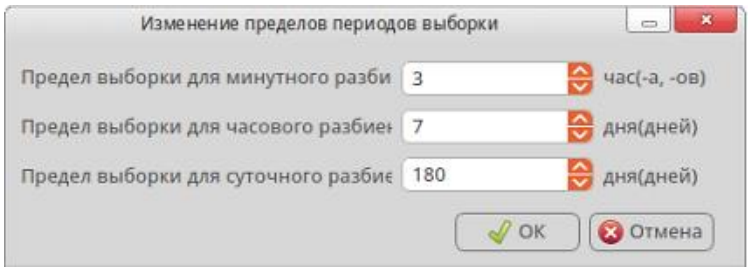


Рис. 102. Диалог изменения пределов периодов выборки для гистограмм

2.6.12. Вывод отчуждаемых журналов

ПМ позволяет отображать и сохранять информацию, получаемую из следующих журналов: безопасности, действий, технического состояния. Информация может быть получена от зарегистрированного сенсора, СУС и собственно с АРМ управления. Для этого в главном меню выбрать пункт меню «Просмотр журналов» > «Журналы безопасности», «Журналы действий», «Журналы технического состояния» (в зависимости от необходимого журнала) (рис. 103). В появившемся диалоге (рис. 104) указать источник журналов (для сенсора выбрать его наименование из всплывающего списка).

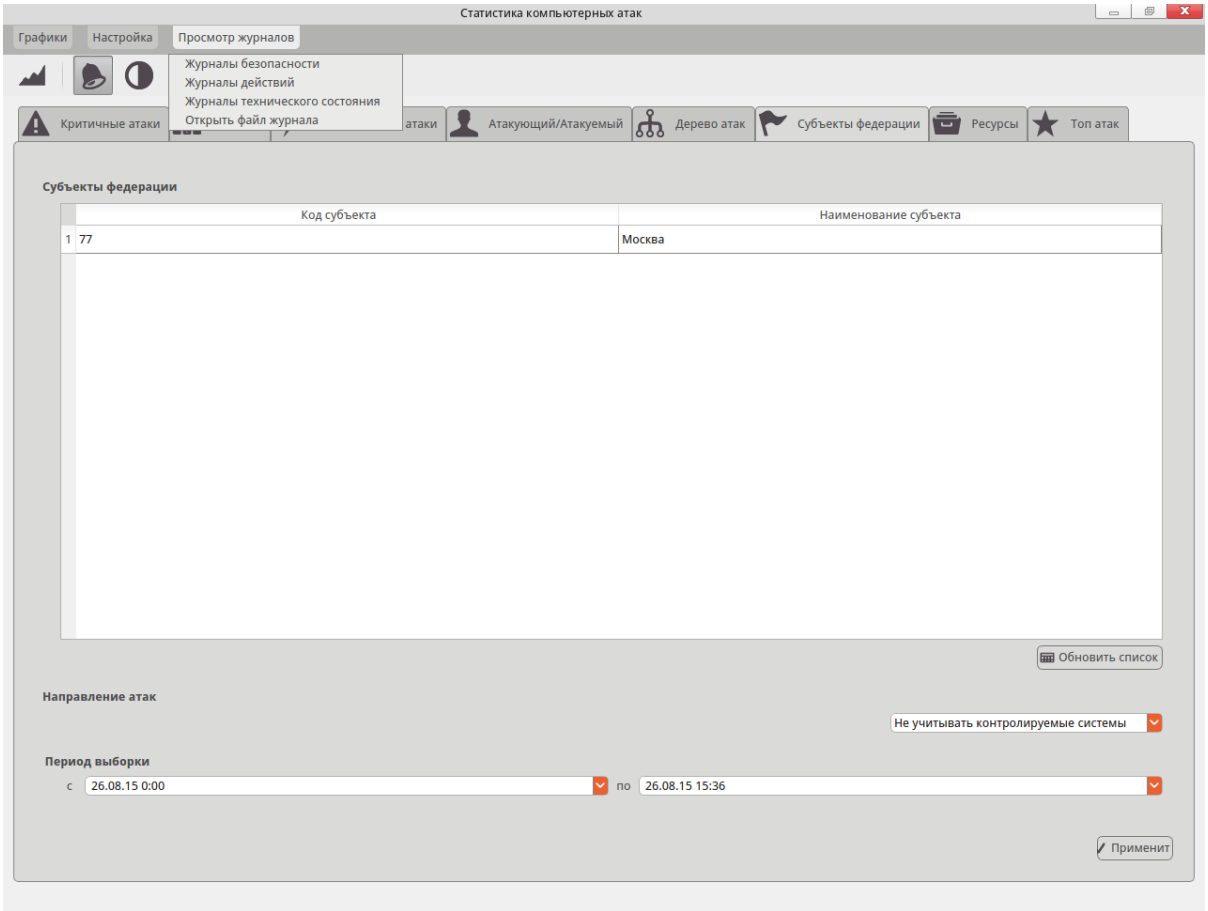


Рис. 103. Пункт меню «Просмотр журналов»

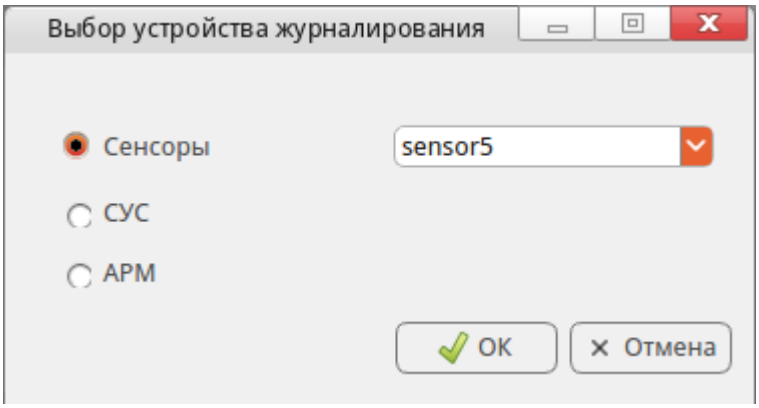


Рис. 104. Диалог «Выбор устройства журналирования»

В результирующем окне (рис. 105) выводится полученные сведения по журналу устройства журналирования.

