УТВЕРЖДЕНО

RU.09445927.425530-03 32 01-ЛУ

СИСТЕМА INVGUARD AS

Программный комплекс invGuard AS-SW

Руководство системного программиста

RU.09445927.425530-03 32 01

Листов 126

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата
0015	29.05.2014			

2014

АННОТАЦИЯ

В данном программном документе приведено руководство системного программиста по настройке и использованию программного комплекса invGuard AS-SW системы invGuard AS (далее Анализатор), предназначенного для сбора статистики по трафику и нагрузке на сетевое оборудование с целью обнаружения и отражения различных атак на сеть передачи данных оператора связи. Анализатор является составной частью системы защиты от сетевых атак (СЗСА) invGuard (далее Система).

В данном программном документе в разделе «Общие сведения о программе» указаны назначение и функции программы и сведения о технических и программных средствах, обеспечивающих выполнение данной программы, а также требования к персоналу.

В разделе «Структура программы» приведены сведения о структуре программы, ее составных частях, о связях между составными частями и о связях с другими программами.

В данном программном документе в разделе «Настройка программы» приведено описание действий по настройке программы на условия конкретного применения.

Оформление программного документа «Руководство системного программиста» произведено по требованиям ЕСПД (ГОСТ 19.101-77, ГОСТ 19.103-77, ГОСТ 19.104-78, ГОСТ 19.105-78, ГОСТ 19.106-78, ГОСТ 19.503-79, ГОСТ 19.604-78).

СОДЕРЖАНИЕ

1. ОБЩИЕ СВЕДЕНИЯ О ПРОГРАММЕ

1.1 Назначение программы

Функциональным назначением Анализатора является обнаружение DoS/DDoS-атак на телекоммуникационное оборудование в высокоскоростных сетях передачи данных и управление аппаратными средствами Системы для отражения (подавления) данных атак.

Программный комплекс разработан для применения в составе системы invGuard AS.

1.2 Функции программы

Основные функции программы состоят в глубоком анализе потоков данных NetFlow и первичного трафика (входящего и исходящего) и сборе статистики по трафику и нагрузке на сетевое оборудование с целью обнаружения DDoS и сигнатурных атак на сеть передачи данных оператора связи.

1.3 Минимальный состав технических средств

Минимальный состав используемых технических (аппаратных) средств:

1) сервер с процессором Intel с частотой не менее 2,9 ГГц;
2) оперативная память объемом не менее 16 Гб;
3) жесткий диск объемом 500 Гб и выше;
4) две сетевые карты LAN не менее 1 Гбит/с.

1.4 Минимальный состав программных средств

Для функционирования программы необходимо следующее программное обеспечение:

1) Локализованная и сертифицированная по требованиям безопасности операционная система (например, РОСА SX «КОБАЛЬТ» 1.0);
2) Apache 2.2 и выше;
3) PHP 5.2 и выше;

4) MySQL 5.1 и выше.

1.5 Требования к персоналу (системному программисту)

Системный программист должен иметь минимум высшее техническое образование.

В перечень задач, выполняемых системным программистом, должны входить:

1) задача поддержания работоспособности технических средств;
2) задача установки (инсталляции) и поддержания работоспособности системных программных средств – операционной системы;
3) задача установки (инсталляции) и поддержания работоспособности Анализатора трафика.

2. СТРУКТУРА ПРОГРАММЫ

2.1 Сведения о структуре программы

Анализатор трафика имеет модульную архитектуру, как показано на рисунке 1.

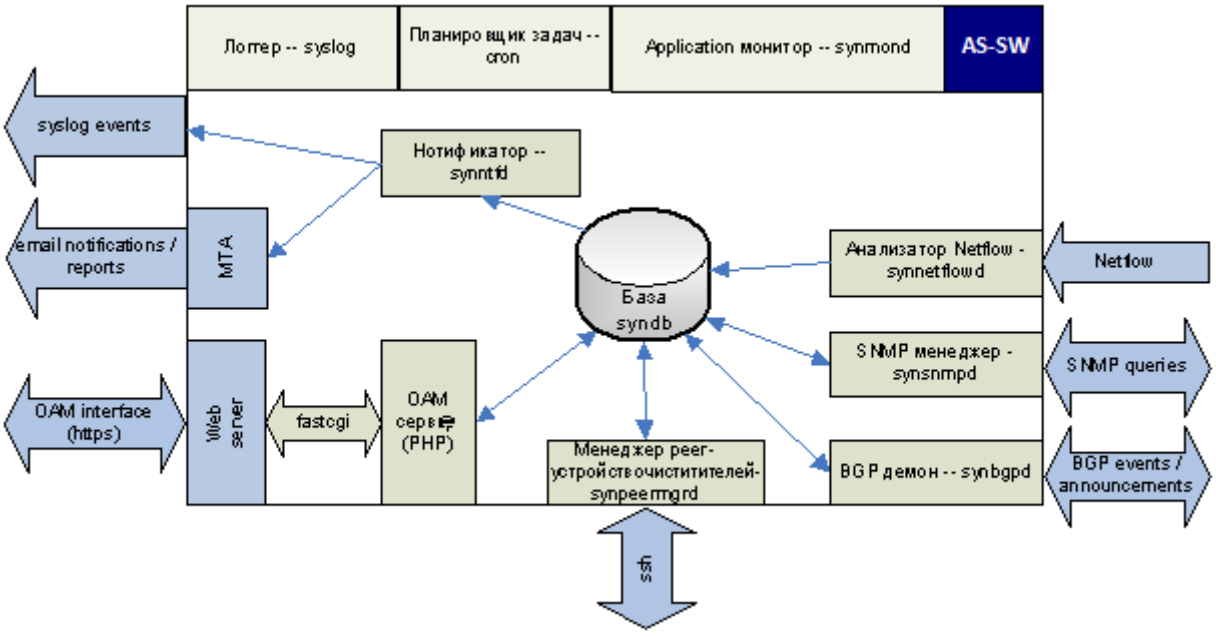

Рисунок 1 – Модульная архитектура Анализатора трафика

Программный комплекс invGuard AS-SW состоит из следующих модулей:

- synmond;
- synnetflowd;
- OAM-сервер;
- synbgpd;
- synsnmpd;
- synpeermgrd;
- synntfd.

Также в состав Анализатора входят Third-party модули:

- Web server / PHP;
- mysql;
- postfix;
- sshd;
- syslog;
- cron.

2.2 Сведения о составных частях программы

SYNMOND

- Обеспечивает общий запуск/остановку всех процессов;
- Мониторинг процессов и рестарт;
- Регулярное удаление старых данных на диске и в базе;
- Мониторинг места на диске и очистка диска при необходимости;
- Мониторинг места в базе данных и удаление устаревших данных при необходимости;
- Мониторинг критических параметров Системы;
- Запуск скрипта резервного копирования.

SYNNETFLOWD

- Сбор статистики на основе анализируемого NetFlow и сохранение ее в БД;
- Агрегация данных;
- Генерация аномалий по детекторам.

OAM-СЕРВЕР

- Изменение конфигурации Системы;
- Получение отчетов о трафике и аномалиях;
- Выполнение управляющих действий (начало/остановка задания подавления атак и т.п.).

SYNBGPD

- Установление BGP-пиринга с роутерами, получение и сохранение в базе маршрутов;
- Обнаружение аномалий по детекторам D6, D7 и D8;
- Отправка BGP-сообщений для начала очистки или перенаправления трафика на альтернативное направление.

SYNSNMPD

- Автоматическое получение списка интерфейсов с роутера и сохранение его в базе;
- Периодический сбор статистики с устройств и сохранение ее в базе;
- Обнаружение аномалий по детектору D1.

SYNPEERMGRD

- Конфигурирование, запуск и остановка заданий подавления атак на очистителях;
- Получение статистики с очистителей и сохранение ее в базе данных;
- Генерация аномалий по порогам статистики, собираемой очистителем;
- Генерация аномалий при перегрузке очистителя.

SYNNTFD

- Рассылка оповещений об аномалиях согласно сконфигурированным правилам;
- Периодическая рассылка отчетов.

Third-party модули

WEB SERVER / PHP

Обеспечение функционирования OAM-сервера.

MYSQL

Сервер базы данных. Обеспечивает хранение всей информации о трафике.

POSTFIX

Агент передачи почты.

SSHD

Обеспечивает защищенное соединение для обмена данными между анализатором и очистителем (ssh / scp).

SYSLOG

Обеспечивает ведение лог файла для всех модулей.

CRON

Обеспечивает запуск задач по расписанию.

2.3 Сведения о связях с другими программами

Система связывается только со своей копией на другом сервере для обмена фингерпринтами.

3. НАСТРОЙКА ПРОГРАММЫ

3.1 Первоначальная настройка Системы

3.1.1 Создание учетных записей пользователей

Чтобы пользователи могли начать работу с Системой, администратор должен создать учетные записи пользователей и распределить их по группам.

3.1.2 Настройка глобальных параметров

На экране «Глобальные настройки» (Администрирование → Пользовательский интерфейс → Глобальные настройки) следует выполнить следующие действия по настройке Системы:

1) выбрать логотип для использования в отчетах при экспорте;
2) изменить адрес тех. Поддержки, отображаемый на всех страницах веб-интерфейса;
3) настроить таймаут регистрации в Системе;
4) настроить период обновления страницы статуса Системы;

5) изменить адрес сайта, используемый в отчетах при экспорте и в почтовых уведомлениях;
6) настроить максимальное количество сообщений в почтовой очереди;
7) настроить количество отображаемых сообщений в ленте событий;
8) выбрать часовой пояс, используемый по умолчанию при создании учетных записей;
9) выбрать способ подавления атак, применяемый по умолчанию.

3.1.3 Экспортирование конфигурации Анализатора

Веб-интерфейс позволяет экспортировать конфигурацию Анализатора в файл для переноса ее на другую Систему или для создания резервной копии. Для экспортирования выполните следующие действия:

- Перейдите на экран «Экспорт» (Администрирование → Общие настройки → Версия конфигурации → Экспорт).
- Если необходимо, чтобы в экспорт попали учетные записи, группы пользователей и права доступа, отметьте флажком соответствующее поле.
- Нажмите «Получить текущую конфигурацию».

Важно: импорт конфигурации возможен, только если версии Систем совпадают.

3.1.4 Импортирование конфигурации Анализатора

Веб-интерфейс позволяет импортировать конфигурацию Анализатора из файла при восстановлении из резервной копии или переносе с другой Системы. Для импортирования выполните следующие действия:

- Перейдите на экран «Импорт» (Администрирование → Общие настройки → Версия конфигурации → Импорт).
- Выберите файл конфигурации для импорта.
- Если необходимо импортировать также учетные записи, группы пользователей и права доступа, поставьте флажок в соответствующее поле.
- Нажмите «Импортировать конфигурацию».

Важно: импорт конфигурации возможен, только если файл конфигурации был создан на Системе той же версии.

3.1.5 История конфигураций

Все изменения, производимые через веб-интерфейс в конфигурации Системы, автоматически записываются в историю конфигураций (Администрирование → Общие настройки → Версия конфигурации → История). В случае необходимости всегда можно вернуться к предыдущей версии конфигурации. Для этого выполните следующие действия:

- Перейдите на экран «История» (Администрирование → Общие настройки → Версия конфигурации → История).
- Выберите версию конфигурации, к которой необходимо вернуться.
- Нажмите «Вернуть конфигурацию к выбранной версии».

3.2 Архитектура Системы

3.2.1 Введение

В этой главе дается описание устройств, из которых состоит Система, а также рассматриваются способы их подключения.

3.2.2 Составные части Системы

Система состоит из одного устройства анализа трафика (Анализатора).

На рисунке 2 представлена структура Системы:

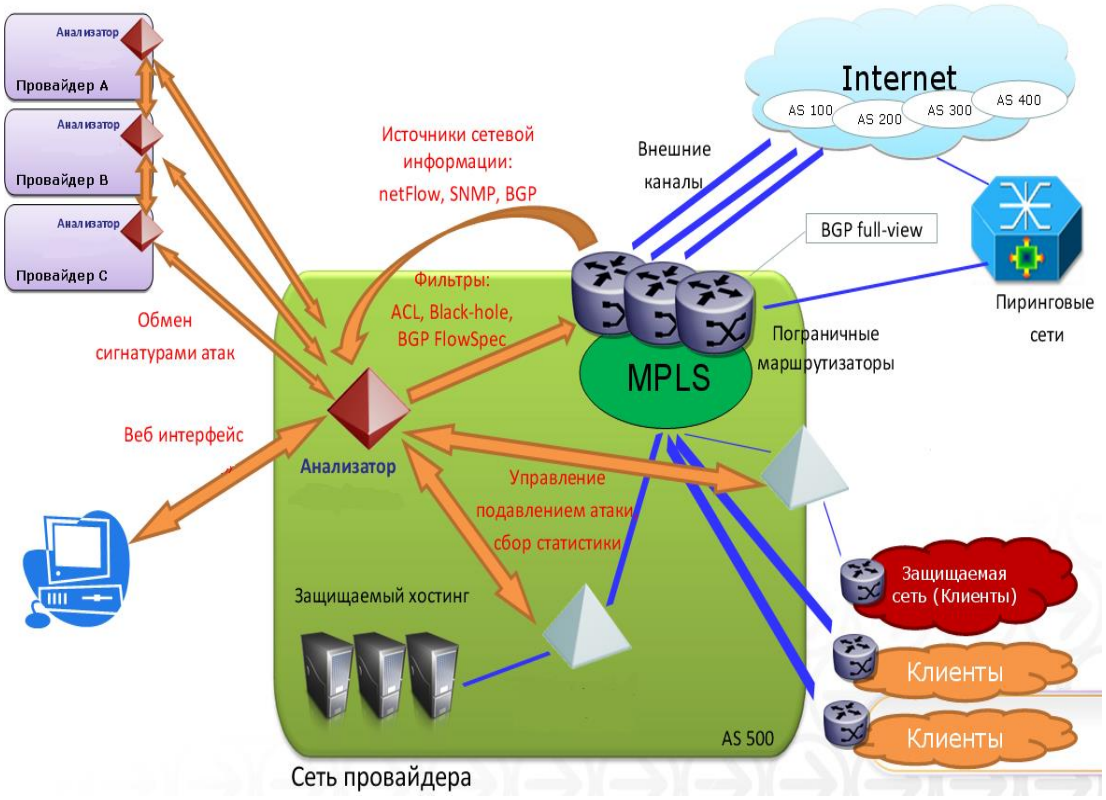

Рисунок 2 – Структура Системы

В таблице 1 приводится описание устройств.

Таблица 1 – Устройства

Устройство	Функция
Анализатор	Измерение, мониторинг трафика, управление заданиями по очистке трафика. Работает с трафиком на канальном и сетевом уровнях стека TCP/IP.

3.2.3 Описание Анализатора

Анализатор трафика имеет 1x1 Gbit Copper Ethernet порт для NetFlow-трафика и 1x1 Gbit Copper Ethernet порт для прочих нужд: доступа к web-интерфейсу управления, для BGP- и SNMP-трафика.

3.3 Установка Анализатора

3.3.1 Установка операционной системы

Перед установкой Анализатора убедитесь, что в системе установлены: Apache 2.2 и выше, PHP 5.2 и выше, MySQL 5.1 и выше.

В качестве операционной системы Анализатора используется дистрибутив локализованной и сертифицированной по требованиям безопасности операционной системы РОСА SX «КОБАЛЬТ» 1.0.

Процесс установки системы зависит от конкретной аппаратной платформы, ниже описаны основные этапы.

Замечание: В процессе инсталляции все данные, находящиеся на сервере, будут утеряны.

1) Перед установкой BIOS сервера должен быть настроен на следующий порядок загрузки:
   а) CD-DVD ROM;
   б) Жесткий диск.
2) Включите сервер, вставьте стандартный диск установки ОС Роса, перезагрузить сервер. Загрузится программа установки с компакт-диска.
3) В меню «Welcome to POCA SX64 "COBALT"» выберите пункт
   – Install or upgrade an existing system

   и нажмите клавишу Enter. Начнется загрузка программы установки.
4) В появившемся экране программы установки в диалоге «Disk Found» выберите «Skip».
5) Запустится графический интерфейс пользователя программы установки с возможностью работы с мышью. На экране приветствия нажмите «Next».
6) Следующий диалог - диалог выбора языка для процесса инсталляции. Выберите «Russian (Русский)», нажмите «Next».

7) Диалог выбора раскладки клавиатуры. Выберите «Русская», если не выбрана. Нажмите «Next».
8) «Какой тип устройств будет использоваться при установке?» – выберите «Стандартные накопители», нажать «Далее».
9) В диалоге «Присвойте этому компьютеру имя...» поставьте имя по умолчанию.
10) В диалоге выбора часового пояса выберите часовой пояс, например, «Европа/Москва», нажмите «Далее».
11) Введите пароль для пользователя root в верхней строке диалога и в строке подтверждения второй раз. Нажмите «Далее».

Замечание: пароль пользователя root необходимо запомнить, так как он необходим далее в процессе установки.

12) Диалог «Какой тип установки вы предпочитаете?» - выберите «Все пространство», нажмите «Далее», подтвердите действие нажатием кнопки «Сохранить изменения на диск» в появившемся диалоге. Происходит создание файловой системы.
13) Выберите тип системы: «Software Dewelopment workstation», нажмите «Далее». Запустится процесс установки пакетов и конфигурации, который может занять некоторое время.
14) После окончания установки нажмите кнопку «Перезагрузка».
15) ОС Роса загрузится с жесткого диска. На экране приветствия нажмите кнопку «Вперед».
16) Экран информации о лицензии, нажмите «Вперед».
17) Экран добавления пользователя, введите в форму информацию о пользователе: имя (логин), полное имя, пароль и подтверждение пароля. Нажмите «Вперед».
18) Экран установки времени - установите время, нажмите «Готово».
19) Возникнет приглашение для входа в систему. Нажмите на имя пользователя, по запросу введите пароль. Вход выполнен, появится рабочий стол пользователя.

20) Перезагрузите сервер.

3.4 Процесс установки invGuard AS-SW

3.4.1 Требования и порядок установки компонентов и драйверов для возможности выполнения инсталляции

3.4.2 Настройка портов управления для доступа к системе

Настройка портов системы производиться путём редактирования файлов в соответствии с техническим решением:

1) /etc/udev/rules.d/70-persistent-net.rules
2) /proc/net/vlan/config
3) /etc/sysconfig/network-scripts/ifcfg-eth*
4) /etc/sysconfig/iptables

3.4.3 Установка драйвера Broadcom

Пример инструкций, используемых при установке драйвера Broadcom:

1) modinfo bnx2x
2) ip addr
3) ethtool eth0
4) ethtool eth1
5) ethtool eth2
6) rpm -qa | grep netx
7) rmmod bnx2x
8) modinfo bnx2x
9) rm /lib/modules/2.6.32-279.19.1.res6.x86_64/kernel/drivers/net/bnx2x/bnx2x.ko
10) depmod -a
11) modinfo bnx2x
12) rm /lib/modules/2.6.32-279.19.1.res6.x86_64/updates/bnx2x.ko
13) depmod -a
14) modinfo bnx2x
15) rpm -ivh netxtreme2-7.10.12-2.rhel5u10.src.rpm

16) cd /root/rpmbuild

17) rpmbuild --nodeps -bb SPECS/kmp-netxtreme2.spec

18) cp SPECS/kmp-netxtreme2.spec SPECS/kmp-netxtreme2.spec_orig

19) nano SPECS/kmp-netxtreme2.spec

20) rpmbuild --nodeps -bb SPECS/kmp-netxtreme2.spec

21) cd RPMS/x86_64/

22) rpm --nodeps -ivh kmod-netxtreme2-7.10.12-2.rhel5u10.x86_64.rpm

23) rpm -qa | grep netx

24) modprobe bnx2x

25) modinfo bnx2x

26) dmesg | grep bnx2x

27) dmesg | grep eth0

28) dmesg | grep eth1

29) ip addr

30) ethtool eth0

31) ethtool eth1

32) lspci -vvv | less

3.4.4 Установка драйвера Intel

Устанавливается ixgbe драйвер (пример инструкций по установке драйвера сетевого чипсета приведён п. 3.4.3)

3.4.5 Процесс установки Анализатора

Дистрибутив Анализатора представляет собой архив на оптическом диске, поставляемый с Системой и включающий в себя все необходимые приложения и библиотеки, используемые для работы Системы. Во время установки пакетов, инсталлятор запрашивает у пользователя конфигурационную информацию.

