ФУНКЦИОНАЛЬНАЯ СПЕЦИФИКАЦИЯ ПРОГРАММНОГО ПРОДУКТА «СПЕКТР АКТИВ 139»

ООО «ПРОКОН»

Москва 2021

**Общее описание**

Комплект программного обеспечения «Спектр Актив 139» установленное на сервер оператора связи предназначено для съема трафика, устанавливаемое на сетях операторов фиксированной и мобильной связи.

«Спектр Актив 139» соответствует требованиям следующих нормативных актов:

1. Приказ Минкомсвязи России № 83 от 16.04.2014 г. «Об утверждении Правил применения оборудования систем коммутации, включая программное обеспечение, обеспечивающего выполнение установленных действий при проведении оперативно-розыскных мероприятий».

2. Приказ Минкомсвязи России № 139 от 15.04.2019 г. «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, утвержденные приказом Министерства связи и массовых коммуникаций Российской Федерации от 16.04.2014 N 83».

Настроенный комплект программ обеспечивает взаимодействие с информационными системами, содержащими базы данных абонентов оператора связи и предоставленных им услугах связи (далее ИС БД ОРМ), обеспечивающими выполнение установленных действий при проведении оперативно-разыскных мероприятий, и передачу статистической информации обо всех соединениях абонентов, а также текстовых сообщений пользователей услугами связи, голосовой информации, изображений, звуков, видео-, иных сообщений пользователей услугами связи в полном объеме или в соответствии заданным критериям фильтрации сообщений.

«Спектр Актив 139» разработан для применения в серверных платформах. Устанавливается на заранее подготовленную операционную систему Astra Linux Релиз “Орёл”. Работа на других операционных системах не проверялась.

**Требования к оборудованию для установки программного обеспечения «Спектр Актив 139»**

1. Для CPU указано только количество физических ядер, предполагается, что это современные (не ниже 2017 года) процессоры Intel Xeon с тактовой частотой не менее 2,2GHz. Однопроцессорные решения до 18 ядер, выше 18 ядер допускаются двухпроцессорные

2. Предполагается, что все диски поддерживают горячую замену и используется аппаратный дисковый контроллер. (Под ОС - 2 ssd диска по 120 ГБ)

3. Сетевые интерфейсы для захвата трафика 1 GbE – медь, 10 GbE – оптика. Intel как вендор сетевых карт принципиально важен, т.к. используемые для захвата трафика без потерь технологии завязаны на драйверы igb / ixgbe / i40е.



**Требования к подаче трафика для использования программного обеспечения «Спектр Актив 139»**

1 Абонентский Трафик

1.1 Зеркалирующее оборудование должно обеспечивать подачу трафика в сторону С2 без потерь в случае SPAN, желательно использовать оптические сплиттеры.

1.2 Трафик должен быть двунаправленный.

1.3 Трафик должен содержать данные до NAT.

2 Трафик авторизации абонентов.

(Наиболее часто используется RADIUS-протокол, соответственно, в качестве примера приводится информация для этого протокола)

2.1 Требования к формированию RADIUS приведены в RFC 2865, 2866 И 5080

 https://tools.ietf.org/html/rfc28

 https://tools.ietf.org/html/rfc2866

 https://tools.ietf.org/html/rfc5080

2.2 В Минимальной выгрузке должны присутствовать пакеты access-request и access-accept.

2.3 RADIUS-пакеты должны содержать следующий минимальный набор полей:

Access request packets:

required: User\_Name | Cisco Vendor Account\_Info

required: NAS\_Identifier | NAS\_IP\_Address

required: NAS\_Port\_Id | NAS\_Port

Access accept packets:

required: User\_Name | Cisco Vendor Account\_Info

required: NAS\_Identifier | NAS\_IP\_Address

required: Framed\_IP\_Address

required: NAS\_Port\_Id | NAS\_Port

2.4 В сообщениях запрос-ответ должна прослеживаться клиент-серверная связность по ip-адресам, портам и id.

