

УТВЕРЖДЕН

RU.АЦВТ.425760-01 30 01-ЛЮ

Программный комплекс invGUARD CS-SW 2.0

**Формуляр**

RU.АЦВТ.425760-01 30 01

Листов 22

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата
0161	 20.07.2020			

## АННОТАЦИЯ

В данном программном документе в разделе «Общие указания» приводятся общие указания для обслуживающего персонала по эксплуатации программного изделия «Программный комплекс invGUARD CS-SW 2.0», заполнению и ведению его формуляра.

В разделе «Общие сведения» указано наименование программного изделия, его обозначение, наименование предприятия изготовителя, версия программного изделия и другие общие сведения о программном изделии.

В разделе «Основные характеристики» приводятся необходимые при эксплуатации программного изделия значения основных функциональных характеристик.

В разделе «Комплектность» перечислены все непосредственно входящие в программное изделие компоненты и другие программные изделия, а также документация в соответствии с комплектностью.

В разделе «Свидетельство о приёмке» приведено свидетельство о приёмке программного изделия, подписанное лицами, ответственными за приёмку.

В данном формуляре в разделе «Сведения о рекламациях» регистрируют все предъявленные рекламации, их содержание и принятые меры.

В разделе «Сведения о хранении» указаны сроки хранения программного изделия.

В данном программном документе в разделе «Сведения о закреплении программного изделия при эксплуатации» указаны фамилии и должности лиц за которыми закреплено программное изделие.

В разделе «Сведения об изменениях» указано основание для внесения изменений, содержание изменений с указанием его порядкового номера, а также должность, фамилия и подпись лица, ответственного за проведение изменения.

Раздел «Особые пометки» предназначен для специальных отметок, которые вносятся во время эксплуатации программного изделия.

СОДЕРЖАНИЕ

АННОТАЦИЯ	2
1. ОБЩИЕ УКАЗАНИЯ	4
2. ОБЩИЕ СВЕДЕНИЯ	6
3. ОСНОВНЫЕ ХАРАКТЕРИСТИКИ	7
4. УКАЗАНИЯ ПО ЭКСПЛУАТАЦИИ	9
5. КОМПЛЕКТНОСТЬ	12
6. ПЕРИОДИЧЕСКИЙ КОНТРОЛЬ ОСНОВНЫХ ХАРАКТЕРИСТИК ПРИ ЭКСПЛУАТАЦИИ И ХРАНЕНИИ	13
7. СВИДЕТЕЛЬСТВО О ПРИЁМКЕ	14
8. СВИДЕТЕЛЬСТВО ОБ УПАКОВКЕ И МАРКИРОВКЕ	15
9. ГАРАНТИЙНЫЕ ОБЯЗАТЕЛЬСТВА	16
10. СВЕДЕНИЯ О РЕКЛАМАЦИЯХ	17
11. СВЕДЕНИЯ О ХРАНЕНИИ	18
12. СВЕДЕНИЯ О ЗАКРЕПЛЕНИИ ПРОГРАММНОГО ИЗДЕЛИЯ ПРИ ЭКСПЛУАТАЦИИ	19
13. СВЕДЕНИЯ ОБ ИЗМЕНЕНИЯХ	20
14. ОСОБЫЕ ОТМЕТКИ	21
ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ	22

## 1. ОБЩИЕ УКАЗАНИЯ

1.1. Ввод в эксплуатацию Программного комплекса invGUARD CS-SW 2.0 (далее по тексту – программное изделие или изделие или Очиститель или ПК invGUARD CS-SW 2.0) проводится в соответствии с настоящим формуляром и другими эксплуатационными документами согласно RU.АЦВТ.425760-01 20 01 «Программный комплекс invGUARD CS-SW 2.0. Ведомость эксплуатационных документов».

1.2. В случае обнаружения дефектов на компакт-диске с загрузочным модулем изделия следует обращаться к поставщику.

1.3. Формуляр должен находиться у должностного лица, ответственного за эксплуатацию изделия. Все записи в формуляре должны производиться только черными чернилами, отчетливо и аккуратно. Подчистки, помарки и незаверенные исправления НЕ ДОПУСКАЮТСЯ.

