

УТВЕРЖДЕНО

18678659.00001-03 30 02-ЛУ

**ПРОГРАММНЫЙ КОМПЛЕКС
РЕТРОСПЕКТИВНОГО АНАЛИЗА СЕТЕВОГО ТРАФИКА
«СТЕТОСКОП» ВЕРСИИ 3.0**

Формуляр

18678659.00001-03 30 02

Серийный номер: _____

2022

СОДЕРЖАНИЕ

1	Общие указания	3
2	Общие сведения	4
3	Основные характеристики	5
4	Комплектность	12
5	Свидетельство о приемке	13
6	Свидетельство об упаковке	14
7	Гарантии изготовителя	15
8	Обновление ПО в процессе эксплуатации изделия	16
9	Периодический контроль процесса эксплуатации изделия	17
10	Сведения о рекламациях	21
11	Сведения о хранении	23
12	Особые отметки	24
	Лист регистрации изменений	25

Все права защищены. Полное или частичное копирование материалов без письменного согласования с ООО «ЦСС-Безопасность» запрещено.

1 ОБЩИЕ УКАЗАНИЯ

1.1 Перед эксплуатацией программного комплекса ретроспективного анализа сетевого трафика «Стетоскоп» версии 3.0 (далее по тексту - изделие), необходимо ознакомиться с настоящим формуляром, а также с документами:

- 18678659.00001-03 31 02 Описание применения;
- 18678659.00001-03 32 02 Руководство администратора;
- 18678659.00001-03 34 02 Руководство оператора.

1.2 Формуляр является документом, удостоверяющим основные параметры и технические возможности изделия, отражающим его техническое состояние и содержащим сведения, которые вносятся в формуляр в период эксплуатации изделия.

1.3 Формуляр является документом, удостоверяющим гарантии Изготовителя и содержащим сведения о сертификации изделия.

1.4 Формуляр входит в комплект поставки и должен постоянно находиться в подразделении, осуществляющем эксплуатацию изделия.

1.5 Все записи в формуляр должны производиться только чернилами, отчетливо и аккуратно. Подчистки, помарки и незаверенные исправления не допускаются.

2 ОБЩИЕ СВЕДЕНИЯ

2.1 Наименование программного изделия: Программный комплекс ретроспективного анализа сетевого трафика «Стетоскоп» версии 3.0.

2.2 Обозначение программного изделия: 18678659.00001-03.

2.3 Наименование изготовителя: Общество с ограниченной ответственностью «ЦСС-Безопасность» (ООО «ЦСС-Безопасность»).

2.4 Контакты службы технической поддержки изделия:
+7 (495) 960-72-72, support@ssecline.ru.

2.5 Изделие поставляется на компакт-диске, содержащем файл-архив «stet-3.0.<версия ПК>_<версия ОС>.tar.gz» (<версия ПК> - минорная версия релиза ПК Стетоскоп, <версия ОС> - версия ядра ОС Linux Ubuntu) с программными модулями, информационным обеспечением и скриптами автоматизации установки, а также файлы с эксплуатационной документацией в формате PDF.

2.6 Изделие предназначено для исполнения на серверах архитектуры Intel x86-64 или на гостевых виртуальных машинах эмулирующих архитектуру Intel x86-64, под управлением операционной системы семейства Linux - Ubuntu 18.04.5 LTS (Версия ядра Linux 4.15.0-144-generic).

2.7 Для функционирования изделия требуется не менее двух сетевых интерфейсов: один для организации управления, второй – для захвата сетевых потоков. Для захвата сетевых потоков может использоваться несколько сетевых интерфейсов, в том числе для организации мостового соединения с функцией bypass. Для реализации функции bypass между двумя сетевыми интерфейсами требуется поддержка со стороны сетевой карты. Примером подобной сетевой картой может служить изделие «PE2G4BPI35A Bypass Adapter» (4 x 1 Гбит/с) или «PE210G2BPI9 Ethernet Bypass» (2 x 10 Гбит/с).

