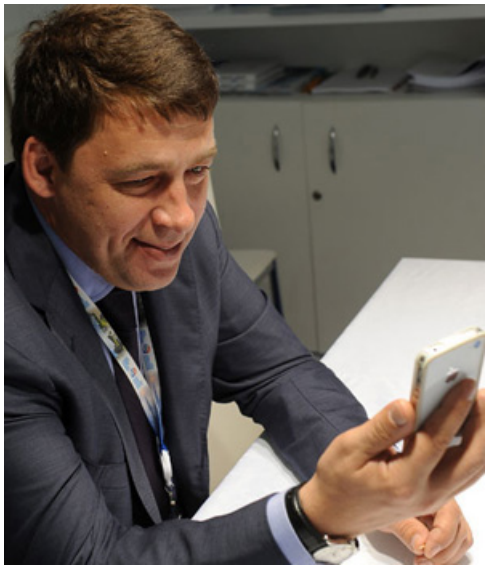
Автор: Артур Скальский © Babr24.com Источник: Znak.com РАССЛЕДОВАНИЯ, РОССИЯ 12793
19.12.2014, 00:36 831

«Тс-с-с. Об этом не по телефону»

Кто, как и зачем прослушивает ваши разговоры и читает переписку. Исследование Znak.com



«Не по телефону». «Сейчас перезвоню с другого номера». «Давай выйдем на улицу, прогуляемся, тут лучше не говорить». Такие фразы прочно вошли в жизнь российского истеблишмента, а ведь еще несколько лет назад жалующихся на прослушку телефонов и кабинетов принимали за полусумасшедших, вроде тех, кто носит шапочки из фольги и верит в зомбирующие лучи КГБ. Сегодня все знают: слушают всех, слушают без оглядки на закон и материалы этих прослушек чаще используют не в суде, а в политических интригах, доносах, провокациях. Znak.com поговорил с одним из профессионалов теневого рынка электронной разведки, чтобы выяснить, как работает эта сфера.

Кто слушает

На языке правоохранительных органов прослушка телефонов и контроль интернет-трафика называются аббревиатурой «СОРМ» - «Система технических средств для обеспечения функций оперативно-розыскных мероприятий». СОРМ-1 – это комплекс мероприятий, направленных на прослушку мобильной связи, СОРМ-2 – мобильного интернет-трафика. Сегодня такие методы расследования выходят на первый план, затмевая традиционные криминалистические подходы. Соответственно, подразделения, отвечающие за СОРМ, становятся все более влиятельными в составе органов внутренних дел. В Свердловской области это, например, бюро специальных технических мероприятий (БСТМ) ГУ МВД по Свердловской области и оперативно-технический отдел (ОТО) УФСБ по Свердловской области.

По закону, прослушка телефонов и контроль интернет-трафика возможны только по решению суда. Правда, закон позволяет следователям «включать запись» и без такового, если дело срочное и прослушка необходима для предотвращения готовящегося преступления. Примерно по такому же принципу следователям «в виде исключения» разрешают проводить обыски, получая санкцию суда уже постфактум. Как и в случае с обысками, часто правоохранители пользуются этой нормой, чтобы получать бесконтрольный доступ к чужим тайнам.

Существуют также способы легализовать незаконную прослушку, поместив имя и телефон нужной персоны в длинный перечень подозреваемых по какому-нибудь уголовному делу. Как говорят источники в органах, судьи почти никогда не вникают, каким образом та или иная фамилия связана с уголовным делом, и подписывают разрешения «одним махом». Такие судебные решения носят гриф «секретно», и кто оказался в списках «на прослушку», гражданам не узнать никогда.

Впрочем, специалисты, занимающиеся прослушкой, говорят: сегодня все чаще граждан «ставят на запись» и вовсе без каких-либо решений суда. У каждого оператора связи установлена аппаратура, позволяющая силовикам в любое время получать доступ к разговорам любого клиента (к этому операторов обязывает закон). А в региональном управлении ФСБ есть терминал удаленного доступа, с помощью которого можно в несколько кликов начать слушать любого пользователя мобильной связи.