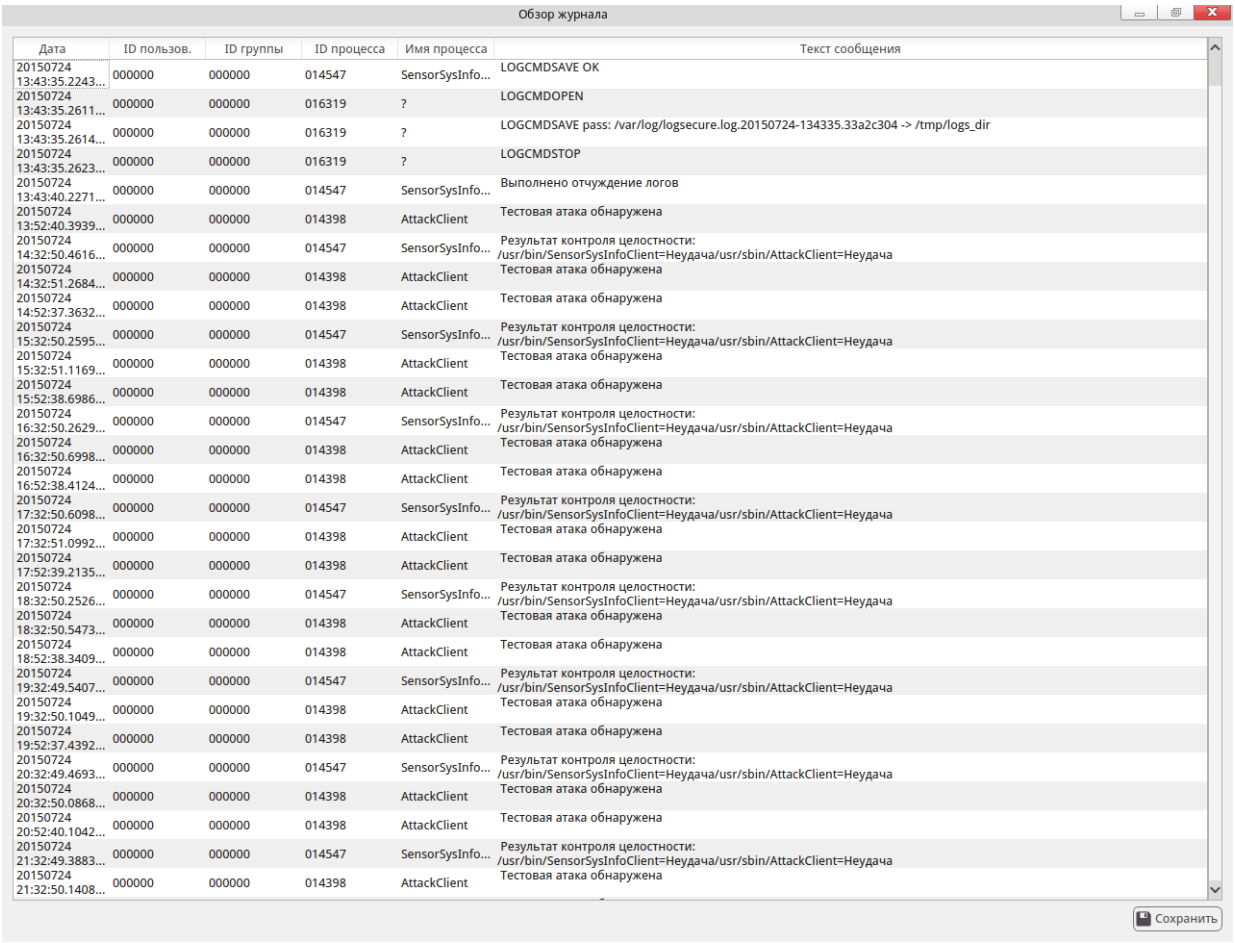


Рис. 105. Окно результата вывода журнала

В данном окне можно производить сортировку данных по полям таблицы, путем нажатия на соответствующий заголовок таблицы, а также устанавливать фильтрацию. Для установки критериев фильтраций необходимо выделить одну из записей таблицы, по полю и значению которой будет проводиться фильтрация и нажать правой клавишей мыши. В появившемся контекстном меню выбрать пунк «Фильтр». В появившемся диалоге (рис. 106) при необходимости откорректировать значение, используемое для фильтрации (для редактирования доступно только последнее значение поля «Значение»).

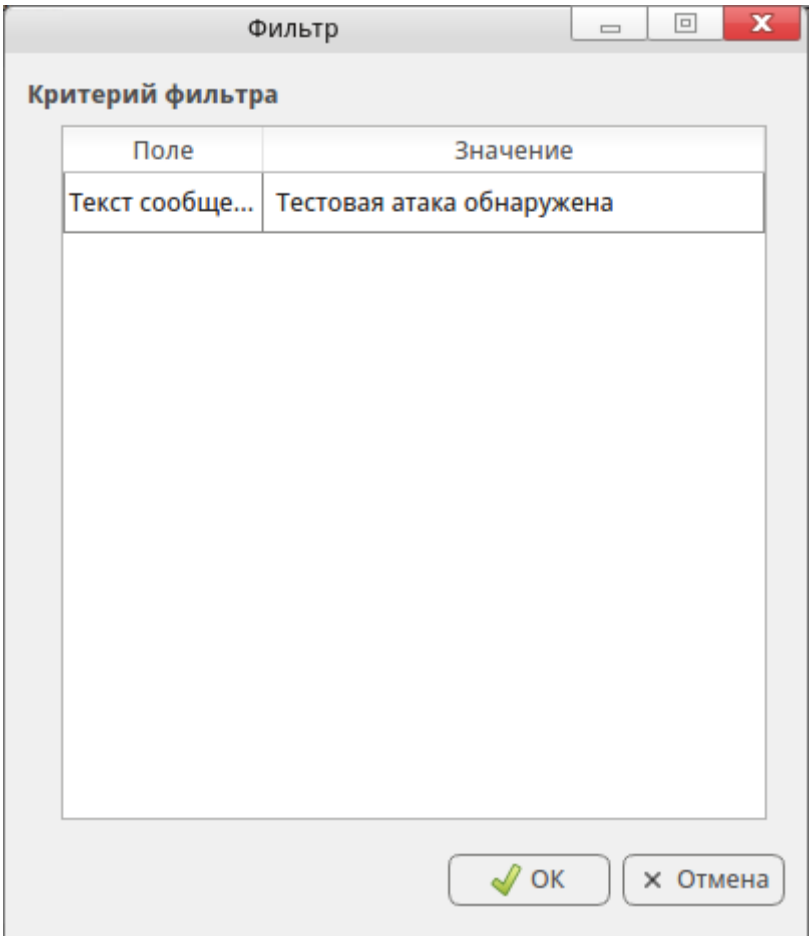


Рис. 106. Диалог «Фильтр»

Окно результата фильтрации будет выводить записи только с учетом заданных критериев фильтрации. При использовании фильтра записи в таблице изменят цвет шрифта на синий (рис. 107).

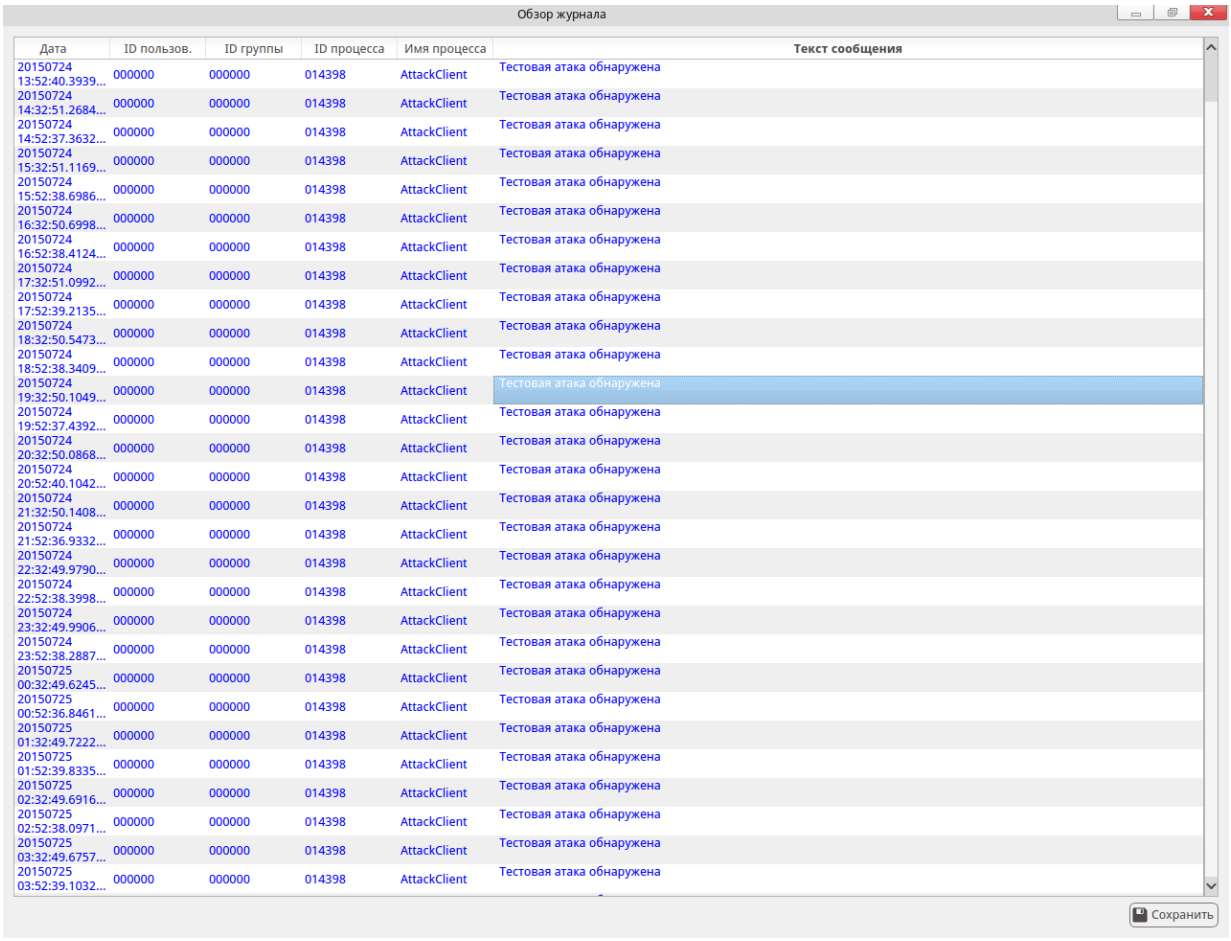


Рис. 107. Результат выполнения фильтрации

Для отмены фильтрации нажмите правой клавишей мыши и в появившемся контекстном меню выберите пункт «Убрать фильтр». Шрифт записей таблицы изменит цвет на значения цвета шрифта по умолчанию.

