НИКА X

ЦИТАДЕЛЬ
ГРУППА КОМПАНИЙ

Программный комплекс «Вектор-IP-374» (ПК «Вектор-IP-374»)

Описание функциональных характеристик

Версия 2.0, ноябрь 2022

2022

Тел.: +7 495 280-04-39
E-mail: info@nikasorm.ru
www.nikasorm.ru

СОДЕРЖАНИЕ

Тел.: +7 495 280-04-39
E-mail: info@nikasorm.ru
www.nikasorm.ru

ВВЕДЕНИЕ

Настоящий документ содержит описание функциональных характеристик программного обеспечения – Программный комплекс «Вектор-IP-374» (ПК «Вектор-IP-374»), предназначенного для установки на программно-аппаратный комплекс (ПАК) «Вектор-IP-374» в составе с программно-аппаратными модулями (ПАМ) «Вектор-IP-374-XXXXXX-XXXXXX.XXXXXX», производства ООО «Ника-Х».

ИНФОРМАЦИЯ О ПРАВЕ СОБСТВЕННОСТИ

Тел.: +7 495 280-04-39
E-mail: info@nikasorm.ru
www.nikasorm.ru

1. Описание функциональных возможностей и области применения

Программный комплекс «Вектор-IP-374» (ПК «Вектор-IP-374»), предназначен для установки на программно-аппаратный комплекс (ПАК) «Вектор-IP-374» в составе с программно-аппаратными модулями (ПАМ) «Вектор-IP-374-XXXXXX-XXXXXX.XXXXXX».

Область применения: в системах обеспечения ОРМ в соответствии с требованиями НПА: приказы Минкомсвязи РФ №83 от 16.04.2014 г., № 139 от 15.04.2019 г., №573 от 29.10.2018 г., ФЗ-374 на всех видах сетей операторов связи.

Функциональные возможности: перехват информации путем пассивного подключения к каналам 1/10/100GE, генерация статистических сообщений. Прием трафика и обработка протоколов 1-7 уровня МВОС, протоколов сигнализации GTP-C, RADIUS, DIAMETR. Одновременный контроль до 100000 абонентов по критериям отбора, декодирование отобранной информации. Формирование и индексация глобальных идентификаторов, осуществление группировки IP пакетов по принадлежности контенту с записью в БД, обработка запросов от ИС на поиск статистики и соответствующего контента.

Программный комплекс «Вектор-IP-374» (ПК «Вектор-IP-374») состоит из следующих модулей: «Cenzor_S», «WRHG», «Dpdk.reader_S», «SORM», «Xmanager_S», «Rconsole_S», «Replicator», «SXDPWR», «SGN», «ZetAgent_S», «IPMIMON», «Rbal», «Rext», «Rout».

Данные модули включены в установочный файл ПК «Вектор-IP-374» как компоненты, не предполагают самостоятельной установки и эксплуатации, настраиваются специалистами ООО «Ника-Х» и поставляются исключительно в составе ПАК, производимых ООО «Ника-Х».

Конфигурация модулей в ПК «Вектор-IP-374» зависит от видов предоставляемых услуг связи оператором связи, количества и типов используемых интерфейсов в точках съема копии трафика.

Внимание! Программный комплекс «Вектор-IP-374» (ПК «Вектор-IP-374») поставляется исключительно в предустановленном виде и является СПО (специальным программным обеспечением) для установки на ТС ОРМ (технические средства для проведения оперативно-розыскных мероприятий) и не предполагает самостоятельной установки и обновления.

Тел.: +7 495 280-04-39
E-mail: info@nikasorm.ru
www.nikasorm.ru

2. Функции ПК «Вектор-IP-374» в составе ТС ОРМ сетей передачи данных

Согласно требованиям Правил применения оборудования коммутации и маршрутизации пакетов информации сетей передачи данных, включая программное обеспечение, обеспечивающего выполнение установленных действий при проведении оперативно-розыскных мероприятий, в соответствии с требованиями приказа Минкомсвязи РФ №83 от 16.04.2014 г., № 139 от 15.04.2019 г. программный комплекс «Вектор-IP-374» (ПК «Вектор-IP-374») в составе ТС ОРМ обеспечивает выполнение следующих функций:

- Подключение к сети передачи данных с использованием не менее одного из следующих интерфейсов: 10GBASE-S, 10GBASE-L, 10GBASE-E, 10GBASE-LX4, 10GBASE-CX4, 1000 BASE-X, GBE, 100 BASE-X, 100 BASE-T, 10 BASE-F, Ethernet, STM-1, STM-4, STM-16, STM-64, E1, E3, E4, V.24/V.28, X.21/V.11, V.35/V.28, V.36/V.11.
- Подключение 16 ПУ для управления техническими средствами ОРМ с использованием интерфейса Ethernet IEEE 802.3 TX и назначением одного из ПУ головным.
- Подключение ИС БД ОРМ.
- Взаимодействие с ПУ и ИС БД ОРМ в соответствии с протоколами взаимодействия ТС ОРМ с ПУ и ИС БД ОРМ.
- Обработку всех пакетов данных, поступающих на интерфейсы подключения ТС ОРМ к сети передачи данных, с целью передачи в ИС БД ОРМ статистической информации и содержимого сообщений пользователей услугами связи, отбора и передачи на ПУ информации, относящейся к контролируемым соединениям и (или) сообщениям электросвязи, в процессе установления соединений и (или) передачи сообщений электросвязи, в соответствии с заданными с ПУ следующими параметрами контроля: постоянный IP-адрес (IPv.4; IPv.6); IP-адреса, определяемые по маске; имя учетной записи пользователя, используемое для идентификации пользователя услуг связи при доступе к сети передачи данных и телематическим услугам связи; электронный почтовый адрес для всех почтовых сервисов с применением протоколов SMTP, POP3, IMAP4, не использующих средства защиты информации, включая криптографические; 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; телефонный номер пользователя (вызываемого и (или) вызывающего); идентификатор абонентской телефонной линии, используемый для идентификации пользователя услуг связи при доступе к сети передачи данных и телематическим услугам связи; идентификатор вызываемого и

Тел.: +7 495 280-04-39
E-mail: info@nikasorm.ru
www.nikasorm.ru

вызывающего пользователя услуг связи по передаче данных для целей передачи голосовой информации; международный идентификатор абонента сети подвижной связи (IMSI); международный идентификатор мобильного оборудования (IMEI); уникальный идентификатор оборудования сетей передачи данных (MAC-адрес); идентификатор служб обмена сообщениями, включая ICQ; мобильный идентификационный номер мобильной абонентской радиостанции (MIN); унифицированный идентификатор ресурса (URI); доменное имя сервера; код, тип и поле прикладного протокола; тип содержимого прикладного протокола; параметры в формате синтаксиса правил отбора и фильтрации трафика.

- Отбор и передачу на ПУ информации не менее чем по 2000 значениям параметров контроля, для всех подключенных ПУ.
- Удаление всех параметров контроля и отобранной информации при сбоях технических средств ОРМ, при пропадании электропитания и перезапуске технических средств ОРМ с ПУ.
- Передачу на ПУ 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;
- Возможность хранения отобранной информации объемом не менее 2 Гбайт в энергозависимой памяти, предназначенной для выравнивания нагрузки в канале связи с ПУ.
- Обработку всех данных, поступающих на технические средства ОРМ от сети передачи данных, в соответствии с классом ТС ОРМ, указанным в таблице 1.

Таблица 1. Классы ТС ОРМ.

Класс ТС ОРМ	**Скорость потока информации, поступающей на ТС ОРМ, Мбит/с, не менее**	**Суммарная скорость передачи данных на выходе ТС ОРМ, предназначенном для связи с ПУ, Мбит/с**
I	100	Не менее 5% от скорости поступающего на ТС ОРМ потока информации
II	400	
III	900	
IV	4 000	> 100
V	9 000	> 100
VI	20 000	> 1000
VII	100 000	> 1000

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

Тел.: +7 495 280-04-39
E-mail: info@nikasorm.ru
www.nikasorm.ru

сообщений. При отсутствии заданных головным ПУ критериев фильтрации сообщения пользователей услугами связи передаются техническими средствами ОРМ в ИС БД ОРМ в полном объеме. Технические средства ОРМ должны обеспечивать обработку до 2000 критериев фильтрации сообщений.