По закону, право вести прослушку имеют несколько специальных служб. Кроме самой ФСБ, это МВД, ФСКН, ГУФСИН, таможня, ФСО, СВР. Но контроль за самой аппаратурой, обеспечивающей работу СОРМ-1 и СОРМ-2, находится именно у ФСБ. Как объясняют специалисты, чтобы поставить тот или иной номер на прослушку, сотрудникам из полицейского бюро специальных технических мероприятий не обязательно бежать в ФСБ и просить нажать кнопочку: в МВД и других органах, ведущих оперативно-разыскную деятельность, есть собственные терминалы доступа. Но они подключены «через ФСБ», то есть главный ключ все равно расположен у чекистов.

«Поэтому, например, в деле по прослушкам Ройзмана сложно будет перевести все стрелки на полицейских и сделать вид, что ФСБ ни при чем», - говорит собеседник Znak.com. По его словам, ответственность за несанкционированную прослушку и ее утечку в любом случае несут два ведомства.

«Зачем вам столько телефонов?»

Как уберечься от прослушки? Почти никак. Во-первых, бесполезно менять SIM-карты: на прослушку ставят не номер мобильного, а уникальный номер телефонного аппарата (IMEI). Какая бы симка не была установлена в телефоне, он все равно будет «в прямом эфире».

Многие представители истеблишмента и бизнесмены носят с собой несколько телефонов, считая, что один «обычный» слушается, а другие – «левые» - нет. «Это наивно, - говорит собеседник Znak.com. – Если человека поставили на прослушку, сотрудники органов постоянно получают информацию о местонахождении его телефона. Для этого в телефоне не обязательно должен быть установлен модуль GPS, местоположение даже самой простой и дешевой трубки определяется по базовым станциям с точностью до одного метра. И если вы таскаете с собой несколько трубок, по данным геолокации видно, что рядом с вашим «основным» номером всегда есть 2-3 других. Их тоже сразу же ставят на прослушку, поэтому ходить с кучей телефонов совершенно бессмысленно».

Впрочем, есть небольшой фокус с двумя трубками, который позволяет относительно надежно сохранить тайну переговоров. «Допустим, есть два аппарата – А и В. А используется постоянно, и есть основания полагать, что его слушают. В – для конфиденциальных разговоров, зарегистрирован на другое лицо. В этом случае А и В никогда не должны быть включены одновременно и рядом. Если нужно сделать звонок по «секретному» телефону В, вы выключаете А, отъезжаете подальше, в зону действия другой базовой станции, потом включаете В, делаете звонок. Потом выключаете В, снова едете к другой базовой станции и уже тогда включаете А», - рассказывает наш собеседник. Другой способ – постоянно хранить «секретный» телефон в каком-нибудь скрытом месте, всякий раз приезжая к нему с выключенным «основным» мобильником.

Особо осторожные жертвы прослушек предпочитают выключать телефон во время важного разговора или прятать его куда подальше. Собеседник Znak.com подтверждает, что возможность записи через телефон в режиме ожидания существует, но такая технология применяется нечасто. «В этих случаях используется т.н. микрофонный эффект. Такое можно сделать, только если в непосредственной близости от собеседников работает команда специалистов. Приемник сигнала и средство записи должны находиться где-то недалеко», - поясняет он.