Для сохранения полученного журнала необходимо нажать кнопку «Сохранить» В появившемся диалоге (рис. 108) указать наименование файла журнала и нажать кнопку «Сохранить».

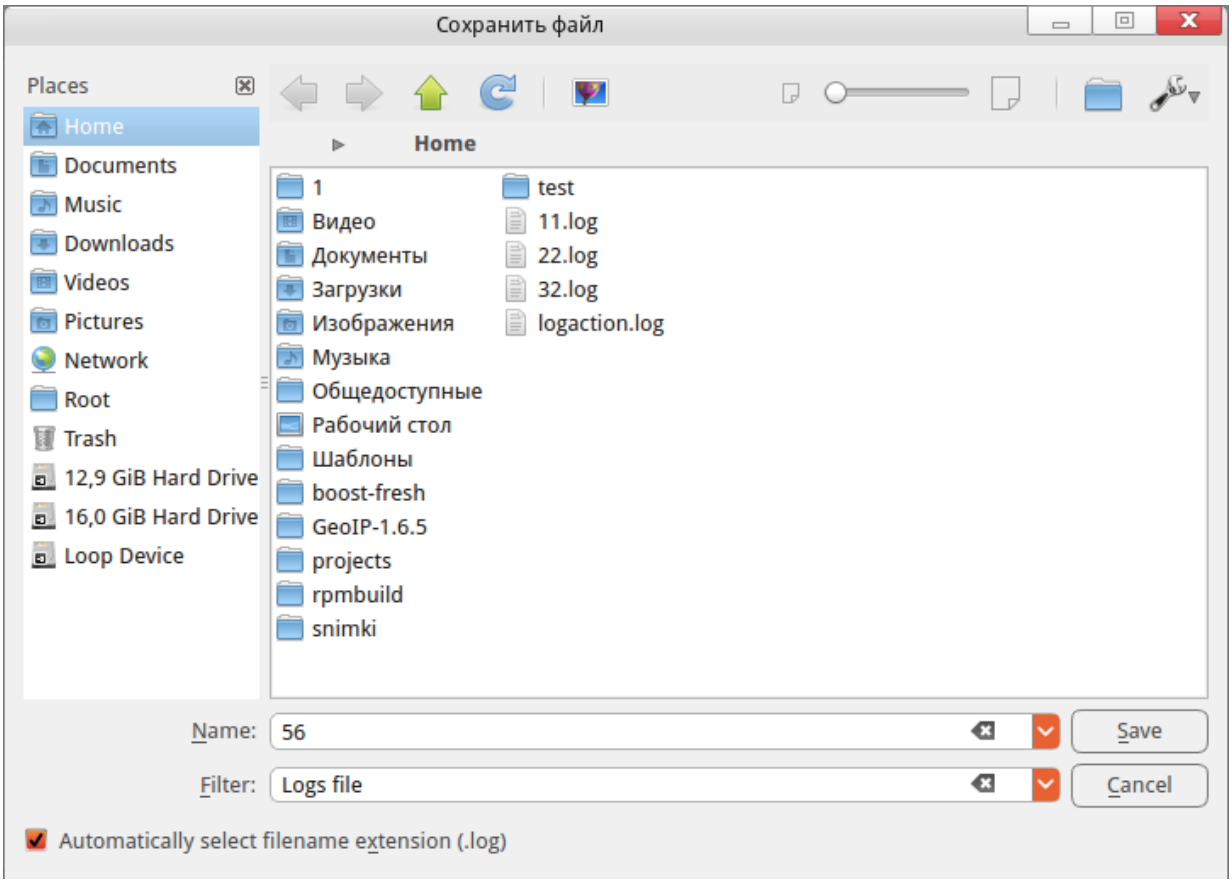


Рис. 108. Сохранение журнала

Для открытия сохраненного журнала необходимо в главном меню выбрать пункт «Просмотр журналов» > «Открыть файл журнала». В появившемся диалоге (рис. 109) указать необходимый файл журнала.

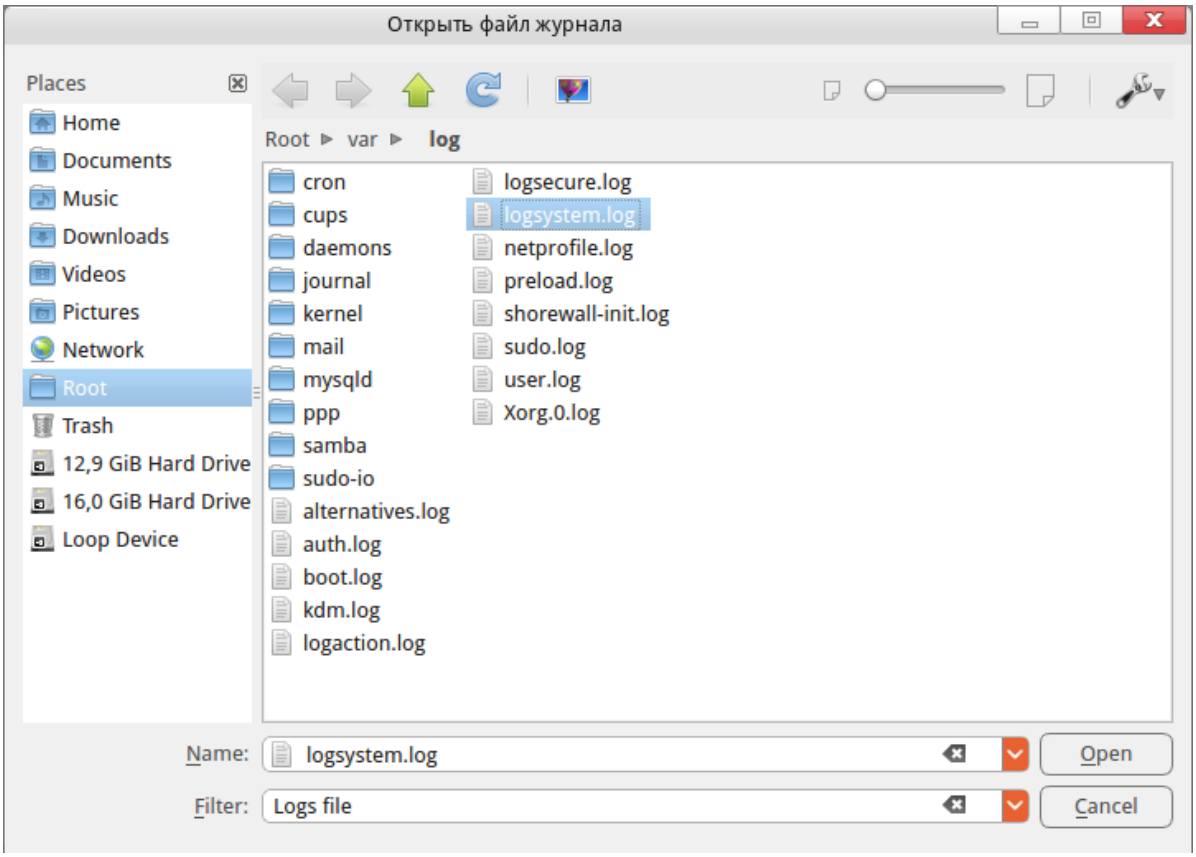


Рис. 109. Диалог открытия файла журнала

Примечание – при экспорте файла журнала он удаляется с ЭВМ и создается новый, содержащий запись об отчуждении предыдущего файла журнала с указанием его контрольной суммы.

2.7. Сообщения системному администратору

При возникновении проблем в процессе функционирования ПС «АРМ УС» диагностические сообщения выводятся в три файла `/var/log/logaction`, `/var/log/logsecure` и `/var/log/logsystem`.

Основные сообщения представлены в таблице 2.

Таблица 2. Основные сообщения

Сообщение ОС	Значение	Файл
SensorControlGUIClient	Команда удаления сенсора выполнена	/var/log/ logaction
SensorControlGUIClient	Команда самотестирования сенсора отправлена	/var/log/ logaction
SensorControlGUIClient	Получена команда самотестирования СУС	/var/log/logaction
SensorControlGUIClient	Получена команда самотестирования сенсора с УИС 5	/var/log/logaction

Сообщение ОС	Значение	Файл
SensorControlGUIClient	Команда обновления сенсора отправлена	/var/log/logaction
SensorControlGUIClient	Получен результат самотестирования сенсора с УИС 0	/var/log/logaction
SensorControlGUIClient	Получена команда обновления правил на сенсоре Плутон	/var/log/logaction
SensorControlGUIClient	Получена команда очистки таблиц БД	/var/log/logaction
SensorControlGUIClient	Команда очистки таблиц БД завершена успешно	/var/log/logaction
SensorControlGUIClient	Параметры доступа к БД заданы не полностью. Запустите программу InitDB_P	/var/log/logsystem
SensorControlGUIClient	LOGCMDOPEN	/var/log/logsystem

3. УСТАНОВКА И НАСТРОЙКА ПС «СЕНСОР»

3.1. Установка ПС «Сенсор»

3.1.1. Среда установки

Установка ПС «Сенсор» осуществляется на технические средства с установленной операционной системой Astra linux Special Edition «Смоленск» 1.5.

