УТВЕРЖДЕНО

RU.09445927.425530-04 34 01-ЛУ

СИСТЕМА INVGUARD CS

Программный комплекс invGuard CS-SW

Руководство оператора

RU.09445927.425530-04 34 01

Листов 23

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата
0041	29.05.2014			

2014

АННОТАЦИЯ

В данном программном документе приведено руководство оператора по применению и эксплуатации программного комплекса invGuard CS-SW системы invGuard CS (далее Очиститель), предназначенного для исследования и фильтрации вредоносного трафика в сетях передачи данных операторов связи. Очиститель является составной частью системы защиты от сетевых атак (СЗСА) invGuard (далее Система).

В данном программном документе в разделе «Назначение программы» указаны сведения о назначении программы и информация, достаточная для понимания функций программы и ее эксплуатации.

В разделе «Условия выполнения программы» указаны условия, необходимые для выполнения программы (минимальный состав аппаратных и программных средств и т.п.).

В данном программном документе в разделе «Выполнение программы» указана последовательность действий оператора, обеспечивающих загрузку, запуск, выполнение и завершение программы, приведено описание функций, формата и возможных вариантов команд, с помощью которых оператор осуществляет загрузку и управляет выполнением программы.

В разделе «Сообщения оператору» приведены тексты сообщений, выдаваемых в ходе выполнения программы.

Оформление программного документа «Руководство оператора» 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 19.505-79, ГОСТ 19.604-78).

СОДЕРЖАНИЕ

1. НАЗНАЧЕНИЕ ПРОГРАММЫ

1.1 Функциональное назначение программы

Функциональным назначением Очистителя является исследование и фильтрация вредоносного трафика, направленного на очистку (исследование).

1.2 Эксплуатационное назначение программы

Программный комплекс разработан для применения в составе системы invGuard CS, входящей в СЗСА invGuard.

Пользователями Системы должны быть специалисты в области сетевой безопасности, ответственные за эксплуатацию телекоммуникационного оборудования.

2. УСЛОВИЯ ВЫПОЛНЕНИИЯ ПРОГРАММЫ

2.1 Минимальный состав аппаратных средств

Минимальный состав используемых технических (аппаратных) средств:

1) сервер с процессором Intel с частотой не менее 2,0 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;
5) плата TILE-Gx36.

2.2 Минимальный состав программных средств

Для функционирования программы необходимо следующие компоненты:

1) Локализованная и сертифицированная по требованиям безопасности операционная система (например, РОСА SX «КОБАЛЬТ» 1.0).

3. ВЫПОЛНЕНИЕ ПРОГРАММЫ

3.1 Вход и выход из системы

3.1.1 Введение

Управление Очистителем возможно только с помощью веб-интерфейса системы invGuard AS (далее Анализатор). Прежде чем использовать веб-интерфейс, убедитесь, что на ПЭВМ установлен веб-браузер.

3.1.2 Принятие сертификата

При первом входе в систему возможно появление сообщения о том, что сертификат, используемый на сайте, является недействительным. Для продолжения работы с веб-интерфейсом необходимо принять сертификат безопасности. В дальнейшем это предупреждение появляться не будет.

3.1.3 Вход в веб-интерфейс пользователя

Для обеспечения автоматизации процесса управления может использоваться веб-интерфейс Анализатора, в котором часть пунктов меню используются для управления заданиями Очистителя (см. рисунок 1).