**2. Состав и описание работы**

На схеме представлена структурная схема программного обеспечения «Спектр Актив 139»



Спектр Актив состоит из трёх основных модулей:

1.Анализатор сетевого трафика – съёмник (sniffer).

Съёмник выполняет задачу анализа сетевого трафика и фильтрации пакетов по заданным критериям.

2.Брокер сообщений RabbitMQ.

Связывает между собой java-приложение и sniffer. Программный брокер сообщений на основе стандарта AMQP — тиражируемое связующее программное обеспечение, ориентированное на обработку сообщений. Создан на основе системы Open Telecom Platform, написан на языке Erlang, в качестве движка базы данных для хранения сообщений использует Mnesia.Состоит из сервера, библиотек поддержки протоколов HTTP, XMPP и STOMP[en], клиентских библиотек AMQP для Java и .NET Framework и различных плагинов (таких как плагины для мониторинга и управления через HTTP или веб-интерфейс или плагин «Shovel» для передачи сообщений между брокерами). Имеется реализация клиентов для доступа к RabbitMQ для целого ряда языков программирования, в том числе для Perl, Python, Ruby, PHP. Поддерживается горизонтальное масштабирование для построения кластерных решений.

3.Java – приложение.

Java приложение включает в себя часть бизнес-логики и осуществляет возможность взаимодействия комплекса «Спектр Актив 139» с программно-аппаратными комплексами (Пульт управления ФСБ, ПУ) ФСБ.

Комплекс программ «Спектр Актив 139» устанавливается на серверные платформы с операционной системой Astra Linux Релиз “Орёл” и требует установки дополнительных библиотек. Все они бесплатные, создаются и распространяются в соответствии с моделью разработки свободного и открытого программного обеспечения.

Сервер с установленным на нём программным обеспечением «Спектр Актив 139» подключается к сети оператора связи пассивно посредством оптических ответвителей или SPAN порта, по которым подается абонентский и авторизационный недекодированный трафик. Количество и типы интерфейсов определяются в зависимости от объемом и особенностей подаваемого трафика. Посредством выделенного порта осуществляется подключение с Пункту Управления ФСБ (далее ПУ). Внутри сетевого соединения предусматривается возможность создания виртуальной сети VPN (Virtual Private Network) по протоколу туннелирования второго уровня L2TP (IPSec VPN) для туннелирования всего рабочего TCP/IP трафика. Также устройство подключается к ИС БД ОРМ для выгрузки статистической информации и содержимого соединений. Количество и типы интерфейсов определяются в зависимости от объемом подаваемого трафика со стороны оператора. При поступлении внешних команд на установку контролей со стороны ПУ происходит анализ обрабатываемого трафика и отбор пакетов данных, удовлетворяющих критериям отбора. В зависимости от типов контролей на интерфейсы подключения ПУ передаются либо недекодированные данные в порядке их прохождения через точки съемника, либо данные, декодированные до протоколов прикладных уровней, в формате сообщений, приведенных в Приложении №2 Приказа №139. При наличии подключения к ИС БД ОРМ осуществляется передача статистической информации в полном объеме. Содержимое соединений передается в соответствии с установленными с ПУ фильтрами, по которым трафик исключается из передачи на ИС БД ОРМ. При отсутствии заданных критериев фильтрации сообщения пользователей услугами связи передается в полном объёме. Формат сообщений обмена между устройством и ИС БД ОРМ соответствует требованиям, приведенным в Приложении №2.1 Приказа №139.

