УТВЕРЖДЕН

RU.АЦВТ.62.01.29-01 31 01-ЛУ

Программный комплекс invGUARD СЕКАТОР

Описание применения

RU.АЦВТ.62.01.29-01 31 01

Листов 18

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата
0189	12.01.2024			

2024

АННОТАЦИЯ

В данном программном документе приведено описание применения программного изделия «Программный комплекс invGUARD СЕКАТОР» (далее – ПК invGUARD СЕКАТОР, Очиститель или программа).

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 статистических данных 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 (API);

- сформированных с использованием собственного графического интерфейса пользователя.

2) Сбор статистических данных о пропущенном и обработанном трафике, отображение их в пользовательском интерфейсе и передача Анализатору трафика или другой программе с использованием собственного API.

1.4 Ограничения, накладываемые на область применения программы

1.4.1 При применении Очистителя необходимо избежать маршрутной петли (routing loops) – см. Рисунок 1.

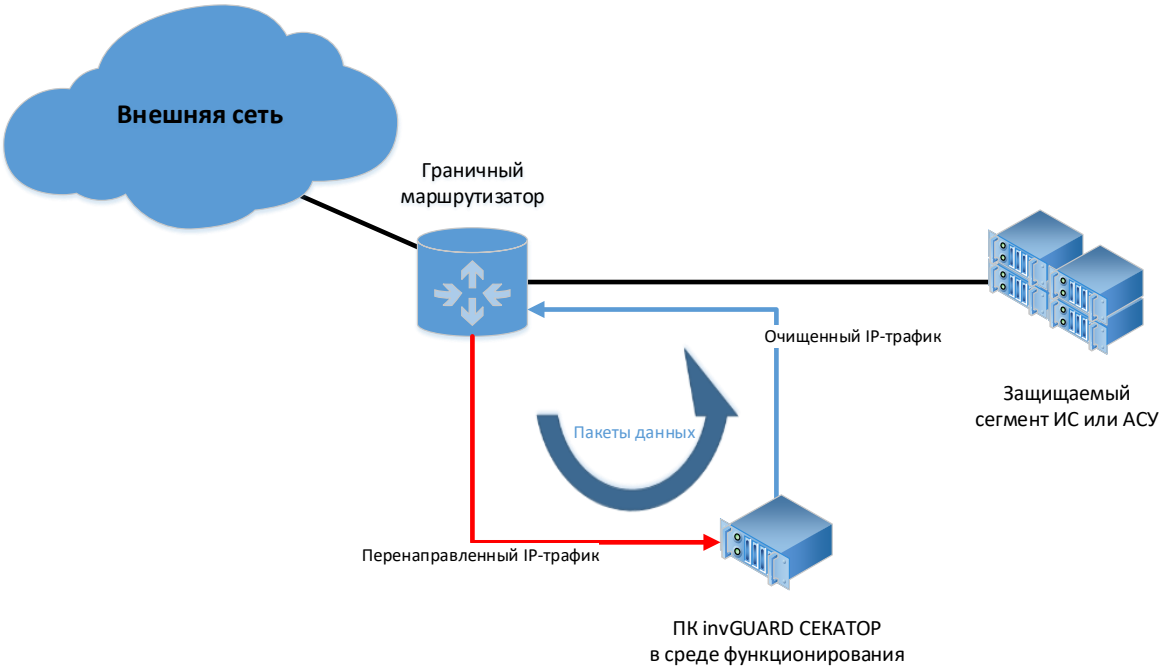

Рисунок 1 – Схема маршрутной петли

2. УСЛОВИЯ ПРИМЕНЕНИЯ

2.1 Требования к техническим (аппаратным) средствам

Минимальный состав используемых технических (аппаратных) средств:

1) сервер на базе процессора Intel Xeon 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) сетевая карта, поддерживающая технологию XDP для обеспечения пропуска входящего и исходящего трафика.

2.2 Требования к программным средствам (другим программам)

Очиститель функционирует под управлением операционной системы Debian версии 12 или или Astra Linux Server 1.8.1.

2.3 Общие характеристики входной информации

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

2.4 Общие характеристики выходной информации

Выходной информацией является отфильтрованный (очищенный) трафик (далее – исходящий трафик), данные о заданиях и работе программы, отображаемые в графическом интерфейсе пользователя, статистические данные об обработанном трафике, записи журналов системных событий, сохраненные дампы трафика.

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.62.01.29-01 30 01 «Формуляр») должен один раз в неделю проводить проверку правильности работы.

2.6 Требования и условия технического и технологического характера

Очиститель может применяться как с использованием Анализатора трафика, так и без.

Логически Очиститель подключается к двум сетям:

Внешней сети – сеть, из которой приходит трафик, требующий очистки;

Внутренней сети – сеть, в которой расположены защищаемые ресурсы.

Используется асимметричная схема подключения, при которой Очиститель «видит» трафик только в одном направлении – из внешней сети во внутреннюю.

В нормальном режиме работы вычислительной сети («Без атаки») трафик из внешней сети направляется непосредственно во внутреннюю сеть. Очиститель не оказывается влияние на трафик.

В аномальном режиме работы вычислительной сети («Под атакой») маршрут прохождения трафика в защищаемую сеть изменяется посредством отправки BGP-анонса на пограничный маршрутизатор, и трафик из внешней сети направляется во внутреннюю сеть через Очиститель. Маршрут обратного трафика (из защищаемой сети во внешнюю сеть) в данном случае не изменяется.

Возможно использование Очистителя в режиме постоянной фильтрации трафика из внешней во внутреннюю сеть. В таком случае схема его применения аналогична варианту «Под атакой».

Для обеспечения работы Очистителя требуется реализация схемы включения в сегмент вычислительной сети с учетом типовых схем применения.

2.6.1 Типовая схема применения Очистителя в ИС и АСУ «Без атаки» с использованием Анализатора трафика – см. Рисунок 2.

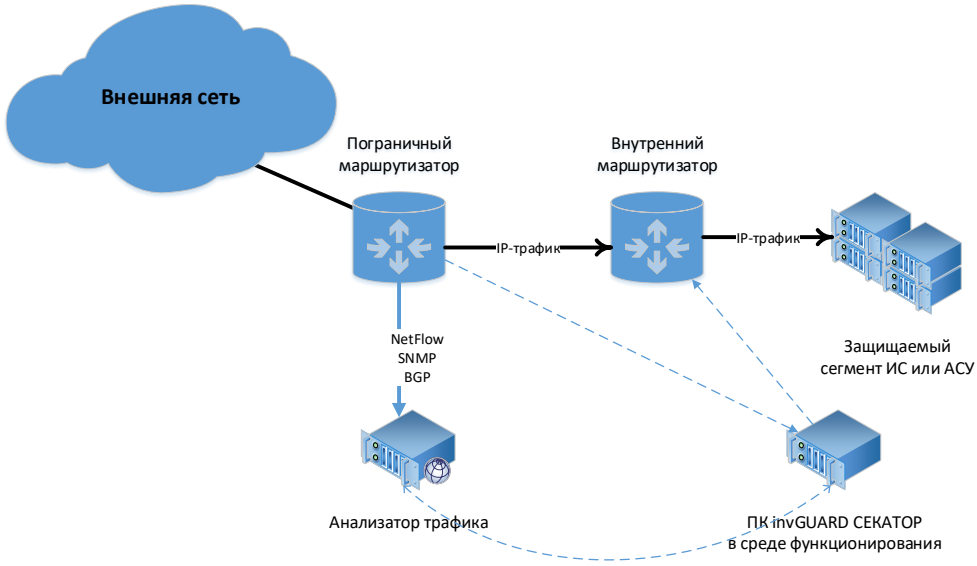

Рисунок 2 – Типовая схема применения Очистителя в ИС и АСУ «Без атаки» с использованием Анализатора трафика

2.6.2 Типовая схема применения Очистителя в ИС и АСУ «Под атакой» с использованием Анализатора трафика – см. Рисунок 3.

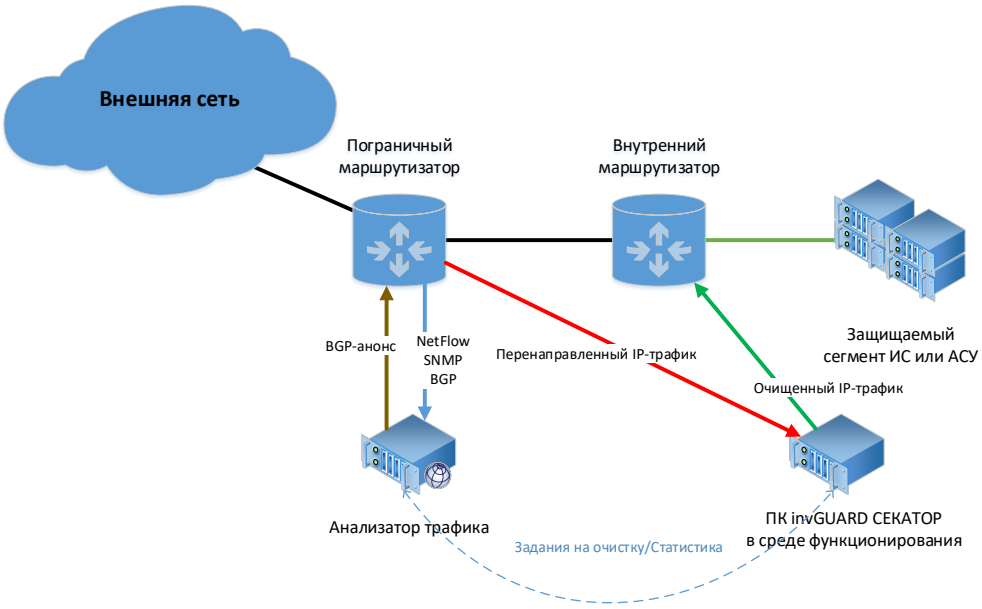

Рисунок 3 – Типовая схема применения Очистителя в ИС и АСУ «Под атакой» с использованием Анализатора трафика

2.6.3 Типовая схема применения Очистителя в ИС и АСУ «Без атаки» без использования Анализатора трафика – см. Рисунок 4.

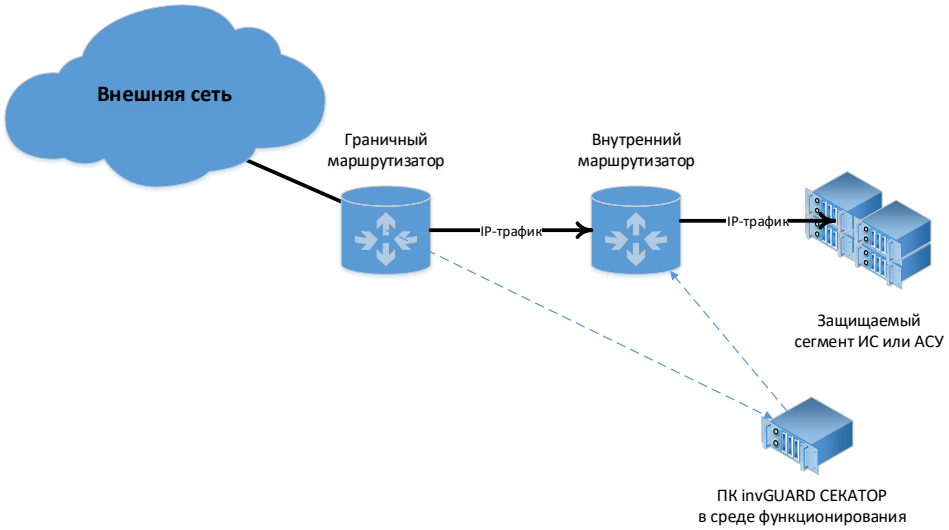

Рисунок 4 – Типовая схема применения Очистителя в ИС и АСУ «Без атаки» без использования Анализатора трафика

2.6.4 Типовая схема применения Очистителя в ИС и АСУ «Под атакой» без использования Анализатора трафика – см. Рисунок 5.

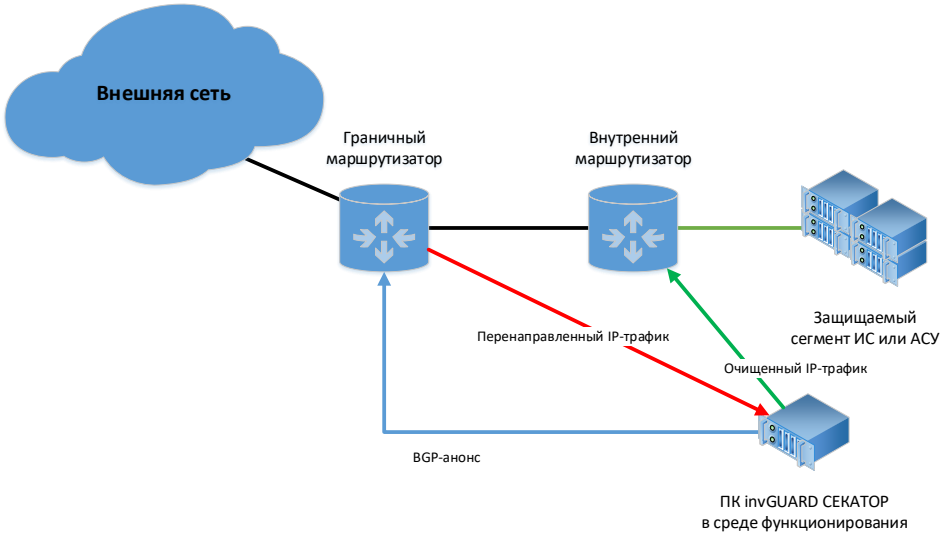

Рисунок 5 – Типовая схема применения Очистителя в ИС и АСУ «Под атакой» без использования Анализатора трафика

3. ОПИСАНИЕ ЗАДАЧИ

3.1 Определения задачи

Основная задача, решаемая Очистителем – интеллектуальная фильтрация направленного на его вход трафика с блокированием вредоносной составляющей и пропуском легитимной.