Замечание: при развертывании Анализатора, поверх установленного старые версии базы данных и приложений, удаляются. Пользователи базы данных пересоздаются.

Для установки invGuard AS-SW:

Подключите и смонтируйте диск с операционной системы ROSA SX64 "COBALT" (mount -t iso9660 /dev/sr0 /media/ROSA-SX64-1.0);

- Проверьте контрольную сумму дистрибутива. Контрольная сумма должна соответствовать значению, приведенному в документе RU.09445927.425530-03 30 01 «Формуляр».
- Скопируйте и распакуйте дистрибутив с Анализатором в домашний каталог пользователя, используя команды:

1) tar -xvf install_analyzer_2015-01-23_v.1.19.tar.gz

2) cd install_analyzer

Структура исходных файлов и директорий:

1) 3d_conf

2) 3d_party

3) bin

4) cfg

5) install_commands.txt

6) scripts

7) www

- Откройте консоль пользователя «root» и введите команды:

1) yum install libstdc++.so.6

2) yum install glibc.i686

3) yum install lm_sensors-libs.i686

4) yum install mysql-libs.i686

5) yum install libpcap.i686

6) yum install mysql-server

7) yum install expect.x86_64

8) yum install php

9) yum install mod_ssl

10) yum install php-mysql

11) yum install php-gd php-mbstring

12) yum install php-xml

13) yum install ncurses-devel-5.7-3.20090208.res6.i686

14) yum install pcre.i686

15) rpm -i ./3d_party/libnfnetlink0-1.0.1-45.1.x86_64.rpm

16) rpm -i ./3d_party/libnetfilter_conntrack3-1.0.1-1.8.x86_64.rpm

17) rpm -i ./3d_party/conntrack-tools-1.0.0-8.12.x86_64.rpm

18) rpm -i ./3d_party/lm_sensors-3.1.1-17.res6.x86_64.rpm

19) rpm -i ./3d_party/xerces-c-3.0.1-20.el6.i686.rpm

20) rpm -i ./3d_party/snmp++-3.2.25-1.fc15.i686.rpm

21) rpm -U --oldpackage ./3d_party/procps-3.2.8-25.el6.i686.rpm

22) rpm -ivh ./3d_party/php-process-5.3.3-14.res6.x86_64.rpm

23) rpm -ivh /media/ROSA-SX64-1.0/Packages/libmcrypt-2.5.8-9.res6.x86_64.rpm

24) rpm -ivh /media/ROSA-SX64-1.0/Packages/php-mcrypt-5.3.3-1.res6.x86_64.rpm

25) mkdir -p /usr/bin/syn

26) cp ./bin/* /usr/bin/syn

27) mkdir -p /etc/syn

28) cp -R ./cfg/* /etc/syn/

29) cd ./3d_party/

30) tar -xvf ./cmake-2.8.12.2.tar.gz

31) cd ./cmake-2.8.12.2

32) ./configure --prefix=/usr

33) make all install

34) cd -

35) cd ../3d_party/libssh-0.3.4/build/

36) cmake -DCMAKE_INSTALL_PREFIX=/usr ..

37) make all install

38) cd -

39) cp ../3d_party/libssh.so.3.4.0 /usr/lib/

40) cd ../3d_party/
41) tar -xvf ./whois_5.2.0.tar.xz
42) cd whois-5.2.0
43) make
44) make install
45) cd -
46) rpm --force -ivh tzdata-2014h-1.res6.noarch.rpm
47) rpm --force -ivh tzdata-java-2014h-1.res6.noarch.rpm
48) rpm -ivh screen-4.0.3-16.el6.x86_64.rpm
49) useradd syn --create-home
50) passwd syn
51) введите synsyn
52) useradd www --create-home
53) cd ..
54) cp ./3d_conf/my.cnf /etc/my.cnf
55) service mysqld restart
56) mysql_tzinfo_to_sql /usr/share/zoneinfo | mysql -u root mysql
57) mysql -u root -e "create database install_syn"
58) mysql -u root -e "create user 'syn'@'localhost' identified by 'synsyn'"
59) mysql -u root -e "create user 'syn'@'%' identified by 'synsyn'"
60) mysql -u root -e "create user 'www'@'localhost' identified by 'wwwwww'"
61) mysql -u root -e "create user 'www'@'%' identified by 'wwwwww'"
62) mysql -u root -e "GRANT ALL PRIVILEGES ON *.* TO 'syn'@'%';"
63) mysql -u root -e "GRANT ALL PRIVILEGES ON *.* TO 'syn'@'localhost';"
64) mysql -u root -e "GRANT ALL PRIVILEGES ON *.* TO 'www'@'%';"
65) mysql -u root -e "GRANT ALL PRIVILEGES ON *.* TO 'www'@'localhost';"
66) mysql -u syn -psynsyn install_syn < ./scripts/install_syn.sql

67) mysql -u syn -psynsyn install_syn -e "DELETE FROM ${MYSQL_DB}.disk_monitor;"
68) mysql -u syn -psynsyn install_syn -e "DELETE FROM ${MYSQL_DB}.disk_partitions;"
69) mysql -u syn -psynsyn install_syn -e "INSERT INTO ${MYSQL_DB}.disk_partitions VALUES (1,'/var/lib/mysql'),(2,'/'),(3,'/var'),(4,'/usr'),(5,'/tmp');"
70) \cp -R ./www/* /home/www
71) chmod -R 777 /home/www
72) chown -R syn:syn /home/www
73) \cp ./3d_conf/etc/php.ini /etc/php.ini
74) \cp ./3d_conf/etc/httpd/conf/httpd.conf /etc/httpd/conf/
75) \cp ./3d_conf/etc/httpd/conf.d/* /etc/httpd/conf.d/
76) chown apache:apache /var/lib/php/session
77) chmod 777 /var/lib/php/session
78) mysql –u syn –p install_syn
79) INSERT INTO `install_syn`.`syn_users`
80) (`user_id`, `user_name`, `pwd_hash`, `real_name`, `is_enabled`, `is_deleted`, `nb_login_failures`, `random_seed`, `auth_group_id`, `auth_type`)
81) VALUES (2, 'adm1', '519c3e52236a6732c3fe2308a67f8b44425a8680', 'adm1', 1, 0, 0, 0, 1, 'local');
82) service httpd restart
83) \cp ./3d_conf/etc/init.d/* /etc/rc.d/init.d/
84) \cp ./3d_conf/sudoers /etc/sudoers
85) \cp ./3d_conf/cron.d/* /etc/cron.d/
86) \cp ./3d_conf/contractd/conntrackd.conf /etc/conntrackd/conntrackd.conf
87) \cp ./3d_conf/etc/postfix/* /etc/postfix/
88) postmap /etc/postfix/sasl_passwd
89) mkdir -p /var/syn/www
90) chown syn:syn /var/syn/www

91) chmod 777 /etc/syn/synntfd/mailq.pl

92) chown syn:syn /etc/syn/synntfd/mailq.pl

93) mkdir -p /var/syn/alerts

94) chown syn:syn /var/syn/alerts

95) service postfix restart

96) mkdir -p /var/log/syn

97) touch /var/log/syn/synsecd.log

98) chown syn:syn /var/log/syn/synsecd.log

99) touch /var/log/conntrackd-stats.log

100) chmod 655 /var/log/conntrackd-stats.log

101) chown syn:syn /var/log/syn/synsecd.log

102) mkdir -p /var/syn/fingerprints

103) chown syn:syn /var/syn/fingerprints

104) mkdir -p /var/syn/synsecd

105) chown syn:syn /var/syn/synsecd

106) mkdir -p /var/syn/dumps

107) chown syn:syn /var/syn/dumps

108) mkdir /home/syn/db_data

109) chown mysql:mysql /home/syn/db_data

110) mkdir /home/syn/db_backup_data

111) chown syn:syn /home/syn/db_backup_data

112) mkdir /home/syn/snapshot

113) chown syn:syn /home/syn/snapshot

114) chkconfig --add synmond

115) chkconfig synmond on

116) touch /etc/hostid

117) nano /etc/hostid

118) cp bin/syn_log_rotate_1.5.pl /root

119) chmod 755 /root/syn_log_rotate_1.5.pl

120) ln -s syn_log_rotate_1.5.pl /root/syn_log_rotate.pl

121) crontab -e

122) 30 * * * * /root/syn_log_rotate.pl

#для соединения с invGuard CS-SW(-01)

123) su - syn

124) ssh-keygen -t rsa

125) # remote.server.host – ip адрес очистителя

126) ssh-copy-id -i ~/.ssh/id_rsa.pub root@remote.server.host

На этом инсталляция invGuard AS-SW завершена.

3.4.6 Запуск invGuard AS-SW

После процесса перезагрузки, при подключенном ключе SenseLock, Система запускается автоматически. Старт Системы начинается с запуска демона synmond. Запущенный демон самостоятельно запускает необходимые сервисы Системы.

Для дальнейшей настройки Системы используется веб-интерфейс.

Остановка Системы может быть завершена с помощью команды (пользователь root):

1) $ service synmond stop

3.4.7 Порядок действий по настройке программного комплекса для готовности к работе

Порядок подготовки к работе:

Выполните сбор данных для настройки invGuard AS-SW.

Для маршрутизатора, вносимого в систему, требуются следующие данные (веб форма Администрирование / Мониторинг / Инфраструктура / Роутеры):

- Подключение по BGP
  1) IP-адрес;
  2) BGP ID;
  3) Номер автономной системы в сети Заказчика;
  4) Номер автономной системы для нашей системы (обычно 64555, но остается на усмотрение заказчика);

5) Ключ шифрования MD5 (если применимо, если нет – пустой).

- Подключение по SNMP
  1) IP-адрес;
  2) Версия SNMP;
  3) Community.
- Подключение по NetFlow
  1) IP-адрес;
  2) Порт;
  3) Уровень сэмплирования (sampling rate).

Версия NetFlow (в которой отдает сетевое оборудование Заказчика – может быть NetFlow v5, v9, IPFIX (v10)).

Для конфигурирования сети в системе, требуются следующие данные (веб-форма Администрирование / Мониторинг / Сеть):

- Название сети;
- Номер автономной системы (backbone ASN);
- Адресное пространство сети (заданное префиксами, например, 91.203.194.0/24, их может быть много).

1) создайте учётные записи.

(форма Администрирование / Доступ / Учётные записи)

2) заполните параметры сети.

(форма Администрирование / Мониторинг / Сеть)

3) добавьте роутер в систему.

(форма Администрирование / Мониторинг / Инфраструктура / Роутеры)

4) выполните перезапуск системы.

5) создайте правила автоклассификации интерфейсов роутера.

(форма Администрирование / Мониторинг / Автоконфигурация / Правила)

6) классифицируйте интерфейсы роутера.

(форма Администрирование / Мониторинг / Инфраструктура / Интерфейсы)

3.4.8 Порядок контрольных проверок для определения готовности инсталлированного программного комплекса

Перечень проверок системы после обновления (установки новых версий, патчей):

Через SSH-подключение:

- Состояние запуска необходимых «демонов» для invGuard AS:
  1) synmond;
  2) synnetflowd;
  3) synsnmpd;
  4) synbgpd;
  5) synsecd;
  6) synntfd;
  7) synpeermgrd.
- Проверка наличия свободного места на дисках:
  1) df -h

Доступность веб-интерфейса:

- Проверка суммарного отчета «Система / Статус / Суммарный отчет»:
  1) Наличие данных за последние 5 минут
- Проверка отчета «Система / Статус / Устройства Syn / Статус устройств»:
  2) Количество Flow-записей в секунду – более 0
  3) Состояние системы «Анализатор»: запущен
  4) Netflow – есть подключение (минимально 1/1)
  5) SNMP – есть подключение (минимально 1/1)
  6) BGP – есть подключение (минимально 1/1)
  7) Память – более 0% и менее 100%
  8) Процессор – более 0% и менее 100%
  9) БД – более 0% и менее 100%
- Состояние системы «Очиститель»: запущен
  1) Память – более 0% и менее 100%

2) Процессор – более 0% и менее 100%
3) БД – более 0% и менее 100%

- Проверка отчёта «Система / Статус / Сетевые устройства / Роутеры»:

  По каждому из роутеров (подключенных сетевых устройств в системе):

  1) NetFlow
     а) Трафик bps – наличие значения более 0
     б) Трафик pps – наличие значение более 0
     в) ACL bps – наличие значение более 0
     г) Потоков в секунду – наличие значение более 0
     д) Последний поток – значение «менее 5 минут назад»
  2) SNMP
     а) ЦП – более 0%
     б) Память – более 0%
  3) BGP
     а) Соединение установлено – значение «да» (в случае подключения к роутеру по BGP)
     б) Активных маршрутов – более 0, если соединение установлено

3.5 Настройка invGuard AS-SW

3.5.1 Работа с электронными ключами SenseLock

Работа с комплексом invGuard AS-SW невозможна без использования электронного ключа SenseLock, служащего для защиты комплекса от несанкционированного использования и копирования.

Утилита licenseTool.x, поставляемая совместно с Системой, предназначена для работы с электронными ключами SenseLock. Данная программа предназначена для удаленного обновления ключа, а так же для вывода информации о действующей лицензии.

Использование:

licenseTool.x -p userPin --c2v <filename>

licenseTool.x -p userPin --v2c <filename>

licenseTool.x -p userPin –info

где userPin – пин-код пользователя.

Параметры команд:

-i, --info вывод информации о действующей лицензии.

-C, --c2v генерировать c2v-файл из SenseLock-ключа (от пользователя (customer) к производителю (vendor) в c2v-файле (customer to vendor)).

-V, --v2c загрузить v2c-файл в SenseLock-ключ (v2c – vendor to customer).

Опции:

-v, --verbose
-q, --quite
-h, --help

Пример генерации запроса с секретными данными для лицензии и обновление лицензии:

licenseTool.x -C license.c2v – экспорт лицензии с ключа, для формирования обновлённой лицензии.

licenseTool.x -V license.v2c – обновление лицензии на ключе из v2c-файла.

Сведения о возникших в ходе работы предупреждениях или ошибках фиксируются в системном журнале.

3.5.2 Конфигурационные файлы

Начальная настройка Системы производится на основе данных, заданных пользователем во время установки Системы, и с использованием значений по умолчанию для прочих параметров Системы. После установки администратор может, при необходимости, изменить конфигурационные файлы Системы.

Замечание: изменение конфигурационных файлов может привести к нестабильности работы Системы и даже к ее отключению, поэтому рекомендуется

выполнять данные модификации только после согласования со службой поддержки Системы.

Замечание: параметры, не перечисленные в таблицах этого раздела, изменяться не должны.

1) /etc/syn/syn.conf

Файл /etc/syn/syn.conf содержит настройки доступа к базе данных, а также настройки, необходимые для работы веб-интерфейса и модуля, отвечающего за сбор и анализ NetFlow.

Таблица 2 – Параметры syn.conf (общие)

Название параметра	**Значение по умолчанию**	**Описание**
DB_USER_NAME	syn	Имя пользователя БД.
DB_USER_PASSWORD		Пароль пользователя БД.
DB_HOST_IP	127.0.0.1	IP-адрес БД.
DB_PORT	3306	Порт доступа к БД.
DB_NAME	syn_db	Имя схемы в БД.
SYN_USER_NAME	syn	Имя пользователя, от которого работают основные демоны Системы, не меняется.

Таблица 3 – Параметры syn.conf (веб-интерфейс)

Название параметра	**Значение по умолчанию**	**Описание**
OAM_DB_USER_NAME	www	Имя пользователя, от имени которого работает веб-интерфейс, не меняется.
OAM_DB_PASSWORD	-	Пароль пользователя OAM_DB_USER_NAME для доступа к базе данных, запрашивается инсталлятором.

Название параметра	Значение по умолчанию	Описание
OAM_DB_TIMEOUT	300	Таймаут доступа веб-интерфейса в базе.
RADIUS_HOST	-	IP-адрес RADIUS-сервера.
RADIUS_AUTH_PORT	1812	Порт для аутентификации на RADIUS-сервере.
RADIUS_ACCT_PORT	1813	Порт для обмена информации об учетных записях на RADIUS-сервере.
RADIUS_SECRET	-	Пароль для доступа к RADIUS-серверу, запрашивается инсталлятором.
RADIUS_TIMEOUT	3	Таймаут подключения к RADUIS-сервера.
RADIUS_MAX_TRIES	3	Максимальное количество попыток подключения к RADUIS-серверу.

Таблица 4 – Параметры syn.conf (synnetflowd)

Название параметра	Значение по умолчанию	Описание
SYNNETFLOWD_ANALYSER_THREADS	Количество ядер CPU в системе	Число потоков Анализатора NetFlow.
NETFLOW_INTERFACE_NAME	eth0	Имя сетевого интерфейса для сбора NetFlow записей.

2) /etc/syn/synbgpd.conf

Файл /etc/syn/ synbgpd.conf содержит настройки модуля работы с BGP-данными.

Таблица 5 – Параметры synbgpd.conf (synbgpd)

Название параметра	Значение по умолчанию	Описание
BGP_INTERNAL_BUFFER_SIZE	700	Размер буфера BGP-сообщений, МБ.

3) /etc/syn/synmond.conf

Файл /etc/syn/synmond.conf содержит настройки модуля мониторинга Системы.

Таблица 6 – Параметры synmond.conf (synmond)

Название параметра	Значение по умолчанию	Описание
DBCLEANER_AUTO_MITIGATIONS_COUNT	500000	Максимальное количество автоматических заданий очистки в базе данных. При превышении порога наиболее старые записи удаляются.
DBCLEANER_ANOMALIES_MONTHS	36	Максимальный срок хранения аномалий в базе данных, в месяцах. Устаревшие аномалии удаляются.
DBCLEANER_ANOMALIES_COUNT	10000000	Максимальное количество сохраняемых аномалий в базе данных. При превышении порога наиболее старые аномалии удаляются.
DBCLEANER_BGP_DAYS	90	Максимальный срок хранения BGP-маршрутов в базе данных, в днях. Устаревшие маршруты удаляются.
DBCLEANER_BGPEVENTS_COUNT	155000000	Максимальное количество сохраняемых BGP-маршрутов в базе данных. При превышении порога наиболее старые аномалии удаляются.

Название параметра	Значение по умолчанию	Описание
DBCLEANER_BGPCOMM_COUNT	30000000	Максимальное количество сохраняемых BGP-коммьюнити в базе данных. При превышении порога наиболее старые записи удаляются.
DBCLEANER_HWSTATUS_MONTHS	12	Максимальный срок хранения информации о маршрутизаторах, полученной по SNMP, в месяцах. Устаревшие данные удаляются.
DBCLEANER_IFCSTATUS_MONTHS	12	Максимальный срок хранения информации об интерфейсах, полученной по протоколу SNMP, в месяцах. Устаревшие данные удаляются.
DBCLEANER_TASTATUS_DAYS	90	Максимальный срок хранения данных о параметрах работы Анализатора, в днях. Устаревшие данные удаляются.
DBCLEANER_OAMHISTORY_MONTHS	12	Максимальный срок хранения данных об истории просмотренных страниц веб-интерфейса, в месяцах. Устаревшие данные удаляются.
DBCLEANER_SELFMONITOR_DAYS	90	Максимальный срок хранения данных об использовании ресурсов Анализатора, в днях. Устаревшие данные удаляются.
DBCLEANER_CONFIGHISTORY_DAYS	30	Максимальный срок хранения данных об истории конфигурации, в днях. Устаревшие данные удаляются.

Название параметра	Значение по умолчанию	Описание
DBCLEANER_SYSTEMNFMONITOR_DAYS	90	Максимальный срок хранения статистических данных о параметрах обработки NetFlow, в днях. Устаревшие данные удаляются.
DBCLEANER_INTERFACES_HISTORY_DAYS	365	Максимальный срок хранения данных об истории конфигурации интерфейсов, в днях. Устаревшие данные удаляются.
GARBAGE_COLLECTION_START_TIME	14:30	Время (UTC) запуска «сборщика мусора» – процедуры по очистке базы данных от удаленных пользователем записей. Сборщик мусора запускается раз в сутки в указанное время.
DISKCLEANER_START_TIME	3:00	Время (UTC) запуска очистки диска, раз в сутки в указанные часы.
DATABASE_INTEGRITY_CHECK_START_TIME	14:45	Время (UTC) запуска ежедневной процедуры по проверке целостности базы данных.
DB_CHECK_TABLES_START_TIME	4:00	Время (UTC) ежедневного запуска скрипта по проверке целостности InnoDB-таблиц базы данных.

