ТС ОРМ СОРМович

Функциональная спецификация

ООО «Цитадель»

Содержание

1. ВВЕДЕНИЕ

1.1. ЦЕЛЬ ДОКУМЕНТА

В настоящем документе приведено описание функциональных возможностей программно-аппаратного комплекса «ТС ОРМ «СОРМович» (далее – «ТС ОРМ «СОРМович», ПАК).

1.2. НАЗНАЧЕНИЕ ПАК

«ТС ОРМ «СОРМович» предназначен для обеспечения законного перехвата информации с целью осуществления уполномоченным государственным органом оперативно-розыскной деятельности на сетях документальной электросвязи (СДЭС).

ПАК разработан в соответствии с правилами применения оборудования систем коммутации (далее – Правила), утвержденными приказом №83 [1] Министерства связи и массовых коммуникаций с изменениями, внесенными приказом Министерства цифрового развития, связи и массовых коммуникаций РФ №139[2].

«ТС ОРМ «СОРМович» предназначен для установки на узлах телематических служб и передачи данных (далее – ПД), использующих технологию Ethernet IEEE 802.3 и сетевой протокол передачи данных IP версий 4 или 6 (рекомендации RFC 791 и RFC 1883 соответственно), а также протоколы идентификации пользователей RADIUS (рекомендации RFC 2138 и 2059) или TACACS+, и на узлах сетей подвижной радиотелефонной связи (СППС) стандарта GSM/GPRS, 3G, LTE.

[1] Приказ Министерства связи и массовых коммуникаций РФ от 16 апреля 2016 г. №83 «Об утверждении Правил применения оборудования систем коммутации, включая программное обеспечение, обеспечивающего выполнение установленных действий при проведении оперативно-розыскных мероприятий. Часть III. Правила применения оборудования коммутации и маршрутизации пакетов информации сетей передачи данных, включая программное обеспечение, обеспечивающего выполнение установленных действий при проведении оперативно-розыскных мероприятий»;

[2] Приказ Министерства цифрового развития, связи и массовых коммуникаций РФ от 15 апреля 2019 г. №139 «О внесении изменений в Правила применения оборудования систем коммутации, включая программное обеспечение, обеспечивающего выполнение установленных действий при проведении оперативно-розыскных мероприятий. Часть III. Правила применения оборудования коммутации и маршрутизации пакетов информации сетей передачи данных, включая программное обеспечение, обеспечивающего выполнение установленных действий при проведении оперативно-розыскных мероприятий, утвержденных приказом Министерства связи и массовых коммуникаций РФ от 16.04.2014 №83».

2. ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

Функциональные возможности ПАК «ТС ОРМ «СОРМович» описаны в разделах ниже.

Примечание: в зависимости от конфигурации комплекса функциональные возможности могут различаться.

2.1. ИНТЕРФЕЙСЫ ДОСТУПА К СЕТИ ПЕРЕДАЧИ ДАННЫХ

- Доступ с использованием следующих интерфейсов технологии Ethernet (стандартов IEEE 802.3):
  - 1000BASE-T;
  - 1000BASE-X;
  - 10GBASE-SR;
  - 10GBASE-LR;
  - 100GBASE-SR4;
  - 100GBASE-LR4.

Примечание: Возможность съема трафика с интерфейсов 100GBASE необходимо согласовывать дополнительно.

2.2. ДЕКОДИРУЕМЫЕ ПРОТОКОЛЫ

Декодирование следующих протоколов:

- Протоколы 2/3 уровней модели OSI: 802.3 Ethernet, включая поддержку технологий Pseudo-wire (RFC 4385, RFC 4448); Jumbo frames;
- Почтовые и новостные протоколы;
- Протоколы передачи гипертекстовой информации и файлов;
- Протоколы обмена мгновенными сообщениями (декодирование текстовой переписки (чата) и обмена файлами);
- Протокол Telnet (декодирование текстовой информации; данные перехватываются в виде потоков и в виде объектов прикладных протоколов, передаваемых через Telnet);
- Идентификация использования Skype, OM, TOR, WhatsApp, Viber, SSL, Telegram и др.;
- Идентификация потоков пиринговых сетей (Bittorrent);
- Идентификация использования социальных сетей;
- Протоколы декодирования VoIP-соединений, использующие протоколы RTP/RTCP в качестве транспортного протокола;
- Декодирование данных, передаваемых внутри нешифрованных туннелей протоколов;
- Декодирование протоколов аутентификации;
- Определение фактов авторизации пользователя по протоколам;
- Детектирование потоков терминального доступа;
- Перехват SMS-сообщений в сетях LTE.