**3.Возможности**

Сервер с установленным на нём программным обеспечением «Спектр Актив 139» обеспечивает следующие возможности:

1. Подключение к сети передачи данных с использованием не менее одного из интерфейсов согласно перечню:

интерфейсы с использованием контроля несущей и обнаружением коллизий, включая:

− оптические интерфейсы 10GBASE-S;

− оптические интерфейсы 10GBASE-L;

− оптические интерфейсы 10GBASE-E;

− оптические интерфейсы 10GBASE-LX4;

− электрические интерфейсы 10GBASE-CX4;

− оптические интерфейсы 1000 BASE-X;

− электрический интерфейс GBE;

− оптические интерфейсы 100BASE-X;

− электрические интерфейсы 100BASE-T;

− оптические интерфейсы 10BASE-F;

− электрические интерфейсы EtherNet;

2.Подключение 16-ти пунктов управления техническими средствами ОРМ для управления техническими средствами ОРМ с целью проведения оперативно-разыскных мероприятий с использованием интерфейса EtherNet IEEE 802.3 TX и назначением одного из ПУ ОРМ головным;

3. Взаимодействие с ПУ ОРМ в соответствии с протоколом взаимодействия технических средств ОРМ с ПУ ОРМ, который приведен в Приказах Министерства связи и массовых коммуникаций № 83 от 16.04.2014 г. и № 139 от 15.04.2019 г.

4. Подключение технических и программных средств информационных систем, содержащих базы данных абонентов оператора связи и предоставленных им услугах связи, обеспечивающих выполнение установленных действий при проведении оперативно-разыскных мероприятий (далее – ИС БД ОРМ) в соответствии с Приложением № 2.1 Приказа № 139 от 15.04.2019 г.

5. Обработку всех пакетов данных, поступающих на интерфейсы подключения технических средств ОРМ к сети передачи данных, с целью отбора и передачи на ПУ ОРМ информации, относящейся к контролируемым соединениям и (или) сообщениям электросвязи, в процессе установления соединений и (или) передачи сообщений электросвязи, в соответствии с заданными с ПУ ОРМ следующими параметрами контроля:

а) постоянный IP-адрес (IPv.4, IPv.6);

б)IP-адреса, определяемые по маске;

в) имя учетной записи пользователя, используемое для идентификации пользователя услуг связи при доступе к сети передачи данных и телематическим услугам связи

г) электронный почтовый адрес для всех почтовых сервисов с применением протоколов SMTP, POP3, IMAP4, не использующих средства защиты информации, включая криптографические;

д) электронный почтовый адрес сервисов Web-mail, в том числе mail.ru, yandex.ru, rambler.ru, gmail.com, yahoo.com, aport.ru, rupochta.ru, hotbox.ru, не использующих средства защиты информации, включая криптографические;

е) телефонный номер пользователя (вызываемого и (или) вызывающего);

ж) идентификатор абонентской телефонной линии, используемый для идентификации пользователя услуг связи при доступе к сети передачи данных и телематическим услугам связи;

з) идентификатор вызываемого и вызывающего пользователя услуг связи по передаче данных для целей передачи голосовой информации;

и)международный идентификатор абонента сети подвижной связи (IMSI);

к) международный идентификатор мобильного оборудования (IMEI);

л) уникальный идентификатор оборудования сетей передачи данных (MAC-адрес);

м)идентификатор служб обмена сообщениями, включая ICQ;

н)мобильный идентификационный номер мобильной абонентской радиостанции (MIN),

о) унифицированный идентификатор ресурса (URI);

п) доменное имя сервера;

р) код прикладного протокола;

с) тип прикладного протокола;

т) тип содержимого прикладного протокола;

у) поле прикладного протокола;

ф)параметры в формате синтаксиса правил отбора и фильтрации трафика;

6. Передачу на ПУ ОРМ идентификатора пользователя, используемого для идентификации пользователя услуг связи при доступе к сети передачи данных и телематическим услугам связи;

7. Отбор и передачу на ПУ ОРМ информации не менее чем по 2000 значениям параметров контроля для всех подключенных ПУ ОРМ;

8. Удаление всех параметров контроля и отобранной информации при сбоях технических средств ОРМ, при пропадании электропитания и перезапуске технических средств ОРМ с ПУ ОРМ;

9. Передачу на ПУ ОРМ результатов обработки сообщений протоколов аутентификации и протоколов установления соединений при предоставлении услуг связи по передаче данных для целей передачи голосовой информации, включая информацию о местоположении абонентских терминалов в случае ее наличия в указанных сообщениях;