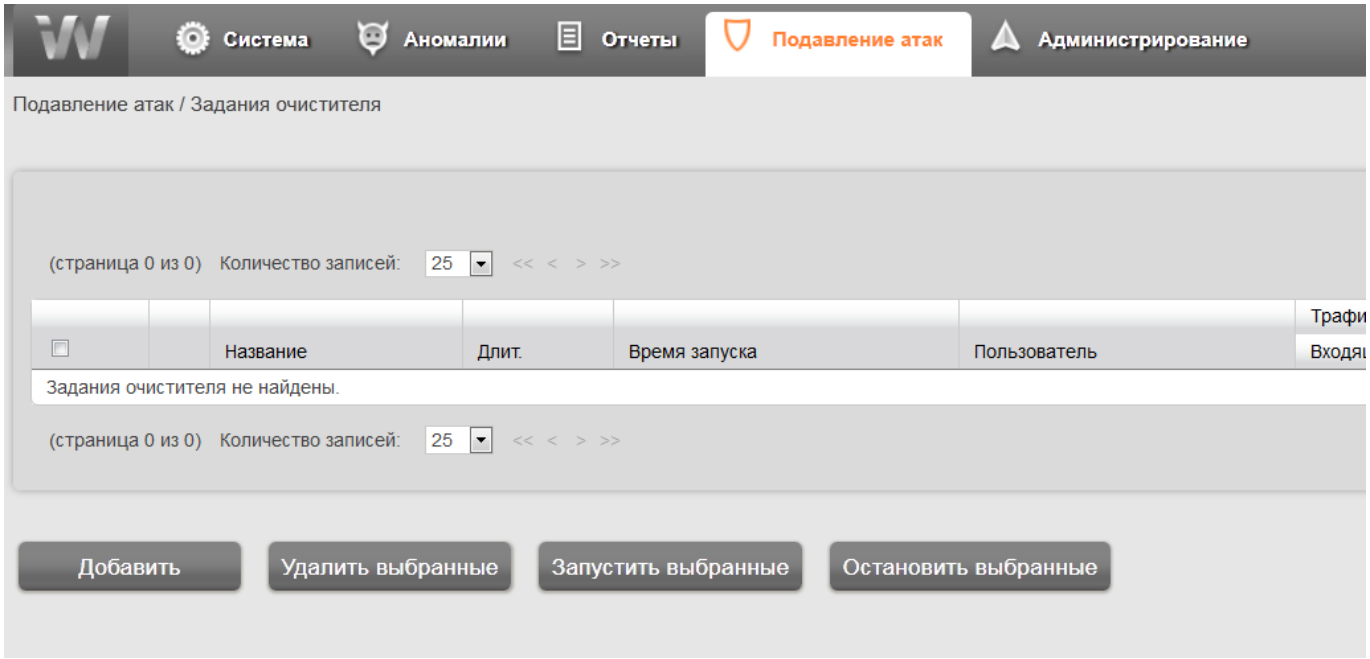

Рисунок 1 – Использование веб-интерфейса Анализатора

Для того чтобы зайти в веб-интерфейс, выполните следующие действия.

1) Запустите веб-браузер.
2) Введите https://<ip-адрес Очистителя>.

Важно: необходимо использовать безопасное соединение и настроить веб-браузер таким образом, чтобы разрешить появление всплывающих окон и прием идентификационных файлов-маркеров (cookies) от веб-интерфейса Очистителя.

3) Если появится сообщение о том, что сертификат безопасности сайта недействителен, следует разрешить использовать сертификат.
4) Введите имя пользователя и пароль.
5) Нажмите «Войти». Откроется суммарный отчет по сети (Система → Статус → Суммарный отчет).
6) Зайдите на вкладку «Задания очистки» (Подавление атак → Задания очистителя).

3.1.4 Выход из веб-интерфейса пользователя

Для выхода из интерфейса пользователя выполните следующие действия.

1) Нажмите «Выход» (с правой стороны навигационного меню).
2) Закройте браузер.

3.1.5 Командный интерфейс Очистителя

Очиститель предоставляет командный интерфейс управления по ssh.

Через command-line interface оператором возможно использование:

- включение;
- выключение;
- очистка трафика включает в себя:
  - запуск задания очистки;
  - остановка задания очистки;

- остановка всех заданий очистки;

– сбор статистики включает в себя:

- текущее состояние очистителя;
- статистика по заданиям очистки;
- статистика по сырому трафику;
- дампинг сырого трафика;
- обнаружение аномалий использования DNS-серверов;

– обработка внештатных ситуаций.

3.2 Функциональность системы

3.2.1 Параметры задания очистки

Параметры задания очистки задаются отдельным xml-файлом.

3.2.2 Статистика по заданию очистки

Очиститель ведет статистику по каждому заданию очистки и раз в минуту предоставляет её пользователю в виде xml-файла.

