Законный перехват в Сети

А. ГОЛЫШКО, канд. техн. наук, г. Москва

"Доверие к подчинённым заканчивается там, где заканчиваются возможности следящего оборудования".

(из памятки для руководителей)

Истоки

Любое государство сильно тем, что может держать под контролем и общество, и его экономическую активность. В разные времена формы, методы контроля и глубина их применения различались, однако за последнее столетие они серьёзно трансформировались вослед развитию коммуникационных технологий. Впрочем, в современных условиях разгула преступности, угрозы терроризма, распространения наркотиков и коррупции не представляется чем-то необычным стремление спецслужб контролировать телефонные переговоры, передачу сообщений с целью предотвращения противоправных действий или поимки преступников. К тому же раз уж информационные технологии приспособлены для оперативного и эффективного сбора информации, то это ценная находка и для шпионов. Поэтому уже сравнительно давно во всех странах мира, в том числе и в РФ, у правоохранительных органов существует возможность осуществлять мероприятия, которые могут предотвращать правонарушения или получать информацию об их подготовке. И хотя даже в странах с самой развитой демократией значительное число граждан имеет об этом представление, они понимают необходимость такой работы. Различия в использовании указанной возможности во всех государствах заключаются, как правило, в объёме полномочий соответствующих ведомств и в его контроле со стороны других ветвей власти и общества. Говорят, прослушивание телефонных разговоров в здании IV Государственной думы производилось еще в 1913 г.

Всё вышеуказанное называется законным перехватом сообщений или LI (Lawful Interception), что подразумевает процесс передачи правоохранительным органам информации, идущей во время сеанса связи между определёнными пользователями телекоммуникационной сети. Законный перехват является санкционированным действием и изначально устроен так, что не даёт пользователю возможности его определить. В разных странах под "правоохранительными органами" подчас подразумеваются одна или несколько организаций (государственная и федеральная полиция, спецслужбы, независимые антикоррупционные комиссии и т. п.). Для определения LI в РФ используется термин СОРМ — система технических средств для осуществления оперативно-разыскных мероприятий (ОРМ). В целом СОРМ является одной из форм оперативно-розыскной деятельности (ОРД), которая осуществляется гласно и негласно оперативными подразделениями государственных органов уполномоченных на то законом, в пределах их полномочий посредством проведения ОРМ, разумеется, в целях защиты жизни, здоровья, прав и свободы человека и гражданина, собственности, обеспечения безопасности общества и государства от преступных посягательств.

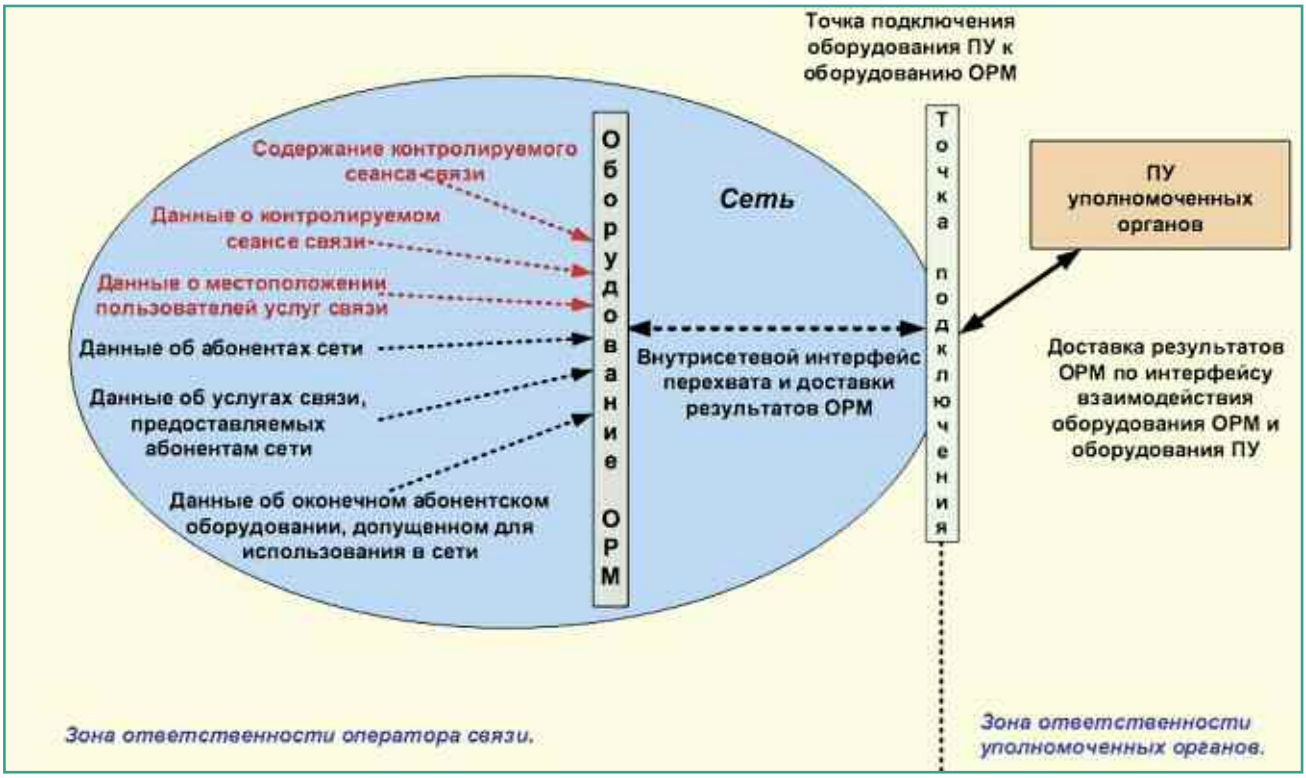
Остаётся добавить, что согласно закону "О связи" РФ, всем местным операторам связи предъявляются требования согласования плана мероприятий по внедрению СОРМ, в противном случае их лицензия может быть аннулирована. Иными словами, все операторы должны установить на своих сетях соответствующее оборудование для обеспечения СОРМ. Однако далее они не могут знать, как это оборудование используется спецслужбами и к каким именно абонентам сети последние проявляют интерес, т. е. несмотря на то, что оператор связи РФ обязан обеспечить функциональность СОРМ в своём оборудовании, он не может получать текущую информацию о работе указанных выше государственных правоохранительных органов при использовании ими оборудования СОРМ.