4) /etc/syn/synsnmpd.conf

Файл /etc/syn/synsnmpd.conf содержит настройки модуля работы с SNMP-данными.

Таблица 7 – параметры synsnmpd.conf (synsnmpd)

Название параметра	Значение по умолчанию	Описание
SNMP_RETRIES	1	Количество попыток повторить запрос при ошибке одного SNMP-запроса.
SNMP_TIMEOUT	8	Таймаут на ожидание ответа от SNMP-агента в секундах.
SNMP_PORT	161	Порт на маршрутизаторе, прослушиваемый SNMP-агентом.

5) /etc/syn/synntfd.conf

Файл /etc/syn/synntfd.conf содержит настройки модуля нотификации.

Таблица 8 – параметры synntfd.conf (synntfd)

Название параметра	Значение по умолчанию	Описание
MAIL_PERIOD_SECONDS	300	Временной интервал в секундах, задающий частоту проверок БД на новые аномалии и отправки почты по ним.
DELAYED_CHECK_INTERVAL	600	Временной интервал в секундах, задающий частоту проверок на аномалии с отправкой почты.

3.6 Обновление invGuard AS-SW

3.6.1 Автоматическое обновление

Для обновления Анализатора в автоматическом режиме необходимо использовать скрипт updater.sh Данный скрипт должен запускаться как бинарный файл с параметрами. Параметры должны быть следующими:

1) updater.sh version analyzer – показывает текущую версию установленного ПК invGuard AS-SW;

2) updater.sh install analyzer – устанавливает текущую базовую версию invGuard AS-SW;
3) updater.sh list analyzer – распечатывает список доступных версий invGuard AS-SW в репозитории.

Скрипт updater.sh необходимо запускать из консоли invGuard AS-SW

После запуска updater.sh считывает свой конфигурационный файл настроек, в котором должны быть прописаны пути установки системы, адрес сервера репозитория, логин и пароль доступа к репозиторию, настройки доступа по сетевому протоколу SSH.

Конфигурацию updater.sh необходимо хранить в файле update_config.xml. Данный файл необходимо расположить в одном каталоге с файлом updater.sh. Файл updater.sh необходимо хранить в каталоге /home пользователя Системы. Дополнительные бинарные файлы и библиотеки должны быть расположены в каталоге /lib/update/*.

Пример файла конфигурации update_config.xml:

```
<?xml version="1.0" encoding="UTF-8"?>
<config>
  <cleaner major_version="000" minor_version="000" build="0001"
host="192.168.20.19" port="22" type="x86"/>
  <analyzer major_version="001" minor_version="001" build="0007"
db_host="127.0.0.1" db_port="3306" db_name="install_syn"/>
  <connection host="192.168.20.19" port="22"/>
  <path>
        <remote main_folder="/opt/updater_check/"/>
        <local backup_folder="/opt/updater/backup/"
tmp_folder="/opt/updater/temp/"/>
        <cleaner backup_folder="/opt/updater/backup2/"
tmp_folder="/opt/updater/temp2/"/>
  </path>
</config>
```

Узел <remote main_folder = “”> описывает путь к файлам репозитория на удаленном сервере.

Узел <local backup_folder=””> описывает путь, куда сохраняется резервная копия текущей версии.

Узел <local tmp_folder =””> описывает путь, куда временно скачиваются файлы обновления из репозитория, для дальнейшей локальной работы с ними.

Узлы <cleaner> и <analyzer> описывают текущие версии, установленных компонентов Системы invGuard.

В командной строке требуется выбрать нужную версию для установки. При запуске скрипта с параметром install устанавливается только базовая версия, находящаяся в репозитории. Если базовая версия ниже, чем предлагается для обновления, то после установки базовой, необходимо выполнять пошаговое обновление до максимальной (см. п. **Ошибка! Источник ссылки не найден.**).

Во время работы скрипта updater.sh и при возникновении ошибочных ситуаций на консольный вывод выводятся информационные сообщения с причинами ошибки, которые должны анализироваться и устраняться администратором.

3.6.2 Обновление в ручном режиме

Для обновления Анализатора в ручном режиме необходимо использовать скрипт updater.sh Данный скрипт должен запускаться как бинарный файл с параметрами. Параметры должны быть следующими:

1) updater.sh version analyzer – показывает текущую версию установленного ПК invGuard AS-SW;
2) updater.sh update analyzer – обновляет версию ПК invGuard AS-SW;
3) updater.sh downgrade analyzer – понижает версию ПК invGuard AS-SW;
4) updater.sh list analyzer – распечатывает список доступных версий invGuard AS-SW в репозитории.

Скрипт updater.sh запускается из консоли invGuard AS-SW.

После запуска updater.sh должен считывает свой конфигурационный файл настроек, в котором должны быть прописаны пути установки системы, адрес

сервера репозитория, логин и пароль доступа к репозиторию, настройки доступа по сетевому протоколу SSH.

Конфигурацию updater.sh необходимо хранить в файле update_config.xml. Данный файл необходимо расположить в одном каталоге с файлом updater.sh. Файл updater.sh необходимо хранить в каталоге /home пользователя Системы. Дополнительные бинарные файлы и библиотеки должны быть расположены в каталоге /lib/update/*. Файл должен соответствовать приведённому в п. 3.6.1

После запуска команды updater.sh с параметрами необходимо подключаться к серверу репозитория по SFTP-протоколу и скачивать *_step.xml файлы. В зависимости от текущей версии Системы необходимо выбирать следующую версию для обновления и далее интерпретатор на базе узлов и команд, записанных в файле *_step.xml, произведёт обновление системы до следующей версии. Версию Анализатора возможно повысить или понизить только на 1 шаг от предыдущей.

Во время работы скрипта updater.sh и при возникновении ошибочных ситуаций на консольный вывод выводятся информационные сообщения с причинами ошибки, которые должны анализироваться и устраняться администратором.

3.7 Мониторинг и настройка сети

3.7.1 Работа с роутерами. Введение

В Системе термин роутер используется для обозначения магистрального маршрутизатора контролируемой сети. Анализатор получает и анализирует NetFlow-дейтаграммы с роутеров, а так же может устанавливать с ними BGP- и SNMP-соединения.

3.7.2 Экран «Роутеры»

Экран «Роутеры» (Администрирование → Мониторинг → Роутеры) перечисляет все роутеры, с которыми работает Анализатор, а также позволяет добавить новый роутер или удалить существующий.

Экран «Роутеры» отображает следующую информацию, см. таблицу 9.

Таблица 9 – Экран «Роутеры»

Колонка	Описание
Наименование / Описание	Наименование и описание роутера
SNMP IP	IP-адрес, который использует Анализатор для запроса SNMP информации.

Колонка	Описание
BGP IP	IP-адрес, который использует Анализатор для установления BGP-соединения.
NetFlow экспорт IP	IP-адрес с которого Анализатор получает NetFlow-дейтаграммы роутера.
NetFlow сэмплирование	Частота выборки (частота дискретизации) роутера, если она установлена вручную. В случае автоматического определения отображается пустое поле.

3.7.3 Добавление и редактирование роутера

Для добавления или редактирования роутера выполните одно из следующих действий:

1) Кликните по названию роутера в списке.
2) Нажмите «Добавить роутер».
3) Заполните параметры, расположенные на следующих вкладках экрана для настройки роутера:
   - вкладка «Описание»;
   - вкладка «SNMP»;
   - вкладка «BGP»;
   - вкладка «Flow».

3.7.4 Настройка описания для роутера

Перейдите на вкладку «Описание».

1) Введите название роутера в поле «Название».
2) Введите описание роутера в поле «Описание» или оставьте поле пустым для получения описания из SNMP MIB.

3.7.5 Настройка SNMP

Анализатор использует SNMP для получения названий и описаний интерфейсов роутера, а так же статистики по ним. Хотя SNMP-настройки являются необязательными, рекомендуется их настроить.

Для настройки SNMP-параметров выполните следующие действия:

1) Перейдите на вкладку «SNMP».
2) Выберите версию SNMP из списка.
3) В зависимости от выбранной версии заполните предложенные Системой поля.

3.7.6 Настройка BGP

Настройка параметров BGP является необязательным шагом, в тоже время, необходимо выполнить эту настройку, если требуется анализ маршрутов с целью получения статистических данных по BGP-атрибутам в разрезе инфраструктурных и наблюдаемых объектов.

Для настройки BGP-параметров выполните следующие действия:

1) Перейдите на вкладку «BGP».
2) Установите флажок «Поддержка BGP».
3) Для использования «чужой» таблицы маршрутизации (другого роутера) укажите роутер в списке «Роутер BGP по умолчанию».

Замечание: используйте этот вариант, если нет возможности настроить BGP-соединение между роутером и Анализатором. Также используйте этот вариант действий, если настраиваете Анализатор для мониторинга нескольких роутеров, имеющих одинаковые или похожие таблицы маршрутизации с целью снижения загрузки ЦП Анализатора.

Если необходимо установить BGP-соединение между роутером и Анализатором, выберите пункт «нет» в списке «Роутер BGP по умолчанию». Заполните предложенные Системой поля.

Установите флажок «Разрешить установку пиринговых отношений между роутером и Анализатором». Флажок позволяет быстро включать/отключать получение BGP-данных с роутера, не теряя его настроек в OAM-интерфейсе.

3.7.7 Настройка Flow

Анализатор производит анализ трафика, основываясь на NetFlow-записях с роутера.

Замечание: не заполняйте эти поля, если необходимо работать только с BGP-информацией (BGP-отчетами) для роутера.

Для настройки Flow параметров выполните следующие действия:

1) Перейдите на вкладку «Flow».
2) Заполните предложенные Системой поля.
3) Поле «Сэмплинг рейт» оставьте пустым для автоматического определения частоты выборки роутера (по заголовку NetFlow-дейтаграмм) или заполните значение вручную.
4) Нажмите «Выбрать интерфейсы для мониторинга» для выбора интерфейсов, которые представляют интерес для анализа трафика.

Замечание: список интерфейсов доступен после установления SNMP-соединения с роутером. Список интерфейсов также заполняется интерфейсами, указанными в NetFlow-записях по мере их поступления.

3.8 Группы роутеров

3.8.1 Введение

Разбивка роутеров по группам помогает эффективно управлять Системой в сети с множеством роутеров.

3.8.2 Создание и редактирование группы роутеров

Экран «Группы роутеров» (Администрирование → Мониторинг → Группы роутеров) перечисляет все группы, которые настроены, а также позволяет создать новую или удалить существующую.

Находясь на экране, выполните одно из следующих действий:

– кликните по названию группы в списке;

– нажмите «Добавить группу».

После этого выполните следующие действия:

1) Введите название группы роутеров в поле «Название».
2) Введите описание в поле «Описание».
3) Нажмите «Добавить/удалить роутеры» для редактирования списка роутеров, которые будут входить в группу.

Замечание: роутер может принадлежать только к одной группе. Для перемещения роутера между группами удалите его из первой группы и только после этого добавляйте во вторую.

4) Нажмите «Сохранить».

3.8.3 Удаление группы роутеров

Для удаления группы роутеров выполните следующие действия:

1) Перейдите на экран «Группы роутеров» (Администрирование → Мониторинг → Группы роутеров).
2) Установите галочки для тех групп, которые необходимо удалить.
3) Нажмите «Удалить выбранные».

3.8.4 Автоклассификация

Анализатор позволяет проводить автоматическую классификацию интерфейсов, используя набор правил, заданных пользователем, а также эвристический алгоритм для определения типа, основываясь на характеристиках потока трафика через интерфейс и BGP-атрибутах трафика в том числе. Автоматическая классификация не вызывает изменений в конфигурации Системы в автоматическом режиме. Конечное решение об изменении конфигурации принимает пользователь.

В этом смысле автоматическая классификация является помощником, но не заменяет пользователя.

Область работы механизма автоклассификации не ограничивается только типами интерфейсов, а включает в себя также:

1) граничные значения трафика на интерфейсах;
2) добавление интерфейса во множество граничных интерфейсов наблюдаемого объекта.

Автоклассификация работает для всех контролируемых интерфейсов Системы, но отдельные правила могут быть ограничены подмножеством интерфейсов, подходящих под заданные условия.

3.8.5 Работа с правилами автоклассификации

Экран «Правила» (Администрирование → Мониторинг → Автоконфигурация → Правила) перечисляет все правила, которые были раннее созданы, а также позволяет добавить новые, удалить существующие и изменить порядок правил.

Порядок правил на экране играет важную роль в процессе автоклассификации. Правило с меньшим номером выполняется первым. Если интерфейс классифицирован правилом, он не рассматривается с применением последующих правил.

3.8.6 Создание и редактирование правила автоклассификации

Для создания или редактирования правила автоклассификации выполните следующие действия:

1) Перейдите на экран «Правила» (Администрирование → Мониторинг → Автоконфигурация → Правила).
2) Выполните одно из следующих действий:
   − кликните по названию существующего правила в списке;
   − нажмите «Добавить правило».
3) Введите название правила в поле «Название».
4) Введите описание в поле «Описание».
5) Укажите порядковый номер в поле «Порядковый номер правила».

Замечание: система использует номер правила для определения порядка выполнения правила. Правило с меньшим номером выполняется первым. Если применение правила позволило классифицировать интерфейс, последующие правила не рассматриваются.

6) Перейдите на вкладку «Сопоставление».

7) Выберите роутеры, для которых должно срабатывать правило в поле «Роутеры», или оставьте это поле пустым, если правило действует для всех роутеров.

8) Введите маску подсети в поле «Маска подсети интерфейса». Правило будет срабатывать только для интерфейсов, IP-адреса которых подходят под указанную маску. Для выбора всех интерфейсов оставьте поле пустым.

9) Введите описание интерфейсов регулярным выражением в поле «Описание регулярного выражения интерфейса». Рассматривается только описание интерфейса, название не рассматривается. Оставьте поле пустым для выбора всех интерфейсов.

10) Перейдите на вкладку «Действие». На этой вкладке указывается, что должно делать правило автоклассификации для интерфейса, с которым прошел этап сопоставления.

11) Для определения типа интерфейса:

- используйте режим «Автоматическое определение типа» для использования эвристического алгоритма принятия решения о типе интерфейса;
- используйте режим «Ручной выбор типа» для выбора типа вручную и выберите тип из раскрывающегося списка.

12) Для добавления интерфейса в граничные интерфейсы наблюдаемого объекта:

- поставьте галочку «Добавление интерфейса в границу наблюдаемого объекта»;
- выберите направление интерфейса на наблюдаемый объект из раскрывающегося списка «Расположение»;
- нажмите «Выбрать объекты» для выбора наблюдаемых объектов, граничные интерфейсы которых будут определены.

13) Для установки пороговых значений трафика на интерфейсе установите флажок «Верхний порог» и/или «Нижний порог» и введите значения в поля.

3.8.7 Ручной запуск автоклассификации

Автоклассификация всегда может быть запущена вручную, например, после изменений в конфигурации сети, добавления нового роутера, новых интерфейсов.

Для запуска процесса автоклассификации выполните следующие действия:

1) Перейдите на экран «Правила» (Администрирование → Мониторинг → Автоконфигурация → Правила);
2) Нажмите «Запустить процесс автоклассификации интерфейсов».

Если кнопка «Запустить процесс автоклассификации интерфейсов» отключена, то процесс автоклассификации выполняется в данный момент времени. Узнать время запуска процесса можно по сообщению справа от кнопки.

Замечание: длительность процесса зависит от использования правила с эвристическим анализом. Если подобное правило не задано, то процесс длится не более пяти минут. Если эвристическое правило задано, то длительность процесса задается на экране «Сеть» (Администрирование → Мониторинг → Сеть) на вкладке «Дополнительно».

3.8.8 Экран результатов автоклассификации

Экран с результатами автоклассификации «Результаты» (Администрирование → Мониторинг → Автоконфигурация → Результаты) предоставляет информацию о предлагаемых Системой изменениях для интерфейсов в соответствии с заданными правилами.

На экране перечисляются интерфейсы, текущая конфигурация которых отличается от рекомендуемой по результатам анализа.

Замечание: если в настроенной Системе на странице результатов перечислено большое количество интерфейсов, это может указывать на проблемы с BGP-соединением Анализатора и роутеров или на серьезные изменения в инфраструктуре сети.

Для перечисленных интерфейсов экран позволяет:

1) посмотреть текущую конфигурацию (черным цветом);

2) предлагаемую конфигурацию (синим цветом) с указанием сработавшего правила;

3) сделать изменения в конфигурации интерфейса, выбрав предлагаемые настройки или указав любые другие.

При сохранении экран проверяет, не были ли выполнены изменения для интерфейсов (тип, пороги, границы наблюдаемых объектов), которые сохраняет другой пользователь в то же самое время. Если конфигурация интерфейсов успела измениться, экран предложит посмотреть новую конфигурацию или продолжить и сохранить изменения.

После сохранения экран открывается заново, список интерфейсов включает интерфейсы, для которых предлагаемая Системой конфигурация отличается от текущей. Рекомендуется сохранять данные на экране чаще, список будет обновляться и содержать только те интерфейсы, которые все еще отличаются от предлагаемой конфигурации.

3.8.9 Ручная установка типа интерфейса

Тип интерфейса может быть установлен вручную в любой момент, с отключением автоматической классификации.

Замечание: отключение автоклассификации для интерфейса рекомендуется только в том случае, если для него автоклассификация часто срабатывает неправильно. В остальных случаях автоклассификация может помочь заметить проблемы, связанные с интерфейсом, при изменении его типа, что может указывать, например, на инфраструктурную проблему.

3.9 Настройка интерфейсов

3.9.1 Введение

Анализатор автоматически определяет интерфейсы на каждом роутере, используя информацию из NetFlow-дейтаграмм и осуществляя периодический опрос роутеров по протоколу SNMP.

3.9.2 Экран «Интерфейсы»

Экран «Интерфейсы» (Администрирование → Мониторинг → Инфраструктура → Интерфейсы) отображает информацию по известным Анализатору наблюдаемым интерфейсам в табличном виде.

Для удобства поиска интерфейса используйте поле «Поиск интерфейсов» вверху экрана. Поле позволяет фильтровать данные об интерфейсах по следующим параметрам:

1) название;
2) описание;
3) IP-адрес;
4) роутер;
5) SNMP-индекс интерфейса на роутере;
6) ASN соседа, к которому подключен интерфейс;
7) тип.

Замечание: в таблице могут быть интерфейсы с названием «New interface #nnn». Это интерфейсы, найденные по NetFlow-дейтаграммам, но еще не обнаруженные через SNMP. Подобная ситуация возможна, если не настроено подключение Анализатора к роутеру по SNMP-протоколу. В таком случае название для интерфейса можно настроить вручную. Число nnn является SNMP-индексом интерфейса на роутере.

3.9.3 Детальная статистика по интерфейсам

Детальной статистикой для интерфейса называется статистика по:

1) приложениям;
2) BGP-атрибутам;
3) объектам;
4) размерам пакетов;
5) протоколам;
6) QoS;
7) потреблению трафика.

По умолчанию Анализатор собирает детальную статистику только для внешних интерфейсов и не собирает для всех остальных.

Для включения подробной статистики интерфейса используйте экран «Редактирование интерфейса».

3.9.4 Пороговые значения по интерфейсам

Анализатор позволяет отслеживать поток трафика на интерфейсах и выход его за заданные пороговые значения.

Настраиваются как верхнее, так и нижнее пороговое значение трафика. В случае выхода трафика за пределы обозначенных пороговых значений Анализатор регистрирует аномалию. Пороговые значения задаются в процентах от пропускной способности интерфейса. Для интерфейсов, у которых не установлены пороговые значения, Анализатор использует значения по умолчанию, настраиваемые на экране «Пороги по трафику» (Администрирование → Детекция → Пороги по трафику).

Замечание: Анализатор не регистрирует аномалии по трафику для интерфейсов, скорость которых ниже 55 Мбит/с.

3.9.5 Редактирование интерфейса

Для редактирования интерфейса выполните следующие действия:

1) Перейдите на экран «Интерфейсы» (Администрирование → Мониторинг → Инфраструктура → Интерфейсы).

2) Кликните на название или индекс интерфейса в таблице.

3) В появившемся окне редактирования интерфейса установите требуемые параметры.

4) Нажмите «Сохранить.

Для уточнения порядка действий при решении типовых задач используйте информацию из таблицы 10.