3.2.2.1 Статистика по состоянию очистителя

Очиститель ведет статистику по использованию процессора, памяти, количеству заданий очистки, количеству трафика и т. п. и раз в минуту выводит результат в виде xml-файла.

3.2.2.2 Статистика по raw-трафику

Очиститель по запросу пользователя ведет статистику по всему трафику, который через него проходит, и раз в пять минут формирует соответствующий xml-файл.

3.2.2.3 Конфигурационные файлы syn

Конфигурация Очистителя представлена следующими файлами, расположенными в syn/syn/config:

– config.xml, содержит общие параметры Очистителя;

– config.txt, описывает параметры логирования;

– statparams.xml, описывает параметры собираемой по сырому трафику статистики.

3.2.2.4 Интерфейс пользователя

Очиститель управляется посредством командной утилиты synctl, описанной в 3.3.2.1. Информация о текущем состоянии Очистителя, статистические данные доступны в виде объектов файловой системы.

3.3 Модели поведения системы

3.3.1 Описание поведения системы

3.3.1.1 Запуск системы

Запуск системы осуществляется в следующем порядке:

– После загрузки операционная система запускает модуль управления Очистителем при помощи init.d-скрипта и утилиты synctl;

– По команде startsystem утилиты synctl происходит загрузка образа Очистителя в Tilera и его запуск.

3.3.1.2 Остановка системы

Остановка системы происходит в следующем порядке:

– Операционная система или утилита synctl посылает сигнал завершения работы модулю управления при помощи команды stopsystem утилиты synctl;

– Модуль управления выполняет действия по остановке системы.

3.3.1.3 Изменение конфигурационных параметров

Изменение конфигурации системы осуществляется в следующем порядке:

– Пользователь редактирует один или несколько конфигурационных файлов;

– Пользователь запускает утилиту synctl с командой reconfigure;

– Применение новых конфигурационных параметров происходит по сигналу модуля управления, при этом перечитывается конфигурационный файл настроек Очистителя;

– Модуль управления выполняет необходимые действия по конфигурированию системы и докладывает результат утилите synctl при помощи ответного сообщения;

– Утилита synctl выводит пользователю сообщение о результате конфигурирования системы.

3.3.1.4 Запуск задания очистки

Запуск задания очистки осуществляется в следующем порядке.

– Пользователь создаёт файл с параметрами задания очистки в каталоге /syn/mitigs;

– Пользователь запускает утилиту synctl командой start с указанием пути к файлу, содержащему параметры задания очистки трафика;

– Утилита synctl посылает модулю управления сообщение start для запуска задания очистки трафика;

– Модуль управления выполняет действия, необходимые для запуска задания очистки, и путем ответного сообщения докладывает результат утилите synctl;

– Утилита synctl выводит пользователю сообщение о результате запуска задания очистки.

3.3.1.5 Остановка задания очистки

Задание очистки может быть остановлено при помощи утилиты synctl.

Остановка задания очистки по запросу пользователя осуществляется в следующем порядке.

– Пользователь вызывает утилиту synctl с командой stop и идентификатором задания очистки, которое следует остановить;

– Утилита synctl посылает сообщение stop модулю управления о необходимости остановить указанное задание очистки;

– Модуль управления выполняет действия по остановке задания очистки и в ответном сообщении докладывает результат выполнения утилите synctl;

– Утилита synctl выводит пользователю результат остановки задания очистки.

3.3.1.6 Очистка трафика

В режиме очистки трафика решаются следующие задачи:

– очистка трафика согласно заданным правилам;

– сбор и агрегация статистики по количеству отброшенных/пропущенных пакетов, а также статистики по специфическим для фильтров характеристикам.

Модуль фильтров получает пакеты от модуля ввода. Если пакет не подлежит фильтрации, он сразу отправляется на модуль вывода, в противном случае он подвергается соответствующим его сигнатуре методам исследования. Далее пакет может быть либо отброшен, либо передан модулю вывода.

