УТВЕРЖДЕН

RU.АЦВТ.425760-01 31 01-ЛУ

Программный комплекс invGUARD CS-SW 2.0

Описание применения

RU.АЦВТ.425760-01 31 01

Листов 10

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата
0163	20.07.2020			

2020

АННОТАЦИЯ

В данном программном документе приведено описание применения программного изделия «Программный комплекс invGUARD CS-SW 2.0» (далее – Очиститель или ПК invGUARD CS-SW 2.0).

Очиститель предназначен для защиты информационной системы, её средств, систем связи и передачи данных, а также автоматизированной системы управления и её компонентов от угроз безопасности информации, направленных на отказ в обслуживании.

В данном программном документе в разделе «Назначение программы» приведено описание назначения программы, возможности данной программы, а также ее основные характеристики и ограничения, накладываемые на область применения программы.

В разделе «Условия применения» указаны условия, необходимые для выполнения программы (требования к необходимым для данной программы техническим средствам, и другим программам, общие характеристики входной и выходной информации).

В разделе «Входные и выходные данные» указаны сведения о входных и выходных данных.

Оформление программного документа «Описание применения» 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 19.502-78, ГОСТ 19.604-78).

СОДЕРЖАНИЕ

1. НАЗНАЧЕНИЕ ПРОГРАММЫ

1.1 Назначение программы

Очиститель предназначен для использования в информационных системах (ИС) и автоматизированных системах управления (АСУ), функционирующих на базе вычислительных сетей для защиты их от угроз безопасности информации, направленных на отказ в обслуживании, посредством фильтрации вредоносного трафика, а также для сбора статистики по обработанному трафику.

1.2 Возможности программы

Очиститель обеспечивает обнаружение и блокирование в направленном на его вход трафике следующей основной угрозы безопасности информации, направленной на отказ в обслуживании:

преднамеренное несанкционированное воздействие на ИС или АСУ со стороны внешних нарушителей, действующих из информационно-телекоммуникационных сетей, в том числе сетей международного информационного обмена с целью довести её до отказа, то есть создание таких условий, при которых пользователи не могут получить доступ к предоставляемым системным ресурсам, либо этот доступ затруднён.

К таким угрозам безопасности относятся как атаки типа отказ в обслуживании (DoS-атаки), так и распределенные DoS-атаки (DDoS-атаки).

1.3 Основные характеристики программы

Очиститель обеспечивает возможность выполнения перечисленных ниже функций:

1) Интеллектуальная фильтрация сетевого трафика, на основании полученных заданий:

- от программных комплексов invGUARD AS-SW или invGUARD AI-SW (анализаторов трафика);

- от внешних программ посредством собственного программного интерфейса управления (API);

- сформированных с использованием собственного графического интерфейса пользователя.

2) Сбор статистики о пропущенном и обработанном трафике, отображение ее в пользовательском интерфейсе и передача анализатору трафика или другой программе с использованием собственного API.

1.4 Ограничения, накладываемые на область применения программы

При применении Очистителя необходимо избежать маршрутной петли (routing loops).

Типовая схема применения Очистителя в ИС и АСУ – см. Рисунок 1.

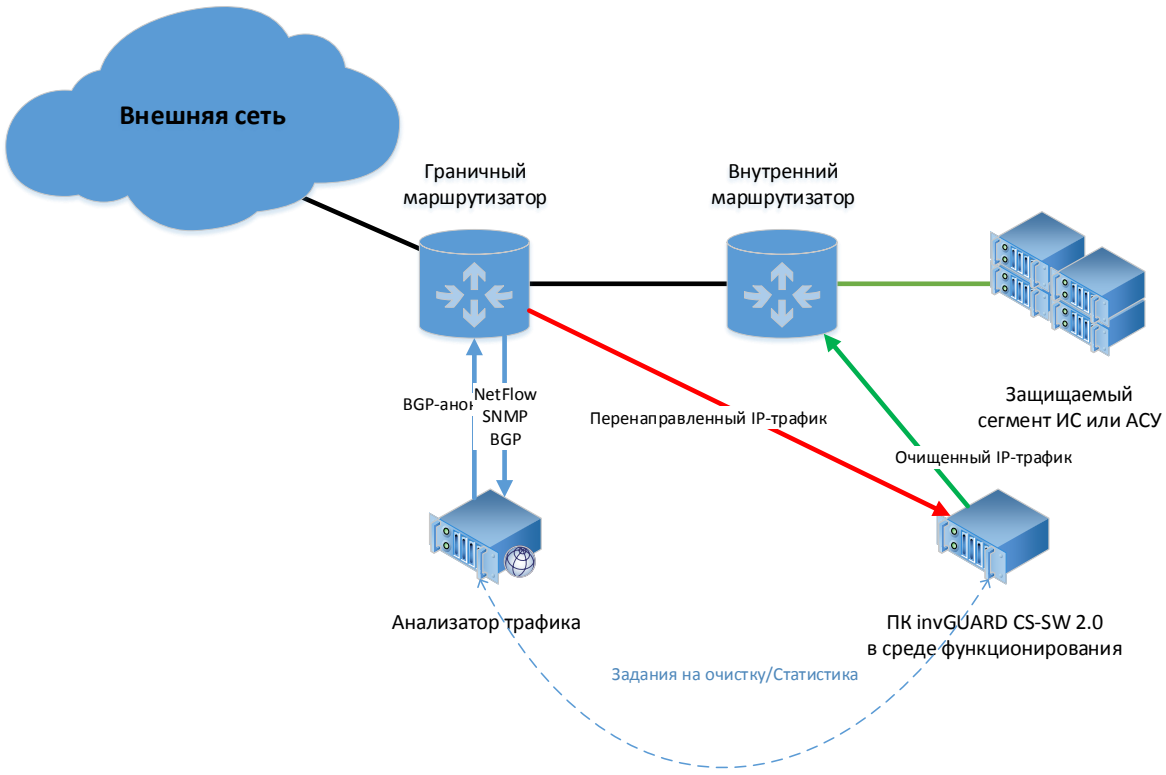

Рисунок 1 – Типовая схема применения Очистителя в ИС и АСУ

2. УСЛОВИЯ ПРИМЕНЕНИЯ

2.1 Требования к техническим (аппаратным) средствам

Минимальный состав используемых технических (аппаратных) средств:

1) сервер на базе процессора Intel с 8 и более вычислительными ядрами и частотой не менее 2,0 ГГц;

2) оперативная память объемом не менее 32 Гб;

3) жесткий диск объемом 500 Гб и выше;

4) сетевой порт Ethernet для управления;

5) двухпортовая сетевая карта Intel, поддерживающая технологию DPDK для обеспечения пропуска входящего и исходящего трафика. Плата должна быть реализована на чипсете из списка http://dpdk.org/doc/nics.

2.2 Требования к программным средствам (другим программам)

Очиститель функционирует под управлением операционных систем Debian версий 9, 10.

2.3 Общие характеристики входной информации

В качестве входных данных Очиститель принимает ответвлённый (перенаправленный посредством BGP-анонса) трафик (далее – входящий трафик), задания, полученные от анализаторов трафика и внешних программ посредством собственного программного интерфейса управления (API), а так же задания сформированные с использованием собственного графического интерфейса пользователя.

2.4 Общие характеристики выходной информации

Выходными данными являются отфильтрованный (очищенный) трафик (далее – исходящий трафик), статистические отчеты об обработанном трафике, записи журналов системных событий.

2.5 Требования и условия организационного характера

Для обеспечения работоспособности программы, оперативный персонал службы, ответственной за эксплуатацию (перечисленный в разделе «Сведения о закреплении программного изделия при эксплуатации» программного документа

RU.АЦВТ.425760-01 30 01 «Формуляр») должен один раз в неделю проводить проверку правильности работы и загрузки.

2.6 Требования и условия технологического характера

Для работы программы не требуется обеспечения каких-либо особых требований и условий технологического характера.

3. ОПИСАНИЕ ЗАДАЧИ

Описание задачи и методы её решения приведены в разделе «Описание логической структуры» документа RU.АЦВТ.425760-01 13 01 «Описание программы».

4. ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

4.1 Сведения о входных данных

Входными данными очистителя являются:

1) входящий трафик;

2) задания, полученные от анализаторов трафика и внешних программ посредством собственного программного интерфейса управления (API), а так же задания сформированные с использованием собственного графического интерфейса пользователя, а именно:

- сервисные функции;
- функции конфигурации;
- функции сохранения дампа трафика.

4.2 Сведения о выходных данных

Выходными данными очистителя являются:

1) исходящий трафик;

2) сохраненные дампы трафика;

3) журналы системных событий;

4) данные о:

- состоянии и статистике работы Очистителя;
- состоянии и статистике работы заданий Очистителя;
- статистике по входящему трафику.

ПРИЛОЖЕНИЕ 1

ПЕРЕЧЕНЬ ТЕРМИНОВ

В настоящем документе применяют следующие термины с соответствующими определениями.

Маршрутная петля (routing loops)	это маршруты в сети передачи данных, которые приводят на один и тот же маршрутизатор более одного раза. Появление маршрутных петель нежелательно, так как трафику приходится проходить дополнительный путь для того, чтобы прибыть на тот же самый маршрутизатор. Таким образом, происходит задержка трафика, либо трафик не доставляется сетям-получателям. Из-за маршрутных петель сеть передачи данных подвергается избыточной нагрузке, что приводит к большому числу операций по обработке поступающего трафика на причастных маршрутизаторах.
Ответвлённый трафик	подлежащий контролю сетевой трафик, направленный на устройство анализа через специальные сетевые ответвители, установленные в контролируемой сети.

ПРИЛОЖЕНИЕ 2

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

Border Gateway Protocol (динамический протокол маршрутизации).

DoS-атака	Сетевая атака типа Denial-Of-Service (отказ в обслуживании).
DDoS-атака	Сетевая атака типа Distributed Denial-Of-Service (распределенная атака отказа в обслуживании).
IP	Internet Protocol («межсетевой протокол») – маршрутизируемый протокол сетевого уровня стека TCP/IP. Именно IP стал тем протоколом, который объединил отдельные компьютерные сети во всемирную сеть Интернет.
ИС	Информационная система.
АСУ	Автоматизированная система управления.

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					