Таблица 10 – Действия для решения типовых задач в диалоге редактирования интерфейса

Задача	**Последовательность действий**
Выключение наблюдения за интерфейсом. Статистика интерфейса не будет собираться.	В поле «Мониторинг» выберите значение «Выкл».
Установка названия / описания / скорости интерфейса из SNMP MIB.	Очистите соответствующее поле «Название» / «Описание» / «Скорость». В течение 5 минут данные будут обновлены из SNMP MIB.
Выключение автоматической классификации интерфейса. Используйте, если Система предлагает неправильный тип интерфейса.	1) Выберите «Выключено» в поле «Автоматическая классификация». 2) Установите тип интерфейса в поле «Тип».
Установка соседского ASN, к которому непосредственно подключен интерфейс. Весь трафик интерфейса будет отнесен к трафику, идущему к и от соседа.	1) Выберите «Выключено» в поле «Автоматическая классификация». 2) Установите внешний тип интерфейса в поле «Тип».
Включение / отключение сбора детальной статистики по трафику интерфейса.	Выберите соответствующий вариант: «Включена» или «Выключена» в поле «Детальная статистика». **Замечание:** вариант «По умолчанию» включает детальную статистику для внешнего интерфейса.

3.10 Резервное копирование и восстановление

3.10.1 Требования к Системе, необходимые для функционирования резервного копирования данных

Для обеспечения работоспособности функциональности резервного копирования данных, необходимо выполнение следующих условий:

1) при инсталляции Системы должен быть корректным образом настроен LVM;
2) на диске должно быть достаточно места для хранения данных.

3.10.1.1 Установка LVM

Для работы Системы создания резервных копий Анализатора необходимо, чтобы в Системе был установлен и настроен пакет LVM (версии 2).

Основные требования:

1) должна быть создана группа томов (volume group). В ней должны быть созданы разделы для хранения компонентов Системы и логический том с именем dbbackup для создания резервной копии Системы, который должен быть подмонтирован к каталогу /var/dbbackup.
2) В группе томов должно оставаться свободное место. В нем создается временный раздел (не менее 1 Гб) при создании резервной копии базы.

Возможны два варианта установки LVM:

1) В процессе установки чистой Системы на машину (см. 3.3.1).
2) После установки, используя средства администрирования LVM.

Предполагается, что большинство команд выполняется из-под пользователя root.

3.10.1.2 Установка LVM в работающей Системе

1) Если операционная система уже установлена, необходимо убедиться, что LVM также установлен. В противном случае – установить его.

Если следующая команда выполняется, значит LVM установлен.

```
$> lvdisplay --version
```

Если пакет LVM не установлен, надо его установить.

```
$> yum install lvm2
```

2) Для работы с LVM необходим раздел на диске, который будет использоваться для хранения группы томов. Можно создать такой раздел при инсталляции системы или выделить на дополнительном физическом диске.

Создание раздела можно выполнить при помощи программы cfdisk (На примере dbbackup). Для созданного раздела надо установить тип Linux LVM (код 8E).

Команда

```
$> fdisk –l
```

должна показать этот раздел в списке. В нашем примере его имя: /dev/hda4.

```
  Device Boot  Start  End  Blocks  Id System
/dev/hda1      1  243  1951866 83 Linux
/dev/hda2     244  608  2931862+ 83 Linux
/dev/hda3     609  624  128520 82 Linux swap / Solaris
/dev/hda4     625  1044  3373650 8e Linux LVM
```

3) Выполните очистку начала раздела (первый сектор).

```
$> dd if=/dev/zeros of=/dev/hda4 bs=512 count=1
```

Замечание: осторожно! Убедитесь, что указан именно диск с LVM!

4) Перезагрузите компьютер.

```
$> shutdown -r now
```

5) Создайте физический том.

```
$> pvcreate /dev/hda4
```

6) Создайте группу.

```
$> vgcreate <Название lvm группы> /dev/hda4
```

7) Создайте логический том.

```
$> lvcreate --size 10G -n dbdata <Название lvm группы>
```

8) Создайте файловую систему в томе.

```
$> mkfs.ext3 /dev/<Название lvm группы>/dbbackup
```

9) Создайте точку монтирования.

```
$> mkdir /var/dbbackup
```

10) Настройте автоматическое монтирование раздела при загрузке компьютера. Для этого добавьте следующие строки в файл /etc/fstab.

```
/dev/<Название lvm группы>/dbdata /var/dbbackup auto noatime 0 0
```

Подмонтируйте раздел при помощи следующей команды:

```
$> mount /dev/<Название lvm группы>/dbbackup
```

3.10.2 Резервное копирование данных

Для резервного копирования данных Системы необходимо выполнить следующие действия:

1) Перейдите к экрану «Архивирование» (Администрирование → Общие настройки → Архивирование).

2) Нажмите кнопку «Запустить сейчас». Должно появиться диалоговое окно «Архивирование системы будет запущено в течение 5 минут».

3) Сообщения о ходе выполнения процедуры выводятся в элемент управления «Журнал архивирования».

4) Результирующий архив с расширением gz должен появиться в директории /var/dbbackup/.

3.10.3 Настройка периодического запуска процедуры резервного копирования данных

Анализатор имеет возможность автоматического запуска процедуры резервного копирования данных. Для настройки параметров автоматического запуска необходимо выполнить следующие действия:

1) Перейдите к экрану «Архивирование» (Администрирование → Общие настройки → Архивирование).

2) Установите кнопку-флажок «Включить архивирование» в положение «включено».

3) При помощи выпадающего списка «Периодичность» укажите, насколько часто должно проводиться резервное копирование данных. Разрешается установить следующие значения: «ежедневно, каждый понедельник, каждый вторник» и т.д.

4) При помощи элемента управления «Время» укажите время запуска процедуры.

5) Нажмите кнопку «Сохранить».

Для отключения автоматического запуска процедуры резервного копирования данных достаточно выставить кнопку-флажок «Включить архивирование» в положение «выключено».

3.10.4 Восстановление Системы

Для восстановления Системы из архива, полученного при помощи процедуры резервного копирования данных, необходимо выполнить следующие действия:

1) Зарегистрируйтесь в консольном интерфейсе Системы с учетной записью root.

2) Остановите Систему при помощи команды /usr/bin/syn/synmond stopall.

3) Убедитесь при помощи команды ps в отсутствии следующих процессов: mysqld, mysqld_safe.

4) Переместите содержимое директории /var/lib/mysql в /var/lib/mysql/reserve.

5) Распакуйте содержимое выбранного ранее архива в директорию /var/lib/mysql.

6) Запустите MySQL в безопасном режиме при помощи команды /usr/bin/mysqld_safe.

7) Убедитесь в корректной работе демона mysql.

8) Остановите mysqld_safe.

9) Удалите содержимое директории /var/lib/mysql/reserve.

10) В случае если после запуска процедур резервного копирования выполнялось обновление Системы, может возникнуть необходимость выполнить восстановление не только содержимого базы данных, но и других файлов Системы:

исполняемых файлов /usr/bin/syn, конфигурационных файлов /etc/syn, конфигурационных файлов third-party демонов, файлов веб-интерфейса /home/www.

11) Запустите Систему при помощи команды /usr/bin/syn/synmond start.

3.11 Настройка границ сети

3.11.1 Введение

Для определения Анализатором принадлежности трафика к внутреннему пространству сети, необходимо правильно настроить границы сети. Это необходимо для различения объектов внутренней сети и внешних сетей. Внутреннее пространство сети должно быть определено для анализа потоков трафика, выявления DoS-атак и других аномалий.

3.11.2 Backbnone ASN

Автономная система (Autonomous system AS) – это система IP-сетей и маршрутизаторов, управляемых одним или несколькими операторами, имеющими единую политику маршрутизации с Интернетом.

ASN (Autonomous System Number) – номер автономной системы.

Backbone ASN – номер автономной системы, которая принадлежит наблюдаемой сети.

3.11.3 Настройка контролируемой сети

Перейдите на экран «Сеть» (Администрирование → Мониторинг → Сеть) и заполните параметры, расположенные на вкладках.

1) Вкладка «Описание».

2) Вкладка «Адресное пространство».

3) Вкладка «Дополнительно».

3.11.4 Настройка описания сети

1) Введите название сети в поле «Название».

2) Введите номера автономных систем (ASN), которые принадлежат наблюдаемой сети в поле «Backbone ASN-ы».

3.11.5 Настройка адресного пространства сети

1) В поле «Префиксы локального адресного пространства» введите диапазоны адресов, которые принадлежат наблюдаемой сети.
2) В поле «Дыры в локальном адресном пространстве» введите список диапазонов адресов, которые нужно исключить из локального адресного пространства наблюдаемой сети.

3.11.6 Настройка дополнительных параметров

Выберите длительность эвристического анализа для автоклассификации интерфейсов на вкладке «Дополнительно».

Параметр «длительность эвристического анализа» определяет интервал времени, за который будут взяты данные для классификации интерфейса.

3.12 Настройка взаимодействия между маршрутизатором и Анализатором

3.12.1 Требования к настройке протокола SNMP на маршрутизаторе

Анализатор ведет опрос SNMP OID, перечисленных в таблице 11.

Таблица 11 – SNMP OID, опрашиваемые Анализатором

SNMP OID	**SNMP Object**
SNMPv2-MIB	
iso.org.dod.internet.mgmt.mib-2.system	
1.3.6.1.2.1.1.1.0	.sysDescr
1.3.6.1.2.1.1.3.0	.sysUpTime
1.3.6.1.2.1.1.2.0	.sysObjectID
ENTITY-MIB	

SNMP OID	SNMP Object
.iso.org.dod.internet.mgmt.mib-2.entityMIB.entityMIBObjects.entityPhysical.entPhysicalTable.entPhysicalEntry	
1.3.6.1.2.1.47.1.1.1.1.11	.entPhysicalSerialNum
1.3.6.1.2.1.47.1.1.1.1.5	.entPhysicalClass
IF-MIB	
.iso.org.dod.internet.mgmt.mib-2.interfaces	
1.3.6.1.2.1.2.1.0	.ifNumber
.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry	
1.3.6.1.2.1.2.2.1.1	.ifIndex
1.3.6.1.2.1.2.2.1.2	.ifDescr
1.3.6.1.2.1.2.2.1.8	.ifOper.Status
1.3.6.1.2.1.2.2.1.4	.ifEntry.ifMtu
.iso.org.dod.internet.mgmt.mib-2.ifMIB.ifMIBObjects.ifXTable.ifXEntry	
1.3.6.1.2.1.31.1.1.1.15	.ifHiSpeed
1.3.6.1.2.1.31.1.1.1.1	.ifName
1.3.6.1.2.1.31.1.1.1.18	.ifAlias
1.3.6.1.2.1.31.1.1.1.6	.ifHCInOctets
1.3.6.1.2.1.31.1.1.1.7	.ifHCInUcastPkts
1.3.6.1.2.1.31.1.1.1.8	.ifHCInMulticastPkts
1.3.6.1.2.1.31.1.1.1.9	.ifHCInBroadcastPkts
1.3.6.1.2.1.31.1.1.1.10	.ifHCOutOctets
1.3.6.1.2.1.31.1.1.1.11	.ifHCOutUcastPkts
1.3.6.1.2.1.31.1.1.1.12	.ifHCOutMulticastPkts
1.3.6.1.2.1.31.1.1.1.13	.ifHCInBroadcastPkts

SNMP OID	SNMP Object
.iso.org.dod.internet.mgmt.mib-2.ip.ipAddrTable.ipAddrEntry	
1.3.6.1.2.1.4.20.1.2	.ipAdEntIfIndex
1.3.6.1.2.1.4.20.1.3	.ipAdEntNetMask
JUNIPER-MIB	
.iso.org.dod.internet.private.enterprises.juniperMIB.jnxMibs.jnxBoxAnatomy.jnxOperatingTable.jnxOperatingEntry	
1.3.6.1.4.1.2636.3.1.13.1.8.9.1.0.0	.jnxOperatingCPU
1.3.6.1.4.1.2636.3.1.13.1.11.9.1.0.0	.jnxOperatingBuffer
.iso.org.dod.internet.private.enterprises.juniperMIB.jnxMibs.jnxIpv4.jnxIpv4Config.jnxIpv4AddrTable.jnxIpv4AddrEntry	
1.3.6.1.4.1.2636.3.12.1.1.1.2	.jnxIpv4AdEntAddr
1.3.6.1.4.1.2636.3.12.1.1.1.3	.jnxIpv4AdEntNetMask
.iso.org.dod.internet.private.enterprises.juniperMIB.jnxMibs.jnxBoxAnatomy	
1.3.6.1.4.1.2636.3.1.3.0	.jnxBoxSerialNo
CISCO-PROCESS-MIB	
.iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoProcessMIB.ciscoProcessMIBObjects.cpmCPU.cpmCPUTotalTable.cpmCPUTotalEntry	
1.3.6.1.4.1.9.9.109.1.1.1.1.8	.cpmCPUTotal5minRev
1.3.6.1.4.1.9.9.109.1.1.1.1.2	.cpmCPUTotalPhysicalIndex
CISCO-MEMORY-POOL-MIB	
.iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoMemoryPoolMIB.ciscoMemoryPoolObjects.ciscoMemoryPoolTable.ciscoMemoryPoolEntry	
1.3.6.1.4.1.9.9.48.1.1.1.5.1	.ciscoMemoryPoolUsed
1.3.6.1.4.1.9.9.48.1.1.1.6.1	.ciscoMemoryPoolFree
.iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoIPIfMIB.ciscoIPIfMIBObjects.ciiIPAddressConfiguration.ciiIPAddressTable.ciiIPAddressEntry	

SNMP OID	SNMP Object
1.3.6.1.4.1.9.9.309.1.1.2.1.3	.ciiIPAddressIfIndex
1.3.6.1.4.1.9.9.309.1.1.2.1.2	.ciiIPAddress
1.3.6.1.4.1.9.9.309.1.1.2.1.1	.ciiIPAddressType
1.3.6.1.4.1.9.9.309.1.1.2.1.4	.ciiIPAddressPrefixLength
OLD-CISCO-CPU MIB	
1.3.6.1.4.1.9.3.6.3.0	.iso.org.dod.internet.private.enterprises.cisco.temporary.chassis.chassisId
1.3.6.1.4.1.9.2.1.58.0	.iso.org.dod.internet.private.enterprises.cisco.local.lsystem.avgBusy5

3.12.2 Требования к настройке протокола NetFlow на маршрутизаторе

Анализатор поддерживает сбор и обработку NetFlow версии 5, 10 (IPFIX), а так же NetFlow версии 9. Особое внимание при настройке экспорта NetFlow на маршрутизаторе следует обратить на следующие параметры:

1) Частота выборки NetFlow (sampling rate) – указывает, из скольких пакетов берется один для генерирования NetFlow. Типичные значения этого параметра – от 500 до 2500. Высокие значения sampling rate снижают загрузку маршрутизатора и Анализатора, однако также снижают качество отслеживания «мелких» атак. Низкие значения этого параметра повышают точность детектирования атак, но и существенно возрастает нагрузка на маршрутизатор и Анализатор. Рекомендуется подбирать значение частоты выборки NetFlow эмпирически, исходя из масштаба контролируемой сети и допустимой загрузки маршрутизаторов и Анализатора.

2) Время хранения NetFlow-записи в кэше маршрутизатора – указывает промежуток времени, в течение которого NetFlow-запись может находиться в кэше маршрутизатора. По умолчанию Cisco маршрутизаторы хранят NetFlow-запись в кэше в течение получаса. Такое значение может привести к следующим последствиям: NetFlow-запись может быть признана устаревшей и отброшена

Анализатором, а время обнаружения атаки существенно увеличится. Рекомендуется ставить значение времени хранения не более одной минуты.

Для включения экспорта NetFlow на Cisco IOS маршрутизаторах необходимо выполнить следующие команды:

ip flow-export destination <IP адрес Анализатора> <Порт Анализатора для NetFlow>;
ip flow-export version 5;
ip flow-export source loopback 0;
ip flow-sampling-mode packet-interval <Коэффициент сэмплинга>;
ip flow-cache timeout active 1.

Далее необходимо включить NetFlow для каждого из наблюдаемых интерфейсов, на которых есть входящий трафик:

ip flow ingress;
ip route-cache flow sampled.

3.12.3 Требования к настройке протокола BGP на маршрутизаторе

Анализатор использует BGP для выполнения следующих задач:

1) получение таблиц маршрутизации для расчета статистических характеристик сетевого трафика;
2) подавление сетевых атак при помощи методов Blackhole и FlowSpec.

Анализатор трафика не является BGP-маршрутизатором в том смысле, что не выполняет маршрутизацию трафика в сети и не анонсирует полученные им маршруты.

Существуют различные схемы подключения Анализатора по BGP:

1) iBGP, где каждый наблюдаемый маршрутизатор является отражателем маршрутов (route reflector) для Анализатора. В этом случае Анализатор имеет наиболее точную информацию о таблице маршрутизации, поскольку маршрутизаторы анонсируют только те маршруты, которые ими непосредственно и используются. В том числе, Анализатор

получает и те маршруты, которые маршрутизатор получил по протоколу iBGP.

2) Обычный iBGP, без отражателя маршрутов. В этом случае каждый маршрутизатор посылает те eBGP-маршруты, которые являются лучшими с точки зрения процесса отбора BGP. В соответствии с правилами iBGP-маршруты, полученные по iBGP, не посылаются другим iBGP-маршрутизаторам. Особое внимание следует обратить на то обстоятельство, что если для одного и того же префикса маршрутизатор узнает два маршрута – один по eBGP, а другой – по iBGP, и маршрут, полученный по iBGP, будет признан предпочтительным, то ни один из двух маршрутов не будет анонсирован Анализатору. То есть, в данной схеме подключения Анализатор не получает полноценной информации о таблицах маршрутизации.

3) eBGP-соединение. В этой схеме контролируемая сеть будет представлена как некоторая внешняя для Анализатора сущность, в том смысле, что анонсируемые Анализатору по eBGP маршруты не будут содержать информации об особенностях маршрутизации внутри контролируемой сети. Использование такой схемы BGP-соединения крайне не рекомендуется.

С точки зрения подавления атак при помощи BGP описанные выше схемы подключения могут быть рассмотрены и под другим углом:

1) В случае iBGP-соединения между Анализатором и маршрутизаторами маршрут необходимо анонсировать всем маршрутизаторам – автоматического распространения маршрута по BGP не будет.

2) В случае eBGP-соединения между Анализатором и маршрутизатором маршрут будет анонсирован «за пределы» маршрутизатора по протоколу BGP.

Кроме схемы подключения особое внимание следует обратить и на настройки экспорта BGP-сообщений: такие BGP-атрибуты, как BGP-коммьюнити, не должны отбрасываться маршрутизатором при анонсировании маршрутов.

Для запуска заданий подавления атак типа BGP Flow Specification на маршрутизаторе необходимо настроить эту возможность.

Типичная настройка BGP на Cisco-маршрутизаторе выглядит так (настройки для BGP Flow Specification не указаны):

```
router bgp <AS number>
neighbor <IP адрес Анализатора> remote-as <AS number>
neighbor <IP адрес Анализатора> description TA
neighbor <IP адрес Анализатора> send-community
neighbor <IP адрес Анализатора> route-reflector-client
```

3.13 Настройка обмена сигнатурами атак между дружественными Анализаторами

Для обмена сигнатурами атак между дружественными Анализаторами необходимо настроить беспарольный SSH-доступ для пользователя syn на каждом из двух Анализаторов.

Дальнейшие настройки выполняются при помощи экрана «Устройства».

3.14 Настройка метода подавления атак при помощи выполнения скриптов на удаленном хосте

В данной главе приведен пример настойки удаленного хоста «host» с операционной системой Debian для выполнения на нем удаленных скриптов. Допустим, необходимо выполнять SSH-скрипт с учетной записью пользователя user.

1) Сгенерируйте пару ключей при помощи команды «ssh-keygen –t rsa».
2) Добавьте открытый ключ пользователя в /home/user/.ssh/authorized_keys компьютера «host».

Дальнейшие настройки могут быть выполнены при помощи экрана «Скрипты для отражения атак».

3.15 Настройка анализатора для учета multicast-трафика

3.15.1 Введение

Технология многоадресной (multicast) передачи данных позволяет посылать трафик от одного хоста к нескольким хостам одновременно. Многоадресная рассылка используется с целью уменьшения загрузки каналов. Если в контролируемой сети используется multicast-трафик, следует настроить Анализатор для учета multicast-трафика, входящего в сеть. По умолчанию данная опция выключена.