2.3. ПОДДЕРЖКА ПРОТОКОЛОВ АВТОРИЗАЦИИ АБОНЕНТОВ

ПАК «ТС ОРМ «СОРМович» позволяет осуществлять идентификацию абонентов, авторизующихся по следующим протоколам:

- RADIUS;
- TACACS+;
- Diameter;
- GTP-C.

2.4. ОТБОР ИНФОРМАЦИИ

- Отбор информационных сообщений и данных контролируемых пользователей на основе критериев отбора, задаваемых пользователем через ПУ.
- Возможность перехвата только статистической информации по заданным критериям отбора.
- Возможность перехвата статистики VoIP.
- Фиксирование фактов подключения и отключения пользователей сети оператора (на основе данных, извлекаемых из сообщений протоколов RADIUS, TACACS+, DIAMETER, GTP-C) в соответствии с установленными критериями отбора.
- Отбор TCP- и UDP-сессий (в том числе для нестандартных протоколов) по критериям отбора.
- Возможность исключения из отбираемых данных информации определённого типа с разграничением по категориям.
- Отбор информации на основе комбинации критериев с использованием логических операторов «И», «ИЛИ» и «НЕ».
- Поиск ключевых слов в кодировках: Win1251, DOS-866, ISO-8859.5, KOI-8r, UTF-8, MAC, UTF-16 (LE & BE), UTF-32 (LE & BE).
- Регистрозависимый и регистронезависимый поиск ключевых слов.
- Поиск ключевых слов и фраз, в том числе в потоковых данных, сжатых по алгоритму gzip/deflate.
- Поиск ключевых слов в сообщениях электронной почты, в том числе в форматах quoted printable и Base-64.
- Для прикладных протоколов SMTP, POP3, IMAP4, NNTP, HTTP, FTP перехват протокольных заголовков, содержащих, в том числе, имя пользователя и пароль (если данные поля присутствуют в заголовке).
- Режим перехвата цепочек объектов, когда для перехваченного по заданным критериям электронного письма либо сообщения службы обмена мгновенными сообщениями ставится на контроль электронный адрес, либо идентификатор отправителя сообщения. В дальнейшем перехватываются все электронные письма или сообщения, отправленные или полученные данным адресатом (пользователем системы обмена мгновенными сообщениями).
- Режим автоматической постановки на контроль IP-адреса пользователя сети оператора, чьи информационные сообщения были отобраны по идентификаторам 3 уровня модели OSI и выше (например, IP адрес, адрес электронной почты и т.д.). В дальнейшем перехватываются все информационные сообщения, отправленные или полученные пользователем в рамках сеанса связи.

- Режим перехвата извещений о подключении/отключении пользователей сети оператора, чьи информационные сообщения были отобраны по идентификаторам 3 уровня модели OSI и выше. Данный режим позволяет сопоставлять перехваченные данные с информацией о пользователях сети оператора. Например, при контроле по адресу электронной почты перехватываются не только электронные письма, отправляемые либо получаемые объектом наблюдения, но и факты начала и окончания сеанса связи.

2.5. ВЗАИМОДЕЙСТВИЕ

ПАК «ТС ОРМ «СОРМович» обеспечивает взаимодействие с:

- С ПУ в соответствии с протоколом взаимодействия ТС ОРМ с ПУ, приведенному в приложении №2 к Правилам (утвержденным Приказом №83 с изменениями, внесенными Приказом №139).
- С ИС БД ОРМ в соответствии с протоколом взаимодействия, приведенным в приложении №2.1 к Правилам (утвержденным Приказом №83 с изменениями, внесенными Приказом №139).