3 ОСНОВНЫЕ ХАРАКТЕРИСТИКИ

3.1 Изделие, предустановленное на аппаратную платформу или гостевую виртуальную машину, позволяет осуществлять контроль всего сетевого трафика Организации (локального и взаимодействия с сетью Интернет), обнаруживать атаки злоумышленников и контролировать соблюдение политики информационной безопасности. Изделие является эффективным и удобным инструментом для анализа сетевых взаимодействий и контроля сетевой активности пользователей, программного обеспечения и аппаратных компонентов.

Изделие предназначено для:

- организации захвата, записи и индексации сетевого трафика;
- анализа передаваемых по сети данных с целью выявления атак и аномалий, генерации событий информационной безопасности;
- сбора и визуализации статистики сетевых сессий и передаваемых данных;
- выявления используемых сетевых протоколов, форматов и служб;
- определения географической принадлежности и DNS-имен IP-адресов взаимодействующих сетевых субъектов;
- экспорта по требованию оператора образцов сетевого трафика и перенаправления сетевого трафика на внешние анализаторы;
- перенаправления системных событий и событий информационной безопасности (далее по тексту – ИБ) на внешние системы обработки событий (к примеру, системы мониторинга и управления ИБ, SIEM-системы).

3.2 Изделие предназначено для подразделений ИБ и IT, компаний, заинтересованных в контроле интернет-активности своих сотрудников, сетевых взаимодействий, установленного программного обеспечения и

оборудования. Одно изделие одновременно позволяет обрабатывать сетевые потоки с нескольких сетевых интерфейсов.

3.3 В зависимости от характеристик аппаратной платформы изделие позволяет обрабатывать сетевые потоки на скорости до 10 Гбит/с в каждом направлении сетевого трафика (т.е. суммарно до 20 Гбит/с).

3.4 Для обработки сетевых потоков на скорости до 10 Гбит/с в каждом направлении (суммарно 20 Гбит/с) рекомендуются следующие параметры аппаратной платформы:

- сервер в корпусе 19”, монтируемом в стандартную коммуникационную стойку;
- центральный процессор с не менее 10 вычислительными ядрами с частотой не менее 2.0 ГГц;
- оперативная память не менее 256 ГБ;
- постоянно запоминающее устройство (далее - ПЗУ) №1 для операционной системы не менее 64 ГБ;
- ПЗУ №2 для хранения индекса и событий журналов аудита не менее 4 ТБ;
- ПЗУ №3 для хранения образцов записанного трафика суммарно не менее 120 ТБ (Расширение объема ПЗУ №3 позволит увеличить срок хранения образцов записанного трафика);
- поддержка ядра ОС Linux версии 4;
- один сетевой интерфейс, работающий на скорости не менее 1 Гбит/с, для реализации канала управления. Для реализации отказоустойчивого канала управления рекомендуется выделять два сетевых интерфейса;
- один и более сетевых интерфейсов с чипсетами Intel, работающих на скорости 10 Гбит/с для захвата сетевого трафика.

3.5 Для обработки сетевых потоков на скорости до 1 Гбит/с в каждом направлении (суммарно 2 Гбит/с) рекомендуются следующие параметры аппаратной платформы:

- сервер в корпусе 19”, монтируемом в стандартную коммуникационную стойку или ПК;
- центральный процессор с не менее 4 вычислительными ядрами с частотой не менее 2.0 ГГц;
- оперативная память не менее 64 ГБ;
- постоянно запоминающее устройство (далее - ПЗУ) №1 для операционной системы не менее 64 ГБ;
- ПЗУ №2 для хранения индекса и событий журналов аудита не менее 256 ГБ;
- ПЗУ №3 для хранения образцов записанного трафика суммарно не менее 12 ТБ (Расширение объема ПЗУ №3 позволит увеличить срок хранения образцов записанного трафика);
- поддержка ядра ОС Linux версии 4;
- один сетевой интерфейс, работающий на скорости не менее 1 Гбит/с, для реализации канала управления. Для реализации отказоустойчивого канала управления рекомендуется выделять два сетевых интерфейса;
- один и более сетевых интерфейсов с чипсетами Intel, работающих на скорости 1 Гбит/с для захвата трафика.