Замечание: когда опция учета multicast-трафика выключена, Анализатор учитывает этот трафика как отброшенный.

3.15.2 Multicast-трафик

Multicast-трафик – это трафик, посланный от одного исходящего адреса к одному целевому адресу, к которому могут обратиться сразу несколько человек. Multicast-адрес – это идентификатор группы хостов, названных multicast-группой. В IPv4 эти адреса лежат в диапазоне от 224.0.0.0 до 239.255.255.255 (224.0.0.0/4).

Анализатор считает, что трафик является multicast-трафиком, если он отвечает следующим требованиям:

1) информация получена из NetFlow v5;
2) исходящий интерфейс равен 0 (что обычно соответствует отброшенному трафику);
3) IP-адрес назначения принадлежит какому-либо из целевых диапазонов, заданных на странице конфигурации «Multicast» (Администрирование → Мониторинг → Приложения → Multicast).

Ссылка: смотрите главу «Включение учета multicast-трафика» на странице 66 для получения подробной информации.

3.15.3 Отчеты multicast

После активации слежения за multicast-трафиком полученные данные отображаются в отчетах по multicast-трафику (Отчеты → Состояние сети → Multicast).

3.15.4 Включение учета multicast-трафика

Для включения слежения за multicast-трафиком выполните следующие действия:

1) Перейдите на экран «Multicast» (Администрирование → Мониторинг → Приложения → Multicast).
2) В поле «Обнаружение multicast-передачи» выберите вариант «Включено».

Замечание: после включения обнаружение multicast проверьте, что роутеры поддерживают передачу multicast-пакетов.

1) Заполните поле «Параметры multicast-передачи».
2) Нажмите «Сохранить».

3.16 Настройка уведомлений об аномалиях

3.16.1 Введение

Анализатор может быть настроен для рассылки почтовых уведомлений при возникновении аномалии.

3.16.2 Настройка уведомлений

В таблице 12 приведен список экранов для настройки параметров уведомления об аномалиях.

Таблица 12 – Экраны настройки уведомлений

Экран	Путь к экрану	Глава с описанием
«Глобальные настройки уведомлений»	Администрирование → Уведомления → Глобальные настройки	«Конфигурация глобальных настроек уведомлений»
«Группы»	Администрирование → Уведомления → Группы	«Экран Группы»
«Правила»	Администрирование → Уведомления → Правила	«Экран правила»

3.17 Настройка Анализатора для детектирования аномалий

3.17.1 Введение

Анализатор использует различные детекторы для распознавания аномалий.

Каждый детектор имеет ряд специфических настроек, которые могут быть выполнены на соответствующих экранах.

В этой главе дается описание детекторов и экранов для их настройки.

3.17.2 Настройка детекции BGP-аномалий

3.17.2.1 Введение

Анализатор детектирует BGP-аномалии следующих типов:

1) BGP-нестабильность – превышение заданного порогового количества BGP-обновлений на роутере за пятиминутный интервал.
2) Подделка BGP – обнаружение извещения BGP локального пространства адресов другой внешней автономной системой.
3) BGP-ловушка – изменение маршрута или nexthop для отслеживаемого CIDR-блока (входящего в контролируемую сеть).

3.17.2.2 Настройка детекции BGP-нестабильности, подделки BGP и ловушек

Для настройки детекции BGP-нестабильности и подделки BGP выполните следующие действия:

1) Перейдите на экран «Нестабильность BGP» (Администрирование → Детекция → BGP → Нестабильность BGP).
2) Чтобы включить детектирование нестабильности BGP, поставьте флажок «Детектировать нестабильность BGP».
3) Задайте пороговое значение количества BGP-обновлений за 5 минут, при превышении которого должен сработать детектор.
4) Чтобы детектировать взлом BGP, поставьте флажок «Детектировать взлом BGP».

Замечание: детектирование BGP-взломов зависит от правильной настройки адресного пространства контролируемой сети и ASN на экране «Сеть» (Администрирование → Мониторинг → Сеть).

5) Нажмите «Сохранить».

3.17.2.3 Создание и редактирование BGP-ловушек

Используйте BGP-ловушки для того, чтобы получать оповещения об изменении маршрута или nexthop, касающихся указанных CIDR-блоков, входящих в контролируемую сеть.

Экран «Ловушки» (Администрирование → Детекция → BGP → Ловушки) отображает список уже сконфигурированных BGP-ловушек и содержит следующие значения: название ловушки, CIDR-блоки, отслеживаемые события, группа для уведомлений.

Для создания или редактирования BGP-ловушки выполните следующие действия:

1) Перейдите на экран «Ловушки» (Администрирование → Детекция → BGP → Ловушки).

2) Находясь на экране, выполните одно из следующих действий:

   а) нажмите «Создать новую ловушку»;

   б) кликните на название существующей ловушки, чтобы редактировать ее.

3) Введите название ловушки в поле «Название».

4) В поле «Префиксы» введите CIDR-блоки, разделенные пробелом, которые система должна отслеживать (например, 192.168.100.0/24).

5) В поле «События» выберите события, которые следует отслеживать.

6) Выберите группу уведомлений в поле «Группа уведомлений».

Замечание: можно выбрать значение «Нет группы». В этом случае Анализатор будет отправлять оповещения группе по умолчанию.

7) Нажмите «Сохранить».

3.17.2.4 Удаление BGP-ловушек

Для удаления BGP-ловушки выполните следующие действия:

1) Перейдите на экран «Ловушки» (Администрирование → Детекция → BGP → Ловушки).

2) Поставьте флажки для BGP-ловушек, которые нужно удалить.

3) Нажмите «Удалить выбранные».

3.17.2.5 О пространстве «темных» IP-адресов и их детектировании

Анализатор считает опасным любой трафик, который он видит как направленный к области «темных» IP-адресов. В том числе, трафик хостов, которые выполняют сканирование хоста, в области «темных» IP. Значительное увеличение трафика «темных» IP может обозначать появление нового вредоносного ПО, червей, или других угроз, распространяющихся через сеть.

3.18 Настройка глобальных настроек детектирования

3.18.1 Введение

Анализатор позволяет задать глобальные настройки детекторов, которые будут применены ко всем наблюдаемым объектам, интерфейсам, если для них не указаны специфические настройки. Анализатор контролирует потоки трафика, идущие в область или из области «темных» IP. «Темные» IP – это область неиспользуемых адресов и потоки, направленные в неё или из неё могут указывать на активность червей или сканирование диапазона адресов.

3.18.2 Настройка детекции «темных» IP

До того как Анализатор начнет детектировать пространство «темных» IP, необходимо включить детекцию «темных» IP и сконфигурировать CIDR-блоки назначения (CIDR-блоки источников настраивать не обязательно) на экране «Темные IP» (Администрирование → Детекция → Темные IP).

Для конфигурирования детекции темных IP выполните следующие действия:

1) Перейдите на экран «Темные IP» (Администрирование → Детекция → Темные IP).
2) Для включения детекции темных IP выберите опцию «Включено», для отключения – «Выключено».
3) Введите CIDR-блоки источников.
4) Введите CIDR-блоки назначения.
5) Чтобы трафик, идущий с адресов «CIDR-блоки источников» на адреса «CIDR-блоки назначения», не считать «темным», поставьте галочку у соответствующего поля.
6) Задайте пороги для уведомлений о «темных» IP. Для отключения оставьте поле пустым.
7) Нажмите «Сохранить».

3.18.3 Настройка глобальных порогов для интерфейсов и наблюдаемых объектов

Настройка глобальных порогов для интерфейсов и наблюдаемых объектов производится на экране «Пороги по трафику» (Администрирование → Детекция → Пороги по трафику).

3.18.4 Об использовании порогов для интерфейсов

В случае если средний трафик интерфейса за одну минуту превышает верхний порог или меньше нижнего порога, Анализатор создает аномалию. По умолчанию для всех интерфейсов верхний порог составляет 95% (95 Мбит/с для 100 Мбит/с интерфейса, 950 Мбит/с для 1 Гбит/с интерфейса и т.д.), нижний не задан.

3.18.5 Конфигурация порогов по трафику

Экран «Пороги по трафику» позволяет настроить пороговые оповещения для наблюдаемых объектов и интерфейсов.

Для конфигурации порогов по трафику выполните следующие действия:

1) Перейдите на экран «Пороги по трафику» (Администрирование → Детекция → Пороги по трафику);
2) Установите значения верхнего и нижнего порога для интерфейсов. Для этого выполните одно из следующих действий:
   - установите значение от 1 до 100 для включения детектора;
   - установите значение порога в «0» для использования значения по умолчанию;
   - установите значение порога в «-1» для отключения детектора.
3) Установите флаг «Следить за трафиком наблюдаемых объектов», чтобы Анализатор генерировал аномалии о превышении пороговых значений трафика идущего с объекта и на объект.

4) Установите значения верхнего и нижнего порога для наблюдаемых объектов. Для этого выполните одно из следующих действий:

   – установите значение от 1 до 100 для включения детектора;

   – установите значение порога в «0» для использования значения по умолчанию.

5) Нажмите «Сохранить».

3.18.6 Конфигурация глобальных настроек детектора по шаблонным пакетам

Для настройки детектора по шаблонным пакетам выполните следующие действия:

1) Перейдите на экран «Настройки детектирования» (Администрирование → Детекция → Настройки детектирования).

2) В разделе «Шаблонные пакеты» в поле «Время детектирования» выберите количество минут, которое Система будет ждать, до того как отправит оповещение.

Замечание: по умолчанию установлено значение 2 минуты.

1) Выполните следующие шаги, см. таблицу 13.

Таблица 13 – Шаги для настройки детектора по шаблонным пакетам

Задача	Действия
Отключить настройки детектора по шаблонным пакетам для наблюдаемых объектов.	Выберите «Выключено».

Задача	Действия
Включить настройки детектора по шаблонным пакетам для наблюдаемых объектов.	1) Выберите «Включено»; 2) Нажмите «Редактировать»; 3) Выставьте настройки для всех сигнатур в открывшемся диалоговом окне настроек детектора по шаблонным пакетам для наблюдаемых объектов; 4) Нажмите «Сохранить».

2) Повторите действия п.3, чтобы задать настройки для остальных хостов.

3) Нажмите «Сохранить».

3.18.7 Конфигурация глобальных настроек детектора по профилю поведения объекта

Для настройки детектирования по профилю поведения объекта выполните следующие действия:

1) Перейдите на экран «Настройки детектирования» (Администрирование → Детекция → Настройки детектирования).

2) В разделе «Профили» в поле «Время детектирования» выберите количество минут, которое Система будет ждать, до того как отправит оповещение.

Замечание: по умолчанию установлено значение 5 минут.

3) Поставьте флажок у поля «Следить за исходящим трафиком» для включения этой опции или сбросьте флажок для отключения.

Замечание: по умолчанию опция включена.

4) Чтобы оставить настройки по умолчанию, выберите «Включено» у соответствующего поля. Чтобы не оставлять настройки по умолчанию, выберите «Выключено».

5) Нажмите «Сохранить».

3.18.8 Конфигурация детектора по профилю поведения объекта

При включении настроек по умолчанию в конфигурации глобальных настроек детектора для профилей становится видимой кнопка «Редактировать». При её нажатии открывается окно конфигурации детектора по профилю поведения объекта.

В открывшемся диалоговом окне необходимо заполнить предложенные поля и нажать «Сохранить».

3.18.9 О настройке автоматического вычисления пороговых значений

Минимальное значение серьезности отражает минимальную серьезность, определенную автоматическим вычислением.

Минимальное значение порога отражает минимальное значение, определенное автоматическим вычислением.

Автоматическое вычисление никогда не даст опуститься серьезности и порогу ниже этих значений. Если вычисленное значение ниже, Анализатор будет использовать минимальное значение порога.

3.18.10 Настройки автоматического вычисления пороговых значений

Для настройки автоматического вычисления пороговых значений выполните следующие действия:

1) Перейдите на экран «Настройки детектирования» (Администрирование → Детекция → Настройки детектирования).

2) Заполните необходимые поля.

Замечание: по умолчанию параметры имеют следующие значения: Процентиль для оценки серьезности - 95, множитель для оценки серьезности - 1.1, процентиль для вычисления порога – 40.

3) Нажмите «Сохранить».

3.18.11 Настройки отклонения DNS-запросов от тренда

Для настройки отклонения DNS-запросов от тренда выполните следующие действия:

1) Перейдите на экран «Настройки детектирования» (Администрирование → Детекция → Настройки детектирования).
2) Заполните необходимые поля.
3) Нажмите «Сохранить».

3.18.12 Конфигурация глобальных настроек уведомлений

3.18.12.1 Введение

Экран «Глобальные настройки» (Администрирование → Уведомления → Глобальные настройки) позволяет настроить глобальные параметры уведомлений: группа уведомлений по умолчанию, параметры SMTP-сервера для отправки почты и др.

3.18.12.2 Об SMTP-настройках

Необходимо указать SMTP-настройки так, чтобы Система могла отправлять оповещения на E-mail.

Анализатор поддерживает пароль аутентификации SMTP-серверов.

Можно ввести имя пользователя и пароль для аутентификации через защищенный паролем SMTP-сервер.

3.18.12.3 Экран «Глобальные настройки»

Для конфигурации глобальных настроек уведомлений выполните следующие действия:

1) Перейдите на экран «Глобальные настройки» (Администрирование → Уведомления → Глобальные настройки).
2) В поле «Таймаут NetFlow» введите количество секунд, которое Система должна ждать, прежде чем отправит уведомление.

3) В поле «Группа уведомлений по умолчанию» из раскрывающегося списка выберите группу, которой Система вышлет уведомление.

4) Заполните остальные поля, содержащие SMTP-настройки и подпись для письма.

5) Нажмите «Сохранить».

3.19 Учетные записи пользователей, права доступа, группы пользователей

3.19.1 Введение

Веб-интерфейс предоставляет доступ ко всей функциональности Системы, позволяет строить разнообразные отчеты, подавлять атаки, производить настройку Систему. Для доступа к веб-интерфейсу используется Система учетных записей, базирующаяся на группах пользователей и правах доступа – токенах. Каждая группа пользователей может быть настроена на доступ только к определенной функциональности и отчетности. Термины «учетная запись» и «пользователь» используемые в этой главе являются синонимами.

3.19.2 Мониторинг пользователей

3.19.2.1 Экран «История аккаунтов»

Экран «История аккаунтов» (Система → Статус → Устройства Syn → История аккаунтов) показывает всех пользователей, которые в настоящий момент работают в веб-интерфейсе, или заходили в него раньше. Используйте этот экран для следующих целей:

1) отслеживание попыток получения доступа к Анализатору с использованием неправильного пароля;
2) отслеживания доступа к Анализатору пользователями;
3) анализа периода времени и продолжительности, сколько пользователи работали с Системой.

Экран «История аккаунтов» отображает следующую информацию, см. таблицу 14.

Таблица 14 – Экран «История аккаунтов»

Колонка	Описание
Учетная запись	Логин пользователя.
IP-адрес	IP-адрес компьютера пользователя.
Время входа в систему	Время входа в Систему.
Продолжительность	Продолжительность работы пользователя с Системой. При ошибке авторизации отображается красная надпись «ошибка авторизации».

3.19.2.2 Экран «Интерфейс пользователя»

Экран «Интерфейс пользователя» (Система → Интерфейс пользователя) показывает историю посещения экранов, а также все URL-адреса на которые переходил пользователь.

Используйте этот экран для следующих целей:

1) анализа использования различных экранов пользователями;
2) анализа продолжительности загрузки различных экранов;
3) отслеживание попыток получения доступа к Анализатору с использованием неправильных URL-адресов.

Таблица 15 - Экран «Интерфейс пользователя»

Колонка	Описание
Дата	Дата и время посещения страницы.
Пользователь	Логин пользователя, посетившего страницу.
IP-адрес	IP-адрес пользователя, посетившего страницу.
Страницы	URL адрес экрана. Если URL является ссылкой на существующий экран, он отображается в виде ссылки, по которой можно перейти. Все остальные URL-ы не являются ссылками, т.к. являются вспомогательными AJAX запросами экранов и т.п.

Колонка	Описание
Время	Время загрузки страницы (в секундах).

3.19.3 Права доступа

3.19.3.1 Введение

В этой главе дается описание механизма регулирования прав доступа пользователей к функциям веб-интерфейса, описываются соответствующие экраны. Права доступа также называются токенами, это синонимы.

3.19.3.2 Права доступа

Механизм регулирования прав доступа пользователей к функциям веб-интерфейса характеризуется следующим, см. рисунок 3:

1) ограничение доступа работает на уровне отдельных экранов веб-интерфейса;
2) доступ к отдельным экранам определяют токены;
3) существует фиксированное количество токенов, часть из них имеет настройки по умолчанию, часть нет, но они все могут быть настроены;
4) токены назначаются для групп пользователей, таким образом, доступ отдельного пользователя к экрану регулируется через его группу.

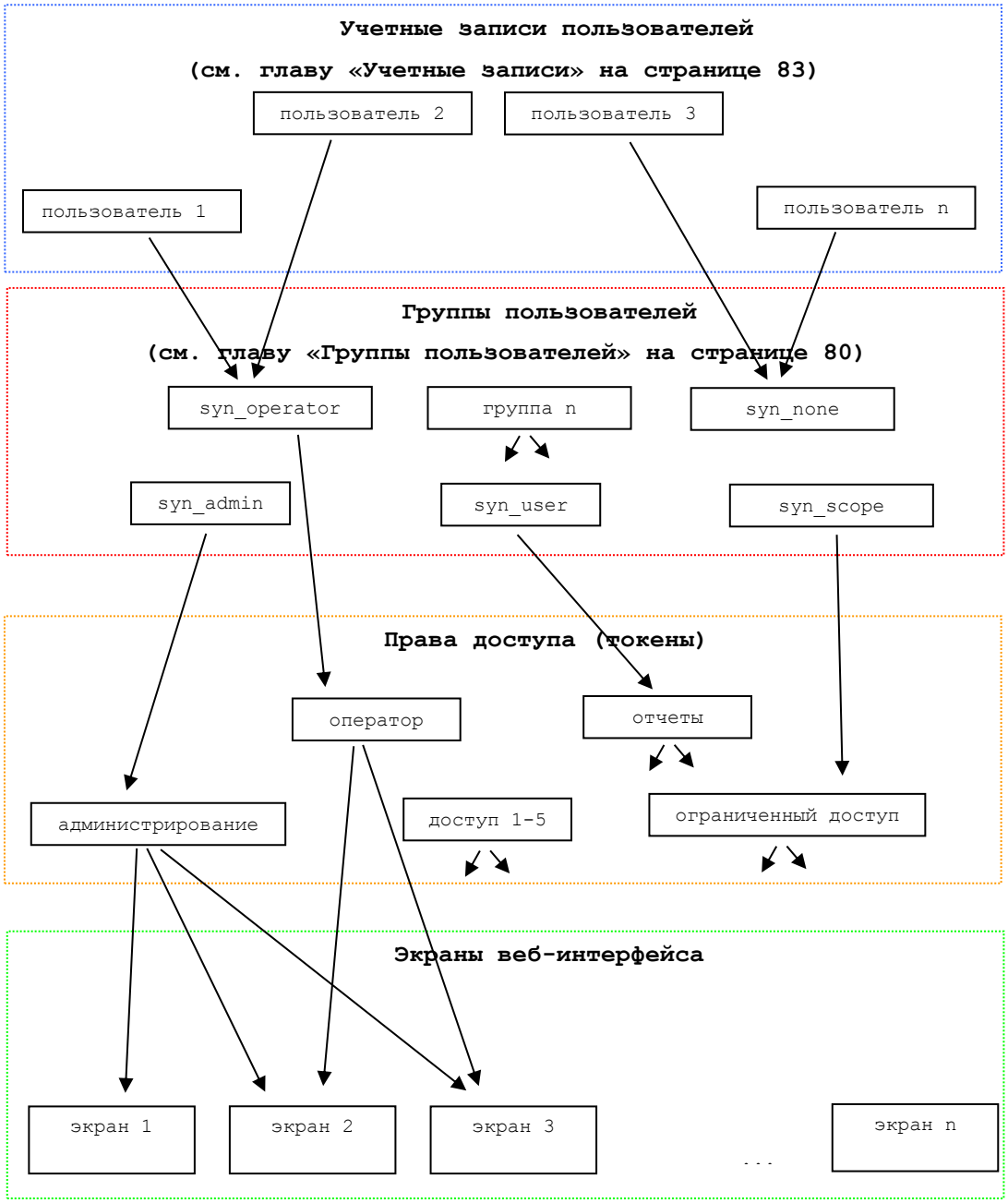

Рисунок 3 – Схема регулирования прав доступа

3.19.3.3 Экран «Права доступа»

Экран «Права доступа» (Администрирование → Доступ → Права доступа) позволяет настроить доступ к экранам веб-интерфейса для токенов.