При установке ОС необходимо задать пароль учетной записи операционной системы «root», которая играет роль учетной записи привилегированного технологического пользователя в ПС «Сенсор». Данная учетная запись используется только при технологических операциях по установке и диагностике ПО.

3.1.2. Установка ПС «Сенсор»

Перед установкой необходимо выполнить следующие подготовительные операции с техническим средством (ТС), на которое устанавливается ПС «Сенсор»:

– проверить правильность подключения клавиатуры и дисплея (KVM-панели) к ТС;

– в случае использования KVM-панели – переключить KVM-панель на взаимодействие с ТС;

– включить ТС;

– при отсутствии в составе ТС CD/DVD-привода – подключить переносной CD/DVD-привод к свободному USB-разъему ТС.

Для выполнения установки ПС «Сенсор» следует поместить оптический диск с установочными пакетами ПС «Сенсор» в CD/DVD-привод.

Далее необходимо нажать на клавиатуре (KVM-панели) ТС комбинацию клавиш «Ctrl+Alt+F2» и на запрос операционной системы ввести имя и пароль привилегированного технологического пользователя «root».

Примечание – Привилегированный технологический пользователь «root» создается при установке операционной системы.

После ввода учетных данных привилегированного технологического пользователя будет предоставлен доступ к командной строке операционной системы, в которой необходимо выполнить:

1. Скопировать инсталляционные пакеты ПС Сенсор в локальный каталог /opt/debs. (см. Приложение Г. «Содержимое дистрибутива СОВ ПАК Плутон»).
2. Установить системные пакеты из репозитария Астры:
   >apt-get -y install libglib2.0 libssl-dev libboost-serialization1.55 \
   libboost-system1.55 libboost-thread1.55 libpq-dev libtool flex liblzo2-dev \
   libdbi-dev libdbi-perl libdbd-pg-perl bison locales-all *qt4* dkms make patch module-assistant
3. Подготовить ядерные модули с zc:
   >m-a prepare
4. Проверить сборку и наличие модулей ядра:
   >find /lib -name "*zc*.ko"
   /lib/modules/4.2.0-23-generic/kernel/drivers/net/ethernet/intel/igb_zc/igb_zc.ko
   /lib/modules/4.2.0-23-generic/kernel/drivers/net/ethernet/intel/fm10k_zc/fm10k_zc.ko
   /lib/modules/4.2.0-23-generic/kernel/drivers/net/ethernet/intel/i40e_zc/i40e_zc.ko
   /lib/modules/4.2.0-23-generic/kernel/drivers/net/ethernet/intel/ixgbe_zc/ixgbe_zc.ko
   /lib/modules/4.2.0-23-generic/kernel/drivers/net/ethernet/intel/e1000e_zc/e1000e_zc.ko
   /lib/modules/4.2.0-23-generic/kernel/drivers/media/usb/gspca/gspca_zc3xx.ko
   /lib/modules/4.2.0-23-pax/kernel/drivers/media/usb/gspca/gspca_zc3xx.ko
5. Установить пакеты ПС Сенсор:
   >dpkg -i --force overwrite /opt/debs/*.deb
6. Настроить привязку динамических ссылок в ldconfig:
   >echo -e "/usr/local/KDAB/KDReports-1.4.0/lib \n
   /usr/local/lib \n
   /usr/lib/zo \n
   /usr/local/lib/pluto \n
   /usr/lib/x86_64-linux-gnu/qt4/plugins/designer \n
   /usr/local/lib/pluto/observer \n" > /etc/ld.so.conf.d/sensor.conf
   ldconfig
7. Настроить и запустить сервис протоколирования событий:
   >chkconfig genericlogd on

>service genericlogd start

8. Создать пользователя для запуска сервиса snort:

   >useradd -m snort -s /dev/null

9. Создать конфигурационный файл через оболочку tinyshell:

   >tinysh

   $set sensor name <имя_сенсора>

   $set sensor id <идентификатор_сенсора>

   $sensor commit

10. Настроить параметры в конфигурационном файле:

    >vim /usr/share/zo/etc/SensID.conf

    General]

    SENSOR_NAME=Pluton-Astra-Sensor-dvm208

    SID=208

    IP_SUS=<IP-адрес СУС>

    DUMP=

    SUS=<имя_сетевого_интерфейса_для_доступа_к_СУС(eth0)>

    RECORD_INTO_RAM=50000

    TIME=

    SHMFILE=/usr/local/bin/snort

    SHMSIZE=104857600

    SENSORSENDMODE=packet

    SENSORSEND=shmem

    SENSORMODE=original

    EMBODIMENT=0

    SELFTEST_UTILITY=ping -p 707ac38c875b0fd8d78d09214256b2fb -b 255.255.255.255 -c 1 -I eth0

    SELFTEST_SIGNATURE=0, 1

    INTERFACES=eth0

    DNAMACS=00:50:56:99:4f:8b

    SELFTESTATTACK=1

SELFTEST=1

11.Принять параметры конфигурации и запустить сенсор через оболочку tinyshell:

>tinysh

$sensor commit

$sensor start

12. Запустить ПС Сенсор через сервис:

>service sensor start

Примечание – правила для snort обновляются только после регистрации Сенсора в АРМ СОВ ПАК Плутон (SensorControlGUIClient)

13. По завершении установки необходимо перезагрузить систему командой:

reboot

Внимание! Выполнение перезагрузки после установки обязательно, в противном случае корректная настройка и запуск ПС «Сенсор» будут невозможны.

После перезагрузки следует:

– нажать на клавиатуре (KVM-панели) ТС комбинацию клавиш «Ctrl+Alt+F2»;

– ввести рабочее имя и пароль технологического пользователя (заводская установка – «admin»/«admin»), после чего будет произведен вход в командную среду технологического пользователя, предоставляющую доступ к технологическим возможностям ПС «Сенсор»;

– изменить пароль технологического пользователя (правила формирования паролей определяются действующим на объекте эксплуатации порядком), для чего в командной среде технологического пользователя выполнить команду:

```
user passwd admin
```

– в ответ на запрос системы дважды ввести новый пароль;

– при необходимости создать одного или несколько дополнительных технологических пользователей, выполнив команду:

```
user add <имя_пользователя>
```

– занести учетные данные технологического пользователя(-ей) в документ учета, предусмотренный действующим на объекте эксплуатации порядком учета

паролей (если предусмотрено);

– выполнить настройку программных средств согласно п. 3.1.3;

– завершить сеанс работы, для чего на клавиатуре KVM-панели нажать комбинацию клавиш «Ctrl+D».

3.1.3. Настройка ПС «Сенсор»

Действия по настройке ПС «Сенсор» выполняются в специальной командной среде. Процедура входа в командную среду описана в п. 3.4.

Для выполнения настройки ПС «Сенсор» следует выполнить в командной среде команды:

```
sensor stop
set sensor
```

Произойдет переход в режим изменения конфигурационных параметров ПС.

Далее необходимо установить конфигурационные параметры, выполнив команды установки параметров:

```
name <имя сенсора, выводимое оператору>
id <уникальный числовой идентификатор сенсора>
mode ids
throughput 1gbit
interface <имя интерфейса приема трафика>
timenotification 1
susip <ip-адрес сервера управления сенсорами>
susinterface <имя сетевого интерфейса, посредством  которого
осуществляется взаимодействие с СУС>
susinterfaceip <ip-адрес, назначаемый интерфейсу взаимодействия с
СУС>
netmask <маска подсети, посредством  которой осуществляется
взаимодействие с СУС>
statanalizerport 9995
susport 2323
```

Значения всех параметров функционирования ПС «Сенсор» и примеры их задания приведены в таблице 1.