- Поддержку критериев фильтрации следующих типов: IP-адресов; идентификаторов виртуальных сетей VLAN, MPLS; диапазонов портов; унифицированного идентификатора ресурса (URI); доменного имени сервера; кода прикладного протокола; типа прикладного протокола; типа содержимого прикладного протокола; поля прикладного протокола; критериев в формате синтаксиса правил отбора и фильтрации трафика.
- ТС ОРМ обеспечивают контроль собственного функционирования и передачу на головной ПУ информации о текущем техническом состоянии, а в случае отсутствия соединения с ПУ технические средства ОРМ должны обеспечивать сохранение в энергонезависимой памяти такой информации и передачу ее на ПУ при восстановлении соединения.
- ТС ОРМ не должны оказывать влияние на работоспособность средств связи сети передачи данных, должны быть выполнены в отдельном корпусе, оснащенном запирающими устройствами, исключающими возможность свободного доступа к аппаратным элементам ТС ОРМ.

3. Функции ПК «Вектор-IP-374» в составе технических средств ИС БД ОРМ

Посредством ИС БД ОРМ осуществляется накопление, хранение, поиск и предоставление по запросу с ПУ субъекту ОРД в автоматическом режиме информации об абонентах и оказанных пользователям услугах связи, в том числе о фактах приема, передачи, доставки и (или) обработки голосовой информации, текстовых сообщений, изображений, звуков, видео- или иных сообщений пользователей услугами связи, содержании голосовой информации, текстовых сообщений, изображений, звуков, видео- или иных сообщений пользователей услугами связи, а также иной информации.

Взаимодействие технических и программных средств ИС БД ОРМ с ПУ должно осуществляться по пяти каналам передачи данных: канал управления (кпд1); канал данных (кпд2); канал мониторинга (кпд3); канал неформатированных данных (кпд4); канал доставки сообщений пользователей услугами связи (кпд5).

Тел.: +7 495 280-04-39
E-mail: info@nikasorm.ru
www.nikasorm.ru

Посредством ПК «Вектор-IP-374», технических и программных средств ИС БД ОРМ обеспечиваются:

- Сбор и обработка информации, из различных источников для наполнения и формирования баз данных для последующего ее накопления, хранения и предоставления по запросу ПУ.
- Накопление и хранение на срок до 6 месяцев текстовых сообщений, изображений, звуков, видео- или иных сообщений пользователей услугами связи (при наличии лицензий на услуги связи по предоставлению каналов связи, услуги связи в сети передачи данных, за исключением передачи голосовой информации, телематические услуги связи) с момента окончания их приема, передачи, доставки и (или) обработки.
- Автоматическое удаление сообщений электросвязи пользователей услугами связи в соответствии пунктом 8 Правил хранения операторами связи текстовых сообщений пользователей услугами связи, изображений, звуков, видео- и иных сообщений пользователей услугами связи, утвержденных постановлением Правительства Российской Федерации от 12.04.2018 № 445.
- Контроль времени поступления из сетей связи информации и информирование ПУ о превышении значений.
- Накопление, хранение и обработка информации об абонентах и других пользователях данной сети, о выделенных абонентам телефонных номерах и кодах идентификации, об оказанных абонентам услугах связи и иной информации, необходимой для выполнения возложенных на уполномоченные государственные органы задач по проведению ОРМ в случаях, установленных федеральными законами, в течение трех лет.
- Поиск запрашиваемой с ПУ информации, хранимой в технических и программных средствах ИС БД ОРМ.
- Защита от несанкционированного доступа и информирование ПУ о попытках такого доступа.
- Контроль работоспособности и загруженности технических и программных средств ИС БД ОРМ.
- Контроль за соблюдением предоставленных прав доступа к хранящейся в технических и программных средствах ИС БД ОРМ информации.
- Круглосуточный удаленный доступ со стороны операторов ПУ к хранящейся в технических и программных средствах ИС БД ОРМ информации.
- Реализация протокола взаимодействия технических и программных средств ИС БД ОРМ и оборудования ПУ.