Для настройки доступа выполните следующие действия:

1) Выберите токен из раскрывающегося списка поля «Токен».

2) Установите флажки напротив тех экранов, которые разрешено использовать этому токену. Используйте вспомогательные элементы управления, перечисленные в таблице 16.

Таблица 16 – Элементы управления

Элемент управления	Назначение
	Просмотр всего списка экранов
	Сворачивание списка экранов до верхнего уровня
	Разрешение доступа ко всем экранам
	Запрет доступа ко всем экранам

3) Нажмите «Сохранить».

3.19.4 Группы пользователей

3.19.4.1 Введение

В этой главе дается описание групп пользователей, функций, которые они выполняют, экранов настройки.

3.19.4.2 Группы пользователей

Группы пользователей необходимы для того, чтобы назначить одинаковые права доступа нескольким пользователям, связанным по одинаковым выполняемым функциям, регулировать права не на уровне отдельных учетных записей, а сразу для всех.

Группе пользователей назначается один или несколько токенов для регулирования прав доступа. Группа имеет права доступа к экранам равные объединению прав всех токенов.

По умолчанию в Системе предопределены пять групп пользователей, см. таблицу 17, эти группы не редактируются, но на их базе можно создать свои.

Таблица 17 – Группы пользователей

Группа	Описание	Права доступа
syn_admin	Полный доступ к чтению и записи на всех экранах Системы.	Администрирование
syn_operator	Просмотр отчетов, аномалий, работа с задачами подавления атак, работа с наблюдаемыми объектами.	Оператор
syn_user	Просмотр отчетов, аномалий, работа с задачами подавления атак; действия по настройке Системы исключены.	Отчеты
syn_scope	Просмотр отчетов по наблюдаемым объектам, аномалий для клиентов, работа с задачами подавления атак.	Ограниченный доступ
syn_none	Доступ закрыт. Группа, в которую переводятся пользователи при удалении их группы. Можно использовать для блокировки пользователей.	

3.19.4.3 Экран «Группы»

Экран «Группы» (Администрирование → Доступ → Группы) показывает существующие в Системе группы пользователей.

Для каждой группы указываются назначенные токены доступа. Группа определяет права для всех пользователей входящих в нее.

Экран отображает группы пользователей в виде таблицы, описание колонок см. таблицу 18.

Таблица 18 - Таблица групп пользователей

Колонка	Описание
Название группы	Название группы
Описание	Описание группы

Колонка	Описание
Права	Названия назначенных группе прав
Наблюдаемый объект	Наблюдаемый объект, доступ к которому разрешен пользователям данной группы. Если это поле задано, то пользователи группы могут просматривать и редактировать информацию, касающуюся только указанного наблюдаемого объекта и его дочерних объектов. Группа, для которой задан наблюдаемый объект – группа ограниченных пользователей.
Копировать	Ссылка для копирования группы.
Удалить	Ссылка для удаления группы. Только для групп созданных вручную.

3.19.4.4 Создание группы пользователей

В дополнение к заданным группам по умолчанию можно создавать свои собственные на экране «Группы» (Администрирование → Доступ → Группы).

Для создания новой группы пользователей выполните следующие шаги:

1) Нажмите «Создать новую группу».
2) Заполните поле «Название».
3) Если нужно, заполните поле «Описание».
4) Перейдите на вкладку «Права».
5) Выберите тип пользователя: обычный или ограниченный.
6) Выберите для группы один или несколько наборов прав доступа.
7) Если тип пользователя ограниченный, выберите наблюдаемый объект в поле «Наблюдаемый объект». В этом случае работа пользователя с Системой будет ограничена просмотром отчетов, аномалий и операциями только над этим объектом и его дочерними объектами.
8) Нажмите «Сохранить».

3.19.4.5 Редактирование группы пользователей

Для редактирования группы пользователей выполните следующие шаги:

1) Кликните на название группы в таблице групп. Откроется экран редактирования группы.
2) Редактируйте поля, которые нужно изменить.
3) Нажмите «Сохранить».

Замечание: нельзя редактировать группы, созданные в Системе по умолчанию.

3.19.4.6 Копирование группы пользователей

При создании похожих по свойствам групп быстрее и надежнее скопировать настройки уже созданной группы в новую группу. Для копирования выполните следующие шаги:

1) Кликните на «копировать» в таблице групп. Откроется экран копирования группы.
2) Редактируйте поля, которые нужно изменить.
3) Нажмите «Сохранить».

3.20 Учетные записи

3.20.1 Введение

В этой главе дается описание учетных записей, функций, которые они выполняют, экранов настройки. Термины «учетная запись» и «пользователь» являются синонимами.

3.20.2 Учетные записи

Учетные записи необходимы для предоставления доступа в веб-интерфейс. Учетная запись является индивидуальной для каждого отдельного пользователя Системы. Индивидуальность обусловлена соображениями безопасности, такими как пароль, возможность блокировки отдельных пользователей, анализ действий пользователей.

Права доступа пользователя к веб-интерфейсу назначаются через группу, в которую он входит.

3.20.3 Экран «Учетные записи»

Экран «Учетные записи» (Администрирование → Доступ → Учетные записи) отображает все созданные в Системе учетные записи и их характеристики. Экран позволяет создавать, редактировать, удалять учетные записи, а также просматривать детальную информацию по ним.

Экран отображает пользователей в виде таблицы, описание колонок см. таблицу 19.

Таблица 19 – Экран «Учетные записи»

Колонка	Описание
☑	Выбор пользователей для удаления или блокирования.
Логин	Логин пользователя, является ссылкой на страницу редактирования настроек.
Настоящее имя	Настоящее имя пользователя, является ссылкой на страницу редактирования настроек.
Группа	Группа, к которой принадлежит пользователь.
E-mail	E-mail пользователя.
Последний IP	IP-адрес, с которого пользователь заходил в веб-интерфейс в последний раз.
Последний вход в систему	Дата и время последнего входа в Систему.
Заблокирован	Заблокирован ли пользователь (да/нет).
На сайте	Работает ли пользователь с веб-интерфейсом в данный момент (да/нет).
Тип аутентификации	Тип аутентификации.

Замечание: возможна ситуация, когда и в колонке «Заблокирован», и в колонке «На сайте» для учетной записи дан утвердительный ответ. Это происходит,

если пользователь работает с Системой и одновременно он (или кто-то другой) в другом окне браузера при попытке зайти на сайт вводит неправильный пароль, исчерпывает количество попыток и блокирует доступ. В этой ситуации учетная запись блокируется, но пользователь, ранее зашедший в Систему, сохраняет возможность работать.

3.20.4 Создание и редактирование учетных записей

Используйте экран «Учетные записи» для создания и редактирования настроек пользовательских аккаунтов. Так как добавление и редактирование пользователя делается на одной и той же странице, описание в этой главе подходит к обоим действиям.

3.20.5 Права доступа учетной записи

Права доступа учетной записи назначаются в соответствии с группой пользователей, к которой она принадлежит.

3.20.6 Выбор надежного пароля

При создании учетной записи пользователя необходимо выбирать пароль, который содержит достаточное сочетание букв и цифр. Пароль должен отвечать следующим критериям:

1) не меньше 5 символов;
2) не больше 20 символов;
3) нельзя вводить исключительно цифры;
4) разрешенные символы: символы латинского алфавита, русского алфавита, строчные и прописные буквы, цифры, тире, точка, подчеркивание.

3.20.7 Выбор логина

Логин должен отвечать следующим критериям:

1) не меньше 5 символов;
2) не больше 20 символов;

3) разрешенные символы: символы латинского алфавита, русского алфавита, строчные и прописные буквы, цифры, тире, точка, подчеркивание.

3.20.8 Процедура создания или редактирования учетной записи

Для создания или редактирования учетной записи выполните следующие действия:

1) Перейдите на экран «Учетные записи» (Администрирование → Доступ → Учетные записи).
2) Сделайте одно из двух:
   а) добавьте пользователя, нажав «Создать нового пользователя»;
   б) редактируйте пользователя, нажав ссылку на логине или имени пользователя в таблице учетных записей;
3) Система отобразит экран редактирования аккаунта пользователя.
4) Заполните предложенные поля.

Замечание: при вводе пароля Система будет отображать вводимые символы в виде звездочек (*) чтобы скрыть пароль.

Замечание: предлагаемый здесь по умолчанию часовой пояс задается на экране «Глобальные настройки» (Администрирование → Пользовательский интерфейс → Глобальные настройки).

5) Нажмите «Сохранить».

Замечание: в любой момент времени пользователь может нажать на строку с датой и временем в правом верхнем углу экрана и установить другой часовой пояс.

3.20.9 Удаление учетных записей

Для удаления учетных записей выполните следующие действия:

1) Перейдите на экран «Учетные записи» (Администрирование → Доступ → Учетные записи).
2) Поставьте флажки для тех пользователей, которых необходимо удалить.
3) Нажмите «Удалить».

3.20.10 Блокировка учетной записи

Заблокированный пользователь не может войти в Систему. Пользователь может быть заблокирован администратором, при этом он сразу же теряет возможность работы с Системой. Пользователь блокируется автоматически при вводе неправильного пароля больше разрешенного числа попыток. Для блокировки пользователей вручную выполните следующие действия:

1) Перейдите на экран «Учетные записи» (Администрирование → Доступ → Учетные записи).
2) В левом столбце открывшейся таблицы аккаунтов поставьте флажки для тех пользователей, которых нужно заблокировать.
3) Нажмите «Заблокировать выбранных».

Замечание: с момента блокировки пользователя он не может открыть ни один экран.

3.20.11 Разблокировка учетной записи

1) Перейдите на экран «Учетные записи» (Администрирование → Доступ → Учетные записи).
2) Кликните на имя того пользователя, которого необходимо разблокировать. Откроется экран редактирования учетной записи.
3) Поставьте галочку у поля «Доступ разрешен».
4) Нажмите «Сохранить».

3.20.12 Таймаут логина

На экране «Глобальные настройки» (Администрирование → Пользовательский интерфейс → Глобальные настройки) можно задать таймаут логина – время бездействия, через которое веб-интерфейс блокируется, и пользователь может продолжить работу с ним только после ввода своего логина и пароля.

3.21 Настройка блокировки при ошибках авторизации

3.21.1 Введение

Анализатор может быть настроен так, чтобы учетная запись блокировалась после определенного количества неудачных попыток авторизации.

3.21.2 Максимальное допустимое количество попыток ввода неправильного пароля пользователем

Чтобы задать максимальное допустимое количество попыток ввода неправильного пароля выполните следующие шаги:

1) Перейдите на экран «Опции» (Администрирование → Доступ → Опции).

2) Заполните поле «Количество попыток».

Замечание: чтобы задать неограниченное количество попыток, введите «0».

3) Нажмите «Внести изменения».

3.21.3 Белый список адресов

На экране «Опции» (Администрирование → Доступ → Опции) можно задать белый список адресов, с которых пользователь с правами администратора может зайти в Систему даже в том случае, если он заблокирован. Администратор – это пользователь группы syn_admin.

Важно: категорически рекомендуется заполнить белый список перед использованием Системы, иначе может возникнуть ситуация, когда администратор не может войти в Систему.

3.22 Ограниченные пользователи

3.22.1 Введение

Веб-интерфейс Анализатора позволяет клиентам компании получить прямой доступ к отчетам, аномалиям и заданиям на подавление атак. Использование веб-интерфейса клиентами напрямую позволяет предоставить более высокий уровень сервиса, клиенты могут сами просматривать информацию и работать с Системой на

том уровне, который разрешен администратором, при этом, не создавая рисков по безопасности Системы.

Учетные записи клиентов имеющих прямой доступ к веб-интерфейсу также называются ограниченными пользователями, так как работа с веб-интерфейсом ограничивается как по части доступа к экранам, так и по функциям на этих экранах.

Ограниченные пользователи в своих действиях в веб-интерфейсе ограничены наблюдаемыми объектами, к которым они привязаны через группу пользователей. Отчеты и аномалии отображаются только для этих объектов и их дочерних. Задания на подавления атак могут быть созданы только в рамках CIDR-адресов этих объектов и их дочерних.

3.22.2 Понимания принципов создания ограниченного пользователя

Все ограничения пользователя следуют из ограничений заданных группой пользователей, в которой он находится. Ограниченный пользователь создается в Системе точно так же как и обычный пользователь, через Систему учетных записей. Учетная запись ограниченного пользователя отличается только тем, что используется специальная группа.

Группа для ограниченных пользователей создается с привязкой к наблюдаемому объекту. Ограниченные пользователи в этой группе при работе могут взаимодействовать только с этим объектом и с его дочерними объектами.

3.22.3 Безопасность Системы

Доступ ограниченных пользователей к Системе ограничен как экранами (задается через права доступа), так и объектами (задается через группы пользователей). Дополнительно в Системе существует жесткое программное ограничение для ограниченных пользователей на просмотр и работу с объектами инфраструктуры. Ограниченные пользователи не могут получить доступ к отчетам или экранам для работы с инфраструктурой, даже если эти экраны разрешены настройками прав доступа.

3.23 Настройка глобальных параметров

3.23.1 Глобальные настройки веб-интерфейса

3.23.1.1 Введение

Глобальными настройка веб-интерфейса называются параметры, влияющие на внешний вид и функциональность веб-интерфейса для всех пользователей.

Редактирование глобальных настроек веб-интерфейса производится на экране «Глобальные настройки» (Администрирование → Пользовательский интерфейс → Глобальные настройки).

3.23.1.2 Выбор логотипа

Логотип отображается в шапке отчетов экспортированных в формат PDF. Чтобы установить или сменить логотип Системы, выполните следующие шаги:

1) Нажмите «Обзор», рядом с полем «Выбор логотипа».

2) Выберите изображение логотипа.

3) Нажмите «Загрузить».

3.23.1.3 Системные настройки

В разделе «Системные настройки» можно установить следующие параметры:

1) Электронный адрес технической поддержки.

E-mail, на который должны приходить заявки и вопросы пользователей в техническую поддержку. Если E-mail технической поддержки указан, он отображается на каждой странице в правом нижнем углу.

2) Таймаут логина.

Время бездействия пользователя, через которое веб-интерфейс блокируется и пользователь может продолжить работу с ним, только после ввода своего логина и пароля в появившейся форме.

3) Период обновления статусной страницы.

Период обновления экрана «Суммарный отчет» (Система → Статус → Суммарный отчет).

4) Адрес сайта.

Адрес сайта используется для ссылок в письмах и экспортированных отчетах.

5) Максимальное количество сообщений в почтовой очереди.

Максимально допустимое количество сообщений в почтовой очереди. При отправке почты Анализатор создает аномалию отправки почты, если в почтовой очереди накопилось больше указанного количества сообщений.

6) Количество отображаемых сообщений в ленте событий.

7) Часовой пояс.

Часовой пояс, установленный в Системе по умолчанию. Используется как вариант по умолчанию при создании новых учетных записей пользователей.

3.23.1.4 Настройки по умолчанию

Здесь может быть выбран способ отражения атак по умолчанию. Допустимые значения:

1) сгенерировать фильтр;

2) фингерпринт;

3) blackhole;

4) flow Specification.

3.24 Соответствие номеров и названий

3.24.1 Введение

Экран «Соответствие номеров и названий» (Администрирование → Пользовательский интерфейс → Соответствие номеров и названий) позволяет назначать названия для TCP- и UDP-портов, AS-номеров и типов обслуживания TOS. Заданные соответствия используются только при выводе отчетов по трафику.

Важно: заданные соответствия не используются в экранах настройки Системы, создания правил и т.п.

3.24.2 Экран «Соответствие номеров и названий»

Добавить соответствия можно двумя способами.

1) Загрузить из файла. Для этого выполните следующие действия:
   а) нажмите «Обзор»;
   б) выберите нужный файл;
   в) выберите кодировку загружаемого файла;
   г) нажмите «Отправить файл».
2) Ввести соответствия в текстовое поле. Для этого:
   а) введите номера и названия в текстовое поле;
   б) нажмите «Сохранить».

3.25 Группы приложений

3.25.1 Введение

Экран «Группы» (Администрирование → Мониторинг → Приложения → Группы) позволяет объединить TCP- и UDP-порты в группы приложений.

3.25.2 Экран «Группы»

Группы приложений – это коллекция TCP- и/или UDP-портов. Группы приложений позволяют комбинировать подобные или зависимые группы портов для более удобного мониторинга изучаемых приложений или групп приложений. И группы приложений, и отдельные порты отображаются в отчетах «Все приложения» (Отчеты → … → Приложения → Все).

На экране «Группы приложений» отображается таблица, которая содержит следующую информацию, см. таблицу 20.

Таблица 20 – Группы приложений

Колонка	Описание
☑	Используйте для удаления групп.
Наименование	Название группы приложений.
TCP-порты	Список TCP-портов, принадлежащих к данной группе приложений.

Колонка	Описание
UDP-порты	Список UDP-портов, принадлежащих к данной группе приложений.

3.25.2.1 Создание группы приложений

Для создания группы приложений выполните следующие действия:

1) Перейдите на экран «Группы» (Администрирование → Мониторинг → Приложения → Группы).
2) Нажмите «Создать новую группу». Откроется экран создания группы.
3) Заполните предложенные поля.
4) Нажмите «Сохранить».

3.25.3 Редактирование группы приложений

Для редактирования группы приложений выполните следующие действия:

1) Перейдите на экран «Группы» (Администрирование → Мониторинг → Приложения → Группы).
2) Кликните на название группы. Откроется экран редактирования группы.
3) Внесите необходимые изменения.
4) Нажмите «Сохранить».

3.25.4 Удаление групп приложений

Для удаления групп приложений выполните следующие действия:

1) Перейдите на экран «Группы» (Администрирование → Мониторинг → Приложения → Группы).
2) Установите флажки для групп, которые нужно удалить.
3) Нажмите «Удалить выбранные».

3.26 Настройка мониторинга состояния Системы

3.26.1 Введение

Экран «Мониторинг состояния Системы» (Администрирование → Детекция → Мониторинг состояния Системы) позволяет настроить Анализатор для создания аномалий, когда происходит операционная ошибка. Эти сообщения помогают идентифицировать сбои и их причины, как только те произошли.

Можно настроить Анализатор на отправку оповещения через e-mail, используя экран «Аномалии мониторинга Системы».

3.26.1.1 Мониторинг состояния Системы

Анализатор отображает аномалии мониторинга Системы на следующих экранах:

1) состояние Системы: экран «Суммарный отчет» (Система → Статус → Суммарный отчет) отображает активность по аномалиям за последние 24 часа, суммарный отчет по сетевому трафику за последние 24 часа и топ 5 текущих и прошедших аномалий: DoS и Системных событий.
2) аномалии: экран «Все события» (Аномалии → Все события).

3.26.1.2 Включение мониторинга состояния Системы

По умолчанию на Анализаторе выключены уведомления для аномалий во избежание спама. Для включения уведомлений для аномалий выполните следующие действия:

1) Перейдите на экран «Глобальные настройки» (Администрирование → Уведомления → Глобальные настройки).
2) Выберите группу, которую хотите сделать группой по умолчанию в поле «Группа уведомлений по умолчанию».
3) Нажмите «Сохранить».

3.26.1.3 Настройка параметров мониторинга состояния Системы

Для настройки параметров мониторинга состояния Системы выполните следующие действия:

1) Перейдите на экран «Мониторинг состояния системы» (Администрирование → Детекция → Мониторинг состояния системы).
2) Поставите галочку в поле «Мониторинг посторонних процессов», чтобы Анализатор создавал аномалии при обнаружении посторонних процессов в Системе.
3) Если значения по умолчанию в остальных полях не подходят, измените их.
4) Нажмите «Сохранить».

3.26.1.4 Отключение мониторинга состояния Системы

Для отключения мониторинга состояния Системы выполните следующие действия:

1) Перейдите на экран «Мониторинг состояния системы» (Администрирование → Детекция → Мониторинг состояния системы).
2) Снимите галочку «Включить мониторинг системы».
3) Нажмите «Сохранить».