1.4. Перед эксплуатацией изделия необходимо внимательно ознакомиться с соответствующими эксплуатационными документами:

- RU.АЦВТ.425760-01 20 01 Ведомость эксплуатационных документов;
- RU.АЦВТ.425760-01 31 01 Описание применения;
- RU.АЦВТ.425760-01 32 01 Руководство системного программиста;
- RU.АЦВТ.425760-01 34 01 Руководство оператора.

1.5. Свидетельство о приёмке, после проведения необходимых испытаний на соответствие техническим условиям, при передаче данного программного изделия в эксплуатацию, подписывается лицами, ответственными за приёмку:

- руководителем предприятия-изготовителя, в состав которого входит подразделение, ответственное за эксплуатацию;
- должностным лицом, отвечающим за качество (ОТК).

1.6. Раздел «Сведения о рекламациях» заполняется лицом, ответственным за эксплуатацию, в случае обнаружения ошибок и недочетов в программном изделии в ходе эксплуатации.

1.7. В разделе «Сведения о хранении» указываются сроки хранения программного изделия. Заполняется начальником подразделения, ответственного за эксплуатацию.

1.8. Раздел «Сведения о закреплении программного изделия при эксплуатации» заполняется начальником подразделения, ответственного за эксплуатацию. В данном разделе, кроме начальника подразделения, ответственного за эксплуатацию, указываются непосредственные исполнители, т.е. лица, непосредственно производящие техническое обслуживание программного изделия и т.д.

1.9. Раздел «Сведения об изменениях» заполняется представителем предприятия-изготовителя данного программного изделия. Данный раздел заполняется в случаях модернизации, обновления программного изделия, устранении ошибок и недочетов, указанных в рекламации.

1.10. Раздел «Особые отметки» заполняется в случае необходимости специальных отметок в ходе эксплуатации лицами, ответственными за эксплуатацию.

1.11. Формуляр должен находиться в подразделении, ответственном за эксплуатацию программного изделия.

2. ОБЩИЕ СВЕДЕНИЯ Наименование программного изделия: Программный комплекс invGUARD CS-SW 2.0. Обозначение программного изделия: RU.АЦВТ.425760-01.

2.2. Наименование предприятия-изготовителя: ООО «Иновентика технолоджес».

2.3. Версия программного изделия: 2.0.

2.4. Размер программного изделия: 1605660 байт.

2.5. Контрольная сумма дистрибутива подсчитанная по алгоритму «ВКС» с использованием программы «ФИКС» (версия 2.0.2): fadb82c2.

2.6. Формат имени архива дистрибутива: cleaner\_N.0-M.tar

где: N — версия программного комплекса;

M — версия модификации в рамках текущей версии программного комплекса.

2.7. Программное изделие функционирует под управлением операционной системы Debian версий 9, 10.

### 3. ОСНОВНЫЕ ХАРАКТЕРИСТИКИ

3.1. 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.