Каждый фильтр считает базовую статистику по отброшенным/полученным/ необработанным пакетам для каждого задания очистки и по запросу передает эту статистику модулю статистики для агрегации. Модуль статистики каждую минуту

выдает агрегированную статистику по каждому заданию очистки трафика в виде xml-файла.

Для каждого задания очистки существует период времени, в течение которого оно должно проводиться. Модуль управления завершает задание очистки в случае, если время его истекло.

3.3.1.7 Сбор статистики по сырому трафику

Весь трафик, поступающий на Очиститель, может подвергаться исследованию на предмет расчёта разного рода статистики. Поскольку процедура фильтрации трафика является более приоритетной задачей, модуль статистики не должен задерживать пакеты на выходе модуля ввода. Модуль статистики никому не передает пакеты для дополнительного исследования.

Раз в пять минут модуль статистики выдает статистику по сырому трафику в виде xml-файла.

3.3.1.8 Сбор статистики по состоянию очистителя

Модуль статистики ведет мониторинг состояния Очистителя и каждые пять минут выдает статистику по использованию ресурсов Очистителя в виде xml-файла.

3.3.1.9 Дампинг сырого трафика

Модуль статистики может по запросу пользователя собирать образцы пакетов сырого трафика для выбранного задания очистки и сохранять их в бинарном виде. Одновременно может вестись несколько процессов дампинга трафика.

Запуск дампинга осуществляется при помощи команды startdumping утилиты synctl с указанием идентификатора задания очистки и названием файла, в который будут складываться сырые пакеты. Утилита synctl посылает сообщение модулю статистики о начале процесса сбора образцов сырого трафика для данного задания очистки. Задание очистки должно быть активно в данный момент. Если задание очистки в данный момент не активно, утилита synctl выдает соответствующее сообщение об ошибке.

В случае успеха запуска процедуры дампинга в syslog делается запись об успешном запуске процедуры дампинга.

Остановка дампинга производится либо пользователем при помощи команды synctl stopdumping, либо по окончанию процедуры очистки, либо по достижении файлом максимального размера, указанного в конфигурационном файле очистителя. В случае остановки процедуры дампинга в syslog отсылается запись об остановке дампинга. Пользователь должен перезапустить дампинг вручную.

3.3.1.10 Внештатные ситуации

Управляющий модуль должен иметь возможность перезапускать сам себя в случае ошибки. Управляющий модуль с периодом, описанным в конфигурационном файле, опрашивает другие модули на предмет их состояния. В случае, если модуль находится в состоянии ошибки либо выгружен, то он перезапускается управляющим модулем.

Если система не может восстановить нормальную работу в течение 10 секунд с момента возникновения ошибки, она должна завершить работу и направить трафик по его обычному пути.

Факт ошибки и результат перезапуска сохраняется в виде файла в каталоге syn/syn/alerts/.

Перезапускаются ли задания очистки после перезапуска модулей, определяется пользователем системы в конфигурационном файле.

3.3.2 Спецификация функций управления

3.3.2.1 Утилита synctl

Пользовательский интерфейс системы представлен утилитой synctl, которая служит для управления заданиями очистки на Очистителе.

3.3.2.1.1 Перечень команд утилиты synctl

Таблица 1 – Команды утилиты synctl

Команда	Описание
startsystem	Запустить систему
stopsystem	Остановить систему
start	Запустить задание очистки
stop	Остановить задание очистки
stopall	Остановить все задания очистки
list	Список запущенных заданий очистки
reconfigure	Перечитать конфигурационные файлы
startdumping	Запустить дампинг сырого трафика для данного задания очистки
stopdumping	Остановить дампинг сырого трафика
settime xxxx	Установить время на Tilera
gettime	Получить текущее время с Tilera
ping	Проверить состояние Очистителя на Tilera

startsystem

Система может быть запущена при помощи вызова утилиты synctl с параметром startsystem.

Утилита synctl запускает модуль управления без параметров и дожидается старта модуля управления. Модуль управления выполняет основные действия по инициализации системы.

Доступность модуля управления проверяется на основании ответа на сообщение ping утилиты synctl.

В случае успеха пользователю выводится сообщение «Система запущена». (SUCCESS в режиме noverbose).