Таблица 1 - Параметры функционирования ПС «Сенсор»

Параметр	Пример	Значение параметра
`name <строка>`	`name TP-Sensor-13`	Символьное имя сенсора; выводится оператору
`id <id сенсора>`	`id 17`	Числовой идентификатор сенсора; должен быть уникальным в пределах множества всех сенсоров,

		функционирующих в иерархической структуре СОВ ПАК «Плутон»
mode ids	mode ids	Режим работы сенсора; для ПС «Сенсор» - всегда «ids»
throughput 1gbit	throughput 1gbit	Пропускная способность интерфейса захвата трафика
susip <ip сервера управления сенсорами>	susip 10.1.1.3	IP-адрес, по которому доступен сетевой интерфейс ПТК «Сервер УС», принимающий данные от сенсора
susinterface <интерфейс взаимодействия с СУС>	susinterface eth3	Имя сетевого интерфейса сенсора, посредством которого производится обмен данными с ПТК «Сервер УС»
susinterfaceip <ip, назначаемый интерфейсу взаимодействия с СУС>	susinterface eth3	IP-адрес, назначаемый сетевому интерфейсу сенсора, посредством которого производится обмен данными с ПТК «Сервер УС»
netmask <маска подсети>	netmask 24	Маска подсети для сети передачи данных, соединяющей ПТК «Сенсор» и ПТК «Сервер УС»
interface <имя интерфейса захвата трафика>	interface eth0	Имя сетевого интерфейса сенсора, подключенного к контролируемому каналу передачи данных; на этом интерфейсе производится захват анализируемого трафика
scanerinterface <имя интерфейса захвата>	scanerinterface eth0	То же, что interface; параметр поддерживается для обеспечения обратной совместимости
statanalizerport <порт>	statanalizerport 9995	Номер TCP-порта статистического анализатора на ПТК «Сервер УС»; на этот порт сенсор будет отправлять данные о количественных характеристиках сетевого трафика для выявления аномалий методом статистического анализатора; стандартное значение – 9995
susport <порт>	susport 2323	Номер TCP-порта на ПТК «Сервер УС» для обмена сообщениями о событиях информационной безопасности; стандартное значение – 2323
timenotification <n>	timenotification 1	Период отправки сообщений на ПТК «Сервер УС» (в секундах);

		стандартное значение – 1
selftestinterval <n>	selftestinterval 20	Периодичность проведения самотестирвоания (в секундах)
cpuforuse <n>	cpuforuse 10	Количество процессорных ядер, используемых сигнатурным анализатором
dnadrivers <драйвер>	dnadrivers ixgb	Разрешает перевод в dna-режим сетевых интерфейсов, управляемых заданным драйвером
dnainterface <mac>	dnainterface 00:1F:38:DE:56:21	Сетевые интерфейсы, конфигурируемые для работы в dna-режиме
dnapair <mac1> <mac2>	dnapair 00:1F:38:DE:56:21 00:1F:38:DE:32:31	Задает соответствие входных и выходных сетевых интерфейсов, сконфигурированных для работы в dna-режиме
dumpinterfaces <интерфейс>	dumpinterfaces eth0	Игнорируется; параметр поддерживается для обеспечения обратной совместимости
savepackages enable/disable	savepackages enable	Разрешает/запрещает сохранение старых версий пакетов
susrealip <реальный ip-адрес сервера управления сенсорами>	susrealip 10.2.0.1	Реальный ip-адрес ПТК «Сервер УС» при организации защищенного туннеля
certificatepath <путь к файлу с клиентским сертификатом>	certificatepath /opt/var/cert-sensor13.crt	Задает клиентский сертификат для авторизации при организации защищенного туннеля

По окончании внесения изменений следует выйти из режима изменения конфигурационных параметров нажатием комбинации клавиш Ctrl+D.

Для того, чтобы измененные параметры вступили в силу, необходимо применить сделанные изменения, выполнив команду:

```
sensor commit
```

Затем следует запустить ПО командой:

```
sensor start
```

Если ПС «Сенсор» должно функционировать в составе отказоустойчивого кластера сенсоров, то на каждом из сенсоров – узлов кластера следует после настройки конфигурационных параметров сенсора выполнить команду:

```
set cluster <ip узла 1> <ip узла 2> … <ip узла N>
```

где <ip узла 1> <ip узла 2> … <ip узла N> - перечисление ip-адресов всех сенсоров, всходящих в кластер. В качестве ip-адресов следует задавать ip-адреса сенсоров в сети передачи данных, объединяющей узлы кластера. Необходимо задавать одинаковый набор ip-адресов в команде на каждом сенсоре, входящем в один кластер.

3.2. Запуск и останов ПС «Сенсор»

Запуск и останов ПС «Сенсор» выполняется в автоматическом режиме в процессе запуска и останова операционной системы.

Для запуска ПС без перезапуска ОС необходимо в специальной командной среде ПС «Сенсор» выполнить команду (процедура входа в специальной командную среду описана в п. 3.4):

```
sensor start
```

Для останова ПС без останова ОС необходимо в специальной командной среде ПС «Сенсор» выполнить команду:

```
sensor stop
```

3.3. Просмотр электронных журналов регистрации событий

По команде администратора безопасности СОВ поддерживается возможность экспорта электронных журналов в ПС «АРМ управления сенсорами», при этом каждый журнал сопровождается его контрольной суммой. По результатам экспорта журнал очищается, а первой записью нового журнала ПС «Сенсор» производит запись об его отчуждении с указанием контрольной суммы. ПС «АРМ управления сенсорами» позволяет проводить аудит записей ЭЖР посредством графического интерфейса с поддержкой поиска, сортировки и фильтрации записей.

При настройке ПС «Сенсор» для просмотра записей ЭЖР также может применяться специальная командная среда, предоставляющая доступ к возможностям диагностики и настройки ПС «Сенсор». Процедура входа в командную среду описана в п. 3.4.

Для просмотра электронных журналов ПС «Сенсор» следует выполнить в командной среде команды:

```
show log system
show log action
show log secure
```

Чтение записей ЭЖР пользователем или иными программными средствами, кроме как путем отчуждения электронного журнала и проведения аудита с помощью ПС «АРМ УС» или посредством специальной командной среды, не предусматривается.

3.4. Использование специальной командной среды

Для начальной настройки, проверки и восстановления работоспособности ПО ПС «Сенсор» используется специальная командная среда, предоставляющая доступ к возможностям диагностики и настройки ПС «Сенсор».

Список всех команд, доступных из командной среды ПС «Сенсор», с указанием выполняемых командами действий и примерами использования приведен в приложении В к настоящему руководству.

3.4.1. Вход в командную среду ПС «Сенсор»

Чтобы войти в командную среду ПС «Сенсор» с локальной консоли (KVM-панели), необходимо:

– нажать на клавиатуре (KVM-панели) комбинацию клавиш «Ctrl+Alt+F2», на экране появится запрос на ввод рабочего имени и пароля пользователя;

– ввести имя и пароль технологического пользователя «admin».

Чтобы войти в командную среду ПС «Сенсор» по сети с удаленного узла (при наличии такой возможности), необходимо на удаленном узле, функционирующем под управлением операционной системы Astra linux Special Edition «Смоленск» 1.5, выполнить команду:

```
ssh <ip-адрес изделия>
```

где в качестве параметра <ip-адрес изделия> задать ip-адрес ПС «Сенсор». В ответ на запрос необходимо ввести имя и пароль технологического пользователя «admin».

П р и м е ч а н и е – Технологический пользователь «admin» автоматически создается при установке ПО. Пароль технологического пользователя должен быть установлен в процессе

наладочных работ (настройка по умолчанию - «admin»). Также в процессе подготовки ПС «Сенсор» к использованию могут быть заведены дополнительные учетные записи технологических пользователей.

3.4.2. Выполнение команд

Для выполнения команды можно либо набрать ее на клавиатуре полностью, либо набрать несколько первых символов команды и нажать клавишу «Tab». Если набранным первым символам соответствует несколько команд, будет выведена подсказка с возможными вариантами, после чего можно откорректировать набранную команду. Если набранным первым символам соответствует одна команда, введенное начало команды в строке ввода автоматически будет дополнено недостающими символами.

Большинство команд требует задания одного или нескольких параметров. Для просмотра списка требуемых параметров после набора команды также можно нажать клавишу «Tab» для вывода необходимых параметров команды. Если команда требует параметр, значение которого выбирается из списка, по нажатию клавиши «Tab» будет выведен список возможных значений параметра. Для вывода подсказки, поясняющей действие, выполняемое командой, необходимо после набора команды набрать на клавиатуре символ «?».

Для выполнения набранной команды следует нажать клавишу «Enter».

Команды, выполняющие логически связанные действия, логически объединяются в группы. Команды в группе начинаются с одного и того же слова или нескольких слов. Это позволяет выполнять нескольких команд одной группы, не набирая каждую из них полностью: достаточно ввести общие начальные слова для группы команд и нажать клавишу «Enter», в результате чего произойдет переход в режим выполнения команд данной группы. В этом режиме требуется вводить только завершающую часть команд, опуская общее для группы команд начало. Для возврата из режима выполнения команд той или иной группы в режим ввода команд полностью следует нажать комбинацию клавиш «Ctrl+D».

