

телеком

Без права на конфиденциальность

тарифный план

(Окончание. Начало на стр. 25)

Специальная техника по перехвату телефонных переговоров есть сегодня не только у профессионалов. По словам экспертов, цены на подобное оборудование на черном рынке упали до очень низкого уровня. Сканеры, которые свободно прослушивают до восьми мобильных номеров, можно приобрести за \$200, а системы, позволяющие отследить переговоры уже 10 тыс. абонентов, стоят до \$50 тыс. Если прикупить еще и цифровой синтезатор речи за несколько тысяч долларов, можно создать практически идеальную систему формирования компромата и, например, подделывать голоса мнимых жертв ДТП с целью выманивания денег у родственников.

Программы для прослушивания абонентов («МегаФон», МТС и «Вымпелком») предлагают также различные сайты в интернете. Корреспондент «Ъ-Телекома» обратилась по одному из таких объявлений и получила вполне развернутое объяснение, как пользоваться софтом, а также «список часто задаваемых вопросов». Главным из них был: «Могут ли спецслужбы вычислить меня с данным устройством?». Ответ продавца: «Нет, так как комплект пассивный и оператор связи его не видит». Покупателю предлагалось оплатить покупку через банк и получить программу через DHL или просто скачать ПО с указанного веб-адреса. В пресс-службе МТС «Ъ-Телекома» сообщили, что о существовании подобных предложений компании ничего не известно. А Роман Проклов из «МегаФона» сказал, что компания в курсе подобных предложений, и назвал их «чистой воды мошенничеством», однако отметил, что, поскольку тема конфиденциальности переговоров актуальна для ряда абонентов, «МегаФон» уже не первый год занимается вопросами дополнительной защиты трафика: «Одним из экономически выгодных путей решения данной проблемы является использование принципа абонентского шифрования с применением так называемых наложенных средств защиты информации».

Судебные акустики

Специалисты утверждают: даже в условиях, когда прослушивающие устройства и программы доступны обычным людям, защитить телефонные переговоры возможно. По словам генерального директора компании-разработчика решений в области безопасности связи «Сигналком» Владимира Смирнова, для этого необходима «совокупность мероприятий»: «Прослушивание телефонных переговоров может осуществляться по акустическому каналу, а также путем подключения с помощью специальной аппаратуры к каналу связи абонента в непосредственной от него близости или у оператора связи. Для блокирования первого канала утечки необходимо быть уверенным в отсутствии прослушивающих устройств в помещениях, откуда ведутся переговоры. А для защиты в канале связи — использовать специальную аппаратуру, обеспечивающую шифрование речевого сигнала, передаваемого в цифровом виде». При этом специальная аппаратура должна быть установлена у каждого абонента, с кем ведутся переговоры. То есть даже лучший криптосмартфон или шифратор будут бесполезны, если ваш собеседник пользуется обычным телефоном.

Желающих приобрести криптотелефон, в который встроены средства шифрования разговора, или специальную программу для защиты от прослушки в России хватает. Однако доверие к отечественным разработчикам у потенциальных клиентов крайне низкое. И это неудивительно: до последнего времени ведущим и чуть ли не единственным отечественным производителем криптотелефонов была созданная под эгидой ФСБ компания «Атлас». Стоимость телефона «SMP-Атлас» — около \$2 тыс. А криптографическая защита реализуется путем использования государственных алгоритмов шифрования по ГОСТ 28147–89, которые долгие годы исследовали спецслужбы.

Сегодня перед выходом на рынок любые устройства, защищающие от прослушивания телефонных переговоров, натыкаются на ряд серьезных ограничений. В России все компании-производители криптографических устройств обязаны использовать в своих телефонах только государственный алгоритм. Естественно, это не лучшим образом сказывается на до-



«Билайн» и МТС несколько лет пытаются вывести на рынок канадский коммуникатор BlackBerry. Однако устройство не может пройти сертификацию ФСБ из-за стойкого алгоритма шифрования ФОТО АР

верии потребителей. После того как в 2005 году разработчик криптографических устройств «Анкорт» заявил на выставке «Связь-Экспоком» о начале выпуска в России своего криптосмартфона, компания получила около 65 тыс. заявок. Потенциальным покупателям было известно, что собственные криптоалгоритмы компании более 15 лет использовались для защиты финансовых платежей в ЦБ. Но вскоре клиенты узнали о том, что в новом криптосмартфоне будет применяться государственный алгоритм, а в комплекте поставки для пользователей не будет генератора ключей. В результате число желающих приобрести телефон резко упало.

