|  |
| --- |
|   |
| **министерство ЦИФРОВОГО РАЗВИТИЯ, связи и массовых коммуникаций российской федерации** |
|  |
| **приказ** |
|  | № |  |
| Москва |

**О внесении изменений в Требования 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, утвержденные приказом Министерства связи и массовых коммуникаций Российской Федерации
от 29.10.2018 № 573**

В соответствии со статьей 41 и 64 Федерального закона от 7 июля 2003 г. № 126‑ФЗ «О связи» (Собрание законодательства Российской Федерации, 2003, № 28, ст. 2895; 2014, № 26, ст. 3366; 2021, № 11, ст. 1709), пунктами 4 и 12 Правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-разыскную деятельность, утвержденных постановлением Правительства Российской Федерации от 27 августа 2005 г. № 538 (Собрание законодательства Российской Федерации, 2005, № 36, ст. 3704; 2018, № 3, ст. 556; № 40, ст. 6142) и пунктами 5 − 8 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 апреля 2018 г. № 445 (Собрание законодательства Российской Федерации, 2018, № 17 , ст. 2489; № 49, ст. 7600),

ПРИКАЗЫВАЮ:

Утвердить прилагаемые изменения, которые вносятся в Требования 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-разыскных мероприятий, утвержденные приказом Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 29.10.2018 № 573.

Министр М.И. Шадаев

УТВЕРЖДЕНЫ

приказом Министерства

цифрового развития, связи и массовых

коммуникаций Российской Федерации

от\_\_\_\_\_\_\_\_\_\_\_\_\_2022 г. №\_\_\_\_\_

**ИЗМЕНЕНИЯ**

**в Требования 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, утвержденные приказом Министерства цифрового развития связи и массовых коммуникаций Российской Федерации
от 29.10.2018 № 573**

1. Подпункт 15 пункта 19 изложить в следующей редакции:

«15) взаимодействие с техническими средствами ОРМ в соответствии с протоколом взаимодействия, приведенным в приложении № 3 к Правилам применения оборудования систем коммутации, включая программное обеспечение, обеспечивающего выполнение установленных действий при проведении оперативно-розыскных мероприятий. Часть IV. Правила применения оборудования систем коммутации, включая программное обеспечение и технические средства накопления голосовой информации, обеспечивающего выполнение установленных действий при проведении оперативно-розыскных мероприятий, утвержденным приказом Министерства связи и массовых коммуникаций Российской Федерации от 26.02.2018 № 86 (зарегистрирован Министерством юстиции Российской Федерации 28 марта 2018 г., регистрационный № 50536), официальный интернет-портал правовой информации (<http://www.pravo.gov.ru>), 29.03.2018) (далее соответственно – Протокол взаимодействия с ТС ОРМ НГИ; приложение № 3 Правил, утвержденных Приказом‑86).

При организации подключения к ТС ОРМ НГИ по Протоколу взаимодействия с ТС ОРМ НГИ ИС ОРМ присваивает этим ТС ОРМ отдельный номер TelcoID. Данный номер TelcoID должен присутствовать в соответствующих справочниках, отправляемых на ПУ, в качестве филиала оператора связи и иметь текстовое описание, указывающее на подключение по Протоколу взаимодействия с ТС ОРМ НГИ».

2. В пункте 22:

а) абзац первый изложить в следующей редакции:

«22. Посредством технических и программных средств ИС ОРМ обеспечивается непрерывный 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):»;

б) подпункт 8 изложить в следующей редакции:

«8) передаче прочих сообщений, передаваемых (получаемых) абонентом при помощи закрытых протоколов обмена, а также протокола DNS;»;

в) дополнить подпунктом 11 следующего содержания:

«11) о фактах входа и иных действиях в личном кабинете абонента.».

3. В пункте 23:

а) абзац первый изложить в следующей редакции:

«23. Посредством технических и программных средств ИС ОРМ обеспечиваются непрерывный сбор, накопление и хранение информации о следующих соединениях и сеансах связи абонентов (пользователей услугами телефонной связи) реализованных посредством сетей телефонной связи:»;

б) дополнить абзацем следующего содержания:

«Информация о соединениях абонентов, использующих услуги VoWiFi (WiFi Calling и аналогичные), должна храниться в ИС ОРМ в формате статистических записей о телефонных соединениях абонентов. В качестве информации о местоположении должны указываться географические координаты абонентского устройства, либо IP-адрес и порт точки доступа WiFi-сети. В случае одновременного наличия актуальной информации о нескольких типах местоположения абонента следует дополнительно формировать отдельные статистические записи, соответствующие обновлению местоположения в мобильной сети связи.».