С развитием информационных технологий СОРМ приобретает дополнительные функции. Например, изначально СОРМ предназначался для прослушивания телефонных разговоров в сетях фиксированной и мобильной связи. С ростом популярности сети Интернет и всё увеличивающимся числом возможных способов доступа к ней законный перехват сообщений в рамках телефонных сетей стал менее эффективным, чем это было ранее. Поэтому в СОРМ добавили возможность анализа передаваемых/получаемых пользователем данных (к примеру, электронной почты). А уж какой простор для ОРМ предоставляют социальные сети... Осуществление ОРМ в Интернете журналисты иногда называют СОРМ-2. Ну а функции СОРМ изображены на **рисунке**.

Что есть СОРМ

Всё указанное ниже можно найти в Сети (и через Сеть можно найти того, кто это нашёл). В целом система СОРМ включает в себя три компонента:

тел. 608-83-05
Приём статей: mail@radio.ru
Вопросы: consult@radio.ru



— аппаратно-программная часть, которая установлена у оператора связи;

— удалённый пункт управления (ПУ), который установлен у правоохранительных органов;

— каналы передачи данных для связи с пунктом удалённого управления, которые обеспечивают операторы.

Технологии СОРМ можно условно разделить на три основных подхода. В случае пассивного съёма информации оборудование СОРМ является независимым от сети элементом, управляемым и контролируемым органами безопасности. Пассивный съёмник получает полную копию проходящих в сети данных, фильтрует, декодирует и передаёт в центр мониторинга перехваченные метаданные и искомое содержимое.

При активном перехвате оборудование СОРМ является элементом сети и получает необходимые данные напрямую от других сетевых компонентов. В этом случае сетевое оборудование оператора должно иметь, по крайней мере, базовые возможности по обеспечению перехвата.

Каждый из перечисленных подходов имеет свои плюсы и минусы, поэтому существует гибридное решение, которое представляет собой комбинацию из пассивного съёма и активного взаимодействия с сетевым оборудованием. Например, на сервере аутентификации, хранящем персональные данные абонента, по определённому признаку запрашивается IP-адрес абонента. После этого на сетевой маршрутизатор с функциями перехвата подаётся команда на трансляцию соответствующего трафика на модуль обработки, обработанная информация отправляется в центр мониторинга. В отдельных элементах сети при невозможности получения искомой информации на этом участке применяются устройства пассивного съёма.

Применительно к телефонной сети общего пользования (ТфОП) система СОРМ позволяет контролировать все исходящие и входящие вызовы определённых абонентов данной станции, включая вызовы с переадресацией и сокращённым набором номера; по команде из ПУ осуществлять разъединения установленного соединения абонента, блокировку входящих и исходящих соединений; конспиративно подключаться к любым абонентским линиям (в том числе находящимся в состоянии установленного соединения) и осуществлять запись разговоров. При этом по каждому контролируемому вызову ПУ может быть получена всевозможная информация о состоявшемся соединении, включая телефонные номера абонентов, продолжительность разговора и пр.

Если в качестве примера рассматривать интернет-провайдера, то работа СОРМ выглядит следующим образом. У провайдера установлено специальное устройство, которое подключается непосредственно к интернет-каналу, а оборудование провайдера для организации доступа в Интернет подключено уже к оборудованию СОРМ. В результате получаем, что весь входящий и исходящий трафик будет проходить через специальное устройство, а значит, в случае необходимости сможет быть перехвачен правоохранительными органами.

В целом СОРМ обеспечивает два режима передачи — статистической информации и полной информации. При работе в первом режиме на удалённый пункт управления должна передаваться информация о времени начала/завершения сеанса связи, сетевые адреса (имена) пользователей. Режим передачи полной информации отличается тем, что помимо перечисленных сведений передаётся информация, которую принимает или отправляет пользователь. В целом СОРМ обладает надёжной системой защиты. Получение каких-либо данных несанкционированным путём невозможно.

Следует ещё раз отметить, что непосредственно СОРМ является лишь фрагментом всей ОРД и может быть дополнен различными вспомогательными приложениями для автоматизации дальнейшей обработки всей полученной информации. К примеру, в сетях связи уже внедряется оборудование, позволяющее детально расшифровать IP-трафик и определить контент, проходящий по сети связи, с целью воздействия на его прохождение или для дифференцирования его тарификации. Разумеется, это оборудование может использоваться и для активного перехвата. В журнале уже говорилось о том, что существуют специализированные платформы для анализа больших объёмов данных, которые позволяют отслеживать поведение в сети всех пользователей в своём домене, определить различные форматы файлов, включая текстовые, изображения, видео, аудио, а также SMS во всех сетях, включая локальные, фиксированные и мобильные всех стандартов. Подобная система помогает правовым органам легально осуществлять мониторинг общественных мнений и формирования преступных сообществ, выявлять и блокировать нелегальные или террористические действия, управлять обычным поведением в сети и ограничивать распространение вредоносных контентов.

Внедрение

Важно понимание того, насколько законный перехват сообщений значим для правоохранительных органов, которые используют его как мощный инструмент противодействия криминальным преступникам и нарушителям национальной безопасности. Он используется не только для сбора очевидных свидетельств правонарушений и их последующего представления в суде, но и для отслеживания криминальных нарушителей через телекоммуникационное взаимодействие. Правительства всего мира настаивают на обеспечении адекватной системы законного перехвата сообщений, прежде чем компания сможет получить лицензию на осуществление своей коммерческой деятельности по предоставлению услуг связи. Процесс внедрения СОРМ не так прост и состоит из получения необходимых согласований, закупки и монтажа оборудования и его тщательного тестирования.

По мнению ряда специалистов, со временем СОРМ, безусловно, должна стать элементом сети оператора связи и для повышения эффективности СОРМ она должна представлять, по сути, собой параллельную специализированную защищённую сеть связи.

Преступность постоянно ищет способы обхождения любых правил, о чём уже рассказывалось на страницах журнала. Именно поэтому требуется, чтобы все используемые в стране оборудование и ПО были сертифицированы спецслужбами. Ну а использование несертифицированных продуктов сразу же привлечёт внимание соответствующих органов. В частности, недавно индийское правительство блокировало сервис BlackBerry, пока его владельцами не были раскрыты соответствующие коды. Осенью прошлого года директор ФСБ России заявил, что у его службы будут "рабочие контакты" с Google, Skype и "другими представителями интернет-сообщества", использующими свою криптографию в глобальном масштабе.

Кстати, спецслужбам США по решению суда открыты персональные данные абонентов сотовой связи и зарегистрированных пользователей интернет-ресурсов — имена, телефоны, адреса электронной почты, номера кредиток. По отдельному запросу спецслужб США (при наличии судебного решения) интернет-сервисы могут устанавливать постоянное наблюдение за пользователем, как следует из закрытых инструкций Skype, PayPal и Microsoft, опубликованных в базе данных Cryptome. Однако интернет-компании зачастую стараются скрыть данные клиентов от спецслужб, но таковы уж часто несовпадающие интересы бизнеса и государства. Ну и ещё одной немаловажной отрицательной стороной законного перехвата во всём мире является незаконная возможность подкупа соответствующих сотрудников. Персонал, как известно, одна из самых уязвимых составляющих любой деятельности, и на то в каждом государстве есть своё реагирование.

С возможными злоупотреблениями каждое государство борется по-своему. Минимизировать подобные риски призваны, как правило, многочисленные процедуры контроля, вводимые в системы законного перехвата, а также наличие третьего лица, контролирующего процесс перехвата. В частности, в большинстве западных государств законный перехват регламентирован многочисленными фазами проверки и соблюдения баланса. Например, правоохранительный орган не имеет прямого доступа к телекоммуникационной сети и её ресурсам, а процесс получения документа, непосредственно разрешающего перехват, отделён от самих механизмов перехвата. Подобное разделение функций является хорошей возможностью инспектирования деятельности правоохранительных органов, которая проводится регулярно.

Технологические вызовы XXI века

Повсеместный переход к пакетным сетям соответственно изменил условия осуществления СОРМ. Прежде всего, возникла всемирная IP-связанность объектов. Резко выросло количество видов персональных IP-коммуникаций: различные виды телефонии (фиксированная или мобильная, глобальная смесь TDM и VoIP), SMS, MMS, e-mail, ICQ, MSN и другие интернет-пейджеры, чаты, блоги, веб-форумы, Skype и пр. Кроме того, в отличие от традиционных телефонных сетей, в IP-сетях нет жёсткой топологической иерархии, поэтому "траектория" обмена IP-пакетами не фиксирована и может изменяться динамически прямо во время даже одного сеанса связи. В связи с этим отсутствуют и очевидные точки подключения оборудования для съёма информации. Кроме того, объект наблюдения больше не привязан к абонентскому терминалу: один и тот же индивидуум может подключаться к IP-сети из самых разных мест и любыми способами.

Реализация СОРМ для сетей IP-телефонии затруднена из-за независимости потоков сигнализации и пользовательского трафика в таких сетях. Для этого операторам требуется внедрять пограничные контроллеры сессий (SBC) и принудительно дублировать на них весь голосовой трафик. Для закрытых сетей (Skype) и интернет-служб нужны свои подходы, да и проблемы взаимодействия с ними становятся глобальными. В частности, в прошлом году президент США Б. Обама поставил перед своими спецслужбами задачу обеспечения законного перехвата информации в этих сервисах. Доступ к Skype может быть попросту заблокирован аппаратными средствами. Подобные решения предлагают на рынке компании Cisco, Verint, Narus, Verso Technologies. Эти решения используются в Китае, Вьетнаме, Египте, Пакистане, Саудовской Аравии.

Одна из проблем — рост количества съёмников, в которых концентрируется трафик объекта наблюдения. При наблюдении с разных съёмников возникает вопрос "собирания" трафика интересующего объекта. Помимо этого, приходится "собирать" всю цепь коммуникации: телефонный разговор — электронная почта — SMS — разговор через Skype и другие средства связи. Необходимы новые методы идентификации объекта наблюдения, поскольку способов и точек подключения к сети очень много. Да и объём трафика растёт очень быстро, что затрудняет его хранение в полном объёме для последующего анализа. Однако и это решаемо.

Разумеется, рост системной сложности СОРМ приводит к её удорожанию. Наконец, нельзя забывать, что СОРМ выполняет государственные задачи, поэтому разработчикам системы предстоит решать вопросы организации работы СОРМ в глобальной сети, взаимодействия с аналогичными службами других стран, с зарубежными провайдерами услуг и решений. Очевидно, что СОРМ сегодня становится частью комплекса вопросов сетевой безопасности и информационной защиты и поэтому начинает представлять интерес для операторов связи, которые до сих пор схожие проблемы решали самостоятельно. Поэтому очевидно, что в будущем СОРМ должна стать частью систем сетевого управления, единообразно решая задачи и самого оператора, и государственной безопасности.

Зарубежные "расширения"

Аналоги отечественной СОРМ (т. е. LI) существуют во всём мире и внедряются в эксплуатацию уже достаточно долгое время всеми ведущими мировыми державами. Внутреннее устройство систем поддержки ОРМ обычно конфиденциально или даже засекречено, однако цель всегда одна и та же: обеспечение негласного оперативного контроля над информацией, передаваемой и хранящейся в сетях связи. Предъявляемые к таким системам требования различны и формируются соответствующими государственными органами. Различие требований характеризуется не только приложениями системы, но и используемой архитектурой построения, средой доставки и способом построения общей модели взаимодействия компонентов системы. Порой функциональные возможности подобных систем выходят за рамки "законного перехвата".

В частности, ещё в 1947 г. спецслужбы США и Великобритании заключили между собой сепаратное соглашение о полном взаимодействии в области радиоэлектронного шпионажа. Позже, по инициативе Великобритании, к сотрудничеству были приглашены наиболее "близкие" англоязычные государства: Канада, Австралия и Новая Зеландия. Но анализом и дешифровкой перехваченных данных занимаются только спецслужбы США и Великобритании. К настоящему времени всё это превратилось в американскую систему "Echelon", которая действует в масштабах пяти государств — США, Канады, Австралии, Новой Зеландии, Великобритании — благодаря тому, что она управляет национальными системами ОРМ указанных государств через спутники связи. Обслуживанием национальных систем занимаются весьма важные организации: "Агентство национальной безопасности США" ("National Security Agency" — NSA), "Комитет безопасности и контроля интеллектуальных сведений" ("Security Intelligence Review

(Окончание см. на с. 20)

тел. 608-83-05
Приём статей: mail@radio.ru
Вопросы: consult@radio.ru
РАДИО № 5, 2012

Законный перехват в Сети

Окончание. Начало см. на с. 11

Committee" — SIRC) Канады, "Управление Защитой Сигналов" ("Defense Signals Directorate" — DSD) Австралии, "Правительственное Бюро Безопасности Коммуникаций" ("Government Communications Security Bureau" — GCSB) Новой Зеландии и "Штаб Правительственных Коммуникаций" ("Government Communications Headquarters" — GCHQ) Великобритании. Однако наличие данной системы не означает, что в указанных странах отсутствуют свои аналоги СОРМ, кроме "Echelon". Есть свои особенности LI в Великобритании, Франции, Швеции, Польше, Венгрии, Финляндии и других странах.

Аналогичная "Echelon" система под названием "RES" действует и в масштабе стран Евросоюза. В конце 90-х годов прошлого века, помимо глобальной системы "Echelon", в США была введена в эксплуатацию внутригосударственная система обеспечения ОРМ в глобальной сети Интернет под кодовым названием "Carnivore" (плотоядное животное) или "DCS-1000".

Что касается проекта глобальной электронной системы перехвата (Р-415), куда входит сеть "Echelon", то он был разработан NSA США в 1971 г. Его возможности — перехват и оперативная обработка 99 % информации в любой точке земного шара. Для этого на низкие околоземные орбиты была выведена группировка спутников-шпионов. Их дублируют расположенные по всему миру огромные параболические антенны, сканирующие радиоэфир и центры контроля интернет-сетей в США и Европе. Весь земной шар был поделён на секторы, за каждый из которых несёт ответственность один из "филиалов" сети.

На сегодняшний день мировой объём электронных сообщений оперативно анализировать невозможно. Чтобы справляться с этой задачей, в аналитических центрах Великобритании и США установлены суперкомпьютеры "Cray", объединённые в отдельную сеть под названием "Словарь" (Dictionary). Там же хранятся "ключевые слова", электронные адреса людей и организаций, а также оцифрованные образцы фонем интересующих абонентов. Перехваченные данные сравниваются с этими эталонами на соответствие, и в случае совпадения перехваченная информация заносится в базы данных и идёт на обработку аналитикам. Кстати, о существовании "Echelon" до начала 90-х знали лишь представители спецслужб. На весь мир она "прозвучала" после скандального интервью бывшего сотрудника NSA, который признался, что, помимо защиты национальной безопасности, система регулярно используется для политического сыска и экономического шпионажа, причём даже против своих. По его словам, для "прослушки" практически никогда не требовалось постановления американского суда. А это как в РФ, так и в США расценивается как грубейшее нарушение закона, за которое можно лишиться должности или пойти под суд. Однако, если даже отвлечься от "традиционного" шпионажа, в современных условиях вовремя полученная коммерческая информация о конкурентах порой бесценна, и, к примеру, на Западе уровень реализации такой информации достигает 60—70 %. Ведь воспользоваться ею можно, только если вы технически к ней готовы и обладаете соответствующей индустрией.

В сфере экономики никаких ограничений для "Echelon" не существует. Вся получаемая информация немедленно передаётся в Госдепартамент или в Форин оффис, где в дальнейшем её используют для поддержки своих компаний. Говорят даже, что благодаря "Echelon" в 1995 г. американцам удалось перехватить контракт на сумму 6 млрд долларов у европейского авиационного консорциума "AIRBUS", где ведущую роль играют Германия и Франция. И победителями открытого "тендера" на поставку самолётов в Саудовскую Аравию "оказались" фирмы "Боинг" и "МакДонелл Дуглас".

Приём статей: mail@radio.ru тел. 608-83-05
Вопросы: consult@radio.ru