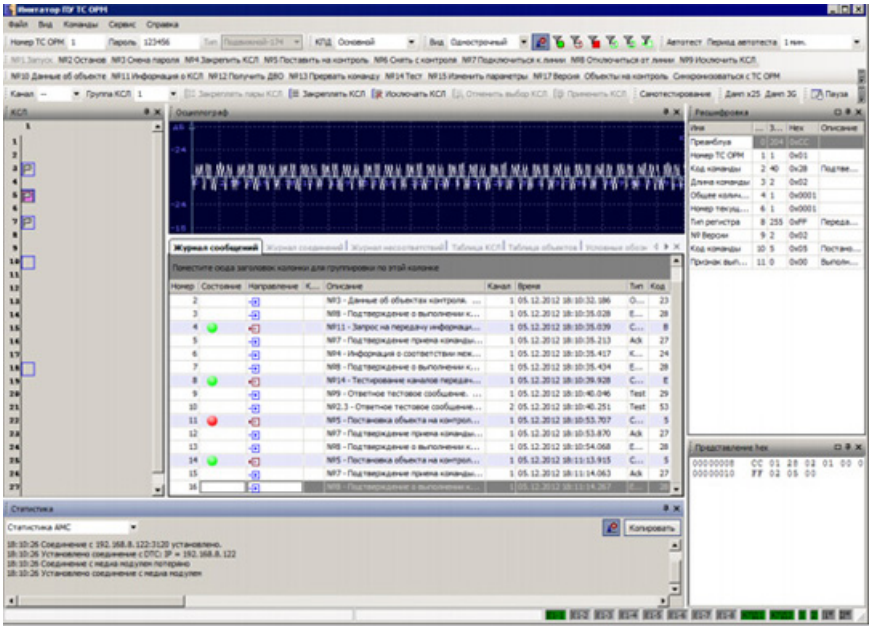
Как это устроено

Другое дело – обычная прослушка. Она может быть массовой. Сегодня в Екатеринбурге мощности ФСБ позволяют слушать одновременно 25-50 тысяч абонентов, в Москве – в сотни раз больше. Основная проблема не в том, как записать информацию, а в том, как ее расшифровать и обработать. В ГУ МВД по Свердловской области, например, есть специальный отдел «аналитиков», которые заняты простой расшифровкой записанных разговоров, превращением аудио в текст. Сейчас свердловские правоохранители, используя как повод подготовку к ЧМ-2018 и ЭКСПО-2020, ставят себе задачу увеличивать аппаратные мощности прослушки. А создать более совершенные системы обработки полученной информации – это уже задача для силовиков не только на российском, но и на мировом уровне. Последние скандалы в США показывают, что российские спецслужбы далеко не единственные увлечены незаконными или полузаконными «мониторингами».

Мировым лидером по созданию систем анализа и обработки данных для спецслужб является американская компания Palantir Technologies. Как утверждает собеседник Znak.com, технологиями Palantir пользуются как американские правительственные организации, например ЦРУ, так и российские – в том числе ФСБ и информационно-аналитический центр правительства РФ. «Последнее с трудом укладывается в голове. Получается, что весь объем правительственной информации, в том числе секретной, идет через американскую систему. Это все равно что Бараку Обаме установить “1С”», - иронизирует собеседник Znak.com.

В России одним из крупнейших поставщиков «аналитического» софта для спецслужб также является Avicomp Services. А аппаратные решения и программы для «мониторинга» (то есть прослушки) активно продает новосибирская компания «Сигнатек». На ее сайте сказано, что она предлагает «субъектам оперативно-разыскной деятельности» «системы мониторинга коммуникаций объектов: телефонных разговоров, факсимильных сеансов, видеозвонков, сообщений SMS, ДВО, ICQ, электронной почты», а также «Системы мониторинга перемещения объектов с визуализацией на карте».

В каталоге продукции есть примеры того, как выглядит интерфейс программы для «мониторинга»



What’sApp или Viber?

С анализом интернет-трафика подозрительных граждан (СОРМ-2) у силовиков дела обстоят пока несколько хуже, чем с прослушкой разговоров. Хотя операторы связи точно так же предоставляют спецслужбам любую информацию, сам анализ этих данных довольно сложен. «Любой смартфон постоянно скачивает и отправляет огромное количество данных. До последнего времени существовала огромная проблема в том, чтобы вычленить из всей этой массы интересующую информацию, например переписку в Skype или WhatsApp. Однако теперь эта задача в целом решена и даже в регионах научились читать интернет-мессенджеры», - рассказывает наш собеседник.