4. Пункт 24 изложить в следующей редакции:

«24. Посредством технических и программных средств ИС ОРМ обеспечивается непрерывный сбор, накопление и хранение информации об изменении местоположения абонентов в соответствии с протоколом, приведенным в разделе «Locations.asn» приложения № 9 к Требованиям, доступную в сети связи, как при предоставлении услуги связи, так и в режиме ожидания вызова (при переключении его обслуживания разными устройствами сети связи, находящимися в разных географических зонах обслуживания, при включении и/или выключении абонентского устройства, при рассылке запросов от средств связи, при любом информационном обмене между абонентским устройством и коммутационным оборудованием, включая пейджинг и периодические запросы обновления местоположения).».

5. Пункт 25 дополнить абзацами следующего содержания:

«ИС ОРМ должна иметь функционал настройки правил формирования строк HTTP-статистики по критериям «Тип запроса (HTTP Request Methods)» и «Тип содержимого (HTTP Content-Type)».

По умолчанию ИС ОРМ должна формировать отдельные строки HTTP-статистики для каждой записи, соответствующей любому из критериев:

- тип запроса POST;

- тип содержимого text/html;

- тип содержимого application/\* (за исключением application/javascript, json, woff).

При наличии нескольких сообщений протокола HTTP в рамках одной TCP-сессии, содержимое данной сессии записывается в полном объеме в единый pcap-файл и соотносится с каждой формируемой строкой HTTP-статистики.

Если в потоке TCP содержатся только сообщения протокола HTTP,
по которым не требуется формировать строки HTTP-статистики, то формируется одна строка HTTP-статистики по первому сообщению протокола HTTP в потоке TCP.

В случае организации вызовов по протоколу STUN через сервисы обмена мгновенными сообщениями в сети «Интернет» требуется накапливать внешние и внутренние сетевые реквизиты абонента и его контакта.

При этом статистические записи об использовании протокола STUN формируются путем формирования дополнительной строки в статистике VoIP-соединений (структура «dataVoipRecord» раздела «ReportsConnections.asn» приложения № 9 к Требованиям). Параметры «voip-calling-number» и voip-called-number блока «DataVoipRecordContent» имеют следующую структуру:

voip-calling-number:

- original-number (stun:[телефонный номер абонента (при наличии)] prvip:[внутренний (серый) IP-адрес абонента: используемые порты] pubip:[внешний (белый) IP-адрес абонента: используемые порты] proxyip:[IP-адрес прокси-сервера: используемые порты (при наличии)]);

- e164-number ([телефонный номер абонента (при наличии)]).

voip-called-number:

- original-number (stun: prvip:[внутренний (серый) IP-адрес абонента: используемые порты] pubip:[внешний (белый) IP-адрес абонента: используемые порты].

Посредством технических и программных средств ИС ОРМ обеспечивается сбор, накопление и хранение информации о DNS-запросах абонентов (пользователей).

Формирование статистических записей DNS-запросов осуществляются с заполнением поля SNI/CN структуры «dataRawFlowsRecord» раздела «ReportsConnections.asn» приложения № 9 к Требованиям по следующим правилам:

- включать доменное имя из запроса пользователя (dns-query);

- в случаях, когда в UDP потоке присутствуют доменные имена, размера большего, чем размер поля SNI/CN – сокращать доменные имена до домена второго уровня и удалять дубли.

При этом результат выполнения задачи поиска с заполнением поля SNI/CN должен включать как TLS, так и DNS-запросы пользователей.».