Повышению уровня доверия к технике, защищающей от прослушивания переговоров, не способствует и сертификация, которую проводит ФСБ. Компания-разработчик обязана согласовать со спецслужбами техническое задание на разработку. Затем назначается испытательная лаборатория, в роли которой обычно выступают, например, подконтрольные ФСБ НТЦ «Атлас» или НИИ «Автоматика». На практике процесс сертификации затягивается на несколько лет. «Причина этого — достаточно большие затраты и невозможность сертифицировать чисто программные решения без аппаратной платформы», — объясняет Владимир Смирнов. — Последнее условие значительно затрудняет сертификацию решений типа нашего Voice Coder Mobile (VCM), так как аппаратные платформы в виде серийных коммуникаторов и смартфонов обновляются каждые полгода и в случае замечаний при сертификации отсутствует реальная возможность доработки». Впрочем, в прошлом году спецслужбы решили слегка ослабить хватку и выпустили новые требования по разработке коммерческих шифраторов для использования их частными структурами: изготовитель не обязан проходить сертификацию, но должен выполнить требования, которые прописываются в лицензии ФСБ.

Кроме того, получение официальной лицензии на любые решения по защите переговоров требует реализации в них режима COPM, то есть системы технических средств по обеспечению функции оперативно-розыскных мероприятий. В соответствии с законом «Об оперативно-розыскной деятельности» на основании судебного решения COPM позволяет спецслужбам удаленно осуществлять прослушивание. Следовательно, как сказал «Ъ-Телекому» представитель одной из компаний-участников рынка, «бизнес-перспектива таких сертифицированных решений представляется достаточно туманной — они могут быть востребованы разве что госорганами». Логика потребителя понять легко: кто гарантирует, что на его конкурентов по бизнесу не решит поработать какой-нибудь активный сотрудник МВД, желающий подзаработать и подкалугурить прослушко- кой, как это было в деле Славинского?

Говорят «МегаФон»

Сегодня единственным оператором, с которым имеют право работать в России разработчики криптографического оборудования, является «МегаФон». Несколько лет

назад компания выиграла конкурс Мининформсвязи на предоставление конфиденциальной связи, которая позволяет шифровать сигнал. Изначально услуга развивалась в Чечне и других кавказских республиках. По словам начальника пресс-службы «МегаФона» на Северном Кавказе Тахира Холикбердиева, услуга «конфиденциальная сотовая связь» была создана для спецслужб, военных и сотрудников правоохранительных органов. Только через несколько лет услуга была введена в коммерческую эксплуатацию. Сейчас воспользоваться ею могут как юридические, так и физические лица. Для этого достаточно приобрести любой тарифный план «МегаФона» в любом регионе России и купить соответствующий телефон. До последнего времени это были исключительно трубки компании «Атлас». Сейчас услугой «конфиденциальная сотовая связь» в стране пользуются более 4 тыс. абонентов, за последний год число пользователей этой услуги увеличилось в два раза. Как отмечает Тахир Холикбердиев, это в основном представители государственных органов власти и крупного бизнеса.

В принципе качественный криптотелефон уже сам по себе является достаточно надежной защитой, так что использовать можно SIM-карты любого оператора связи. Однако по условиям лицензии ФСБ работать компания-разработчик имеет право только с «конфиденциальной связью» «МегаФона». А основное требование, которое выдвигает оператор к своим партнерам: телефон должен быть привязан к конкретной SIM-карте. То есть пользователь произведенного в России устройства не может выбирать оператора. К примеру, «Анкорт» сейчас вынужден изменить свой аппарат так, чтобы телефон мог работать только с «МегаФоном» и блокироваться при смене SIM-карты. По словам президента «Анкорта» Анатолия Клепова, переделка обойдется компании в несколько сотен тысяч долларов. Еще несколько сотен тысяч компания потеряла на уже заключенных в России контрактах. «Многим клиентам пришлось вернуть деньги», — говорит Анатолий Клепов. — Сейчас сложно объяснять людям, почему они могут пользоваться услугами только одного оператора, все привыкли к свободе выбора. Большинство, уезжая за границу, хотя экономят на роуминге. Но пока мы не предложим аппарат в соответствии с требованиями «МегаФона», не сможем продавать в России».