В случае ошибки пользователю выводится сообщение о неудачном запуске системы. (FAILED с последующим описанием ошибки в режиме noverbose).

stopsystem

Система может быть остановлена при помощи вызова утилиты synctl с параметром stopsystem.

Утилита synctl посылает сообщение модулю управления и дожидается ответного сообщения для того, чтобы узнать о результате остановки системы. Далее утилита synctl дожидается исчезновения из системы всех демонов, соответствующих модулям системы. Если в течение 10 секунд данные демоны все ещё числятся в списке процессов, утилита synctl посылает им сигнал «kill -9».

В случае успеха пользователю выводится сообщение «Система остановлена». (SUCCESS в режиме noverbose).

В случае ошибки пользователю выводится сообщение о неудачной остановке системы (FAILED с последующим описанием ошибки в режиме noverbose).

start

Для запуска задания очистки пользователь создает файл с параметрами задания очистки, например, mitig.xml и выполняет команду synctl start mitig.xml.

Утилита synctl проверяет файл mitig.xml на соответствие формату, и посылает сообщение модулю управления. Модуль управления выполняет действия по запуску задания очистки и отправляет ответное сообщение с результатом выполнения утилите synctl.

В случае успеха synctl выводит в основной поток сообщение об успешном запуске задания очистки (SUCCESS в режиме noverbose).

Если задание очистки запустить не удается, synctl выводит сообщение об ошибке в стандартный поток (FAILED с последующим описанием ошибки в режиме noverbose).

stop

Для остановки задания очистки пользователь выполняет команду synctl stop mitig_id.

Здесь mitig_id – идентификатор останавливаемого задания очистки.

Утилита synctl посылает сообщение модулю управления и дожидается ответного сообщения для того, чтобы узнать результат операции.

В случае успеха пользователю выводится сообщение «Задание очистки mitig_id остановлено» (SUCCESS в режиме noverbose).

В случае ошибки пользователю выводится сообщение о неудачной остановке задания очистки (FAILED с последующим описанием ошибки в режиме noverbose).

stopall

synctl останавливает все задания очистки, ведущиеся в данный момент.

Утилита synctl посылает сообщение модулю управления и дожидается ответного сообщения для того, чтобы узнать результат операции.

В случае успеха пользователю выдается сообщение об успешном завершении операции (SUCCESS в режиме noverbose).

В случае ошибки пользователю выводится сообщение об ошибке (FAILED с последующим описанием ошибки в режиме noverbose).

list

Система выводит список заданий очистки, активных в данный момент. Список активных заданий очистки определяется по содержимому каталога syn/syn/.mitigs.

reconfigure

Перечитывает конфигурационные файлы и применяет содержащиеся в нем изменения.

Утилита synctl посылает сообщение модулю управления и дожидается ответного сообщения для того, чтобы узнать результат операции.

В случае успеха пользователю выводится сообщение «Конфигурация успешно изменена» (SUCCESS в режиме noverbose).

В случае неудачи пользователю выводится сообщение «Конфигурация не может быть изменена» (FAILED с последующим описанием ошибки в режиме noverbose).

startdumping

Для запуска процедуры дампинга пользователь выполняет команду:

synctl startdumping mitigID filename,

где:

– mitigID – ID задания очистки, для которого собирается дамп трафика;

– filename – название файла с дампом трафика для данного задания очистки.

Утилита synctl посылает сообщение модулю статистики и дожидается ответного сообщения для того, чтобы узнать результат операции.

В случае успеха пользователю выводится сообщение «Дампинг начат» (SUCCESS в режиме noverbose).

В случае неудачи пользователю выводится сообщение «Дампинг не может быть запущен» (FAILED с последующим описанием ошибки в режиме noverbose).

stopdumping

Для остановки дампинга пользователь выполняет команду:

synctl stopdumping mitigID filename,

где:

– mitigID – ID задания очистки, для которого собирается дамп трафика;

– filename – название файла с дампом трафика для данного задания очистки.

Утилита synctl посылает сообщение модулю статистики и дожидается ответного сообщения для того, чтобы узнать результат операции.