Например, для установки параметров сенсора можно последовательно выполнить команды:

```
set sensor name TP-Sensor-13
set sensor id 13
…
set sensor susip 10.1.1.8
```

К тому же результату приведет выполнение последовательности команд (после выполнения последней команды следует нажать комбинацию клавиш «Ctrl+D»):

```
set sensor
name TP-Sensor-13
id 13
…
susip 10.1.1.8
```

Если выводимые в результате выполнения команды сообщения не помещаются на экране, для прокрутки экрана можно использовать комбинации клавиш «Shift+PageUp» и «Shift+PageDown».

Для повторного заполнения строки ввода ранее выполненной командой используются клавиши «↑» и «↓».

Для завершения сеанса работы в командной среде ПС «Сенсор» следует нажать комбинацию клавиш «Ctrl+D».

3.5. Создание резервной копии настроек ПС «Сенсор» на внешнем носителе

ПС «Сенсор» позволяет создавать и сохранять резервные копии своих настроек на внешнем носителе информации – оптическом компакт-диске формата CD-R/CD-RW или DVD-R/DVD-RW.

Для создания резервной копии настроек ПС необходимо:

– при отсутствии в составе технического средства, на котором установлено ПС «Сенсор», записывающего CD/DVD-привода – подключить переносной записывающий CD/DVD-привод к свободному USB-разъему технического средства;

– вставить чистый компакт-диск в CD/DVD-привод;

– нажать на клавиатуре (KVM-панели) комбинацию клавиш «Ctrl+Alt+F2» и на запрос операционной системы ввести имя и пароль привилегированного технологического пользователя «root»;

– после ввода учетных данных привилегированного технологического пользователя будет предоставлен доступ к командной строке операционной системы, в которой необходимо выполнить команду:

```
backup_config.sh save
```

– дождаться окончания выполнения команды, как показано на рис. 110;

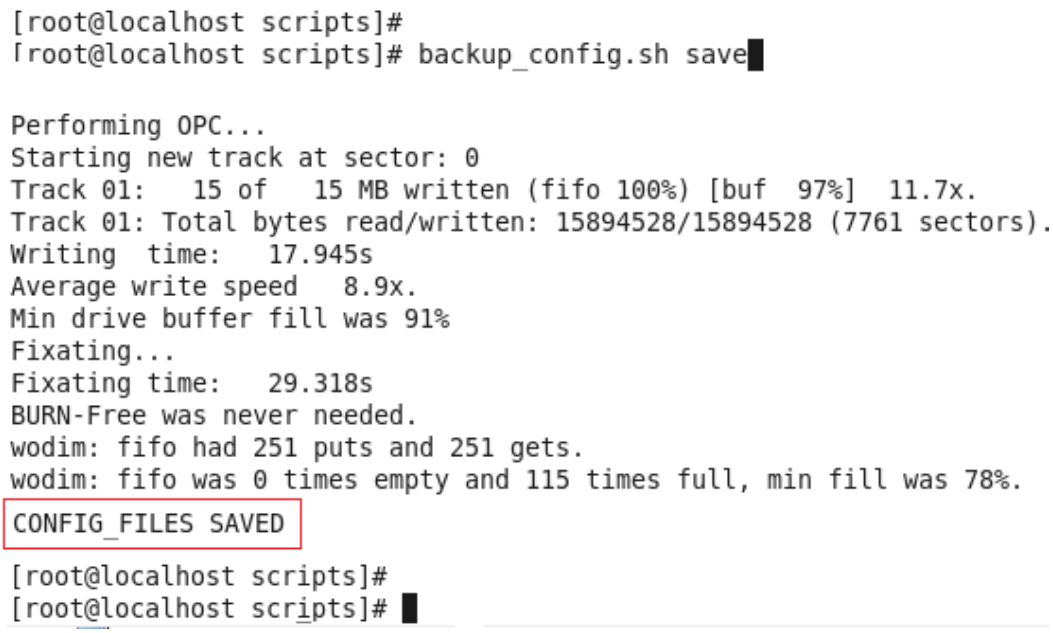


Рис. 110. Сохранение настроек

– в случае, если при выполнении команды диск был извлечен, вернуть его в CD/DVD-привод.

Примечание – Привилегированный технологический пользователь «root» создается при установке операционной системы. При установке ПС «Сенсор» на ПТК «Сервер УС» пароль технологического пользователя должен быть установлен в процессе наладочных и стыковочных работ для ПТК «Сервер УС» (настройка по умолчанию - «12345678»).

3.6. Восстановление настроек ПС «Сенсор» из резервной копии

Для восстановления настроек ПС «Сенсор» из резервной копии следует:

– при отсутствии в составе технического средства, на котором установлено ПС «Сенсор», CD/DVD-привода – подключить переносной CD/DVD-привод к свободному USB-разъему технического средства;

– вставить компакт-диск с резервной копией настроек в CD/DVD-привод;

– нажать на клавиатуре (KVM-панели) комбинацию клавиш «Ctrl+Alt+F2» и на запрос операционной системы ввести имя и пароль привилегированного технологического пользователя «root»;

– после ввода учетных данных привилегированного технологического пользователя будет предоставлен доступ к командной строке операционной системы, в которой необходимо выполнить команду:

```
backup_config.sh restore
```

– дождаться окончания выполнения команды, как показано на рис. 111.

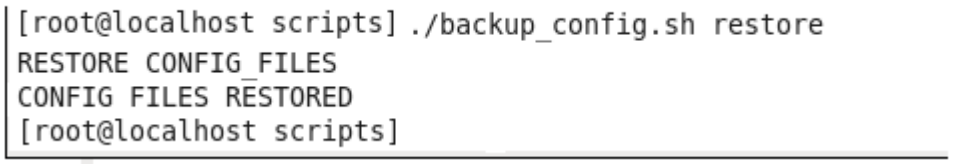


Рис. 111. Восстановление настроек

3.7. Проверка программы

Для проверки основных функций ПС «Сенсор», а также корректности настройки, предусмотрена операция проведения самотестирования.

Проведение самотестирования ПС «Сенсор» предусмотрено следующими способами:

– обязательное прохождение самотестирования при старте ПС «Сенсор»;

– периодическое выполнение самотестирования ПС «Сенсор» через заданный интервал времени (интервал задается при настройке);

– выполнение самотестирования по команде оператора СОВ ПАК «Плутон», подаваемой посредством ПС «АРМ УС».

Результаты самотестирования, проводимого при запуске ПС, и периодического самотестирования фиксируются в электронном журнале регистрации событий ПС «Сенсор». Результаты самотестирования, выполняемого по команде оператора СОВ ПАК «Плутон», отображаются оператору в графическом

интерфейсе ПС «АРМ УС», а также фиксируются в электронном журнале регистрации событий ПС «Сенсор».

В процессе самотестирования производятся следующие проверки:

– проверка целостности программных средств;

– проверка системы журналирования;

– проверка соединения с ПС «Сервер УС»;

– проверка обнаружения компьютерных атак.

При проверке обнаружения компьютерных атак генерируются тестовые атаки и проверяется их обнаружение ПС «Сенсор».

Сообщение с результатом самотестирования содержит информацию о результатах всех проверок в следующем виде:

```
Результат контроля целостности:
<исполняемый модуль 1>=Успех
<исполняемый модуль 2>= Успех
…
<исполняемый модуль N>= Успех
Результат проверки системы журналирования=Успех
Результат проверки передачи СИБ=Успех
Запущена тестовая атака
Тестовая атака обнаружена
```

3.8. Дополнительные возможности

Использование функций ПС «Сенсор» оператором производится посредством ПС «АРМ УС».

При начальной настройке, проверке и восстановлении работоспособности ПС «Сенсор» также может использоваться специальная командная среда, предоставляющая доступ к возможностям диагностики и настройки ПС «Сенсор». Порядок входа в специальную командную среду и её использования определен в п. 3.4 настоящего руководства.

Список всех команд, доступных из командной среды ПС «Сенсор», с указанием выполняемых командами действий и примерами использования приведен в приложении В к настоящему руководству.

Взаимодействие оператора с ПС «Сенсор», кроме как посредством ПС «АРМ УС» или специальной командной среды, не предусматривается.

3.9. Сообщения системному администратору

При возникновении проблем в процессе функционирования ПС «Сенсор» диагностические сообщения заносятся в ЭЖР. Основные сообщения, заносимые в ЭЖР, представлены в таблице 2.