3.6 При установке изделия в разрыв существующей линии связи целесообразно применять сетевые карты с функцией bypass, позволяющей минимизировать риск обрыва связи в случае сбоев в аппаратной или программной частях изделия, включая обесточивание аппаратной платформы.

3.7 Список поддерживаемых и рекомендованных сетевых чипсетов Intel для захвата сетевого трафика: i350, 82580EB, 82580DB, XL710, X550, X710, 82599ES, X540, XXV710, FM10420.

3.8 Изделие выполняет следующие основные функции:

- предупреждает кибератаки на активы компании,
- обнаруживает утечки конфиденциальной информации,
- контролирует действия сотрудников в сети Интернет и локальной сети,
- собирает сетевую статистику и позволяет анализировать весь трафик в удобном формате отчетов,
- собирает доказательную базу и помогает расследовать инциденты ИБ.

3.9 Изделие обладает следующими возможностями:

- захват сетевого трафика с нескольких сетевых интерфейсов;
- гарантированная запись сетевого трафика на диск со скоростью до 20 Гбит/с и предоставление его для анализа;
- расчет и запись статистики сетевого трафика в реальном времени, включает в себя не менее 20 сетевых параметров индексации;
- оперативный мониторинг состояния сети организации в графическом и табличном представлении;
- детализация сетевой активности ранее накопленных данных с учетом специфики расследуемого инцидента, а также возможность применения новых анализаторов и методов анализа;
- выявление аномалий и атак в автоматическом режиме с применением методов математической статистики и машинного обучения;
- перенаправление трафика на внешние системы обнаружения компьютерных атак (COA) или системы обнаружения вторжений: COA «Аргус» (производство ООО «ЦСС»), Snort, Suricata;

- экспорт событий ИБ, встроенных в изделие анализаторов, во внешние системы обработки событий информационной безопасности, включая Комплекс программных средств регистрации, анализа и мониторинга событий ИБ – КПС РАМС ИБ (производство ООО «ЦСС»);
- идентификация географической принадлежности сетевых адресов индексируемого трафика;
- определение более 1000 сетевых протоколов, включая прикладной уровень (приложения и сервисы);
- предоставление внешним системам управления ИБ, включая КПС РАМС ИБ, интерфейс управления изделием и мониторинга состояния изделия.

3.10 Для управления изделием и решения задач анализа сетевого трафика рекомендуется выделить одно или более автоматизированное рабочее место (далее по тексту - АРМ) оператора изделия. Изделие поддерживает одновременную работу нескольких операторов. Интерфейс управления и анализа выполнен в виде WEB-приложения и для работы требует предустановленный на АРМ оператора браузер. Для комфортной работы АРМ оператора должен удовлетворять следующим минимальным требованиям:

- персональный компьютер;
- оперативная память не менее 16 ГБ;
- постоянно запоминающее устройство не менее 128 ГБ;
- центральный процессор с не менее двумя вычислительными ядрами с частотой работы не менее 2.0 ГГц;
- монитор не менее 23” с разрешением не менее FullHD (1920x1080). Для комфортной работы рекомендуется разрешение 4K;
- сетевой интерфейс, работающий на скорости не менее 1 Гбит/с;

– предустановленная операционная система, поддерживающая выполнение следующих браузеров: Mozilla Firefox версии не ниже 52, Google Chrome версии не ниже 53, Microsoft Edge версии не ниже 40.