3.26.2 Мониторинг роутеров

3.26.2.1 Введение

Экран «Роутеры» (Система → Статус → Сетевые устройства → Роутеры) отображает статистику распределения трафика по роутерами и прочую связанную с ними информацию.

По умолчанию отображаются все роутеры, но можно выбрать только одну группу роутеров для отображения.

3.26.2.2 Просмотр информации о роутерах группы

Для просмотра информации о роутерах одной группы выполните следующие действия:

1) выберите группу роутеров в поле «Группа роутеров»;

2) выберите параметр, который должен отображаться на графике.

Замечание: график автоматически обновится, когда все значения будут выбраны.

3.26.2.3 Таблица статуса роутеров

Таблица 21 содержит информацию о статусах роутеров.

Таблица 21 – Таблица статусов роутеров

Колонка	Описание
☑	Определяет, информацию о каком роутере отображать на графике.
Роутер	Название роутера.
NetFlow / Трафик bps	NetFlow-трафик, бит в секунду.
NetFlow / Трафик pps	NetFlow-трафик, пакетов в секунду.
NetFlow / ACL bps	Отбрасываемый роутером NetFlow-трафик, бит в секунду.
NetFlow / Потоков в секунду	Количество NetFlow потоков в секунду.
NetFlow / Необработанных Flow-записей в секунду	Количество необработанных NetFlow-записей в секунду.
NetFlow / Flow-записей в секунду с нарушением последовательности	Количество NetFlow-записей в секунду, полученных с нарушением последовательности. Как правило, указывает на то, что Анализатор не успевает обрабатывать входящие пакеты, для проверки этого используйте параметр «Перегрузка Анализатора» на экране «Статус устройств».
NetFlow / Последний поток	Данные о последнем NetFlow-потоке.
SNMP / ЦП	Процент загрузки процессора.
SNMP / Память	Процент использования памяти.
BGP / Соединение установлено	Установлено ли соединение через BGP: «да» или «нет».

Колонка	Описание
BGP / Активных маршрутов	Количество BGP-маршрутов в таблице маршрутизации роутера, полученных Анализатором с роутера.

3.26.3 Мониторинг интерфейсов

3.26.3.1 Введение

Экран «Роутеры» (Система → Статус → Сетевые устройства → Роутеры) отображает статистику распределения трафика по роутерам и прочую связанную с ними информацию.

3.26.3.2 Просмотр информации об интерфейсах роутера

Чтобы увидеть список интерфейсов роутера, необходимо выбрать роутер из раскрывающегося списка. После выбора автоматически загрузится таблица с информацией об интерфейсах роутера, см. таблицу 22.

Таблица 22 – Информация об интерфейсах

Колонка	Описание
SNMP-индекс	SNMP-индекс интерфейса.
Название	Название интерфейса.
Описание	Описание интерфейса.
Тип	Тип интерфейса. Возможные значения: – внешний; – внутренний; – магистральный; – смешанный; – игнорируемый.
Скорость	Скорость интерфейса, которая может быть либо сконфигурирована пользователем, либо определена Системой автоматически на основе SNMP-данных.
Входящий (SNMP)	Входящий SNMP-трафик.
Исходящий (SNMP)	Исходящий SNMP-трафик.
Отчет NetFlow	Кнопка, открывающая экран «Интерфейс» (Отчеты → Интерфейс → Суммарный отчет → Интерфейс),

Колонка	Описание
	содержащий информацию о NetFlow-трафике для данного интерфейса.
SNMP	Кнопка, открывающая отчет «SNMP счетчики» (Отчеты → Интерфейс → Суммарный отчет → SNMP-счетчики), содержащий SNMP информацию о трафике для данного интерфейса.

3.26.4 Автоконфигурация интерфейсов

3.26.4.1 Цели автоклассификации

1) Определение типа интерфейса (внутренний, внешний, магистральный, смешанный, игнорируемый).
2) Определение соответствия интерфейса объекту с определением направления на объект.
3) Определение пороговых значений трафика на интерфейсе.

3.26.4.2 Экран «Правила»

Экран «Правила» (Администрирование → Мониторинг → Автоконфигурация → Правила) содержит таблицу со следующими полями, см. таблицу 23.

Таблица 23 – Экран «Правила»

Колонка	Описание
☑	Выбор правила для последующего его удаления.
Сорт.	Кнопки для изменения порядка правила. Порядок правила важен, т.к. если правило сработало для интерфейса, следующие правила для него не проверяются.
Правило	Порядок правила, так же является ссылкой на экран редактирования правила.
Наименование	Название правила, так же является ссылкой на экран редактирования правила.
Описание	Описание правила.
Сопоставление	Названия роутеров с которыми сопоставлено данное правило.

Колонка	Описание
Действие	Действия правила.

Механизм автоклассификации работает с правилами в порядке указанном в колонке таблицы «Правило». Если интерфейс классифицирован правилом, то следующие правила для него не проверяются. Механизм автоклассификации не производит изменений в конфигурации интерфейсов, а только предлагает их. Для просмотра предлагаемых изменений используйте экран «Результаты автоконфигурации» (Администрирование → Мониторинг → Автоконфигурация → Результаты). Автоклассификация запускается при нажатии на соответствующую кнопку на экране, а также автоматически каждые 12 часов. Длительность всего процесса автоклассификации при использовании правил с автоматическим определением типа (эвристический анализ) зависит от длительности анализа и задается на экране «Сеть» (Администрирование → Мониторинг → Сеть).

3.26.5 Экран «Результаты автоклассификации»

Экран «Результаты автоклассификации» (Администрирование → Мониторинг → Автоконфигурация → Результаты) позволяет просматривать предлагаемые изменения в конфигурации интерфейсов.

3.27 Мониторинг аппаратной платформы Анализатора

3.27.1 Введение

Для предупреждения аппаратных сбоев и поддержания работоспособности, Система раз в минуту опрашивает аппаратные датчики, настроенные в Системе, сохраняет показания датчиков в базе данных и генерирует аномалии если эти показания выходят за установленные предельные значения.

3.27.2 Просмотр настроенных в Системе аппаратных датчиков

Для просмотра настроенных в Системе аппаратных датчиков выполните следующие действия:

1) Перейдите на экран «Датчики» («Администрирование» → «Анализатор» → «Датчики»).
2) В таблице будут перечислены все настроенные в Системе аппаратные датчики, см. таблицу 24.

Таблица 24 – Поля таблицы на экране «Датчики»

Колонка	Описание
Адаптер	Имя устройства в рамках Системы lmsensors, с которого считываются значения.
Датчик	Имя датчика в рамках Системы lmsensors, с которого считываются значения.
Описание	Пользовательский комментарий к датчику.
Диапазона значений датчика – Минимальное значение	Минимально допустимое значение датчика, при выходе за пределы будет сгенерирована аномалия.
Диапазона значений датчика – Максимальное значение	Максимально допустимое значение датчика, при выходе за пределы будет сгенерирована аномалия.
Единицы измерения	Единицы измерения. Выводятся в тексте аномалии для удобства.
Генерировать предупреждение	Генерировать или нет аномалию при выходе показаний датчика за пределы указанных значений.

3.27.3 Добавление / редактирование аппаратного датчика

Для добавления нового или редактирования существующего аппаратного датчика выполните следующие действия:

1) Перейдите на экран «Датчики» («Администрирование» → «Анализатор» → «Датчики»).
2) В таблице будут перечислены все настроенные в Системе аппаратные датчики.
3) Для редактирования существующего датчика найдите его по имени (колонка «Датчик») и кликните по гиперссылке в названии; для добавления нового датчика выберите «Добавить датчик».

4) На открывшемся экране «Редактирование датчика» в поле «Адаптер» введите название устройства в рамках Системы lmsensors, с которого будут считываться значения. Можно выбрать заранее предустановленный адаптер из списка рядом с полем редактирования.
5) В поле «Датчик» введете название датчика в рамках Системы lmsensors, с которого будут считываться показания.
6) В опциональном поле «Описание» можно ввести краткий комментарий к создаваемому датчику.
7) Если необходимо следить за показаниями датчика и создавать аномалии при выходе показаний за границы заданных значений, отметьте поле «Генерировать аномалию, если показания датчика выходят за пределы допустимых значений», а в поле «Диапазон допустимых значений» введите минимально и максимально допустимые значения датчика.
8) В поле «Единицы измерения» введите единицы измерения показаний датчика. Они будут использованы при генерации аномалии и просмотре отчетов.
9) Нажмите «Сохранить».

3.27.4 Удаление аппаратного датчика

Для прекращения мониторинга аппаратного датчика выполните следующие действия:

1) Перейдите на экран «Датчики» («Администрирование» → «Анализатор» → «Датчики»).
2) В левой колонке отметьте галочками датчики, которые необходимо удалить.
3) Нажмите «Удалить выбранные датчики».

3.27.5 Просмотр датчиков в системе lmsensors

Для конфигурирования и просмотра доступных аппаратных датчиков на уровне Системы необходимы права суперпользователя. Выполните следующие действия:

1) Зайдите в консоль суперпользователем и введите команду «sensors».
2) На экране отобразится список доступных адаптеров и принадлежащих им аппаратных датчиков. Эти названия и необходимо использовать при создании новых аппаратных датчиков.

Замечание: первоначальная настройка системы lmsensors производится при установке Системы.

3.27.6 Системный журнал

3.27.6.1 Введение

Экран «Системный журнал» (Система → Системный журнал) – инструмент для детализации сведений о происходящих в Системе событиях, диагностики поведения программных модулей и возникающих в них ошибок с возможностью переключения уровней без рестарта и со сжатием логов.

Система журналирования внедрена в каждый из 7 программных модулей invGuard AS-SW. Журнал является текстовым файлом (одно событие – одна строка). Протоколирование действий модулей осуществляется в хронологическом порядке.

Для каждого демона создана отдельная конфигурация ведения журнала. Присутствует возможность устанавливать различные уровни логов для разных демонов, т.к. настройка системы журналирования одновременно для всех демонов неудобна. Если файла конфигурации с параметрами ведения журнала нет (или какой-то параметр отсутствует), то используются значения по умолчанию. Значения по умолчанию жестко заданы в коде демона.

Существуют следующие уровни логов: HIGH_DEBUG, DEBUG, INFO, WARNING, ERROR. При выборе уровня существует возможность выбора одного, нескольких одновременно или всех уровней сразу. Например, DEBUG | ERROR |

WARNING – выдает логи отладки, ошибок и предупреждений. Если ни один уровень не задан, значит все события игнорируются.

Для изменения конфигурации логов непосредственно во время работы демона, внедрён обработчик сигнала SIG_USER1. Данный обработчик позволяет менять уровень логов, не останавливая сам демон.

В настройках конфигурации для каждого демона существует параметр, определяющий максимальную длину файла журнала. При достижении этой длины файл журнала закрывается и открываться новый. Название новых файлов соответствует шаблону: имя_демона_YYYYMMDDhhmm.log.

3.27.6.2 Описание файлов журналирования

Файл конфигурации

Расположен /etc/syn/log_config.txt

Содержание/настройки:

LogDirectory="/var/log/syn/"

LogLevel=DEBUG|INFO

LogCatigories=ALL

LogBackupDirectory="/var/log/syn/"

LogFileSize=15000000

LogEnableTimeStamping=true

SynntfdLogLevel=INFO|ERROR|DEBUG|WARNING|HIGH_DEBUG

SynntfdLogFileSize=1500000

Демон SYNMOND

Путь к файлу журнала: /var/log/syn/analizer_synmond.log

Пример записи события в журнал демона SYNMOND:

PID(20740) 30/05/2014 15:48:49.676 [DEBUG] [NO CATEGORY]: [DBMySqlConnection.cpp:172] Connection to database established, thread id = 214959

PID(20740) 30/05/2014 15:48:49.688 [DEBUG] [SYN_DAEMON_CHECK]: [proc/SYNDaemonProcesses.cpp:56] Not running daemon:/usr/bin/syn/synnetflowd

PID(20750) 30/05/2014 15:48:49.789 [DEBUG] [CONTROL_MESSAGE_PROCESSOR]: [configuration/DBStoredParamsUpdater.cpp:86] SYSTHD_CHANGED cleaned from ipc_events

Демон SYNNETFLOWD

Путь к файлу журнала: /var/log/syn/analizer_ synnetflowd.log

Пример записи события в журнал демона SYNNETFLOWD:

PID(20771) 02/06/2014 08:27:50.317 [DEBUG] [NO CATEGORY]: [collector/NFDCollector.cpp:350] NFDCollector::processEvent() :

Queues. Dispatcher: 0/25. Analysers: 1: 1/25 | 2: 0/25 | 3: 0/25 | 4: 1/25 |

PID(20771) 02/06/2014 08:27:50.317 [DEBUG] [NO CATEGORY]: [detector/NFDDetector.cpp:80] NFDDetector::processEvent() : new event received : detector: new statistics arrived

Демон SYNBGPD

Путь к файлу журнала: /var/log/syn/analizer_ synbgpd.log

Пример записи события в журнал демона SYNBGPD:

PID(20939) 31/05/2014 23:57:55.761 [DEBUG] [BGP_PEER_MANAGER]: [PeerManager.cpp:541] PeerManager::processEvents() : Event has been arrived, type = OFFRAMP_STOP

PID(20939) 31/05/2014 23:57:55.761 [DEBUG] [BGP_PEER_MANAGER]: [PeerManager.cpp:639] PeerManager::processEvents() : executing query SELECT event_id FROM ipc_events WHERE etype = 'OFFRAMP_STOP' AND origin_event_id = 95;

Демон SYNSNMPD

Путь к файлу журнала: /var/log/syn/analizer_ synsnmpd.log

Пример записи события в журнал демона SYNSNMPD:

PID(20980) 01/06/2014 13:13:50.540 [DEBUG] [NO CATEGORY]: [Device.cpp:193] Device::refreshDevice() : begin hw_id : 1, timeout = 300

PID(20980) 01/06/2014 13:13:50.541 [DEBUG] [NO CATEGORY]: [Device.cpp:110] Device::checkConnection() : connection is not valid

PID(20980) 01/06/2014 13:13:50.541 [DEBUG] [NO CATEGORY]: [Device.cpp:126] Device::initializeDevice() : begin

Демон SYNPEERMGRD

Путь к файлу журнала: /var/log/syn/analizer_ synpeermgrd.log

Пример записи события в журнал демона SYNPEERMGRD:

PID(20809) 30/05/2014 15:48:50.327 [DEBUG] [NO CATEGORY]: [Daemon.cpp:54] Pid file is obsolete and will be replaced

PID(20809) 30/05/2014 15:48:50.327 [DEBUG] [NO CATEGORY]: [Daemon.cpp:124] Unregister Daemon

PID(20809) 30/05/2014 15:48:50.327 [DEBUG] [NO CATEGORY]: [Daemon.cpp:125] synpeermgrd stop [OK]

Демон SYNNTFD

Путь к файлу журнала: /var/log/syn/analizer_ synntfd.log

Пример записи события в журнал демона SYNNTFD:

PID(20920) 30/05/2014 15:48:50.504 [DEBUG] [NO CATEGORY]: [DBMySqlConnection.cpp:172] Connection to database established, thread id = 214987

PID(20927) 30/05/2014 15:48:50.507 [DEBUG] [NO CATEGORY]: [AnomalyMailer.cpp:109] Using interval from 2014-05-30 15:42:15 to 2014-05-30 15:48:50

PID(20927) 30/05/2014 15:48:50.507 [DEBUG] [NO CATEGORY]: [AnomalyMailer.cpp:111] There new anomalies in the DB count: 1

Демон SYNSECD

Путь к файлу журнала: /var/log/syn/analizer_ synsecd.log

Пример записи события в журнал демона SYNSECD:

PID(20999) 30/05/2014 16:28:51.287 [DEBUG] [NO CATEGORY]: [Daemon.cpp:355] synsecd main cycle of daemon. Refresh Interval is :300

PID(20999) 30/05/2014 16:38:51.456 [DEBUG] [NO CATEGORY]: [Daemon.cpp:355] synsecd main cycle of daemon. Refresh Interval is :300

3.27.7 Статус пользовательского интерфейса

3.27.7.1 Введение

Экран «Интерфейс пользователя» (Система → Интерфейс пользователя) отображает список посещенных экранов с детальной информацией о каждом посещении.

3.27.7.2 Об экране «Интерфейс пользователя»

Экран «Интерфейс пользователя» (Система → Интерфейс пользователя) предоставляет информацию о действиях пользователей в веб-интерфейсе Анализатора. На экране выводится список действий пользователей и количество времени, затраченного Системой на генерацию каждой страницы, см. таблицу 25.

Таблица 25 – Экран «Интерфейс пользователя»

Колонка	Описание
Дата	Дата и время посещения экрана.
Пользователь	Логин пользователя, посетившего экран.
IP-адрес	IP-адрес пользователя, посетившего экран.
Страницы	Адрес экрана.
Время	Время загрузки экрана (в секундах).

3.27.8 Мониторинг сетевых соединений

3.27.8.1 Введение

Сетевое соединение – канал передачи данных между двумя узлами сети. Характеризуется адресом и портом источника, адресом и портом назначения, а также протоколом передачи данных.

В Системе есть возможность записи и фильтрации информации о сетевых соединениях. Запись осуществляется в журналы соединений. По мере заполнения старые журналы архивируются. Фильтрация нужна для того, чтобы создать список известных сетевых подключений (правила для фильтрации) и дальше отслеживать неизвестные подключения, чтобы видеть попытки подключиться к Системе и взломать ее. Правила не фильтруют сам трафик. Соединения, попадающие под действие фильтра, просто не вносятся в журнал, поскольку на фоне множества известных подключений легко пропустить «незаконное» подключение.

В Системе имеется два экрана для просмотра и контроля сетевых соединений – «Журнал» и «Фильтры». Экран «Журнал» служит для просмотра списка сетевых соединений, при этом доступны журналы соединений Анализатора. Экран «Фильтры» служит для создания новых фильтров.

В случае обнаружения «незаконных» подключений Система создает аномалию.

3.27.8.2 Об экране «Журнал»

Экран «Журнал» (Администрирование → Доступ → Сетевые подключения → Журнал) перечисляет обнаруженные сетевые соединения, отсортированные по времени. История соединений считывается либо из всех текущих лог-файлов, либо из лог-файла выбранного устройства, либо из выбранного архивного файла выбранного устройства. Логи и архивы находятся на Анализаторе.

Экран «Журнал» отображает следующую информацию, см. таблицу 26.

Таблица 26 – Экран «Журнал»

Колонка	Описание
Время	Метка времени.
Источник	IP-адрес и порт источника.
Назначение	IP-адрес и порт назначения.
Протокол	Протокол передачи данных.
Дополнительная информация	Информация из лог-файла.
Устройство	Устройство, обнаружившее и поместившее данное сетевое соединение в свой лог.

Также имеется дополнительная колонка с иконкой для быстрого создания правила на основании записи в журнале.

3.27.8.3 Создание правила для фильтрации на основе записи из лог-файла

Выполните следующие действия:

1) Кликните по иконке  в строке таблицы с нужной записью. Появится окно с параметрами правила, соответствующими параметрам строки лога. Если правило по этой строке уже создано, то заголовок окна будет называться «Редактирование правила», если такого правила еще нет, заголовок будет называться «Создание правила».

2) В открывшемся окне отредактируйте следующие параметры:

   а) название;

   б) протокол (введите номер протокола или выберите из списка известных протоколов);

   в) устройство (выберите из списка устройств);

   г) диапазон адресов источника (адрес / длина маски, т.е. количество значимых битов адреса);

   д) диапазон адресов назначения (адрес / длина маски);

   е) диапазон портов источника;

   ж) диапазон портов назначения.

3) Нажмите «Сохранить» для создания нового правила или внесения правок в старое.

Примечания

1) При открытии окна будет создано правило со следующими параметрами: протокол соответствует протоколу из лога, источник точно соответствует источнику из лога (все биты адреса значимы, один порт), назначение точно соответствует назначению из лога (все биты адреса значимы, один порт). По этим же параметрам будет произведен поиск в списке имеющихся правил. Таким образом, любое изменение параметров правила (кроме названия) будет расширением либо изменением диапазона фильтра.

2) Если в логе был IPv4-адрес, то можно ввести только адрес в формате IPv4, если в логе был IPv6-адрес, то можно ввести только адрес в формате IPv6; адрес в другом формате будет признан ошибочным.