Таблица 3. Основные диагностические сообщения ПС «Сенсор»

Программный модуль - источник события	Сообщение	Электронный журнал
AttackClientClient	Тестовая атака обнаружена	Журнал безопасности
SensorSysInfoClient	Сообщения о результате тестирования	Журнал безопасности
SensorSysInfoClient	Получена команда оператора на самотестирование	Журнал действий пользователя
AttackClient	IP адрес СУС не задан или задан неверный	Журнал технического состояния
AttackClient	AttackClient запущен	Журнал технического состояния
AttackClientClient	Соединение с сервером разорвано	Журнал технического состояния
AttackClientClient	Соединение с сервером восстановлено	Журнал технического состояния
SensorSysInfoClient	Проверка системы журналирования	Журнал технического состояния
SensorSysInfoClient	SensorSysInfoClient запущен	Журнал технического состояния
AttackClientClient	Процесс AttackClient уже запущен	Журнал технического состояния

ПЕРЕЧЕНЬ ПРИНЯТЫХ СОКРАЩЕНИЙ

БД	–	база данных
ГИП	–	графический интерфейс пользователя
КА	–	компьютерная атака
ОА	–	объект атаки
ОС	–	операционная система
ПС	–	программное средство
СА	–	субъект атаки
СИБ	–	сообщение информационной безопасности
СОВ	–	система обнаружения вторжений
СПО	–	специальное программное обеспечение
СС	–	состояние сенсора
СУБД	–	система управления базами данных
СУС	–	сервер управления сенсорами
ЭЖР	–	электронный журнал регистрации событий

Приложение А

(справочное)

Таблица А.1 – Перечень команд, поддерживаемых командной средой ПС «Сервер УС»

Команда	Пример	Действие команды
`help`	`help`	Выводит подсказку по использованию командной среды
`quit`	`quit`	Завершает сеанс работы (также выполняется при нажатии комбинации клавиш «Ctrl+D»)
`user add <login>`	`user add ivanov`	Заводит новую учетную запись технологического пользователя
`user passwd <login>`	`user passwd login`	Запрашивает и меняет пароль учетной записи технологического пользователя
`user delete <login>`	`user delete ivanov`	Удаляет учетную запись технологического пользователя
`sus start`	`sus start`	Запускает ПС «Сервер УС»
`sus stop`	`sus stop`	Останавливает ПС «Сервер УС»
`sus restart`	`sus restart`	Перезапускает ПС «Сервер УС»
`sus commit`	`sus commit`	Применяет изменения настроек ПС «Сервер УС», внесенные командами `set sus`
`sus mailcommit`	`sus mailcommit`	Применяет изменения настроек отправки почтовых оповещений, внесенные командами `set mail`
`do ping <ip>`	`do ping 10.1.1.8`	Проверяет доступность сетевого узла по заданному ip-адресу
`do traceroute <ip>`	`do traceroute 10.1.1.8`	Выводит маршрут прохождения пакетов до сетевого узла с заданным ip-адресом
`do reboot`	`do reboot`	Перезагружает аппаратное и программное обеспечение ПС «Сервер УС» (процесс перезагрузки может занимать до 15 минут)
`do poweroff`	`do poweroff`	Выключает ПС «Сервер УС»; после выполнения команды включение ПС «Сенсор» возможно только с помощью кнопки «Power» на передней панели ПС «Сервер УС»

Команда	Пример	Действие команды
`set sus <param> <value>`	`set sus name TP-SUS-1`	Устанавливает значение настроечных параметров ПС «Сервер УС»; перечень настроечных параметров приведен в п. 2.2.4 настоящего руководства
`show sus status`	`show sus status`	Выводит информацию о состоянии ПО ПС «Сервер УС»
`show process top`	`show process top`	Выводит информацию о потреблении ресурсов запущенными процессами
`show process ps`	`show process ps`	Выводит список запущенных процессов
`show mem free`	`show mem free`	Выводит информацию о проценте свободной оперативной памяти
`show disk space`	`show disk space`	Выводит информацию об использовании места на НЖМД
`show net interfaces all`	`show net interfaces all`	Выводит информацию обо всех сетевых интерфейсах ПС «Сервер УС»
`show net interfaces <iface>`	`show net interfaces eth0`	Выводит информацию о сетевом интерфейсе ПС «Сервер УС»
`show net routes`	`show net routes`	Выводит таблицу ip-маршрутизации
`show net connections`	`show net connections`	Выводит информацию об установленных сетевых подключениях
`show net firewall`	`show net firewall`	Выводит информацию о правилах фильтрации встроенного межсетевого экрана
`show log system`	`show log system`	Просмотр электронного журнала системы
`show log secure`	`show log secure`	Просмотр электронного журнала безопасности
`show log action`	`show log action`	Просмотр электронного журнала действий пользователя

Приложение В

(справочное)

Таблица В.1 – Перечень команд, поддерживаемых командной средой ПС «Сенсор»

Команда	Пример	Действие команды
`help`	`help`	Выводит подсказку по использованию командной среды
`quit`	`quit`	Завершает сеанс работы (также выполняется при нажатии комбинации клавиш «Ctrl+D»)
`user add <login>`	`user add ivanov`	Заводит новую учетную запись технологического пользователя
`user passwd <login>`	`user passwd login`	Запрашивает и меняет пароль учетной записи технологического пользователя
`user delete <login>`	`user delete ivanov`	Удаляет учетную запись технологического пользователя
`sensor start`	`sensor start`	Запускает ПС «Сенсор»
`sensor stop`	`sensor stop`	Останавливает ПС «Сенсор»
`sensor restart`	`sensor restart`	Перезапускает ПС «Сенсор»
`sensor checkcfg`	`sensor checkcfg`	Проверяет целостность конфигурационных файлов и базы решающих правил ПС «Сенсор»
`sensor commit`	`sensor commit`	Применяет изменения настроек ПС «Сенсор», внесенные командами set sensor
`do ping <ip>`	`do ping 10.1.1.8`	Проверяет доступность сетевого узла по заданному ip-адресу
`do traceroute <ip>`	`do traceroute 10.1.1.8`	Выводит маршрут прохождения пакетов до сетевого узла с заданным ip-адресом
`do reboot`	`do reboot`	Перезагружает аппаратное и программное обеспечение сенсора (процесс перезагрузки может занимать до 15 минут)
`do poweroff`	`do poweroff`	Выключает ПС «Сенсор»; после выполнения команды включение возможно только с помощью кнопки «Power» на передней панели ПС «Сенсор»
`set sensor <param> <value>`	`set sensor id 13`	Устанавливает значение настроечных параметров ПС

Команда	Пример	Действие команды
		«Сенсор»; перечень настроечных параметров приведен в п. 2.2.4 настоящего руководства
`set cluster <ip1> <ip2> … <ipN>`	`set cluster 10.1.1.1 10.1.1.2`	Переводит сенсор в режим функционирования в составе кластера, состоящего из узлов с указанными ip-адресами
`unset sensor dnainterface <mac>`	`unset sensor dnainterface 00:1F:38:DE:56:21`	Выводит сетевой интерфейс с указанным MAC из dna-режима
`cluster reset`	`cluster reset`	Сбрасывает состояние сенсора в кластере
`cluster stop`	`cluster stop`	Выводит сенсор из кластера и останавливает на сенсоре процессы управления кластером; для повторного ввода сенсора в кластер требуется выполнение команды set cluster
`show sensor status`	`show sensor status`	Выводит информацию о состоянии ПО сенсора
`show sensor interfaces`	`show sensor interfaces`	Выводит таблицу соответствия текущих имен и MAC сетевых интерфейсов сенсора
`show sensor confinterfaces`	`show sensor confinterfaces`	Выводит информацию о сконфигурированных в dna-режиме интерфейсах
`show sensor rules <group>`	`show sensor rules ddos`	Просмотр группы правил сигнатурного анализатора (недоступно, если правила не загружены на сенсор)
`show sensor preproc_rules <group>`	`show sensor preproc_rules decoder`	Просмотр группы препроцессорных правил сигнатурного анализатора; (недоступно, если правила не загружены на сенсор)
`show sensor prepare_rules <group>`	`show sensor prepare_rules smtp`	Просмотр группы прекомпилированных правил сигнатурного анализатора (недоступно, если правила не загружены на сенсор)
`show sensor so_rules <group>`	`show sensor so_rules smtp`	Просмотр группы прекомпилированных правил сигнатурного анализатора; (недоступно, если правила не загружены на сенсор)

