Незримый СОРМ

Игорь АГАПОВ

К 31 марта текущего года все российские операторы связи должны были привести сети в соответствие с приказом Минкомсвязи от 1 апреля 2014 года №83, утвердившим новые требования к техническим средствам оперативно-разыскных мероприятий, которые касаются законного перехвата информации об абонентах связи при пакетной передаче данных. Однако спустя полгода оказалось, что до внедрения новой версии СОРМ (СОРМ-3) операторами еще далеко.

Приказ №83 преследовал, казалось бы, техническую задачу – дополнить существующие «Правила применения оборудования систем коммутации, включая программное обеспечение, обеспечивающего выполнение установленных действий при проведении оперативно-разыскных мероприятий» еще одной частью, касающейся особенностей СОРМ для законного перехвата информации при предоставлении услуг связи на основе технологии пакетной передачи данных. К таким услугам относятся: доступ в Интернет, передача сообщений электронной почты и мессенджеров (ICQ и подобных), IP-телефония (включая такие популярные OTT-сервисы, как Skype, WhatsApp) и другие сервисы. Ранее аналогичными приказами Минкомсвязи были утверждены части I и II этих Правил, касающиеся СОРМ на сетях мобильной и фиксированной телефонной связи соответственно.

Однако приказ №83 еще на стадии подготовки вызвал бурную реакцию в телекоммуникационном сообществе и за его пределами. Высказывались мнения, что принимать эти требования нельзя по различным причинам – от технической неисполнимости до нарушения конституционных прав граждан.

Поводом для острой реакции стали два вводимых новыми правилами существенных отличия от установленных характеристик СОРМ для телефонных сетей. Это, во-первых, большое количество параметров, подлежащих регистрации. Во-вторых, требование обеспечить по команде с пункта управления запись в кольцевой буфер всех пакетов данных, поступающих на интерфейсы подключения СОРМ к сети. Причем этот буфер (хранилище воспроизводимой информации) должен вмещать указанную запись длительностью не менее 12 часов.

Другими словами, по команде уполномоченной специальной службы оператор должен предоставить возможность записывать в течение 12 часов параметры пакетных соединений в своей сети. Как следует из приказа, таких параметров 15 – от постоянного (статического) IP-адреса пользователя до информации о местоположении мобильного терминала в момент соединения. Среди этих параметров и такие, как имя учетной записи (логин) пользователя в разных интернет-сервисах, адрес электронной почты, телефонный номер, идентификаторы пользователя в мессенджерах и другие.

Исходя из текста приказа, можно предположить, что речь идет о 12-часовой записи не всех пакетов данных в сети оператора, а лишь тех, которые касаются так называемых контролируемых соединений, то есть переговоров или переписки только определенных пользователей, которые являются объектами оперативно-разыскных мероприятий. Однако существует возможность и более широкого толкования: необходимо

Организация и функции СОРМ

Источник: Минкомсвязи

Фото: СТАНДАРТ

Начальник отдела государственного регулирования обеспечения функционирования сетей связи и метрологии Департамента регулирования радиочастот и сетей связи Минкомсвязи Михаил Хазов уверен, что операторы связи выполняют установленные приказом №83 требования и могут вводить доработанные СОРМ в сроки, указанные в согласованных органами Федеральной службы безопасности планах

Фото: СТАНДАРТ

И.о. генерального директора ФГУП «Центральный научно-исследовательский институт связи» (ЦНИИС) Андрей Грязев не подтвердил, что кто-либо из операторов обращался в институт для разработки решений по внедрению СОРМ согласно приказу №83

записывать в течение 12 часов всю пакетную информацию в сети оператора. Этот момент еще на стадии обсуждения проекта приказа вызвал возражения со стороны отраслевых специалистов, говоривших о больших затратах на новое оборудование СОРМ. Так, по оценке ПАО «ВымпелКом», расходы крупного оператора на СОРМ-3 должны составить до $100 млн, а Mail.Ru Group в письменном отзыве на проект оценивала эти расходы в $400 млн. В условиях недостаточной нормативной определенности того, кто должен нести расходы на приобретение и установку оборудования СОРМ – операторы связи или государство, такие расходы не могли не вызвать беспокойства у игроков рынка.

Тем не менее приказ №83 был принят Минкомсвязи 16 апреля 2014 года и зарегистрирован Минюстом со сроком исполнения операторами 31 марта 2015 года. Но поговорить о реализации требований приказа на практике до сих пор невозможно.

Как вас теперь называть?

Системы законного перехвата, описанные в приказе №83, с легкой руки средств массовой информации и других представителей заинтересованной общественности стали известны как СОРМ-3. Под этим названием данные системы фигурировали в большинстве публичных обсуждений нашумевшего приказа. Скорее всего, это наименование возникло потому, что именно в части III «Правил применения оборудования систем коммутации...», введенной в действие приказом №83, описаны требования к оборудованию коммутации и маршрутизации пакетов информации сетей передачи данных.

Однако у технических специалистов есть и другое мнение относительно названия этих систем. В частности, заместитель директора отдела разработки программного обеспечения ЗАО «ИскраУралТел» Никита Уржумцев считает, что требования, утвержденные приказом №83, являются лишь развитием функциональности средств оперативно-разыскных мероприятий поколения СОРМ-2.

Такого же мнения, по сообщению начальника отдела по связям с общественностью ПАО «Ростелеком» Андрея Полякова, придерживаются и специалисты этого оператора.

Директор департамента специальных решений ООО «Телеком-Защита» Владислав Морозов разъясняет, что приказ №83 – лишь один из нормативных документов, описывающий системы, известные как СОРМ-2, и детализирующий требования к системам коммутации и маршрутизации применительно к пакетной технологии передачи информации. По мнению представителя «Телеком-Защиты», по-настоящему СОРМ-3 будет описана в документе под названием «Правила применения технических и программных средств информационных систем, содержащих базы данных абонентов оператора связи и предоставленных им услуг связи, обеспечивающих выполнение установленных действий при проведении оперативно-разыскных мероприятий». Этот нормативный акт существует пока лишь в проекте. Согласно информации Минкомсвязи, он будет оформлен в виде части IV все тех же «Правил применения оборудования систем коммутации...».

Сведений о том, какой станет «истинная» СОРМ-3, в открытых источниках немного. Судя по материалам Минкомсвязи, предполагается, что часть IV «Правил применения оборудования систем коммутации...» будет требовать, чтобы СОРМ выполняли роль «агрегатора» всей операторской статистики со сроком ее хранения три года. Собираться и храниться должна будет информация об абонентах (персональные данные), о телефонных номерах, о попытках соединений (в том числе неудачных), об отправителях и получателях сообщений, о биллинговых событиях (пополнение и списание средств на абонентских счетах).

Кроме того, от перспективных СОРМ потребуется поддерживать функции сбора и хранения данных об HTTP-запросах, отправленных и принятых сообщениях электронной почты, местоположении абонента, а также о логах в процессе преобразования сетевых адресов (Network Address Translation, NAT) и наименований портов (Port Address Translation, PAT). Эти СОРМ должны обеспечивать и полнотекстовый поиск в массиве хранящихся данных.

Руководитель проектов ООО «НТЦ Протей» Андрей Нонин также считает разрабатываемый проект «Правил применения технических и программных средств информационных систем, содержащих базы данных абонентов оператора связи...» нормативной базой для СОРМ-3.

Как бы то ни было, приказ Минкомсвязи №83 ввел существенно новые требования к средствам оперативно-разыскных мероприятий на сетях связи, поэтому системы, отвечающие этим требованиям, заслуживают своего особого наименования и могут обозначаться как СОРМ-2.3.

Где СОРМ?

Несмотря на то что министерский приказ обязывал всех операторов связи привести сети в соответствие с его требованиями к 31 марта 2015 года, этого не произошло.

Ни один из операторов «большой тройки» – ПАО «Мобильные ТелеСистемы» (МТС), ПАО «ВымпелКом», ПАО «МегаФон», – а также ООО «Т2 РТК Холдинг» (Tele2) не подтвердили внедрение решений СОРМ-2.3 на своих сетях, отказавшись от подробных комментариев.

В то же время представитель одной из крупных

14


Фото: СТАНДАРТ

Директор департамента специальных решений ООО «Телеком-Защита» Владислав Морозов считает, что по-настоящему СОРМ-3 будет описана в пока только разрабатываемых правилах применения технических и программных средств информационных систем, содержащих базы данных абонентов


Фото: СТАНДАРТ

Генеральный директор ООО «Комфортел» Дмитрий Петров оценивает стоимость СОРМ, соответствующих приказу №83, для региональной сети связи с количеством конечных пользователей до 1 млн в 15-20 млн рублей

сотовых компаний на условиях конфиденциальности сообщил корреспонденту «Стандарта», что основные причины задержки с реализацией операторами требований приказа №83 в отсутствии в настоящий момент аккредитованных организаций, имеющих право проводить сертификацию необходимого оборудования СОРМ. «Как следствие, на рынке нет сертифицированных решений, обеспечивающих в полной мере выполнение требований данного приказа. По нашей оценке, модернизация оборудования согласно приказу №83 начнется в 2016 году», – заявил собеседник «Стандарта».

Андрей Поляков также говорит, что приказ №83 предполагает обязательную сертификацию оборудования СОРМ-2.3, но производители только готовятся к ней. «Сертификат никто из поставщиков пока не получил. Внедрение оборудования СОРМ-2.3 займет несколько лет начиная со следующего года после его сертификации», – сказал представитель «Ростелекома».

Генеральный директор ООО «Комфортел» Дмитрий Петров не называет конкретных сроков возможного внедрения СОРМ-2.3. «Что касается цены этого оборудования, то, по предварительным данным, стоимость решения, соответствующего требованиям приказа №83, составит 15-20 млн рублей для сети масштаба нашей (около 700 тыс. конечных пользователей, включая сети операторов – партнеров по обмену трафиком, – *прим. «Стандарта»*)», – заявил Дмитрий Петров.

Тем не менее начальник отдела государственного регулирования обеспечения функционирования сетей связи и метрологии Департамента регулирования радиочастот и сетей связи Минкомсвязи Михаил Хазов считает, что никакой задержки с установкой оборудования СОРМ-2.3 операторами нет. При этом представитель ведомства указывает на то, что, согласно пункту 7 постановления правительства РФ от 27 августа 2005 года №538, ввод в эксплуатацию СОРМ в сети оператора связи производится в соответствии с планом мероприятий, разработанным органом Федеральной службы безопасности (ФСБ) совместно с игроками рынка. В данном плане указывается, в частности, срок ввода технических средств в эксплуатацию. План разрабатывается в срок до трех месяцев с даты подачи оператором заявления в орган ФСБ.

«По нашим данным, операторы связи выполняют установленные требования», – заявил Михаил Хазов. Он также подчеркнул, что отсутствие после 31 марта внедренных СОРМ-2.3 не оказывает никакого влияния на ввод в строй операторами сетей связи или их фрагментов. «В соответствии с пунктом 10 приказа Минкомсвязи №258от 26 августа 2014 года, при вводе в эксплуатацию технических средств в сети связи допускается по согласованию с ФСБ вместо акта о вводе в строй СОРМ представить комиссии утвержденный план ее внедрения», – пояснил руководитель отдела министерства.

Поэтому, по мнению Михаила Хазова, Минкомсвязи нет необходимости предпринимать какие-либо шаги для ускорения внедрения СОРМ-2.3, так как все необходимые меры уже приняты. «Среди прочего приказом Минкомсвязи №169 от 15 мая 2015 года утверждена методика проведения сертификационных испытаний оборудования коммутации и маршрутизации пакетов информации сетей передачи данных (включая программное обеспечение), обеспечивающего выполнение установленных действий при проведении оперативно-разыскных мероприятий», – сообщил чиновник.

И.о. генерального директора ФГУП «Центральный научно-исследовательский институт связи» (ЦНИИС) Андрей Грязев сообщил, что институт оказывает консультационные и экспертные услуги при внедрении технических средств для оперативно-разыскных мероприятий. ЦНИИС принимал участие в рассмотрении ряда проектов СОРМ-2. Однако руководитель ЦНИИС не подтвердил, что кто-либо из операторов обращался в институт для разработки решений по внедрению СОРМ согласно приказу №83.

И.о. гендиректора ЦНИИС также указал на то, что возможные сроки внедрения операторами СОРМ-2.3 в полном объеме определяются планами внедрения СОРМ, которые подписываются совместно уполномоченными органами ФСБ и операторами связи.

Ни один из опрошенных «Стандартом» операторов связи не сообщил о том, что у него существует такой план. Тем не менее наличие или отсутствие планов внедрения ничего существенно не меняет, потому что в стране нет ни сертифицированного оборудования СОРМ-2.3, ни организаций, имеющих право на его сертификацию.

Советник руководителя Федерального агентства связи (Россвязь) Владимир Калинин сообщил, что в реестре сертифицированных средств связи оборудование СОРМ, соответствующее требованиям приказа Минкомсвязи №83, отсутствует. Кроме того, по его словам, также отсутствуют организации, аккредитованные для проведения сертификационных испытаний оборудования на соответствие требованиям приказа №83.

Как сделать СОРМ-2.3

Производители СОРМ пока не поставляли операторам оборудование для выполнения приказа №83. К тому же ими не решены и вопросы сертификации оборудования СОРМ-2.3.

Никита Уржумцев говорит, что решение, реализующее все требования, предусмотренные приказом №83, находится на этапе

Фото: «НТЦ Протей»

Руководитель проектов ООО «НТЦ Протей» Андрей Нонин видит основную техническую проблему создания новых СОРМ в организации дешевого и одновременно быстрого хранилища данных, адаптированного для решения задач оперативно-разыскных мероприятий

Фото: «ИскраУралТел»

Заместитель директора отдела разработки программного обеспечения ЗАО «ИскраУралТел» Никита Уржумцев подчеркивает, что в регуляторных требованиях к новым СОРМ до сих пор не все прописано однозначно, в нормативных документах существуют так называемые серые зоны, которые могут трактоваться по-разному

разработки. «В России мы еще никому не поставляли нашего решения, при этом в работе находится несколько возможных вариантов его тестовой версии», – сказал представитель «ИскраУралТела».

Он также обратил внимание на недочеты в нормативной базе по СОРМ-2.3. «Есть регулятивные проблемы, в требованиях до сих пор не все прописано однозначно, в нормативных документах существуют так называемые серые зоны, которые могут трактоваться по-разному», – отметил Никита Уржумцев.

Владислав Морозов сообщил, что технические решения, соответствующие приказу №83, находятся на финальных стадиях разработки и тестирования. «Соответственно, сертификацию решения мы начнем ровно в тот момент, когда будем полностью уверены в его работоспособности и успешном прохождении сертификационных испытаний. Ориентировочно планируем сделать это в I квартале 2016 года», – заявил представитель «Телеком-Защиты».

Андрей Нонин подчеркивает сложность разработки СОРМ новых поколений, которые должны обеспечивать хранение большого объема параметров трафика. «Работа с новыми СОРМ – это работа с колоссальными объемами данных, причем выборки из баз данных должны выполняться за разумное время, но операторы не готовы тратиться на большие хранилища данных. В целом, основная техническая проблема – организация дешевого и одновременно быстрого хранилища, адаптированного для решения задач оперативно-разыскных мероприятий», – говорит специалист «НТЦ Протей».

Кроме того, Андрей Нонин обращает внимание, что в России отсутствуют стандарты, определяющие, какие поля данных для каких протоколов передачи информации необходимо собирать с целью взаимодействия со средствами для оперативно-разыскных мероприятий. «Операторы периодически запрашивают решения по СОРМ-3, но рассчитать объем сохраняемых данных в силу отсутствия однозначного стандарта невозможно. Оператор не может предоставить точную информацию по объему и структуре трафика, который должен попасть в базу данных СОРМ, поэтому все расчеты могут содержать погрешности, которые на больших объемах данных могут быть весьма существенны», – указывает Андрей Нонин.

О сложностях разработки СОРМ-2.3 говорят и другие производители. «В части технических трудностей стоит назвать большой объем дискового пространства, которое должно быть в решении для обеспечения циклической записи информации обо всех соединениях всех абонентов в течение последних 12 часов вместе с содержанием этих соединений. Если говорить о всей России, то речь идет о петабайтах информации (а это число с 15 нулями справа). Причем если мы захотим сделать хранение этой информации более надежным, то объем дискового пространства нужно увеличить минимум в два раза», – рассуждает Никита Уржумцев. К тому же, подчеркивает специалист «ИскраУралТела», с каждым годом объем информации, передаваемой по сети, растет (примерно в два раза за два-три года), соответственно, оператор должен будет регулярно закупать новое дисковое пространство для сохранения необходимых объемов данных. Поэтому новые СОРМ – это и вопрос денег.

«С ростом трафика понадобится расширять системы поиска информации, записанной в буфере, для сохранения адекватной скорости выполнения запросов. Оператор не сильно заинтересован в таком вложении денег, так как на СОРМ он ничего не зарабатывает. Другое дело, что без СОРМ он не имеет права предоставлять свои услуги пользователям, и в конечном итоге за СОРМ будут платить рядовые пользователи. Но из-за кризиса доходность в пересчете на абонента снижается, что усложняет для операторов приобретение и поддержание решений СОРМ-2.3», – поделился своей оценкой проблемы Никита Уржумцев.

Владислав Морозов считает, что дополнительные трудности в процессе создания технических средств для оперативно-разыскных мероприятий создает усложнение ИТ-среды. Поэтому наиболее важным моментом, определяющим успешность разработки СОРМ, является выбор аппаратных и программных платформ. «Это тем более важно, что современные тенденции роста трафика требуют все больших мощностей для его обработки, которые при этом должны быть экономически эффективны и оправданны. Неправильный подход к выбору архитектуры решений СОРМ может существенно замедлить скорость разработки и повлияет на привлекательность продукта на рынке», – подчеркнул директор департамента «Телеком-Защиты».

Влияние динамично меняющегося ИТ-мира на спецсредства для оперативно-разыскных мероприятий отметил и Никита Уржумцев. «Потенциально СОРМ-2 должна меняться чаще, чем СОРМ-1, потому что технологии в мире передачи данных меняются очень быстро, ежедневно появляются новые протоколы, модифицируются уже существующие и для декодирования сообщений может потребоваться оперативная реализация вновь появившихся протоколов и их версий на перехватывающем оборудовании», – уверен сотрудник «ИскраУралТела». Так что, по мнению Никиты Уржумцева, «вопросов и сложностей по СОРМ-2.3 довольно много». Остается ждать ответов и решений.