10. Хранение отобранной информации объемом не менее 2 Гбайт в энергозависимой памяти, предназначенной для выравнивания нагрузки в канале связи с ПУ ОРМ;

11. Передачу в ИС БД ОРМ статистической информации обо всех соединениях абонентов;

12. Передачу в ИС БД ОРМ текстовых сообщений пользователей услугами связи, голосовой информации, изображений, звуков, видео-, иных сообщений пользователей услугами связи, за исключением информации, удовлетворяющей заданным головным ПУ критериям фильтрации сообщений. При отсутствии заданных головным ПУ критериев фильтрации сообщения пользователей услугами связи передается техническими средствами ОРМ в ИС БД ОРМ в полном объёме;

13. Поддержку до 2000 критериев критериев фильтрации следующих типов:

а) IP-адресов;

б) идентификаторов виртуальных сетей VLAN, MPLS;

в) диапазонов портов;

г) унифицированного идентификатора ресурса (URI);

д) доменного имени сервера;

е) кода прикладного протокола;

ж) типа прикладного протокола;

з) типа содержимого прикладного протокола;

и) поля прикладного протокола;

к) критериев в формате синтаксиса правил отбора и фильтрации трафика;

14. Обработку всех данных, поступающих на технические средства ОРМ от сети передачи данных, в соответствии с классом технических средств ОРМ

**4. Подготовка к использованию**

Должно быть обеспечено подключение через сетевые разъемы следующих каналов:

1. Канал управления (на период настройки системы);

2. Канал до ПУ УФСБ;

3. Канал для съема абонентского трафика оператора связи;

4. Канал для подключения к ИС БД ОРМ(при необходимости).

Сервер с установленным на нём программным обеспечением «Спектр Актив 139» соответствует следующим характеристикам:

• Взаимодействие с ПУ ОРМ в соответствии с протоколом взаимодействия технических средств ОРМ с ПУ ОРМ, который приведен в Приказах Министерства связи и массовых коммуникаций № 83 от 16.04.2014 г. и № 139 от 15.04.2019 г.;

• Подключение технических и программных средств информационных систем, содержащих базы данных абонентов оператора связи и предоставленных им услугах связи, обеспечивающих выполнение установленных действий при проведении оперативно-разыскных 2 мероприятий (далее – ИС БД ОРМ) в соответствии с Приложением № 2.1 Приказа № 139 от 15.04.2019 г.;

• Обработка всех пакетов данных, поступающих на интерфейсы подключения технических средств ОРМ к сети передачи данных по каналами Ethernet 10/100/1GbE и 10GbE/40GbE (подключение к сплиттеру/SPANпорту);

• Отбор и передача на ПУ информации в соответствии со следующими критериями отбора: MAC-адрес, IP-адрес, IP-маска, диапазон портов, VLAN, логин, телефонный номер, IMSI, IMEI, идентификатор абонентской телефонной линии, MIN, VOIP-идентификатор, почтовый адрес, IM-идентификатор, URI, доменное имя, код, тип, поле и тип содержимого прикладного протокола, в формате tcpdump;

• Передача в ИС БД ОРМ текстовых сообщений пользователей услугами связи, голосовой информации, изображений, звуков, видео-, иных сообщений пользователей услугами связи, за исключением информации, удовлетворяющей заданным головным ПУ критериям фильтрации сообщений: IP-адрес, VLAN, MPLS, URI, диапазонов портов, доменное имя, код, тип, поле и тип содержимого прикладного протокола, в формате tcpdump

• Работа с полным спектром технологий передачи данных и голоса, IGRP, MPLS, GPRS, CDMA, WiMAX, LTE;

• Прием и полное декодирование данных до прикладных протоколов с целью выделения событий электронной переписки, voip звонков, передачи мгновенных сообщений, http и https-активности, событий терминального доступа к оборудованию и передачи данных по протоколу ftp

• Гибкая система мониторинга работоспособности комплекса;

• Обработка всех данных, поступающих на технические средства ОРМ от сети передачи данных, в соответствии с классом технических средств ОРМ.