Команда	Пример	Действие команды
`show cluster status`	`show cluster status`	Выводит текущее состояние узла кластера
`show process top`	`show process top`	Выводит информацию о потреблении ресурсов запущенными процессами
`show process ps`	`show process ps`	Выводит список запущенных процессов
`show mem free`	`show mem free`	Выводит информацию о проценте свободной оперативной памяти
`show disk space`	`show disk space`	Выводит информацию об использовании места на НЖМД
`show net interfaces all`	`show net interfaces all`	Выводит информацию обо всех сетевых интерфейсах сенсора
`show net interfaces <iface>`	`show net interfaces eth0`	Выводит информацию о сетевом интерфейсе сенсора
`show net routes`	`show net routes`	Выводит таблицу ip-маршрутизации
`show net connections`	`show net connections`	Выводит информацию об установленных сетевых подключениях
`show net firewall`	`show net firewall`	Выводит информацию о правилах фильтрации встроенного межсетевого экрана
`show log system`	`show log system`	Просмотр электронного журнала системы
`show log secure`	`show log secure`	Просмотр электронного журнала безопасности
`show log action`	`show log action`	Просмотр электронного журнала действий пользователя

Приложение Г

Таблица Г.1 – Состав дистрибутива СОВ ПАК «Плутон»

Каталог	Имя файла
ПС АРМ УС	armdbmanager_0-1_amd64.deb arm-rulesupdater-0.1.deb attackdatalib_0-1_amd64.deb attackinfoanalyser_0-1_amd64.deb attackobserver-client_0-1_amd64.deb attackobserver-server_0-1_amd64.deb authentication_0-1_amd64.deb basedatalib_0-1_amd64.deb ccis-exept_0-1_amd64.deb ccis-platform_0-1_amd64.deb ccis-ucode_0-1_amd64.deb commanddatalib_0-1_amd64.deb configuration_0-1_amd64.deb connectionmanager_0-1_amd64.deb criticalalertslib_0-1_amd64.deb dbaccesslib_0-1_amd64.deb drawmarble_0-1_amd64.deb firewallcontrol_0-1_amd64.deb genericlog_0-1_amd64.deb gost3411-2012-hashlib_0-1_amd64.deb graphicinfodb_0-1_amd64.deb initarm-p_0-1_amd64.deb initdialoglib_0-1_amd64.deb kdreports-1.4.0_0-1_amd64.deb libgeoip_0-1_amd64.deb libgeoip-data-1.4.7.deb libisocode_0-1_amd64.deb libmaxminddb_0-1_amd64.deb libssh_0-1_amd64.deb marbleattacksrealtimeplugin_0-1_amd64.deb marbleattacksstatisticsplugin_0-1_amd64.deb marblelib_0-1_amd64.deb marblesensorsinfoplugin_0-1_amd64.deb marblesensorsplugin_0-1_amd64.deb msoa-attack_0-1_amd64.deb msoa-info_0-1_amd64.deb observer_0-1_amd64.deb plotlib_0-1_amd64.deb pluto-basics_0-1_amd64.deb

Каталог	Имя файла
	qgeoip_0-1_amd64.deb qhexedit2_0-1_amd64.deb qipinput_0-1_amd64.deb qjson_0-1_amd64.deb qwt_0-1_amd64.deb rtfdoc_0-1_amd64.deb scdblayermanagerslib_0-1_amd64.deb selftest_0-1_amd64.deb sensorcontrolguiclient_0-1_amd64.deb sensorcontrolsystemtypeslib_0-1_amd64.deb sensorsettings_0-1_amd64.deb sensorstateobserver-client_0-1_amd64.deb sensorstateobserver-server_0-1_amd64.deb sensorstateshortdescriptionprovider_0-1_amd64.deb sensorsystemdatalib_0-1_amd64.deb snort-rules-all.deb zntcpclientlib_0-1_amd64.deb zxsensorstatusobserver_0-1_amd64.deb
ПС Сенсор	attackclient_0-1_amd64.deb attackdatalib-ds_0-1_amd64.deb attackdatalib_0-1_amd64.deb authentication_0-1_amd64.deb basedatalib_0-1_amd64.deb ccis-exept_0-1_amd64.deb ccis-platform_0-1_amd64.deb ccis-ucode_0-1_amd64.deb commanddatalib-ds_0-1_amd64.deb commanddatalib_0-1_amd64.deb daq_0-1_amd64.deb dbaccesslib_0-1_amd64.deb e1000e-zc-dkms_3.2.7.1.0_all.deb fm10k-zc-dkms_0.20.1.0_all.deb genericlog_0-1_amd64.deb generic_0-1_amd64.deb gost3411-2012-hashlib_0-1_amd64.deb i40e-zc-dkms_1.5.18.0_all.deb igb-zc-dkms_5.3.3.5.0_all.deb initsensorcli_0-1_amd64.deb initsensor_0-1_amd64.deb ixgbe-zc-dkms_4.1.5.0_all.deb kernel_0-1_amd64.deb libdnet_0-1_amd64.deb libfifobuf_0-1_amd64.deb

Каталог	Имя файла
	libpcap_0-1_amd64.deb libshmem_0-1_amd64.deb lib_0-1_amd64.deb nfdump_0-1_amd64.deb openvpn-2.2.3_0-1_amd64.deb pfring-daq-module_0-1_amd64.deb pfring-daq_0-1_amd64.deb pfring-drivers-zc-dkms_1.3_all.deb qipinput_0-1_amd64.deb qtlockedfile-dev_2.4-1_amd64.deb qtlockedfile_2.4-1_amd64.deb qtsingleapplication-dev_2.6-3_amd64.deb qtsingleapplication_2.6-3_amd64.deb selftest_0-1_amd64.deb sensord-0.1.deb sensorethmonitor_0-1_amd64.deb sensorsysinfoclient_0-1_amd64.deb sensorsystemdatalib_0-1_amd64.deb snort-configs_0-1_amd64.deb snort-rules.deb snort_0-1_amd64.deb tcpdump_0-1_amd64.deb tinysh_0-1_amd64.deb zntcpclientlib_0-1_amd64.deb
ПС СУС	attackanalysingservice_0-1_amd64.deb attackdatalib_0-1_amd64.deb attackdatalib-ds_0-1_amd64.deb attackinfoanalyser_0-1_amd64.deb attackobserver-server_0-1_amd64.deb basedatalib_0-1_amd64.deb ccis-exept_0-1_amd64.deb ccis-platform_0-1_amd64.deb ccis-ucode_0-1_amd64.deb cefgenerate_0-1_amd64.deb commanddatalib_0-1_amd64.deb commanddatalib-ds_0-1_amd64.deb configuration_0-1_amd64.deb connectionmanager_0-1_amd64.deb dbaccesslib_0-1_amd64.deb deploy_database-0.1.deb firewallcontrol_0-1_amd64.deb generic_0-1_amd64.deb genericlog_0-1_amd64.deb

Каталог	Имя файла
	gost3411-2012-hashlib_0-1_amd64.deb graphicinfodb_0-1_amd64.deb initmailcli_0-1_amd64.deb initsuscli_0-1_amd64.deb libemail_0-1_amd64.deb libgeoip_0-1_amd64.deb libgeoip-data-1.4.7.deb libisocode_0-1_amd64.deb libmaxminddb_0-1_amd64.deb libssh_0-1_amd64.deb nfdump_0-1_amd64.deb observer_0-1_amd64.deb pginithelper-0.2.deb pluto-basics_0-1_amd64.deb prioritymanager_0-1_amd64.deb qgeoip_0-1_amd64.deb qhexedit2_0-1_amd64.deb qipinput_0-1_amd64.deb qjson_0-1_amd64.deb qtlockedfile_2.4-1_amd64.deb qtlockedfile-dev_2.4-1_amd64.deb qtsingleapplication_2.6-3_amd64.deb qtsingleapplication-dev_2.6-3_amd64.deb scdblayermanagerslib_0-1_amd64.deb selftest_0-1_amd64.deb sensorcontrolsystemtypeslib_0-1_amd64.deb sensorstateanalysingserver_0-1_amd64.deb sensorstateobserver-server_0-1_amd64.deb sensorstateshortdescriptionprovider_0-1_amd64.deb sensorsystemdatalib_0-1_amd64.deb serverconsole_0-1_amd64.deb serverdbmanager_0-1_amd64.deb serverp.deb tinysh_0-1_amd64.deb zntcpclientlib_0-1_amd64.deb zxsensorstatusobserver_0-1_amd64.deb zxtcpserverlib_0-1_amd64.deb

Л и с т   р е г и с т р а ц и и   и з м е н е н и й

Изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	№ документа	Входящий № сопрово-дительного докум. и дата	Подп.	Дата
	изме-ненных	заме-ненных	новых	аннули-рованных					