3.11 Указания по эксплуатации изделия:

1) при первом входе оператора изделия в WEB-приложение необходимо обязательно сменить пароль по умолчанию, заданный при развертывании изделия. По умолчанию зарегистрирован пользователь «admin» с паролем «passw0rd»;

2) обеспечить наличие администратора информационной системы, отвечающего за встраивание изделия в действующую информационную систему и конфигурирование изделия;

3) при доступе к АРМ оператора изделия должна осуществляться его идентификация и аутентификация;

4) при использовании более одного оператора изделия применять разграничительную политику доступа на основе привилегий пользователей, а также использовать нестандартные имена учетных записей;

5) следовать политике ввода стойкого к подбору пароля изделия, которая должна включать минимальную длину пароля, количество символов верхнего и нижнего регистра, спецсимволов и цифр;

6) осуществлять периодическую смену пароля на доступ к изделию (например, смену пароля осуществлять не реже, чем 1 раз в установленный политикой организации период времени, как правило, 1-3 месяца, а также незамедлительно при подозрении на несанкционированное раскрытие пароля);

7) хранить в секрете идентификаторы и пароли на доступ к изделию;

8) каналы управления изделием должны быть реализованы в пределах контролируемой зоны и должны быть доверенными;

9) удаленное управление изделием за пределами контролируемой зоны или по недоверенным каналам должно осуществляться с помощью сертифицированных средств криптографической защиты информации;

10) установить требуемые политики анализа сетевых потоков и статистики трафика (возможности и правила задания политик анализа описаны в документе «Программный комплекс ретроспективного анализа сетевого трафика «Стетоскоп» версии 3.0. Руководство оператора. 18678659.00001-03 34 02»);

11) необходимо регулярно выполнять анализ системного журнала на предмет отсутствия критичных ошибок.

4 КОМПЛЕКТНОСТЬ

Программный комплекс ретроспективного анализа сетевого трафика «Стетоскоп» версии 3.0, обозначение 18678659.00001-03, поставляется в следующей комплектации:

Обозначение	Наименование	Кол-во	Примечание
Компакт-диски			
-	Программный комплекс ретроспективного анализа сетевого трафика «Стетоскоп» версии 3.0, 18678659.00001-03. Дистрибутив.	1	Диск с программным, информационным обеспечением и документацией (дистрибутив)
Эксплуатационная документация			
18678659.00001-03 30 02	Формуляр	1	Документ в печатном виде
18678659.00001-03 31 02	Описание применения	1	Документ на диске
18678659.00001-03 32 02	Руководство администратора (системного программиста)	1	Документ на диске
18678659.00001-03 34 02	Руководство оператора	1	Документ на диске

Самостоятельная (без санкции Изготовителя) модификация программного обеспечения не допускается.

5 СВИДЕТЕЛЬСТВО О ПРИЕМКЕ

Программный комплекс ретроспективного анализа сетевого трафика
«Стетоскоп» версии 3.0, обозначение 18678659.00001-03.

Серийный номер _____

изготовлено и принято в соответствии с действующей технической
документацией, соответствует эталону, и признано годным для
эксплуатации.

Дата выпуска: _____

Начальник ОТК

М.П.

личная подпись

расшифровка подписи

дата

6 СВИДЕТЕЛЬСТВО ОБ УПАКОВКЕ

Программный комплекс ретроспективного анализа сетевого трафика
«Стетоскоп» версии 3.0, обозначение 18678659.00001-03.

серийный № _____

упаковано ООО «ЦСС-Безопасность» в соответствии с комплектацией
(раздел 4) и согласно требованиям, предусмотренным в действующей
технической документации.

Дата упаковки: _____

Упаковку произвёл

подпись

расшифровка подписи

7 ГАРАНТИИ ИЗГОТОВИТЕЛЯ

7.1 Изготовитель гарантирует работоспособность изделия в соответствии с объявленными характеристиками при соблюдении Пользователем требований эксплуатационной документации на изделие.

7.2 В случае выявления в изделии дефектов, не связанных с нарушением правил эксплуатации, транспортирования и хранения, изделие подлежит рекламации, и Изготовитель обязуется по получении рекламации в возможно короткий срок устранить дефекты своими силами и средствами вплоть до поставки нового изделия, а также принять меры, исключающие эти дефекты во всех остальных экземплярах изделия.