6. Дополнить пунктом 42 следующего содержания:

«42. ИС ОРМ должна обеспечивать передачу на ПУ ОРМ результатов поисковых задач в соответствии с временными характеристиками, приведенными в таблице № 2:

Таблица № 2

|  |  |  |
| --- | --- | --- |
| **№** | **Количество записей в результате выполнения поисковой задачи** | **Время загрузки результатов на ПУ ОРМ** |
| 1 | до 100 000 включительно | < 3 мин |
| 2 | от 100 001 до 200 000 | < 6 мин |
| 3 | от 200 001 до 300 000 | < 9 мин |
| 4 | от 300 001 до 400 000 | < 12 мин |
| 5 | от 400 001 до 500 000 | < 15 мин |
| 6 | от 500 001 до 600 000 | < 18 мин |
| 7 | от 600 001 до 700 000 | < 21 мин |
| 8 | от 700 001 до 800 000 | < 24 мин |
| 9 | от 800 001 до 900 000 | < 27 мин |
| 10 | от 900 001 до 1 000 000 | < 30 мин |

7. В приложении № 1:

а) подпункт 9 пункта 5 дополнить абзацем следующего содержания:

«DNS-запросы абонентов/пользователей услугами связи.»;

б) пункт 5 дополнить подпунктами 11 и 12 следующего содержания:

«11) информацию о соединениях, использующих протокол STUN для организации вызовов посредством Интернет-мессенджеров, включающую:

- телефонный номер абонента;

- внутренние (серые) IP/порт абонента;

- внешние (белые) IP/порт абонента;

- внутренние (серые) IP/порт контакта;

- внешние (белые) IP/порт контакта.

12) информацию о входах и иных действиях в личном кабинете абонента, включающую:

- тип события;

- наименования программы клиента (текстовая строка в произвольном виде, содержащая сведения о наименовании программы, версии, дате обновления, а также иные регистрируемые сведения при передаче);

- идентификатор сообщений пользователей услугами связи.»;

в) подпункт 4 пункта 6 дополнить словами «, а также информацию об IP-адресе и порте точки доступа Wi-Fi-сети»; г) подпункт 10 пункта 9 изложить в следующей редакции:

«10) справочниках с планами внешней и внутренней IP˗адресации, используемой на сети оператора связи с обязательным разделением на пользовательские и служебные подсети;».

8. В приложении № 2:

а) пункт 24 дополнить подпунктами 9-11 следующего содержания:

«9) «Запрос на создание фильтра содержимого соединений сети передачи данных» (CreateFilterRequest);

10) «Запрос на удаление фильтра содержимого соединений сети передачи данных» (DropFilterRequest);

11) «Запрос на получение списка установленных фильтров» (GetFiltersRequest).»;

б) пункт 28 дополнить подпунктами 9-11 следующего содержания:

«9) «Ответ на запрос создания фильтра содержимого соединений сети передачи данных» (CreateFilterResponse);

10) «Ответ на запрос удаления фильтра содержимого соединений сети передачи данных» (DropFilterResponse);

11) «Ответ на запрос получения списка установленных фильтров» (GetFilterResponse).»;

в) абзац четвертый пункта 32 изложить в следующей редакции:

«Задача на поиск информации о действиях абонента в личном кабинете (ValidateEntranceTask)»;

г) пункт 38 дополнить абзацем следующего содержания:

«Результат выполнения поисковой задачи с критерием, содержащим только символ маскирования «\*», содержит все записи, присутствующие в ИС ОРМ по данному типу задач, включая записи, в которых запрашиваемое поле не заполнено.»;

д) пункт 43 изложить в следующей редакции:

«43. При установлении соединения ПУ и ИС ОРМ должны взаимно аутентифицироваться. Аутентификация выполняется установлением SSL/TLS˗соединения поверх установленного TCP˗соединения между ПУ и ИС ОРМ. Для взаимной аутентификации ПУ и ИС ОРМ предварительно создаются X.509–сертификаты, которые должны быть подписаны самоподписанным корневым сертификатом, созданным уполномоченным государственным органом посредством ПУ. ИС ОРМ должна обеспечивать установку указанных корневых сертификатов в качестве доверенных. Созданный для ПУ сертификат используется для аутентификации данного ПУ на одной ИС ОРМ по всем каналам передачи данных – кпд1, кпд2, кпд3, кпд4, кпд5. ПУ и ИС ОРМ используют TLS версии 1.2. Требования к сертификатам (длины ключей, иные параметры) должны быть согласованы для каждой пары ИС ОРМ и ПУ отдельно. В случае невозможности аутентифицировать одну из сторон TCP˗соединение разрывается.»;