3.2 Методы решения

Очиститель осуществляет прием трафика, перенаправленного маршрутизатором в соответствии с полученным BGP-анонсом, который сформирован либо Анализатором трафика, либо самим Очистителем.

Очиститель осуществляет очистку входящего трафика согласно заданным правилам фильтрации – заданиям Очистителя. Источником пакетов служит буфер ввода сетевых портов.

Задания Очистителя содержат перечень используемых фильтров, их параметры и порядок выполнения фильтров.

Для обработки служебного трафика, такого как ARP, NDP, LACP, пакет отправляется в сетевой стек ОС.

Если при выполнении фильтров в обрабатываемом трафике обнаруживается TCP-пакет с установленным флагом SYN, то формируется ответ на такой TCP-пакет (SYN ACK). Очиститель выступает в роли SYN-прокси, и по результатам установки соединения с источником указанного выше TCP-пакета, принимается решение доверять или нет IP-адресу источника TCP-пакетов.

При обнаружении простаивающих TCP-сессий, Очиститель генерирует TCP-пакеты с флагами FIN или RST для сброса таких сессий.

В результате работы Очистителя принимается одно из следующих решений:

пропустить пакет;

отбросить пакет.

Пакеты, не соответствующие ни одному из заданий Очистителя, не обрабатываются и направляются на выходной интерфейс.

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 также 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.

Анализатор трафика	программный или программно-аппаратный комплекс, позволяющий считывать сетевой трафик или информацию о сетевом трафике, анализировать полученные данные и выявлять признаки аномального трафика, в том числе признаки DoS/DDoS-атак.
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 маршрутизаторах.

Ответвлённый трафик	подлежащий контролю сетевой трафик, направленный на устройство анализа через специальные сетевые ответвители, установленные в контролируемой сети.

ПРИЛОЖЕНИЕ 2

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

API	(Application programming interface – интерфейс программирования приложения) – программный интерфейс, то есть описание способов взаимодействия одной компьютерной программы с другими программами.
ARP	Address Resolution Protocol (протокол определения адреса) – протокол в компьютерных сетях, предназначенный для определения MAC-адреса другого компьютера по известному IP-адресу.
BGP	Border Gateway Protocol (динамический протокол маршрутизации).
DoS-атака	Сетевая атака типа Denial-Of-Service (атака на отказ в обслуживании).
DDoS-атака	Сетевая атака типа Distributed Denial-Of-Service (распределенная атака на отказ в обслуживании).
eBPF	extended Berkeley Packet Filter - технология, которая может запускать программы в привилегированном режиме, таком как ядро операционной системы.
IP	Internet Protocol («межсетевой протокол») – маршрутизируемый протокол сетевого уровня стека TCP/IP. IP стал протоколом, который объединил отдельные компьютерные сети во всемирную сеть Интернет.
LACP	Link aggregation control protocol – открытый стандартный протокол агрегирования каналов.

NDP	Neighbor Discovery Protocol (протокол обнаружения соседей) – протокол из набора протоколов TCP/IP, используемый совместно с IPv6. Он работает на сетевом уровне Модели Интернета и ответственен за автонастройку адреса конечных и промежуточных точек сети, обнаружения других узлов на линии, определения адреса других узлов канального уровня, обнаружение конфликта адресов, поиск доступных маршрутизаторов и DNS-серверов, определения префикса адреса и поддержки доступности информации о путях к другим активным соседним узлам.
XDP	eXpress Data Path - это высокопроизводительный путь передачи данных на основе eBPF, который используется для отправки и получения сетевых пакетов с высокой скоростью в обход большей части сетевого стека операционной системы. Он включен в ядро ОС Linux начиная с версии 4.8.
АСУ	Автоматизированная система управления.
ИС	Информационная система.
ОС	Операционная система.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ									
Номера листов (страниц)					Всего листов (страниц) в докум.	№ документа	Входящий № сопроводительного документа и дата	Подп.	Дата
Изм	измененных	замененных	новых	аннулированных					