Крайне небезопасным мессенджером он называет популярный What's App – пересылаемая информация в нем не шифруется. Такое шифрование есть в Skype, и он был бы надежен, если бы владельцы сервиса, зайдя на отечественный рынок, не поделились кодами дешифровки с российскими силовиками. Поэтому сегодня самым надежным можно считать общение по Viber, в котором все данные (и переписка, и разговоры по голосовой связи) шифруются и пока недоступны для отечественных спецслужб («Именно поэтому Viber в первую очередь пытаются запретить», - уверен наш собеседник). Заявленному как «супернадежный» мессенджер сервису «Telegram» источник Znak.com не слишком доверяет, «как и всему, что сделано в России, в том числе Павлом Дуровым».

Еще один относительно надежный способ переписки – использование телефонов BlackBerry, в которых есть собственный сервис обмена сообщениями BlackBerry Messenger. Данные в нем шифруются еще надежнее, чем в Viber, доступа к ним у российских силовиков нет, и, возможно, именно поэтому BBM в России запрещен. Чтобы им пользоваться, приходится покупать телефон в США и «разлочивать» его у российских специалистов.

Крупный разработчик программ и оборудования для СОРМ-2 в России – компания «МФИСОФТ», поставляющая обеспечение для ФСБ. В описании аппаратно-программного комплекса «СОРМович», приведенном на их сайте, говорится, что он может ставить пользователей на контроль по имени учетной записи, номеру телефона, адресу электронной почты, IP и номеру ICQ. Комплекс обеспечивает «обнаружение и перехват почтовых сообщений по адресу электронной почты», «перехват файлов, передаваемых по протоколу FTP», «прослушивание IP-телефонии» и т.п.

За кем следят

Может быть, силовикам бы и хотелось «слушать всех», но в реальности под постоянным наблюдением всего 200-300 человек в Екатеринбурге, говорит собеседник Znak.com. Большинство из них – подозреваемые в экстремизме (в первую очередь исламистского толка) и терроризме, члены находящихся в разработке ОПГ, участники непрозрачных финансовых операций крупного масштаба («обналичники» и т.п.). Лишь не более 10% от всей массы «поднадзорных» слушают по политическому заказу, считает собеседник Znak.com.

«Совершенно точно слушают губернатора, его ближайшее окружение, первых лиц города. Депутатов Заксобрания и гордумы – вряд ли, только если кого-то заказали конкуренты. Но это редкий случай, по телефону никто ничего важного давно не говорит, и тратить по 70 тысяч рублей в день на прослушку конкурента готовы не многие», - рассказывает наш источник.

В последнее время появился еще один проверенный способ стать жертвой прослушки - регулярно критиковать действующую власть или ходить на демонстрации протеста. Конечно, всех участников уличных акций прослушивать не будут, но самых активных – вполне. В Екатеринбурге давно слушают Евгения Ройзмана и Аксану Панову – как оппонентов свердловского губернатора Евгения Куйвашева. В окружении губернатора не скрывают, что распечатки их разговоров регулярно ложатся на стол главе региона.

«ФСБук»

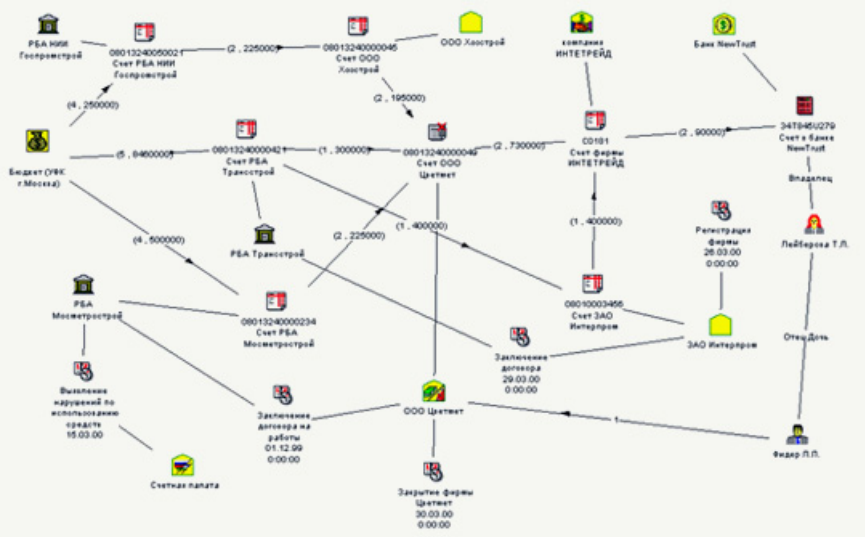
В последнее время все более значимую роль в структуре СОРМ играет анализ информации, собранной в социальных сетях. Спецслужбы имеют доступ ко всей переписке, ведущейся в российских социальных сетях, утверждает собеседник Znak.com. С Facebook дело обстоит сложнее, но и тут тайна общения не гарантирована. «Относительно безопасный способ общения – через западные почтовые сервисы: Gmail, Hotmail, Yahoo, - говорит собеседник Znak.com. – Еще эффективна сеть Tor, гарантирующая анонимность пользователям. С ее помощью, в том числе, американские журналисты общаются со своими информаторами».

Для обмена информацией все больше людей и организаций используют облачные сервисы вроде Dropbox, «Яндекс.Диск», «Google disk» и других. Ими тоже интересуются правоохранительные органы. Из популярных сервисов относительно надежным считается предложение Google, но наш источник советует обратить внимание на Wuala: хранилище, поддерживающее шифрование, с серверами в Швейцарии. Правда, если вы спасаете свои тайны не от российских спецслужб, а от американских, вам вряд ли что-то поможет. Несколько дней назад еще один «сверхбезопасный» облачный сервис Lavabit был таинственным образом закрыт и все его пользователи потеряли свою информацию. Судя по всему, дело в том, что почтой Lavabit пользовался бывший агент ЦРУ Эдвард Сноуден.

Под колпаком

Редкий российский бизнесмен и политик сегодня обсуждает по телефону что-нибудь важнее рыбалки и футбола. Поэтому, помимо анализа собственно текстов переговоров, профессионалы электронной разведки занимаются обработкой больших массивов данных, выявляя математические закономерности, неявные связи,

строя на этом основании гипотезы о взаимодействии тех или иных групп или персон. Материалом для этого могут служить телефонные звонки, электронные письма, банковские операции, операции по регистрации или ликвидации юридических лиц и т.п. Получаются большие схемы, подобные той, что приведены в одной из презентаций уже упоминавшейся компании Avicomp



Перлюстрация электронной переписки, мониторинг телефонных переговоров зашли уже так далеко, как и не снилось авторам романов-антиутопий. Наверное, нередко мощь СОРМов помогает предотвратить подлинные теракты или настоящие преступления. Но для общества куда заметнее случаи, когда методы электронной разведки используются для политического преследования и не имеют никакого отношения к законным процедурам. При этом от бесконтрольной слежки страдают не только оппозиционеры, но и лояльные Кремлю политики. Собранный при помощи электронных средств компромат часто становится орудием элитной борьбы против тех, кто еще недавно сам заказывал прослушку своих врагов. В этом смысле электронная разведка превратилась в опасность, от которой не застрахован никто.

Наша справка: Как уральские политики страдают от слежки и пытаются спастись

От незаконной прослушки страдают все. Директор фонда поддержки гражданских инициатив «Правовая миссия» (Челябинск) Алексей Табалов рассказал Znak.com, что «все его телефонные разговоры прослушивают» и он убеждался в этом неоднократно. Председатель правления фонда «Голос – Урал» Юрий Гурман также заверил нас, что в его организации спецслужбы слушают телефоны и проглядывают переписку к электронной почте. «Знаю, что слушают, и пусть слушают. Хотя мерзко становится», - говорит он.

Депутат Заксобрания Пермского края Владимир Нелюбин рассказал Znak.com, что на входе в некоторые высокие кабинеты нынче принято сдавать телефон секретарю. Сам банкир пользуется классической Nokia, не признает современных мессенджеров и от прослушки защищаться не собирается. А бывший глава администрации губернатора Прикамья Фирдус Алиев убежден, что от прослушки защититься невозможно. «Таких мер не существует, это иллюзия. Только личное общение позволяет максимально исключить утечки, вот и приходится летать [по встречам]», - рассказал он Znak.com.

В «тюменской матрешке» только на Юге, в Тюмени, приучили себя к мессенджерам вроде Viber и WhatsApp: в ХМАО и ЯНАО покрытие 3G намного хуже и пользоваться ими накладно. Зато северные чиновники активно используют аппаратные средства против прослушки. Например, в кабинете одного из высокопоставленных чиновников за шторой стоит «глушилка», которую он включает во время важных разговоров. Как говорят, звук это устройство издает жуткий, поэтому долго говорить, когда он работает, просто физически тяжело.

Этот же управленец рассказывает о мобильной связи совсем фантастические истории. По его словам, сегодня чекисты располагают оборудованием, которое однажды записав тембр вашего голоса, в случае, если им в дальнейшем необходимо вас писать, будет автоматически включаться, по какому бы вы телефону ни говорили. Поэтому менять номера и аппараты не имеет смысла. Довольно подозрительно чиновник относится и к продукции компании Apple, хотя пользуется ею с тех пор, когда президентом стал Дмитрий Медведев, который ввел моду среди госслужащих на iPhone и iPad. Однако он заклеил черной изолентой объективы камер на обоих гаджетах. Чиновник уверен, что с помощью камер за владельцем устройств может вестись наблюдение.

За одним из губернаторов «тюменской матрешки» наблюдали без всяких айфонов. Видеокамера была

обнаружена прямо над кроватью первого лица в служебной резиденции. Кто был заказчиком слежки (ФСБ или частные лица), так до сих пор и не выяснили.

На тюменском Севере, чтобы не стать «находкой для шпионов», еще несколько лет назад использовали старые дедовские методы – там любили менять мобильные телефоны и сим-карты. Один из руководителей крупной компании рассказывал корреспонденту Znak.com о том, что у берега Иртыша в Ханты-Мансийске есть место, проходя над которым катер мог бы сесть на мель, такое количество телефонов там утоплено.

Самые продуманные чиновники и бизнесмены всегда предпочтут личные беседы телефонным разговорам. Более того, как признался один из них, самым надежным способом коммуникации является запись на листке, после чего этот листок просто сжигается.

Дмитрий Колезев, Виталий Сотник, Кирилл Бабушкин, Ирина Щербак, фото Вадима Ахметова

Автор: Артур Скальский © Babr24.com Источник: Znak.com РАССЛЕДОВАНИЯ, РОССИЯ 12793
19.12.2014, 00:36 831
URL: https://babr24.com/?ADE=131553 Bytes: 18450 / 17954 Версия для печати Скачать PDF

Автор текста: **Артур Скальский**.

Телеграм: @tomsk24_link_bot
эл.почта: tomsk.babr@gmail.com

Прислать свою новость

ЗАКАЗАТЬ РАЗМЕЩЕНИЕ:

Рекламная группа "Экватор"
Телеграм: @babrobot_bot
эл.почта: eqquatoria@gmail.com

СТРАТЕГИЧЕСКОЕ СОТРУДНИЧЕСТВО:

эл.почта: babrmarket@gmail.com

Подробнее о размещении

Отказ от ответственности

Правила перепечаток

Соглашение о франчайзинге

Что такое Бабр24

Вакансии

Статистика сайта

Архив

Календарь

Зеркала сайта