е) дополнить пунктом 61 следующего содержания:

«61. ИС ОРМ обеспечивает возможность задания, удаления и запроса установленных фильтров содержимого соединений сети передачи данных при реализации подпункта 2 пункта 27 настоящих требований. ИС ОРМ при этом:

- при получении «Запроса на создание фильтра содержимого соединений сети передачи данных» добавляет заданный фильтр в список, используемый для фильтрации содержимого соединений в сети передачи данных;

- при получении «Запроса на удаление фильтра содержимого соединений сети передачи данных» исключает заданный фильтр из списка, используемого для фильтрации соединений в сети передачи данных;

- обеспечивает запись содержимого соединений сети передачи данных в соответствии с установленными фильтрами:

- при отсутствии установленных правил фильтрации производит запись сетевого трафика в полном объеме;

- при совпадении содержимого соединения с правилом фильтрации исключает данное содержимое из записи.

ИС ОРМ должна обеспечивать возможность настройки фильтра протоколов потокового медиаконтента (параметр protocol-group = 2 структуры «FilterSingleCriteria» раздела «Filters.asn» приложения № 9 к Требованиям) по следующим основным критериям в любой их комбинации:

 - IP-адрес/подсеть;

 - VLAN;

 - MPLS-метка;

 - SNI/URL.

В части предустановленных SNI/URL в обязательном порядке должны быть указаны CDN медиа-потоков видео-сервисов социальных сетей, онлайн-кинотеатров и иных видео-сервисов. Список основных критериев может быть расширен с учетом особенностей трафика, проходящего через сеть связи оператора связи.

При реализации подпункта 1 пункта 27 настоящих требований соответствующие команды управления фильтрацией от ПУ на ИС ОРМ выполняются с параметрами successful = false, error-description содержит произвольное текстовое описание ошибки.».

9. Абзац третий пункта 2 приложения № 4 изложитьв следующей редакции:

«Если на ИС ОРМ передан запрос ПУ «Запрос загрузки данных» (DataLoadRequest), ИС ОРМ направляет «Ответ на запрос загрузки данных» (DataLoadResponse) по кпд1, затем данные блоков отчетов по кпд2 при их наличии.».

10. Пункт 5 приложения № 5 дополнить подпунктом 5 следующего содержания:

«5) процент отфильтрованного трафика в соответствии с установленными на ИС ОРМ фильтрами на запись содержимого.».

11. В приложении № 6:

а) пункт 4 дополнить абзацем следующего содержания:

«Для услуг, предоставляемых в сети подвижной связи, длительность хранения информации о подключении, отключении и изменении местоположения абонентов – 3 суток с момента наступления события, длительность хранения информации о соединениях абонентов в сети передачи данных – 1 сутки с момента наступления события.»;

б) пункт 5 изложить в следующей редакции:

«5. Посредством ИС ОРМ обеспечивается запись в буфер следующей информации в виде архивированных недекодированных файлов:

информация о соединениях и сеансах связи абонентов, реализованных посредством сетей телефонной связи:

- телефонные соединения абонентов, дополненные информацией об идентификаторе потока;

- служебные соединения;

- входящие/исходящие SMS и USSD, как доставленные, так и не доставленные абоненту;

информация о соединениях, инициированных абонентами и другими пользователями и реализованных посредством услуг сети передачи данных;

информация о подключении, отключении и изменении местоположения абонентов – данные, содержащие информацию о параметрах подключения, отключения абонентов и изменения местоположения абонентов, соответствующие следующим событиям:

- присоединение к сети и отключение от сети;

- GTP-C события смены и обновления местоположения включая обновление зоны обслуживания (группы базовых станций);

- события смены зоны обслуживания во время активного вызова либо активной сессии передачи данных, включая смену базовой станции, смену контроллера группы базовых станций, смену обслуживающего коммутатора, смену обслуживающего узла сети передачи данных (SGSN, SGW, либо аналог);

- запросы на дополнительные виды обслуживания.

В случае получения информации о подключении, отключении
и изменении местоположения абонентов, соответствующей иным событиям сети связи, в буфере ИС ОРМ формируются соответствующие статистические записи.