3) Чтобы использовать в качестве источника или назначения единственный IP-адрес, т.е. сделать значимыми все биты IP-адреса, оставьте пустым поле с длиной маски после адреса. Маска будет назначена автоматически. Для IPv4 это 32 бита, для IPv6 – 128 бит. Также можно ввести соответствующее значение вручную.

4) Для того чтобы под действие правила фильтра попадал весь возможный диапазон адресов, введите в поле длину маски 0. Это будет означать, что в поле адреса нет ни одного значимого бита, т.е. совершенно неважно какой адрес.

5) Чтобы максимально расширить диапазон портов, нажмите «Любой» либо оставьте поля портов пустыми. По умолчанию диапазон портов 0-65535.

6) Диапазон портов можно вводить в любом порядке. Например, для того, чтобы правило распространялось на все порты с 10 по 20, можно ввести 20 и 10 или 10 и 20.

7) Для того чтобы использовать единственный порт, введите его в качестве начала и в качестве конца диапазона портов.

Для закрытия окна создания и редактирования правила нажмите «Отмена» или нажмите ESC или кликните иконку закрытия всплывающего окна справа от заголовка окна. При отмене никакие изменения сохранены не будут.

3.27.8.4 Поиск информации на экране «Журнал»

На экране «Журнал» имеются три независимых фильтра для выбора лог-файлов и их фильтрации.

Выбор лог-файлов

При первоначальной загрузке на экране показана информация о сетевых соединениях из всех текущих лог-файлов всех обнаруженных устройств (Анализатор). Если отсутствует лог-файл для Анализатора, это свидетельствует о серьёзной ошибке. Информация об отсутствии лог-файла для Анализатора будет показана в сообщении об ошибке над списком соединений.

Для выбора устройства выберите его наименование из списка «Устройство». После этого будет показана только информация из текущего лог-файла этого устройства и появится список «Архив», содержащий имя текущего лог-файла и всех имеющихся архивных файлов с датой последнего изменения.

Для выбора одного из архивных файлов выберите имя файла из списка «Архив». После этого будет показана информация из выбранного архивного файла.

Информация о том, какой именно архив показан, также имеется слева от списка «Архив».

Для показа информации обо всех активных соединениях выберите пункт «Все устройства» из списка «Устройство».

На экране имеется фильтр, позволяющий найти соединение или группу соединений по совпадению в комментарии, порте, протоколе или IP-адресе. Для фильтрации списка выполните следующие действия:

1) Выберите область поиска в выпадающем списке «Поиск».
2) Введите один из следующих критериев поиска в зависимости от области:
   а) точный IP-адрес или диапазон адресов (IP/маска) для поиска по IP-адресу соединения (поиск будет произведен как по источникам, так и по назначениям);
   б) номер порта или диапазон портов через тире (например, 10-20) для поиска по порту (поиск будет произведен как по источникам, так и по назначениям);

в) протокол или список протоколов через запятую (например, 33,ICMP,TCP), - можно вводить как номера, так и буквенные аббревиатуры в любом регистре (поиск будет произведен как по источникам, так и по назначениям);

г) комментарий или часть комментария для поиска по полю «Дополнительная информация».

3) Нажмите «Найти».

Для отмены фильтрации оставьте поле пустым.

Об экране «Фильтры»

Экран «Фильтры» (Администрирование → Доступ → Сетевые подключения → Фильтры) перечисляет активные правила фильтрации при создании лог-файлов сетевых соединений. Для краткости будем в дальнейшем называть их «правила для фильтрации» или просто «правила». В списке фильтров показан текущий набор правил для фильтрации. Соединения, попадающие под текущий набор правил, в лог-файл не заносятся. Правило не разрывает сетевое соединение и не запрещает создание новых соединений.

Экран «Фильтры» отображает следующую информацию, см. таблицу 27.

Таблица 27 – Экран «Фильтры»

Колонка		**Описание**
№		Номер правила.
Название правила		Необязательное название правила для фильтрации.
Протокол		Протокол передачи данных.
Источник	CIDR	CIDR-источника (IP-адрес/маска).
	Порты	Диапазон портов источника.
Назначение	CIDR	CIDR-назначения (IP-адрес/маска).

Колонка		Описание
	Порты	Диапазон портов назначения.
Устройство		Устройство, на которое распространяется данное правило.

Также имеется чекбокс для выбора правила.

3.27.8.5 Создание и редактирование правил для фильтрации

1) Выполните одно из следующих действий:

- кликните номер правила для редактирования существующего правила;
- нажмите «Создать новое правило (IPv4)» для создания нового правила для фильтрации соединений с IPv4-адресами;
- нажмите «Создать новое правило (IPv6)» для создания нового правила для фильтрации соединений с IPv6-адресами.

Появится окно с параметрами правила. Если правило по этой строке уже создано, заголовок окна будет «Редактирование правила», если такого правила еще нет, заголовок будет «Создание правила» и все поля будут пустыми, кроме поля «Устройство», в котором будет содержаться «Анализатор».

2) В открывшемся окне отредактируйте следующие параметры:

- название;
- протокол (введите номер протокола или выберите из списка известных протоколов);
- устройство (выберите из списка устройств);
- диапазон адресов источника (адрес / длина маски, т.е. количество значимых битов адреса);
- диапазон адресов назначения (адрес / длина маски);
- диапазон портов источника;

– диапазон портов назначения.

3) Нажмите «Сохранить».

Примечания.

1) Если создается IPv4-правило, то можно ввести только адрес в формате IPv4, если создается IPv6-правило, то можно ввести только адрес в формате IPv6; адрес в другом формате будет признан ошибочным. Также невозможно сменить версию IP-протокола для правила путем редактирования.

2) Чтобы использовать в качестве источника или назначения единственный IP-адрес, т.е. сделать значимыми все биты IP-адреса, оставьте пустым поле с длиной маски после адреса. Маска будет назначена автоматически. Для IPv4 это 32 бита, для IPv6 – 128 бит. Также можно ввести соответствующее значение вручную.

3) Для того чтобы под действие правила попадал весь возможный диапазон адресов, введите в поле с длиной маски 0. Это будет означать, что в поле адреса нет ни одного значимого бита, т.е. совершенно неважно, какой адрес.

4) Чтобы максимально расширить диапазон портов, нажмите «Любой» либо оставьте поля портов пустыми. По умолчанию диапазон портов 0-65535.

5) Диапазон портов можно вводить в любом порядке. Например, для того, чтобы правило распространялось на все порты с 10 по 20, можно ввести 20 и 10 или 10 и 20.

6) Для того чтобы использовать единственный порт, введите его и в качестве начала, и в качестве конца диапазона портов.

Для закрытия окна создания и редактирования правила нажмите «Отмена» или клавишу ESC или кликните на иконку закрытия всплывающего окна справа от заголовка окна. При отмене никакие изменения сохранены не будут.

3.27.8.6 Удаление правила фильтрации

Для удаления одного или нескольких правил выполните следующие действия:

1) Отметьте удаляемые правила фильтра в списке правил слева от имени.

2) Нажмите на «Удалить выбранные правила».

3) Нажмите «ОК» для подтверждения удаления.

3.27.8.7 Поиск информации на экране «Фильтры»

На экране «Фильтры» имеются три независимых фильтра для выбора правил и их фильтрации.

Выбор устройства

При первоначальной загрузке на экране показана информация о правилах для всех устройств (Анализатор).

Для выбора устройства выберите его наименование из списка «Устройство». После этого будет показан список правил для этого устройства.

Для показа информации о правилах фильтрации лог-файлов для всех устройств выберите пункт «Все устройства» из списка «Устройство».

Фильтрация правил выбранного устройства

На экране имеется фильтр, позволяющий найти правило или группу правил по совпадению в порте, протоколе, IP-адресе или по номеру правила. Для фильтрации списка выполните следующие действия:

1) Выберите область поиска в выпадающем списке «Поиск».

2) Введите один из следующих критериев поиска в зависимости от области:

а) точный IP-адрес или диапазон адресов (IP/маска) для фильтрации по IP-адресу правила (поиск будет произведен как по источникам, так и по назначениям);

б) номер порта или диапазон портов через тире (например, 10-20) для фильтрации по порту (поиск будет произведен как по источникам, так и по назначениям);

в) протокол или список протоколов через запятую (например, 33,ICMP,TCP), - можно вводить как номера, так и буквенные аббревиатуры в любом регистре (поиск будет произведен как по источникам, так и по назначениям);

г) номер правила или диапазон номеров через тире (например, 100-200) для фильтрации по номеру правила.

3) Нажмите «Найти».

Для отмены фильтрации оставьте поле пустым.

Фильтрация по типу IP-адреса

Для выбора типа IP-адреса выберите один из вариантов:

1) «IPv4» для отображения только правил для IPv4-адресов;

2) «IPv6» для отображения только правил для IPv6-адресов;

3) «Все» для отображения правил для IP-адресов всех типов.

3.27.8.8 Автоматическое создание и удаление правил для известных сетевых соединений

Правила для известных сетевых соединений могут быть созданы и удалены автоматически.

Известными считаются:

1) исходящие соединения с whois-сервером;

2) исходящие SMTP-соединения;

3) исходящие SNMP-соединения Анализатора;

4) исходящие и входящие BGP-соединения Анализатора;

5) входящие UDP-соединения Анализатора;

6) TCP-соединения Анализатора с самим собой;

Для создания правил установите флажок «автоматическая конфигурация правил для известных сетевых подключений».

Для удаления правил снимите флажок «автоматическая конфигурация правил для известных сетевых подключений».

3.28 Сервисные операции с Системой

3.28.1 Версия конфигурации

Конфигурация Системы включает в себя все настройки в экранах администрирования. Можно выполнить экспорт текущей конфигурации или импорт ранее выгруженной.

Любые изменения в экранах администрирования фиксируются, и после каждого изменения создается новая версия конфигурации. Система позволяет откатить конфигурацию на определенное время или до выбранной версии. При откате конфигурации имеется возможность вернуть настройки в прежнее состояние, т.к. фиксируются все изменения, в том числе и событие отката конфигурации.

При изменении версии Системы откат, экспорт (импорт) конфигурации становится невозможен.

3.28.1.1 История конфигурации

Перейдите на экран «История» (Администрирование → Общие настройки → История), чтобы просмотреть историю изменений конфигурации.

В таблице можно увидеть время и авторов изменений настроек Системы. Комментарии показывают, какое действие было выполнено пользователем. Комментарии можно дополнить нажав на значок «+».

Поставьте флажок около строки таблицы с нужной версией и нажмите на кнопку «Откатить конфигурацию до выбранной версии».

Если объект Системы был добавлен (удален) в последней версии, то при откате до более ранней версии он будет удален (восстановлен).

3.28.1.2 Экспорт конфигурации

Перейдите на экран «Экспорт» (Администрирование → Общие настройки → Экспорт) для выгрузки конфигурации. Данные сохраняются в xml-файле. При выборе чекбокса «Добавить в экспорт список пользователей, группы и права доступа» также будет экспортирована информация о пользователях и правах доступа. Для выгрузки нажмите на кнопку «Получить текущую конфигурацию».

3.28.1.3 Импорт конфигурации

Перейдите на экран «Импорт» (Администрирование → Общие настройки → Импорт) для загрузки конфигурации. Нажмите «Обзор» и выберите файл для загрузки данных.

При выборе галочки «Импортировать также список пользователей, группы и права доступа» будут загружены пользователи из файла.

Внимание: при импорте списка пользователей, может быть потерян доступ к Системе, если в импортируемой конфигурации отсутствуют соответствующие учетные записи.

3.29 Архивирование

3.29.1 Введение

Экран «Архивирование» (Администрирование → Общие настройки → Архивирование) позволяет выполнить резервное копирование данных – создать образ директорий диска, которые содержат базу данных, демонов, логи демонов, и в архивированном виде поместить их в /var/dbbackup/backup.

На экране «Архивирование» можно назначить задание, выполняемое по времени для создания архива или выполнить архивирование в данный момент времени.

3.29.2 Создание архива

Для запуска процесса архивирования нажмите «Запустить сейчас». Должно появиться диалоговое окно «Архивирование системы будет запущено в течение 5 минут».

3.29.3 Архивирование по расписанию

Для включения архивирования по расписанию выполните следующие действия:

1) Установите флажок «Включить архивирование».
2) В списке списка «Периодичность» выберите насколько часто должно проводиться резервное копирование данных.
3) Укажите время запуска процедуры при помощи элемента управления «Время».
4) Нажмите «Сохранить».

Для отключения архивирования по расписанию снимите флажок «Включить архивирование».

3.29.4 Журнал архивирования

Журнал архивирования содержит информацию о запуске предыдущих заданий по архивированию и сообщения о ходе текущей задачи по архивированию, если данная задача запущена.

3.29.5 Восстановление Системы из архива

Восстановление Системы из архива доступно при условии наличия терминального доступа к серверу, на котором установлена Система.

3.30 Внешние сервера

Экран «Внешние сервера» (Администрирование → Общие настройки → Внешние сервера) позволяет настроить используемый Системой Whois-сервер.

Для проверки существования Whois-сервера введите его адрес и нажмите «Проверить». Для сохранения адреса Whois-сервера в Системе нажмите «Сохранить».

3.31 Удаление заданий подавления атак

3.31.1 Введение

Экран «Удалить подавление атак» (Администрирование → Общие настройки → Удалить подавление атак) позволяет удалить все задания подавления атак, кроме текущих.

3.31.1.1 Удаление всех заданий

Для удаления всех заданий выполните следующие действия:

1) Выберите вариант «Все задания».
2) Нажмите «Удалить».
3) Нажмите «ОК» для подтверждения удаления.

3.31.2 Удаление аномалий

3.31.2.1 Введение

Экран «Удалить аномалии» (Администрирование → Общие настройки → Удалить аномалии) позволяет удалить все DoS-аномалии, кроме текущих, настроить автоматическое удаление аномалий, а также удалить все DoS-аномалии, соответствующие критерию.

Аномалии, на которые ссылаются задания подавления атак или Фингерпринты, не удаляются. Это сделано специально, чтобы не потерять важный элемент информации, являвшийся основой при создании задания подавления атаки или Фингерпринта. Для удаления этих аномалий необходимо сначала вручную убрать на них все ссылки из заданий подавления атак и Фингерпринтов.

3.31.2.2 Удаление всех аномалий

Для удаления всех аномалий выполните следующие действия:

1) Выберите вариант «Все аномалии».
2) Нажмите «Удалить».
3) Нажмите «ОК» для подтверждения удаления.

3.31.2.3 Удаление аномалий по заданному критерию

Для удаления аномалий по заданному критерию выполните следующие действия:

1) Выберите вариант «Аномалии соответствующие критериям».
2) Укажите критерии удаления:
   - ID аномалии или список;
   - возраст;
   - продолжительность;
   - важность (высокая, средняя, низкая);
   - ресурсы (IP-адреса, наблюдаемые объекты, интерфейсы).
3) Нажмите «Удалить».
4) В появившемся окне со списком аномалий уберите отметку с тех аномалий, которые удалять не следует, если такие имеются.
5) Нажмите «Удалить» для подтверждения удаления отмеченных неактивных аномалий.

Примечание: удалить можно только завершенные аномалии. Если по введенному критерию найдены идущие в данный момент аномалии, они будут помечены как активные в окне со списком найденных аномалий и удалить их будет невозможно.

3.31.2.4 Автоматическое удаление аномалий

Анализатор автоматически удаляет самые старые закончившиеся аномалии при превышении заданного количества аномалий. Задать максимальное количество аномалий можно в конфигурационном файле Системы. По умолчанию это 10 000.

Для задания других критериев автоматического удаления аномалий выполните следующие действия:

1) Перейдите на экране «Удалить подавление атак» (Администрирование → Общие настройки → Удалить подавление атак).
2) Нажмите «Настроить».
3) Отметьте приоритеты аномалий, а также период времени, по истечении которого аномалии с данным приоритетом будут удаляться.
4) Нажмите «Сохранить настройки».

3.32 Управление БД

Экран «Управление БД» (Администрирование → Общие настройки → Управление БД) показывает текущие соединения пользователей с базой данных.

Экран предназначен для администраторов и службы технической поддержки. Он используется для отладки работы Системы, отслеживания долгих запросов к БД, аварийного выключения запросов. Пользоваться экраном должны только подготовленные администраторы и служба техподдержки.

Экран «Управление БД» отображает следующую информацию, см. таблицу 28.

Таблица 28 – Экран «Управление БД»

Колонка	**Описание**
PID	Идентификатор процесса соединения с базой.
Пользователь	Имя пользователя.
Хост	IP-адрес и порт базы данных, с которой установлено соединение.
Время выполнения, секунд	Время выполнения запроса.
Статус	Состояние запроса.

Чтобы разорвать соединения отметьте строку в таблице и нажмите «Завершить выбранные запросы».

Чтобы показать только соединения с базой данных с запросами, выполняемыми в текущий момент времени, установите флажок «Показывать только активные соединения».

Чтобы включить автоматическое обновление установите флажок «Автоматическое обновление».

3.33 RSS-лента

Пункт в меню «RSS-лента» (Администрирование → Общие настройки → RSS-лента) позволяет подписаться на RSS-ленту Системы в браузере или в почтовой программе.

RSS-лента Системы позволяет получать последнюю информацию о событиях в Системе в сжатом формате, оперативно получать информацию о начале, завершении аномалий, о статусе задач по подавлению атак, событиях изменения конфигурации Системы.

4. ПРОВЕРКА ПРОГРАММЫ

Полное описание проверки работоспособности Анализатора приведено в разделе «Методики испытаний» документа RU.09445927.425530-03 51 01 «Программа и методика испытаний»

5. СООБЩЕНИЯ СИСТЕМНОМУ ПРОГРАММИСТУ

Анализатор трафика является серверным программным обеспечением, состоящим из работающих в памяти сервисов, и не работает в интерактивном режиме.

ПРИЛОЖЕНИЕ 1

ПЕРЕЧЕНЬ ТЕРМИНОВ

В настоящем документе применяют следующие термины с соответствующими определениями.

Автономная система	Система IP-сетей и маршрутизаторов, управляемая одним или несколькими операторами и имеющая единую политику маршрутизации с Интернетом.
Детектор аномалий	Программный модуль, реализующий набор алгоритмов для обнаружения аномалий определенного типа и имеющий набор конфигурационных параметров.
Инфраструктурные элементы СПД	Набор устройств и сервисов, обеспечивающих функционирование сети, в том числе: – устройства маршрутизации и пакетной коммутации; – пакетные брандмауэры, анализаторы трафика, системы обнаружения атак; – центры обработки данных и сервера приложений; – беспроводные контроллеры и точки доступа; – устройства обеспечения физической безопасности.

Наблюдаемый объект	Совокупность объектов сети, потоков трафика и сетевых сервисов, рассматриваемая анализатором трафика как единое целое в контексте задач мониторинга обнаружения сетевых угроз.
Очистка трафика	Совокупность механизмов и алгоритмов фильтрации трафика с целью отбрасывания пакетов, классифицированных как аномальные.
Сигнатура трафика / угрозы	Описание существенных характеристик трафика (произвольного или аномального) в виде выражения на специальном языке.
Сетевые сервисы	Приложение или функциональность, поддерживаемая и обеспечиваемая инфраструктурными элементами СПД.
NetFlow	Семейство протоколов, поддерживаемых маршрутизаторами, для предоставления «слепков» трафика.

ПРИЛОЖЕНИЕ 2

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

СПД	Сеть передачи данных.
ACL	Access Control List (список управления доступом).
AS	Autonomous system (автономная система).
BGP	Border Gateway Protocol.
BIOS	Basic input/output system (базовая система ввода-вывода). Предназначается для предоставления операционной системе API-доступа к аппаратуре компьютера и подключенным к нему устройствам.
DoS-атака	Атака типа Denial-Of-Service (отказ обслуживания).
DDoS-атака	Атака типа Distributed Denial-Of-Service (распределенная атака отказа обслуживания).
SNMP	Simple Network Management Protocol.
XML	eXtensibe Markup Language, универсальный текстовый формат для хранения и передачи структурированных данных.

Лист регистрации изменений

Номера листов (страниц)					Всего листов (страниц) в докум.	№ документа	Входящий № сопроводительного документа и дата	Подп.	Дата
Изм	измененных	замененных	новых	аннулированных					
1	-	2-120	-	-	126	ИИ АЦВТ.06-14	-		11.09.2014
2	-	20	-	-	126	ИИ АЦВТ.21-14	-		22.09.2014
3	-	11,12, 120	-	-	126	ИИ АЦВТ.29-14	-		21.10.2014
4									