Тел.: +7 495 280-04-39
E-mail: info@nikasorm.ru
www.nikasorm.ru

- Прием от ПУ запросов об абонентах и других пользователях и предоставленных им услугах связи.
- Передача на ПУ от технических и программных средств ИС БД ОРМ данных в соответствии с поступившими с ПУ запросами.
- Взаимодействие с техническими средствами ОРМ в соответствии с утвержденным протоколом взаимодействия.
- Получение текстовых сообщений, изображений, звуков, видео- или иных сообщений пользователей услугами связи (при наличии лицензий на услуги связи по предоставлению каналов связи, услуги связи в сети передачи данных, за исключением передачи голосовой информации, телематические услуги связи), а также информации об оказанных абонентам услугах связи, в том числе о фактах приема, передачи, доставки и (или) обработки информации, текстовых сообщений, изображений, звуков, видео- или иных сообщений пользователей услугами связи, по запросу с ПУ и передача результатов в соответствии с протоколом взаимодействия ПУ и ИС БД ОРМ.
- Посредством технических и программных средств ИС БД ОРМ обеспечивается ведение в автоматическом режиме системных файлов, содержащих информацию о работе технических и программных средств ИС БД ОРМ.
- Сохранность и доступность для дальнейшего использования ранее накопленных данных при модернизации технических и программных средств ИС БД ОРМ.
- Сбор и накопление информации о соединениях, инициированных абонентами и другими пользователями и реализованных посредством услуг сети передачи данных (при наличии лицензий на услуги связи по предоставлению каналов связи, услуги связи в сети передачи данных, за исключением передачи голосовой информации, телематические услуги связи): подключениях абонента к сети передачи данных и отключениях от сети передачи данных; HTTP-соединениях с информационными ресурсами сети передачи данных; соединениях для передачи почтовых сообщений; передаче электронных сообщений между пользователями (служебных сообщениях, мгновенных сообщениях, коротких сообщениях, мультимедийных сообщениях, отправленных посредством сети передачи данных); голосовой связи посредством сети передачи данных; передаче файловых данных; терминальном доступе к оборудованию для удаленного управления; передаче прочих сообщений, принимаемых (получаемых) абонентом при помощи закрытых протоколов обмена; изменении сетевых адресов пользователей, если такая замена (трансляция) сетевых адресов в процессе оказания услуг

связи осуществляется на оборудовании связи сети передачи данных оператора связи; о кодах идентификации, выделенных абонентам выделенной сети и адресации, используемой в выделенной сети. Информация должна храниться в течение трех лет с момента окончания осуществления таких действий.

- Сбор, накопление и хранение информации о следующих соединениях и сеансах связи абонентов (пользователей услугами телефонной связи) реализованных посредством сетей телефонной связи: телефонных соединениях; входящих/исходящих текстовых коротких сообщениях, как доставленных, так и не доставленных абоненту; служебных соединений; иной информации о телефонных соединениях абонентов и других пользователей телефонной сети связи.
- Накопление и хранение голосовой информации, текстовых сообщений, изображений, звуков, видео- или иных сообщений пользователей услугами связи, в соответствии с пунктом 6 Правил хранения операторами связи текстовых сообщений пользователей услугами связи, голосовой информации, изображений, звуков, видео- и иных сообщений пользователей услугами связи, утвержденных постановлением Правительства Российской Федерации от 12.04.2018 № 445.

4. Стандарты

Программный комплекс «Вектор-IP-374» (ПК «Вектор-IP-374») создан при соблюдении условий и требований, следующих НПА:

- Приказ Минкомсвязи Российской Федерации от 29.10.2018 г. № 573 «Об утверждении требований к техническим и программным средствам информационных систем, содержащих базы данных абонентов оператора связи и предоставленных им услугах связи, а также информацию о пользователях услугами связи и о предоставленных им услугах связи, обеспечивающих выполнение установленных действий при проведении оперативно-розыскных мероприятий»;
- Приказ Минкомсвязи России от 15.04.2019 N 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

Тел.: +7 495 280-04-39
E-mail: info@nikasorm.ru
www.nikasorm.ru

оперативно-розыскных мероприятий», утвержденные приказом Министерства связи и массовых коммуникаций Российской Федерации от 16.04.2014 N 83;

– Федеральный закон от 06.07.2016 № 374-ФЗ «О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности».