ОСОБЕННОСТИ ПОСТРОЕНИЯ системы специальных оперативно-розыскных мероприятий в сетях 5G

В.Тихвинский, д.э.н., академик РАЕН,
профессор МВТУ им. Н.Э.Баумана и МТУСИ,
главный научный сотрудник ФГУП НИИР / vtniir@mail.ru

УДК 621.391.82

Обеспечение законного перехвата сообщений в сетях пятого поколения становится насущной проблемой не только для отражения криминальных и террористических угроз, но и технологической проблемой в условиях изменения парадигмы услуг 5G и появления инновационных технологий передачи данных. В статье анализируется модель и архитектура системы технических средств обеспечения функций оперативно-розыскных мероприятий в сетях 5G, обоснованная Партнерским проектом 3GPP, и проблемные вопросы ее создания.

Введение

Функция законного перехвата сообщений (Lawful Interception) абонентов в сетях 5G позволяет предоставить уполномоченным государственным организациям доступ к частной информации (например, к телефонным разговорам, передаваемым данным, сообщениям SMS, MMS и электронной почты). Согласно российскому законодательству, данная функция обеспечивается системой технических средств для обеспечения функций оперативно-розыскных мероприятий (СОРМ) [1] и представляет собой комплекс технических средств и мер, предназначенных для проведения таких мероприятий в сетях 5G.

Современные системы СОРМ, как и сети мобильной связи, насчитывают несколько поколений, классифицируемых как:

- СОРМ 1 – слежение за аналоговой связью, телефонными переговорами;
- СОРМ 2 – для прослушивания сетей мобильной связи и контроля данных в сетях интернета;
- СОРМ 3 – обеспечивает объединение вышеуказанных поколений систем СОРМ и дополнительно контролирует часть VPN-серверов, прослушивает OTT-приложения: Skype, ICQ и т.п., спутниковую связь и ряд других нововведений. Ключевой фактор системы СОРМ 3 – это единая глобальная база данных, которая взаимно связана с различными направлениями СОРМ.

Система оперативно-розыскных мероприятий в сетях пятого поколения будет отличаться от систем СОРМ мобильных сетей предыдущих поколений (2G/3G/4G). Эти отличия связаны с технологическими особенностями и бизнес-сценариями, реализуемыми в сетях 5G [2].

Во-первых, эти сети основаны на новых технологических принципах, для реализации которых используется полностью виртуальная опорная сеть 5G Core с изменившимися функционалами модулей-функций (NF), а также интерфейсов 5G (NGi), что требует новых возможностей и от СОРМ.

Во-вторых, изменение потенциальных возможностей сетей 5G по скоростям передачи (до 20 Гбит/с)

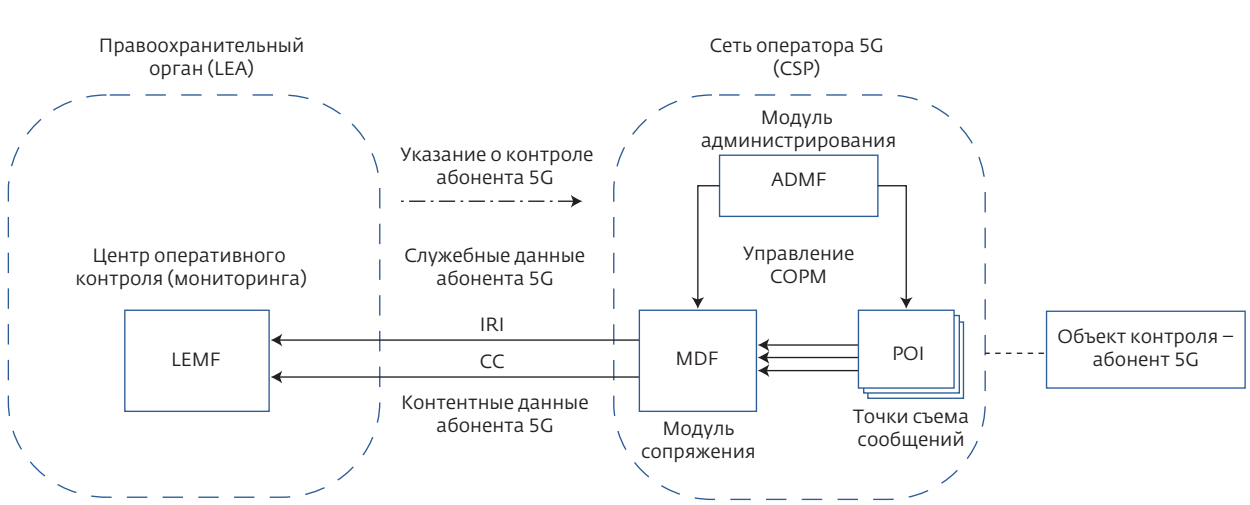

Рис.1. Общая модель COPM в сети 5G

и плотности абонентских устройств (до 1 млн на кв. км), а также появление новых классов устройств, таких как устройства Интернета вещей – IoT (NR Light, eMTC, NB-IoT), беспилотный транспорт (автомобили, БПЛА, водные суда, поезда), видеотерминалов виртуальной, расширенной и дополненной реальности, встроенных систем, которые предъявляют новые требования к средствам мониторинга COPM, ранее не применявшимся в сетях мобильной связи.

В-третьих, большое влияние на сети 5G оказывают организации стандартизации интернета, ориентированные на конфиденциальность данных абонента (такие как IETF), и поставщики нетрадиционного сетевого оборудования OTT с сильными антиправительственными взглядами на контроль передаваемой информации, благодаря чему вводятся новые уровни шифрования и конфиденциальности, что делает многие традиционные инструменты COPM, такие как ловушки IMSI, устаревшими [2].

Стандартизация требований COPM в сетях 5G

Основные нормативные и технические требования к системе COPM сетей 5G разработаны Партнерским проектом 3GPP в Релизе 15 (Фаза 1: разработки 5G для моделей eMBB и URLLC, сентябрь 2018) и в Релизе 16 (Фаза 2: разработки 5G для моделей URLLC и xMTC (mIoT), июнь 2020). Технические спецификации 3GPP по законному перехвату [4–6] охватывают все аспекты COPM, реализуемые в сети 5G, включая:

- общие требования законного перехвата;
- архитектуру и функции законного перехвата;
- протоколы и процедуры для законного перехвата.

Согласно техническим спецификациям 3GPP жизненный цикл COPM состоит из пяти основных этапов. Первый и последний этапы состоят из предоставления данных COPM и отмены предоставления этих данных правоохранительному органу на основе системы оперативно-розыскных мероприятий и законного перехвата сообщений абонентов сети 5G. На трех внутренних этапах система COPM обнаруживает, собирает и доставляет продукт перехвата в органы оперативного контроля правоохранительного органа (LEA). Эти три этапа процесса COPM проводятся каждый раз, когда идентифицируется целевое сообщение, и поэтому могут повторятся многократно в течение жизненного цикла информации COPM.

Стандартизированная 3GPP общая модель COPM в сети 5G (рис.1) состоит из:

- оперативно-технического центра контроля (LEMF), являющегося логическим элементом модели COPM в правоохранительном органе (LEA), который получает информационный продукт перехвата;
- информационного продукта перехвата, включающего два вида сообщений: служебную информацию об абоненте сети 5G (IRI) и контентную информацию абонента (CC);
- модуля администрирования (ADMF), обеспечивающего функции администрирования

оператора 5G (CSP) в интересах СОРМ, включая предоставление и отмену предоставления точек съема информации (POI) и модулей сопряжения (MDF) информационного продукта перехвата;

- точек съема информации (POI), обнаруживающих и фиксирующих сообщения абонента сети 5G на основе информации, предоставленной ADMF, передавая продукт перехвата в функцию посредничества и доставки;
- модулей сопряжения MDF, выполняющих в сети 5G необходимое сопряжение (преобразование) данных перехвата сообщений в форматы данных, отправляемых в оперативно-технический центр контроля LEMF государственного правоохранительного органа LEA.

Контентные данные абонента CC представляют фактический трафик пользователя, подлежащего контролю, который передается по сети 5G с применением целевого идентификатора. Этот трафик включает в себя фактические голосовые сообщения и разговоры, перехваченные и доставленные в таких форматах, как WAV-файлы или IP-сеансы, доставленные в виде пакетов, например PCAP-файлы.

Служебные данные абонента xIRI представляют собой данные, собираемые о пользователе, подлежащем контролю в интересах системы СОРМ. Эти данные состоят из целевых идентификаторов [2] IMSI, GUTI, 5G-GUTI, IMEI, MSISDN и данных об абоненте, включая его неудачные попытки присоединений и вызовов, а также информации об услугах абонента SUPI (5G Subscription Permanent Identifier), используемой для управления профилем услуг, и о местоположении абонента.

Сеть 5G должна обеспечивать возможность СОРМ, которая отвечает соответствующим национальным нормативным и эксплуатационным требованиям. В целом это приводит к формированию следующих требований верхнего уровня к системе СОРМ:

- идентификация цели СОРМ: оператор 5G должен использовать идентификацию пользователя сети, указанную в командном сообщении правоохранительного органа LEA, для обеспечения перехвата сообщений и прослушивания контролируемого абонента. Оператор должен гарантировать, что целевые идентификаторы при необходимости преобразуются сетью 5G в соответствующие идентификаторы, используемые в сети оперативно-технического центра контроля;
- обнаружение объекта СОРМ: сеть связи должна иметь возможность обнаруживать весь контент и метаданные (необходимые для создания сообщений о служебной информации IRI прослушиваемого абонента), связанные с выполненными соединениями и сессиями, чтобы правоохранительный орган LEA полностью понимал контекст связи;
- съем информации: сеть должна быть способна собирать весь контент и метаданные (необходимые для создания сообщений IRI), связанные с целевыми коммуникациями, как предусмотрено в сети для того, чтобы правоохранительный орган LEA полностью понимал контекст связи;
- доставка полученной информации: сеть 5G должна быть в состоянии преобразовать продукт перехвата в согласованный формат правоохранительного органа LEA, чтобы последний мог полностью понять продукт перехвата;
- законность съема информации: способность перехвата сетью должна соответствовать национальному законодательству, ограничениям и режиму отчетности перед правоохранительным органом, включая период СОРМ, продолжительность, территорию, услуги;
- безопасность СОРМ: реализация необнаружимого перехвата, не влияющего на абонентские услуги, то есть законный перехват оператором сети 5G не может быть обнаружен любой стороной, которая не уполномочена правоохранительным органом знать об этом. Информация СОРМ не может быть изменена, исправлена или ухудшена третьей стороной.

Архитектура и интерфейсы системы СОРМ в сетях 5G

Архитектура СОРМ в сетях 5G (рис.2) включает модули системы СОРМ, интерфейсы СОРМ и взаимодействующие модули сети 5G Core, которые представляют собой точки перехвата POI контентной xCC и служебной информации xIRI от целевого абонента сети 5G, подлежащего процедуре СОРМ. Эталонная архитектура СОРМ сети 5G делится на два домена: домен сети 5G (CSP domain) и правоохранительный домен (Law Enforcement domain).

Как видно из рис.2, функциональные модули системы СОРМ на стороне оператора сети 5G (домен CSP) включают:

1. модуль-функцию администрирования СОРМ (ADMF), состоящий из модуля-функции управления перехватом LICF и модуля-функции обеспечения перехвата LIPF;
2. модули-функции сопряжения формата и доставки данных перехвата (MDF), которые делятся на следующие функциональные модули:

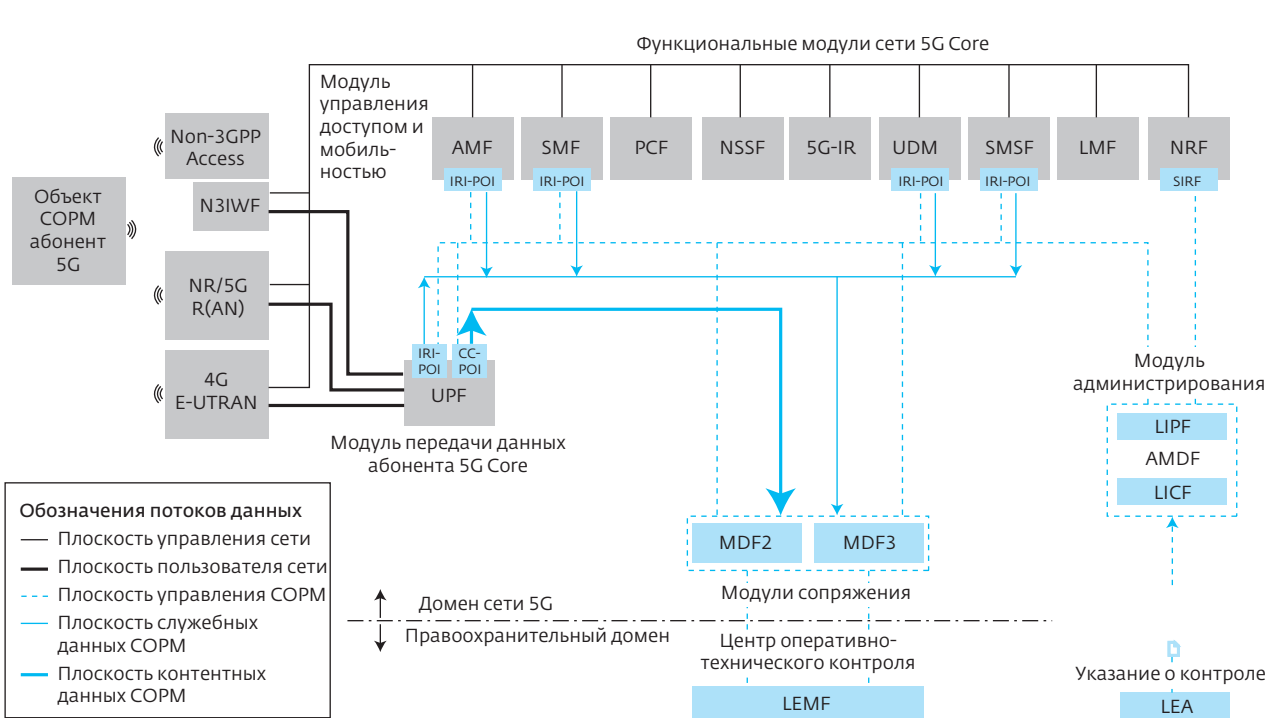

Рис.2. Архитектура СОРМ в сетях 5G. *Источник: [4]*

- модуль сопряжения MDF2, который передает в систему СОРМ из сети 5G служебные данные плоскости управления (Control Plane): идентификаторы и данные регистрации абонента, обновления местоположения, хэндовер, местоположение, идентификаторы сессий, SMS и т.д.;
- модуль сопряжения MDF3, передающий в систему СОРМ из сети 5G данные плоскости пользователя (User Plane), которые передает/принимает контролируемый абонент посредством IP-сессии.

3. Точки съема контентной и служебной информации POI, в число которых входят следующие модули базовой сети 5G Core [2]:
   - передачи данных абонентов UPF (User Plane Function);
   - управления доступом и мобильностью AMF (Core Access and Mobility Management Function);
   - управления сессиями SMF (Session Management Function);
   - унифицированной базы данных UDM (Unified Data Management);
   - поддержки передачи SMS поверх NAS-SMSF (SMS Function);
   - репозитория (хранилища) сетевых функций NRF (NF Repository Function).

В сети 5G Core модуль AMF выполняет функции доступа и мобильности, а в системе СОРМ этот модуль обеспечивает генерирование служебной информации IRI, относящейся к доступу в сеть, регистрации и управлению соединением контролируемого абонентского терминала UE.

Модуль управления LICF, входящий в модуль сопряжения ADMF системы СОРМ, получает командное сообщение (warrant) от правоохранительного органа LEA, а также информацию об объекте перехвата сообщений и предает ее в модуль обеспечения LIPF системы СОРМ. Модуль обеспечения LIPF, входящий в модуль сопряжения ADMF, обеспечивает создание точки привязки съема служебной информации IRI-POI и через интерфейс LI_X1 соединяется напрямую с модулем AMF и модулем передачи служебных данных плоскости управления MDF2.

LIPF также может взаимодействовать с модулем поиска системной информации (SIRF), который отвечает за предоставление модулю обеспечения системной информации о доступных сетевых модулях NF

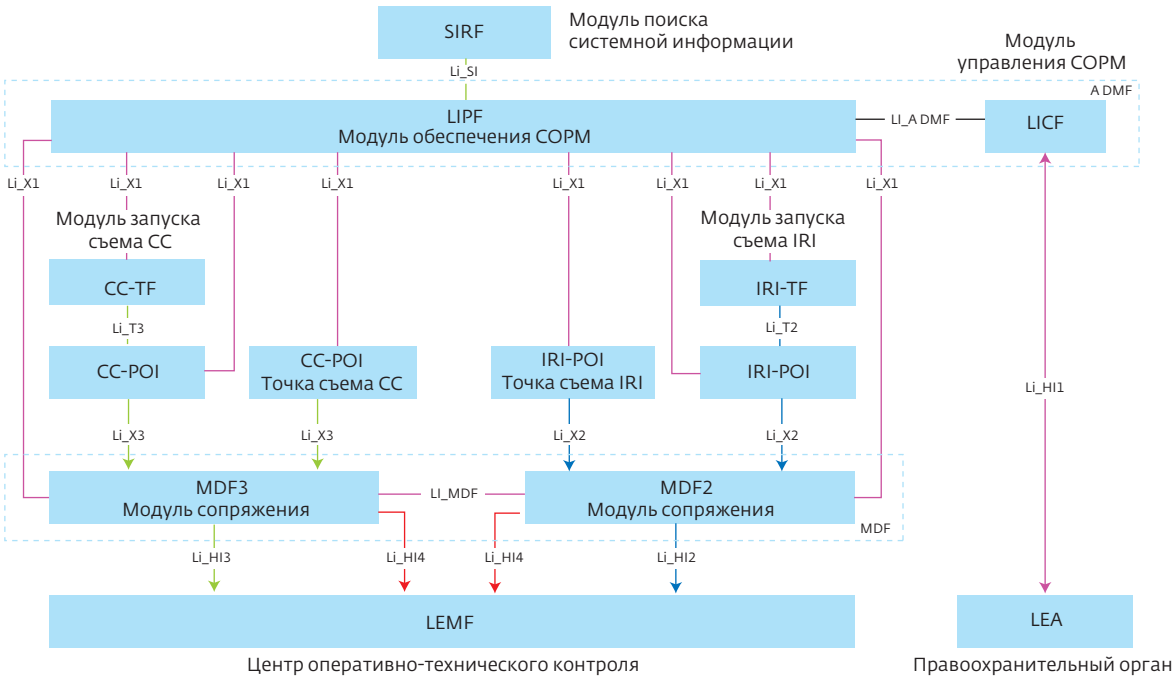

Рис.3. Архитектура СОРМ в сетях 5G. *Источник: [4]*

сети 5G Core в модуле-репозитарии сетевых функций NRF, например для обнаружения модуля AMF в сети 5G. Это взаимодействие осуществляется через интерфейс LI_SI.

Через точку съема служебной информации IRI-POI в модуле AMF система СОРМ получает информацию о доступе в сеть, регистрации в сети, управлении соединением и мобильностью контролируемого абонентского терминала UE. Модуль AMF генерирует и доставляет эту служебную информацию xIRI в модуль сопряжения MDF2 через интерфейс LI_X2. Модуль MDF2 доставляет сообщения IRI как часть данных перехвата в центр оперативно-технического контроля LEMF через интерфейс LI_HI2.

Программное обеспечение СОРМ точек съема информации IRI-POI, CC-POI может быть как встроено в сетевые модули-функции базовой сети 5G Core, так и поставляться в виде отдельного ПО. У крупных вендоров ПО системы СОРМ для точек съема IRI-POI и CC-POI являются встроенными сетевыми функциями.

Интерфейсы системы СОРМ, обеспечивающие передачу контентной xCC и служебной информации xIRI из сети 5G в систему СОРМ, показаны на рис.3.

Анализ использования интерфейсов в архитектуре системы СОРМ сети 5G (рис.3) и функциональных особенностей модулей этой системы позволяет определить их назначение следующим образом.

LI_SI – это интерфейс между модулем поиска системной информации SIRF и модулем обеспечения LIPF системы СОРМ. Модуль SIRF использует данный интерфейс для предоставления системной информации в модуль LIPF. Соответственно, модуль LIPF может запросить модуль SIRF о получении системной информации перед отправкой запроса о предоставлении перехвата в конкретной точке съема POI. Модуль поиска системной информации SIRF также может уведомлять модуль LIPF при каждом изменении состояния системной функции (например, удаление абонента из обслуживания, его миграция в другое местоположение и т. д.).

Совокупность интерфейсов LI_X1 – LI_X3 относится к внутренним интерфейсам системы СОРМ сети 5G и обеспечивает передачу внутрисистемной, служебной и контентной информации внутри системы СОРМ.

Интерфейсы LI_X1 используются в системе СОРМ для управления точками съема информации POI и модулями запуска перехвата сообщений (триггерными функциями) TF. По этим интерфейсам

в систему предоставляется целевая информация о состоянии точек съема POI и модулей TF в ходе перехвата соединений контролируемого абонентского терминала UE. Кроме того, интерфейсы LI_X1 также используются для управления и предоставления в модули сопряжения MDF необходимой информации COPM в формате, используемом в оперативно-техническом центре LEMF.

Интерфейсы LI_X2 используются для передачи служебной информации xIRI контролируемого абонентского терминала UE из сетевых модулей 5G Core (точек съема этой информации IRI-POI) в модуль сопряжения MDF2.

Интерфейсы LI_X3 используются для передачи в реальном времени контентных сообщений xCC контролируемого абонентского терминала UE и связанных метаданных из сетевых модулей 5G Core (точек съема этой информации CC-POI) в модуль сопряжения MDF3.

Интерфейсы LI_HI1 – LI_HI4 относятся к внешним интерфейсам системы COPM сети 5G и называются интерфейсами хэндовера COPM.

Интерфейс LI_HI1 используется для отправки командных сообщений и других запросов от правоохранительного органа LEA в домен CSP сети 5 G на перехват соединений подлежащего контролю абонентского терминала UE. Этот интерфейс может быть электронным или автономным документальным процессом передачи письменных указаний от национальных правоохранительных органов.

Интерфейс LI_HI2 используется для отправки служебных сообщений IRI из модуля сопряжения MDF2 в центр оперативно-технического контроля LEMF.

Интерфейс LI_HI3 используется для отправки контентных сообщений CC из модуля сопряжения MDF3 в центр оперативно-технического контроля LEMF.

Интерфейс LI_HI4 используется модулями сопряжения MDF2 и MDF3 для отправки сообщений в центр оперативно-технического контроля LEMF о готовности MDF2 / MDF3 к работе для перехвата соединений абонентского терминала UE, подлежащего контролю.

Совокупность внутренних интерфейсов LI_T используется для передачи информации о начале съема информации (перехвата) от модуля-функции запуска перехвата TF в точку съема информации POI. В зависимости от вида точки съема информации POI или CC определяются два типа интерфейсов LI_T:

- LI_T2 соединяет модуль-функцию запуска съема IRI-TF непосредственно с точкой съема служебной информации контролируемого абонента IRI-POI;
- LI_T3 соединяет модуль-функцию запуска съема CC-TF непосредственно с точкой съема контентной информации от контролируемого абонента CC-POI.

Интерфейс LI_T2 используется, когда данные от точки съема информации POI передаются через интерфейс LI_X2, а LI_T3 – когда данные от точки съема информации CC передаются через интерфейс LI_X3.

Совокупность внутренних интерфейсов LI_T используется для передачи информации о начале съема информации (перехвата) от модуля-функции запуска перехвата TF в точку съема информации POI.

LI_MDF – внутренний интерфейс между модулями сопряжения MDF2 и MDF3 и используется для взаимодействия этих модулей друг с другом при генерации служебных IRI и контентных CC сообщений.

Построение и использование протоколов системы COPM сетей 5G

Все интерфейсы системы COPM используют типовую реализацию стека протоколов COPM, показанную на рис.4.

Как видно из рис.4, уровень приложений системы COPM отвечает за аутентификацию и шифрованную доставку административных сообщений LEA в адрес оператора сети 5G, а также за доставку записей служебной информации IRI и контентной информации CC. Сеансовый уровень системы COPM инкапсулирует записи служебной информации IRI и контентные данные CC, прежде чем отправить их по соединению с протоколом TCP/IP, чтобы оперативно-технический центр контроля LEMF мог различать сообщения системы COPM. Инкапсуляция записей служебной информации IRI и контентных данных CC осуществляется с использованием протокола ITOT (Transport Service on top of TCP) [8], надстроенного над TCP/IP.

В табл.1 показаны протоколы, используемые в соответствующих внутренних и внешних интерфейсах системы COPM сети 5G [6]. Ряд протоколов для модулей SIRF, MDF и AMDF не определены в технических спецификациях 3GPP, так как они определяются производителями систем COPM по согласованию с оперативно-техническим центром контроля LEMF правоохранительного органа.

Протокол X2 передачи служебной информации IRI должен предоставлять информацию, коррелированную с данными, предоставляемыми в модули MDF через интерфейсы LI_HI2и LI_HI3.

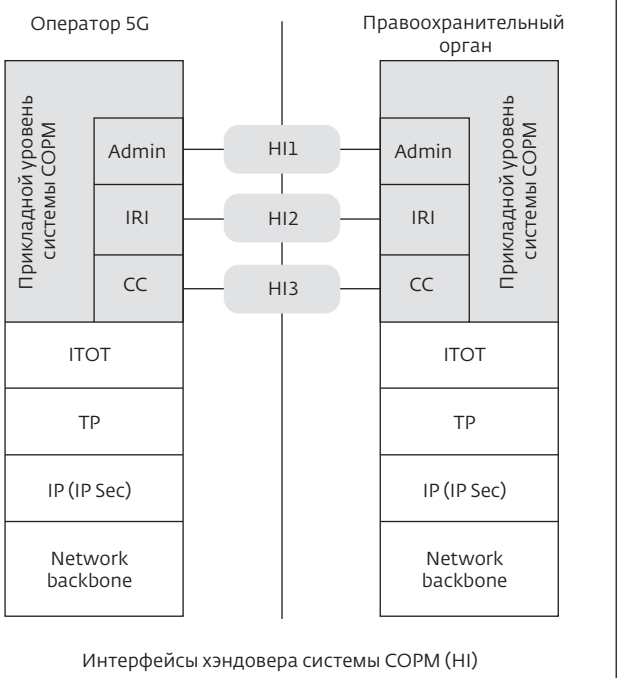

Рис.4. Стек протоколов системы СОРМ.
Источник: [7]

Протокол X3 передачи контентной информации CC должен предоставлять информацию, коррелированную с информацией, предоставляемой в модули сопряжения MDF, и соответствовать требованиям интерфейсов LI_HI2 и LI_HI3 как минимум в части коммутации пакетов для соответствующих стандартов хэндовера системы СОРМ в сети 5G.

Точки съема информации POI отправляют данные в соответствующие модули сопряжения MDF в виде потока блоков протокольных данных (PDU) протоколов X2/X3. Каждый блок PDU отформатирован в соответствии с требованиями ETSI к системам СОРМ [10].

Любой блок PDU протоколов X2 / X3 состоит из трех основных разделов:

- набор обязательных полей заголовка, содержащих идентификаторы, информацию о маршрутизации и корреляции;
- набор дополнительных необязательных атрибутов, передающих дополнительные метаданные о перехваченных сообщениях;
- копия перехваченных сообщений.

К особенностям использования протоколов HI2 и HI3 в системе СОРМ следует отнести:

1. сообщения IRI, отправленные через интерфейс LI_HI2, структурированы как заголовок и полезная нагрузка. Заголовок содержит общую информацию [11], такую как идентификатор LIID, метка времени, информация о корреляции. Полезная нагрузка содержит служебную информацию, связанную с перехватом, которую модуль MDF2 получил от точек съема информации IRI-PO сети 5G. Сообщения IRI, передаваемые по интерфейсу LI_HI2, должны передаваться как полезная нагрузка в поле 3GPP 33128 Defined IRI [12];
2. сообщения CC, отправленные через интерфейс LI_HI3, также как и сообщения IRI, структурированы как заголовок и полезная нагрузка. Заголовок содержит общую информацию [11], такую как идентификатор LIID, метка времени, информация о корреляции. Полезная нагрузка содержит контентную информацию, которую модуль сопряжения MDF3 получил от точек съема информации CC-POI в сети 5G. Данные контекстных сообщений CC, передаваемые по интерфейсу LI_HI3, должны передаваться как полезная нагрузка в поле 3GPP 33128 Defined CC [12].

При использовании транспортного протокола TLS для отправки блоков PDU протоколов X2/X3 в модуль сопряжения MDF из точки съема информации POI открывают соединение TLS поверх TCP-протокола. Протокол TLS используется для выполнения взаимной аутентификации и идентификации между модулями-точками съема информации POI и модулями MDF системы СОРМ, а также для обеспечения конфиденциальности и защиты целостности данных для PDU протоколов X2 / X3.

Точки съема информации POI и модули сопряжения MDF должны поддерживать протокол TLS, как определено в рекомендации IETF RFC 5246 [13], и поддерживать требования рекомендации IETF RFC 7525 [14].

Проблемные вопросы создания систем СОРМ в сетях 5G

Рассмотрим основные проблемные вопросы создания систем СОРМ в сетях 5G, которые необходимо решить вендерам (разработчикам) и уполномоченным правоохранительным органам, чтобы обеспечить минимальное влияние перехода операторов связи на новые сетевые технологии 5G и на процессы оперативно-розыскных мероприятий в этих сетях.

Интерфейс СОРМ	Описание интерфейса системы СОРМ сети 5G	Протокол, используемый в интерфейсе
LI_SI	Используется для предоставления системной информации в LIPF от SIRF	Не определен 3GPP в TS 33128 [6]
LI_X1	Используется для настройки и аудита с прямым предоставлением точек съема POI, TF и модулей сопряжения MDF	ETSI TS 103 221-1 [8]
LI_X1 (управление)	Используется для аудита запущенных точек съема POI	ETSI TS 103 221-1 [8]
LI_X2	Используется для передачи служебной информации xIRI из точек съема IRI-POI в модуль MDF2	ETSI TS 103 221-2 [9]
LI_X3	Используется для передачи контентной информации xCC из точек съема CC-POI в MDF3	ETSI TS 103 221-2 [9]
LI_T2	Используется для передачи информации о запуске от IRI-TF к запущенной точке съема IRI-POI	ETSI TS 103 221-1 [8]
LI_T3	Используется для передачи информации о запуске от модуля CC-TF к запущенной точке съема CC-POI	ETSI TS 103 221-1 [8]
LI_ADMF	Используется для передачи информации о предоставлении перехвата из модуля LICF в LIPF	Не определен 3GPP в TS 33128 [6]
LI_MDF	Используется модулями MDF2 и MDF3 при взаимодействии, необходимом для правильной генерации сообщений CC и IRI из xCC и xIRI	Не определен 3GPP в TS 33128 [6]
LI_HI1	Используется для отправки запроса на прослушивание и другой информации о запросе на перехват от правоохранительного органа LEA оператору сети 5G	ETSI TS 103 120 [6]
LI_HI2	Используется для отправки служебной информации IRI от модуля сопряжения MDF2 в оперативно-технический центр контроля LEMF	ETSI TS 102 232-1 [10] и ETSI TS 102 232-7 [11]
LI_HI3	Используется для отправки контентной информации CC от модуля сопряжения MDF3 в оперативно-технический центр контроля LEMF	ETSI TS 102 232-1 [9] и ETSI TS 102 232-7 [10]
LI_HI4	Используется для отправки уведомлений о проведении прослушивания из модулей сопряжения MDF2 / MDF3 в оперативно-технический центр контроля LEMF	ETSI TS 102 232-1 [9] and ETSI TS 102 232-7 [10]

Высокая пропускная способность сетей 5G

Резкое увеличение пропускной способности и скоростей передачи пакетных данных – до 10–20 Гбит/с создаст множество проблем в различных модулях и обрабатываемых потоках данных систем СОРМ, включая процессы сбора, обработки, хранения, декодирования и анализа перехваченных данных.

Многообразие вариантов архитектуры и развертывания сетей 5G

Партнерский проект 3GPP разработал несколько вариантов (опций) архитектуры и развертывания сетей 5G, сочетающих одновременную работу сетей радиодоступа 4G (LTE) и 5G (NG-RAN), подключенных к опорным сетям с одной базовой сетью EPC или 5G Core. Это разнообразие архитектуры и вариантов развертывания сети 5G влияет на возможности и процессы в системе СОРМ сетей 5G.

Внедрение новой опорной сети 5G Core

Сеть 5G Core отличается от опорной сети предыдущего поколения (4G) и предоставляет набор новых сетевых модулей NF и протоколов NGi, новую сервисно-ориентированную архитектуру на основе сетевых слоев под каждую услугу, а также новые СОРМ-интерфейсы хэндовера (HI) и внутрисетевые СОРМ-интерфейсы (Xi), которые требуют модернизации центров оперативно-технического контроля (мониторинга) и процессов обеспечения СОРМ с учетом появления 5G.

Виртуализация сетевых функций (NFV)

Использование в архитектуре 5G Core виртуализации сетевых функций (NFV) будет создавать множество проблем для пассивного и активного перехвата сообщений, включая перехват inter-host трафика между двумя виртуальными машинам, управление перехватом для динамически создаваемых виртуальных сетевых функций VNF и их компонентов VNFC. Процессы прослушивания и перехвата сообщений системами СОРМ должны будут поддерживать эту новую архитектуру виртуальной опорной сети 5G Core.

Хэндовер между инфраструктурой 5G и 4G

Системы СОРМ должны будут обрабатывать непрерывный перехват сеансов пакетных данных во время передачи обслуживания между сетями с различными технологиями радиодоступа (inter RAT handover): 5G, 4G, Wi-Fi 6E и т.д., при этом используя различные СОРМ-интерфейсы хэндовера (HI) и внутрисетевые СОРМ-интерфейсы (Xi), применяемые на этих сетях.

Национальные особенности систем СОРМ

В российских сетях 4G (LTE) в настоящее время используется два способа реализации систем СОРМ:

1. на основе модели СОРМ 3GPP с использованием модулей-функций AMDF, POI, DF, интерфейсов LI_HI2, LI_HI3 и др.;
2. на основе российского подхода путем внедрения оптических сплиттеров и анализа сигнализации S11-интерфейса и съема данных с S1-интерфейса. Оба интерфейса – S11 и S1 – являются открытыми с точки зрения шифрования и позволяют съем информации СОРМ.

В сетях 5G второй из упомянутых выше вариант СОРМ не может быть реализован, так как все модули сетевых функций 5G Core, согласно предложенной сервисно-ориентированной архитектуре SBA сетей 5G, поддерживают криптографию TLS (Transport layer security – Протокол защиты транспортного уровня) [14] и все сообщения между ними закрыты на транспортном уровне. Протокол TLS дает возможность клиент-серверным приложениям осуществлять связь в сети 5G таким образом, что нельзя производить расшифровку пакетов и осуществить к ним несанкционированный доступ. При необходимости реализации второго варианта российской СОРМ в сети 5G оператор должен будет принудительно отключить шифрование протокола TLS.

Заключение

Созданный Партнерским проектом 3GPP технологический задел по стандартизации требований к системе СОРМ сетей 5G позволяет сформировать национальные требования, учитывающие специфику российского нормативно-правового регулирования вопросов СОРМ и начать разработку системы СОРМ 5G в российском технологическом поле.

Использование в сервисно-ориентированной архитектуре и сетевых функциях 5G Core криптографии на основе протокола TLS, который шифрует и закрывает все сообщения между модулями 5G Core на транспортной уровне, не позволяет реализовать ранее использованные подходы российской СОРМ и потребует от операторов принудительного отключения шифрования в сетях 5G.

ЛИТЕРАТУРА

1. Федеральный закон от 12 августа 1995 года № 144-ФЗ (ред. от 02.08.2019) "Об оперативно-розыскной деятельности"
2. **Тихвинский В.О., Терентьев С.В., Коваль В.А.** Сети мобильной связи 5G: технологии, архитектура и услуги. – М.: Медиа Паблишер, 2019. 376 с.
3. Understanding 5G Lawful Interception Challenges Facing Law Enforcement and Vendor Solutions Under Development / ISS World, September 24, 2019: Online Webinar.
4. 3GPP TS 33126 Security; Lawful Interception requirements
5. 3GPP TS 33127 Security; Lawful Interception (LI) architecture and functions
6. 3GPP TS 33128 Security; Protocol and procedures for Lawful Interception (LI); Stage 3
7. Sharevski Filipo. Towards 5G cellular network forensics // EURASIP Journal on Information Security. 2018. No 8.
8. ETSI TR 101 567. Lawful Interception (LI); Cloud-Virtual Services for Lawful Interception (LI) and Retained Data (RD). ETSI, Sophia Antipolis, 2017.
9. ETSI TS 103 221-1 Lawful Interception (LI); Part 1: Internal Network Interface X1 for Lawful Interception.
10. ETSI TS 103 221-2 Lawful Interception (LI); Part 2: Internal Network Interface X2/X3 for Lawful Interception.
11. ETSI TS 102 232-1 Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 1: Handover specification for IP delivery.
12. ETSI TS 102 232-7 Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 7: Service-specific details for Mobile Services.
13. IETF RFC 5246The Transport Layer Security (TLS) Protocol Version 1.2, August 2008.
14. IETF RFC 7525 Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS), May 2015.