УТВЕРЖДЕНО

RU.09445927.425530-06 31 01-ЛУ

СИСТЕМА INVGUARD CS-01

Программный комплекс invGuard CS-SW-01

Описание применения

RU.09445927.425530-06 31 01

Листов 9

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата
0061	15.11.2014			

2014

АННОТАЦИЯ

В данном программном документе приведено описание применения программного комплекса invGuard CS-SW-01 системы invGuard CS-01 (далее Очиститель).

Очиститель предназначен для фильтрации и исследования вредоносного трафика, а также сбора различной статистики по исследованному трафику.

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 исследования и фильтрации вредоносного трафика, направленного на очистку (исследование).

1.2 Возможности программы

Очиститель осуществляет очистку сетевого трафика путем анализа входящего и исходящего трафика посредством фильтров, а также запись фрагмента трафика с максимальной детализацией при обнаружении сетевых атак.

1.3 Основные характеристики программы

Система обеспечивает возможность выполнения перечисленных ниже функций:

1) Система позволяет производить фильтрацию или очистку нежелательного трафика различными способами;
2) В системе предусмотрена фильтрация с использованием только средств маршрутизации и с помощью специальной аппаратно-программной компоненты «Очиститель трафика»;
3) Система не обязана вести анализ фрагментированных IP-пакетов. При этом пользователь имеет возможность выбора: пропускает Очиститель фрагментированные пакеты или нет;
4) Система позволяет произвести запуск/остановку всех процессов Очистителя одной командой.

1.4 Ограничения, накладываемые на область применения программы

Очиститель предназначен для работы только под управлением операционных систем типа РОСА SX «КОБАЛЬТ» 1.0.

2. УСЛОВИЯ ПРИМЕНЕНИЯ

2.1 Требования к техническим (аппаратным) средствам

Минимальный состав используемых технических (аппаратных) средств:

1) сервер, имеющий минимум 2 многоядерных процессора Intel с 6 и более вычислительными ядрами на каждый и частотой не менее 2,0 ГГц;
2) оперативная память объемом не менее 32 Гб;
3) жесткий диск объемом 500 Гб и выше;
4) двухпортовая сетевая карта Intel, поддерживающая технологию DPDK. Плата должна быть реализована на чипсете из списка http://dpdk.org/doc/nics.

2.2 Требования к программным средствам (другим программам)

Для функционирования программы необходимо следующее программное обеспечение:

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

2.3 Общие характеристики входной информации

В качестве входных данных Очиститель должен принимать ответвлённый трафик.

2.4 Общие характеристики выходной информации

Выходными данными должен быть фильтрованный трафик.

2.5 Требования и условия организационного характера

Для обеспечения работоспособности программы, оперативный персонал службы, ответственной за эксплуатацию Системы (перечисленный в разделе «Сведения о закреплении программного изделия при эксплуатации» программного документа RU.09445927.425530-06 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.09445927.425530-06 13 01 «Описание программы».

4. ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

4.1 Сведения о входных данных

В качестве входных данных Очиститель должен принимать ответвлённый трафик.

4.2 Сведения о выходных данных

Выходными данными должен быть фильтрованный трафик.

ПРИЛОЖЕНИЕ 1

ПЕРЕЧЕНЬ ТЕРМИНОВ

В настоящем документе применяют следующие термины с соответствующими определениями.

NetFlow	Семейство протоколов, поддерживаемых маршрутизаторами, для предоставления "слепков" трафика.
Ответвлённый трафик	подлежащий контролю сетевой трафик, направленный на устройство анализа через специальные сетевые ответвители, установленные в контролируемой сети.

ПРИЛОЖЕНИЕ 2

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

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.

Лист регистрации изменений

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