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

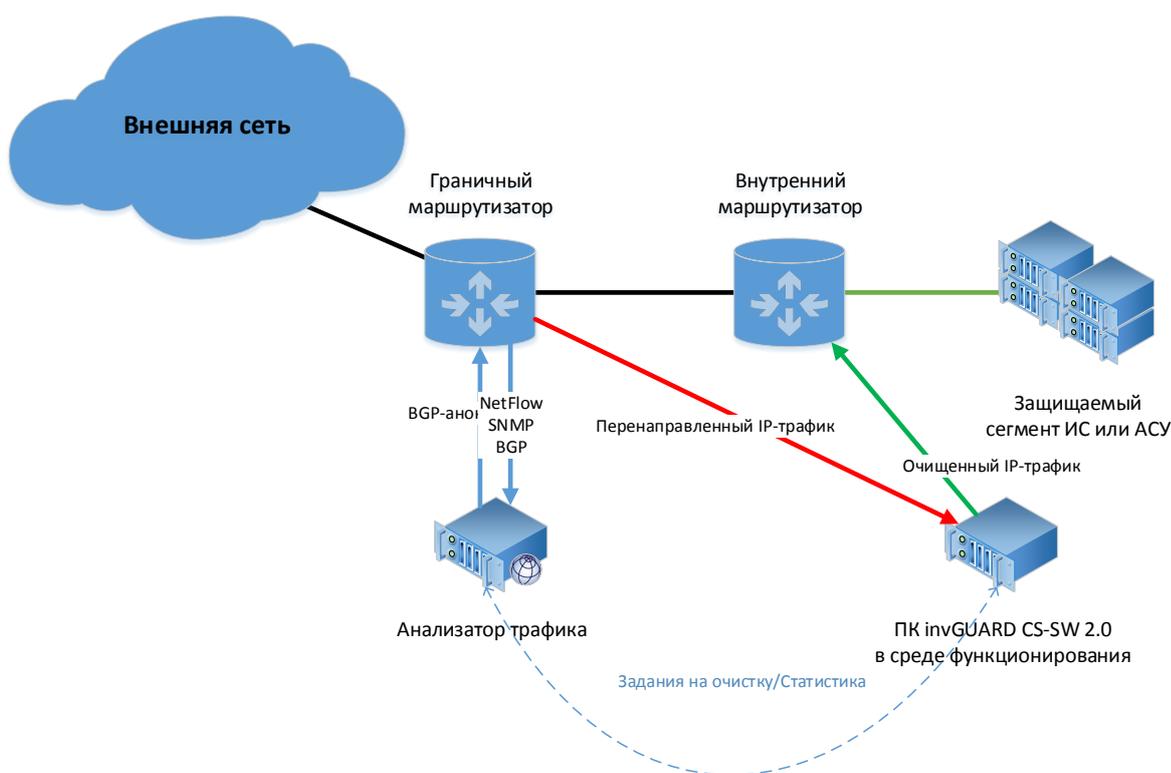


Рисунок 1 – Типовая схема применения Очистителя в ИС и АСУ

#### 3.3. Основные характеристики изделия

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.

#### 4. УКАЗАНИЯ ПО ЭКСПЛУАТАЦИИ

4.1. Для обеспечения стабильного функционирования и эксплуатации изделия техническая конфигурация оборудования должна соответствовать следующим требованиям:

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

оперативная память объемом не менее 32 Гб;

жесткий диск объемом 500 Гб и выше;

сетевой порт Ethernet для управления;

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>.

4.2. Для обеспечения функционирования изделия на сервере должна быть установлена и сконфигурирована серверная операционная система Debian версий 9, 10.

4.3. В процессе эксплуатации изделия его безопасность обеспечивается строгим выполнением персоналом требований организационно-распорядительной и эксплуатационной документации, применением принципов и методов построения среды безопасности изделия.

4.4. Ответственность за создание безопасной среды эксплуатации изделия возлагается на эксплуатирующую организацию.

4.5. Меры по обеспечению безопасной среды эксплуатации изделия должны предусматриваться в составе мер по обеспечению безопасности ИС или АСУ в составе которой оно эксплуатируется.

4.6. Анализ уязвимостей и обновление программного обеспечения

4.6.1. Для безопасной эксплуатации программного обеспечения необходимо выполнять ограничения и рекомендации разработчиков, включенные в документацию на программные изделия:

среду функционирования – серверная операционная система Debian версий 9, 10;

Программный комплекс invGUARD CS-SW 2.0 (Руководство системного программиста. RU.АЦВТ.425760-01 32 01).

4.6.2. Перед началом эксплуатации необходимо изменить существующие (заводские и тестовые) установки, а также пароли на доступ к интерфейсу операционной системы и изделия.

4.6.3. Минимальная длина пароля составляет 6 символов (буквенно-цифровой последовательности длиной  $\geq 6$  символов с добавлением специальных символов (#, \$, \* и т.д.)) с назначением уникального идентификатора каждому пользователю. Рекомендуется использовать пароли длиной не менее 8 символов.