В случае успеха пользователю выводится сообщение «Дампинг остановлен» (SUCCESS в режиме noverbose).

В случае неудачи пользователю выводится сообщение «Дампинг не может быть остановлен» (FAILED с последующим описанием ошибки в режиме noverbose).

Если дампинг остановлен в данный момент времени, то это не считается ошибкой.

settime

Утилита synctl посылает сообщение в Тилеру unix time stamp и дожидается ответного сообщения для того, чтобы узнать результат операции.

В случае успеха пользователю выводится сообщение SUCCESS в режиме noverbose.

В случае неудачи пользователю выводится сообщение FAILED с последующим описанием ошибки в режиме noverbose.

gettime

Утилита synctl запрашивает из Тилеры unix time stamp и дожидается ответного сообщения для того, чтобы узнать результат операции.

В случае успеха пользователю выводится unix time stamp.

В случае неудачи пользователю выводится сообщение FAILED с последующим описанием ошибки в режиме noverbose.

ping

Модуль управления может посылать сообщение ping для проверки доступности и управляемости остальных модулей системы.

Любой модуль обязан ответить на данное сообщение в течение интервала времени, указанного в конфигурационном файле Очистителя в качестве атрибута ping_timeout элемента control.

4. СООБЩЕНИЯ ОПЕРАТОРУ

Для выдачи пользователю диагностических сообщений о возникающих ошибках системы используется каталог etc/syn/alerts/, содержащий файлы с информацией о событиях системы.

Оповещение представляет собой xml-файл с именем TS.xml, где TS отражает время создания оповещения. Корневой элемент файла называется alert и содержит атрибуты type, severity, name, и др. Тривиальным будем называть оповещение, которое описывается атрибутами type, severity, name, ts и, при необходимости, параметром description. Типы оповещений задаются атрибутом name элемента alert и описаны в таблице 3.

Таблица 2 – Атрибуты событий системы

Name	Type	Severity	Описание

Name	Type	Severity	Описание
output_fault	error	hi	Модуль вывода не успевает обрабатывать пакеты. Тривиальное оповещение.
mitig_run_failed	error	hi	Не удалось запустить задание очистки трафика. Параметр “description” содержит описание причины, по которой не удалось начать процесс очистки трафика. Тривиальное сообщение.
mitig_stop_failed	error	hi	Не удалось остановить задание очистки. Параметр «description» содержит описание причины, по которой не удалось остановить задание очистки. Тривиальное сообщение.
config_error	error	hi	Ошибка конфигурации системы. Параметр «description» содержит описание причины, по которой не удалось применить новые параметры системы. Тривиальное сообщение.
start_failed	error	hi	Ошибка запуска системы. Параметр «description» содержит описание причины, по которой не удался запуск системы. Тривиальное сообщение.
module_error	error	hi	Ошибка в модуле системы. Параметр «description» содержит описание ошибки в модуле. Тривиальное сообщение.
restart_module_failed	error	hi	Не удалось перезапустить модуль системы. Параметр «description» содержит описание причины, по которой не удался перезапуск системы. Тривиальное сообщение.
dns_baseline	warning	hi	Частота DNS-запросов отличается от тренда.

ПРИЛОЖЕНИЕ 1

ПЕРЕЧЕНЬ ТЕРМИНОВ

В настоящем документе применяют следующие термины с соответствующими определениями.

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.
NetFlow	Семейство протоколов, поддерживаемых маршрутизаторами, для предоставления "слепков" трафика.

ПРИЛОЖЕНИЕ 2

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

XML	eXtensibe Markup Language, универсальный текстовый формат для хранения и передачи структурированных данных.
SSH	Secure Shell, сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой и туннелирование TCP-соединений.

Лист регистрации изменений

Номера листов (страниц)					Всего листов (страниц) в докум.	№ документа	Входящий № сопрово дительного документа и дата	Подп.	Дата
Изм	изменен ных	заме ненных	новых	аннулиро ванных					
1	-	2-24	-	-	24	ИИ АЦВТ.11-14	-		11.09.2014
1	-	2-22	-	-	22	ИИ АЦВТ.32-14	-		21.10.2014