7.3 Гарантийный срок изделия — 12 (двенадцать) месяца со дня поставки.

7.4 Действия гарантийных обязательств прекращается, если Пользователем внесены изменения в изделие без согласования с Изготовителем.

7.5 Сохранность информации на носителе зависит от качества этого носителя.

Данные о поставке (продаже) изделия:

Дата поставки: _____

Генеральный директор ООО «ЦСС-Безопасность»

С.В. Васильев

М.П.

дата

8 ОБНОВЛЕНИЕ ПО В ПРОЦЕССЕ ЭКСПЛУАТАЦИИ ИЗДЕЛИЯ

Обновление программного обеспечения изделия выполняется только специальным пакетом, полученным у Изготовителя изделия. Процесс обновления описан в документе «Программный комплекс ретроспективного анализа сетевого трафика «Стетоскоп» версии 3.0. Руководство администратора (системного программиста). 18678659.00001-03 32 02».

9 ПЕРИОДИЧЕСКИЙ КОНТРОЛЬ ПРОЦЕССА ЭКСПЛУАТАЦИИ ИЗДЕЛИЯ

Перед началом эксплуатации изделия администратору ИС необходимо соблюсти указания по применению, изложенные в п. 3.11 раздела 3 «Основные характеристики».

Для проведения периодического контроля процесса эксплуатации предназначены нижеследующие таблицы.

Таблица учета сбоев при эксплуатации:

Дата и время сбоя в функционировании	Внешнее проявление сбоя	Причина сбоя	Принятые меры по устранению сбоя и отметка о направлении рекламации	Должность, фамилия и подпись лица, ответственного за устранение сбоя	Примечание

Таблица учета периодического технического обслуживания:

[illegible]

19

Таблица сведений об установке новых версий базы решающих правил:

[illegible]

10 СВЕДЕНИЯ О РЕКЛАМАЦИЯХ

10.1 Рекламации, связанные с эксплуатацией изделия, оформляются в письменном виде с указанием даты обнаружения ошибки, ее описания и условий возникновения.

10.2 Рекламации подписываются руководителем подразделения, принявшего или эксплуатирующего изделие.

10.3 Рекламации направляются Изготовителю по адресу:
119530, г. Москва, Очаковское шоссе, дом 34, ООО «ЦСС-Безопасность».

10.4 Срок рассмотрения рекламации — 1 (один) месяц со дня получения рекламации.

10.5 При несоответствии поставляемого изделия, его тары, упаковки, консервации, маркировки и комплектности требованиям сопроводительной документации, пользователь обязан направить рекламацию предприятию-Изготовителю в течение 60 дней со дня поставки изделия.

10.6 Изготовитель принимает рекламацию, если не установлена вина получателя в возникновении дефекта в изделии.

10.7 Поступающие к Изготовителю рекламации регистрируются в журнале учета рекламаций по форме, представленной далее.

[illegible]

11 СВЕДЕНИЯ О ХРАНЕНИИ

11.1 Носители информации в электронном виде (компакт-диски) с записью программного и информационного обеспечения, эксплуатационных документов хранятся в вертикальном положении на предназначенном для этой цели стеллаже в упаковке, поставленной изготовителем, при комнатной температуре окружающего воздуха от 5 до 35 градусов Цельсия, относительной влажности воздуха не более 65%. Не допускается резкое изменение температуры окружающего воздуха (более 20 градусов Цельсия в час).

11.2 В помещении для хранения носителей информации в электронном виде не должно быть агрессивных примесей (паров кислот, щелочей).

Обозначение и/или название объекта хранения	Дата		Условия хранения	Должность, фамилия и подпись лица, ответственного за хранение
	установки на хранение	Снятия с хранения		

18678659.00001-03 30 02

12 ОСОБЫЕ ОТМЕТКИ

Лист регистрации изменений

[illegible]