4.6.4. Рекомендуется производить смену пароля не реже одного раза в месяц.

4.6.5. Рекомендуется исключить использование потенциально уязвимых служб (DHCP-сервера, FTP-сервера и др.).

4.6.6. Рекомендуется в среде функционирования сконфигурировать автоматический запуск службы iptables, входящей в состав серверной операционной системы и настроить её следующим образом:

политики по умолчанию стандартных цепочек INPUT, FORWARD и OUTPUT устанавливаются в DROP;

разрешается любой трафик в цепочках INPUT и OUTPUT для интерфейса lo;

разрешается трафик, инициированный системой (цепочка OUTPUT);

разрешается трафик для уже установленных или связанных с установленными соединениями (цепочка INPUT);

разрешается доступ к интерфейсу Очистителя с доверенных IP-адресов пользователей системы по протоколу ssh (цепочка INPUT);

разрешается доступ к интерфейсу Очистителя с доверенных IP-адресов пользователей системы по протоколу HTTP, порт 8081 (цепочка INPUT);

разрешается доступ к Очистителю с доверенных IP-адресов маршрутизаторов (роутеров) по протоколу bgp (цепочка INPUT).

4.6.7. В процессе эксплуатации необходимо проверять контрольные суммы неизменяемых файлов программного изделия.

4.6.8. Системный программист (администратор безопасности) должен регулярно отслеживать и устанавливать обновления безопасности для изделия и для среды функционирования.

4.6.9. Необходимо периодически проверять сайт разработчика изделия (<http://www.inoventica-tech.ru/>), разработчика среды функционирования и Банк данных угроз безопасности информации ФСТЭК России (<http://bdu.fstec.ru/vul>) на наличие сведений об уязвимостях и обновлении программного обеспечения (закрывающим уязвимости) Анализатора и среды функционирования.

#### 4.7. Установка обновлений среды функционирования

4.7.1. Установку обновлений среды функционирования проводить в соответствии с указаниями по эксплуатации соответствующего программного изделия.

#### 4.8. Установка обновлений изделия

4.8.1. Обновления изделия, поставляются на компакт-диске или с использованием доверенных электронных каналов передачи данных. В соответствии с процедурой, предусмотренной эксплуатационной документацией, перед установкой обновлений должна осуществляться проверка их целостности методом контрольного суммирования. Установка других обновлений изделия не допускается.

4.8.2. Компакт-диск обновлений поставляется вместе с бюллетенем об изменениях, в котором указывается содержание изменений и способы их внесения.

4.8.3. Порядок установки обновлений изделия содержится в документе RU.АЦВТ.425760-01 32 01.





## 7. СВИДЕТЕЛЬСТВО О ПРИЁМКЕ

Программный комплекс invGuard CS-SW 2.0

наименование программного изделия

RU.АЦВТ.425760-01

обозначение

Зав. № \_\_\_\_\_

Соответствует техническим условиям и признан годным к эксплуатации.

Дата выпуска \_\_\_\_\_

Должность

МП

\_\_\_\_\_

подпись

\_\_\_\_\_

расшифровка подписи

МП

Должность

\_\_\_\_\_

подпись

\_\_\_\_\_

расшифровка подписи



## 9. ГАРАНТИЙНЫЕ ОБЯЗАТЕЛЬСТВА

Предприятие-изготовитель (далее – поставщик) гарантирует соответствие качества изделия требованиям технических условий при условии соблюдения указаний по эксплуатации, условий транспортирования и хранения, установленных эксплуатационной документацией.

В период гарантийного срока эксплуатации гарантируется:

- сохранность информации, размещенной на компакт-диске и считывание ее с этого компакт-диска;
- выполнение изделием функций в соответствии с эксплуатационной документацией.

Действие гарантийных обязательств прекращается, если в гарантийный период пользователь внес в изделие какие-либо изменения или нарушил условия эксплуатации, транспортирования и хранения изделия, установленные эксплуатационной документацией.

Гарантийный срок хранения изделия – 1 год с даты его приемки.