Время обработки информации о подключении, отключении и изменении местоположении абонентов с момента наступления события до момента, когда она становится доступной для запросов ПУ по кпд4, не должно превышать 5 минут.»; в) дополнить пунктом 10 следующего содержания:

«10. Поступающие запросы с ПУ по кпд4 и ответы ИС ОРМ на указанные запросы не должны оказывать влияния на обеспечиваемые ИС ОРМ временные характеристики обработки запросов и поиска информации, указанные в п.п. 34-41 Требований. В организованных каналах передачи данных для доставки информации на ПУ (в соответствии с п. 3 приложения №1 к Требованиям) должна резервироваться пропускная способность, равная или большая среднесуточной скорости поступления данных в циклический буфер.».

12. Приложение № 9 изложить в редакции согласно приложению № 1 к настоящему приказу.

13. В приложении № 13:

а) пункт 2 дополнить абзацем следующего содержания:

«Голосовая информация, получаемая ИС ОРМ от ТС ОРМ НГИ в соответствии с Протоколом взаимодействия с ТС ОРМ НГИ, передается на ПУ в том виде и последовательности, в которых она была получена от ТС ОРМ НГИ без переупаковки и/или перекодирования. ИС ОРМ, при подключении к ТС ОРМ НГИ в качестве дополнительного ПУ, должен выставлять биты поля Transcode в команде получения результатов запроса статистических данных (подпункт 2.2.12 приложения № 3 Правил, утвержденных Приказом-86) равными 0 (получение декодированных данных). В поле data структуры RawRecordContent раздела ReportsDataContent.asn приложения № 9 к Требованиям укладываются байты звуковой информации в формате «a-law», определяемом рекомендацией ITU-T G.711 или с использованием 16 бит в коде ИКМ (PCM) в формате стерео с частотой дискретизации 16 кГц, видео - в соответствии с протоколом 3G-324M с использованием: H.223 для мультиплексирования, H.245 – для управления, G.723.1 (AMR) – для голоса, H.264 (AVC) – для видеоконтента.»;

б) пункт 3 изложить в следующей редакции:

«3. Для изображений, звуков и иных сообщений пользователей услугами связи, передаваемых по сетям передачи данных, информация содержит последовательность кадров канального уровня или датаграмм сетевого уровня в той последовательности, в которой они прошли через точку съема, и записывается в формате pcap.»;

в) дополнить пунктом 4 следующего содержания:

«4. При передаче содержимого соединений по кпд5 соблюдаются следующие правила:

1) Поле «channel» структуры «RawRecordContent» раздела «ReportsDataContent.asn» приложения № 9 к Требованиям должно использоваться в следующих случаях:

- для передачи содержимого соединений из сети передачи данных, которые имеют несколько логических каналов (например – FTP, VoIP). Каждый логический канал разделяется по номеру и содержит данные в формате «pcap». В случае, если размер Pcap-файла больше одного блока данных, то Pcap-файл разбивается на несколько блоков. Заголовок pcap-файла является частью данных и приходит только в первом блоке для определенного канала данных;

- для передачи содержимого соединений, полученных из ТС ОРМ НГИ, в случаях, когда ТС ОРМ НГИ по одному идентификатору соединения возвращает несколько файлов (например, полученных по одному вызову из разных точек съема).

2) Поле «codec-info» структуры «RawRecordContent» раздела «ReportsDataContent.asn» приложения № 9 к Требованиям может быть использовано для передачи типа данных. Пример значений поля «codec-info» приведен в таблице:

**Таблица**

|  |  |  |
| --- | --- | --- |
| **№** | **Значение** | **Описание** |
|  | application/vnd.tcpdump.pcap | Данные в формате pcap для передачи содержимого интернет соединений абонентов |
|  | application/vnd.tsngi.data | Формат для передачи данных для Приказа № 86. Правила заполнения полей приведены ниже. |
|  | image/tiff | Данные в формате многостраничного TIFF документа. Используется для передачи факсов. |
|  | image/t38 | Передача данных в формате факс. |

Значения «tcpdump.pcap» и «tsngi.data» являются основными типами для передачи содержимого соединений. Остальные типы расширяют возможности передачи содержимого соединений. Отсутствие поля «codec-info» эквивалентно заполнению поля «codec-info» значением «application/vnd.tcpdump.pcap».».