Предоставить клиентам более защищенную связь стремятся и другие операторы. «Билайн» и МТС уже несколько лет пытаются вывести на рынок канадский коммуникатор BlackBerry. Однако устройство не может пройти сертификацию ФСБ из-за стойкого алгоритма шифрования. Как полагают специалисты, даже если BlackBerry появится на российский рынок, он будет значительно отличаться от своего западного аналога. В «Вымпелком» тему BlackBerry комментировать отказались. А в пресс-службе МТС «Ъ-Телекому» сообщили, что работают над тем, чтобы в ближайшем будущем предложить коммуникаторы абонентам. Сейчас компания сотрудничает с канадским разработчиком RIM и российскими

государственными службами, чтобы разработать техническое решение, удовлетворяющее требованиям всех сторон».

Между тем многие российские предприниматели уже пользуются коммуникатором через зарубежных операторов связи. «Вы можете приобрести BlackBerry вместе с контрактом западного оператора примерно за \$400, — говорит ведущий аналитик Mobile Research Group Эльдар Муртазин. — Правда, при активном использовании такой вид связи обойдется как минимум в \$50 в день». По словам господина Муртазина, спецслужбы не смогут прочесть почту, отправленную с BlackBerry, если почтовый сервер находится за рубежом. Что касается звонков, то спецслужбы могут либо взломать ключ (это займет много времени), либо обратиться в западные компетентные органы с просьбой предоставить ключ. «Шансы силовиков зависят от конкретной страны. Очевидно, из Великобритании вряд ли что удастся получить», — резюмировал господин Муртазин.

Западный роуминг

Большинство российских разработчиков, а также западные компании вроде австралийской SecureGSM, немецкой CsurtoPhone и итальянской CasperTech все чаще предпочитают не создавать собственные телефоны, а разрабатывать программные решения для защиты переговоров. Причина не только в ограничениях, но и в том, что создание собственного телефона — дело дорогостоящее и требует наличия современного производства. «Технологии развиваются очень быстро», — отмечает Владимир Смирнов. — Чтобы обеспечить постоянно растущий набор и эргономику мобильных устройств, к которым производители привыкли пользователей, надо быть HTC или Nokia».

Большинство желающих защитить свои телефонные переговоры давно покупают телефоны за рубежом, например в Швейцарии, где законодательство гораздо либеральнее. Криптографические устройства западных Rohde & Swartz, Enigma, CsurtoPhone, SecureGSM предоставляют возможность работы с независимыми

сотовыми операторами. При этом пользователи могут сами генерировать ключи. Кстати, например, у Rohde & Swartz есть собственное представительство на территории России. Телефон там не продадут, однако посоветуют обратиться в немецкий офис. Кроме того, многие россияне делают покупки такого рода в Швейцарии. Но там в отличие от Германии продажа криптографического оборудования осуществляется преимущественно юридическими лицами. Поэтому, как сообщили «Ъ-Телекому» в одной из швейцарских компаний, точное количество российских клиентов подсчитать сложно: по законодательству они оформляют сделки на зарегистрированную в Швейцарии компанию. Одна из швейцарских фирм, по словам Анатолия Клепова, давно и довольно успешно использует собственный криптоалгоритм, сертифицированный в ЮАР и Швеции, который в собственном криптосмартфоне «Анкорт» применять не имеет права.

А вот телефоны немецкой компании CsurtoPhone стоимостью чуть больше \$2 тыс. вообще можно свободно приобрести в России. Правда, на сайте торгового партнера компании в России и странах СНГ «Альянс удачи» отмечается, что хотя телефоном можно свободно пользоваться в Европе, Индии, странах Азии, Южной Америки и Африки, для разговоров на территории России рекомендуется «проконсультироваться с квалифицированным юристом». Впрочем, в разговоре с корреспондентом «Ъ-Телекома» сотрудник представительства сказал, что никаких проблем у клиентов обычно не бывает: «Просто не „светите“ этой трубкой, и у вас никто ее не отберет».

Довольно просто приобрести также разработанный западной компанией программный шифратор. Заказать его можно по интернету, а затем загрузить в обычный смартфон. Решение основанной в Австралии россиянами компанией SecureGSM обойдется примерно в \$200–300. О качестве подобных продуктов судить довольно сложно: независимых экспертов на российском рынке почти нет. «Нередко западные компании стремятся снизить затраты на разработку шифраторов и используют уже готовую серийную продукцию для последующей модернизации в криптографическую», — отмечает источник «Ъ-Телекома» в НИИ «Автоматика». — К примеру, криптотелефон Rohde & Swartz сделан на базе сотового телефона Siemens S351. При таком подходе в шифраторах остается много „дыр“, которые криминал может использовать для дешифрования».

Таким образом, пока у российского потребителя выбор невелик. Он может приобрести отечественное морально устаревшее за время сертификации шифровальное устройство, которое к тому же поддерживает государственный алгоритм и работает только с одним оператором. Либо сделать выбор в пользу недорогого западного шифратора, использующего признанные международные алгоритмы, и иметь возможность самостоятельно генерировать ключи. Но при этом такое устройство нередко является довольно слабым в аппаратной части. Можно еще пользоваться BlackBerry, но далеко не всем придется по вкусу тарифы за роуминг. По словам Анатолия Клепова, именно поэтому россияне ничего не используют: ни российский, ни швейцарские, ни немецкие шифраторы. Покупатели не могут сделать выбор — они уже никому не доверяют.



6% УВЕРЕННОСТИ

Для слежки за человеком теперь не нужны специально обученные люди и громоздкие технические средства. Можно нарисовать цифровой портрет гражданина, имея лишь небольшие связи в одной из компаний — операторов сотовой связи. Если раньше телефонная слежка ассоциировалась исключительно с прослушкой, то теперь даже простая телефонная операционистка может погубить ваш бизнес или семью.

С помощью нехитрых манипуляций на рабочем компьютере телефонистка-инсайдер может получить список всех номеров, которые набирал бизнесмен. Затем она выяснит, что на определенные номера бизнесмен звонил чаще, на другие — реже, а третьи вообще набирал всего один раз. Телефонистке достаточно иметь информацию только о номерах, которые использовал абонент — вычислить конкретных людей сможет конкурент предпринимателя, всего лишь пролистав свой список контактов либо купив соответствующую базу данных на «Горбушке».

Используя биллинговую систему, телефонистка увидит, в каких странах мира побывал бизнесмен и где он пользовался роумингом. Используя сведения о географии и продолжительности командировок, легко определить имена тех компаний, с которыми жертва вела переговоры. Ситуация получается крайне неприятная: конкурент получает информацию обо всех шагах, которые предприниматель планирует сделать.

Фактически в руках маленькой телефонистки оказался статистический портрет предпринимателя, то есть его пристрастия в сотовом мире. Телефонистка знает, с кем, когда и как часто говорил бизнесмен. Значит, она обладает весьма содержательной информацией о его деловой и личной жизни. Теоретически бизнесмен может сменить собственный номер, но это произойдет уже после того, как его приватная информация окажется в руках конкурента.

Единственное, что может сделать оператор в данной ситуации, — это постоянно предупреждать своих сотрудников, а также использовать специализированные технические средства для контроля над их работой.

Телефонистка хоть и нарушает российский законодательство, все равно практически ничем не рискует, поскольку обнаружить и тем более доказать факт утечки чрезвычайно трудно. «В практике нашей компании уже встречались такие попытки. Многие компании действительно ловят инсайдеров, но один наш клиент, банк из первой сотни, решил пойти до конца и все же попытаться привлечь женщину-инсайдера к ответственности. Однако тщательная юридическая экспертиза и консультации с правоохранительными органами показали, что мы можем посадить только IP-адрес, но никак не инсайдера», — комментирует Денис Зенкин, директор по маркетингу компании InfoWatch.

В данном примере возможности телефонистки ограничиваются просмотром номеров, на которые звонил тот или иной абонент. Однако в штате операторов имеются сотрудники с более широкими полномочиями. Некоторые из них могут «класть» деньги на счет клиента или, напротив, снимать их с этого счета. В результате вполне реальна ситуация, когда телефонистка заблокирует телефон жертвы в тот момент, когда ему критически важно совершить звонок. Впоследствии деньги на счет ему, конечно, вернут, однако драгоценное время будет безвозвратно потеряно.

Оператор может запретить пересылать сведения за пределы своей компьютерной сети. «Специальные технические средства помогают инсайдеру совершить кражу данных через USB-флешки, любые диски, электронную почту, интернет или принтеры», — комментирует Максим Скида, руководитель направления защиты персональных данных компании Aladdin. — Но никакая даже самая современная технология не защитит от утечки той информации, которая помещается в память инсайдера».

Может показаться, что проблема надумана и никакой опасности на самом деле не существует. Однако утечки из телефонных компаний происходят с завидным постоянством. На протяжении долгих лет в продаже появлялись закрытые базы операторов сотовой и фиксированной связи, содержащие весьма интересные номера. Например, одна из прошлогодних баз содержала вполне реальные номера Владимира Путина и Геннадия Зюганова. И если до президента дозвониться было нельзя, то поговорить с лидером КПРФ — вполне можно.

Формально в России принят федеральный закон «О персональных данных», который обязывает организацию защищать приватную информацию других людей. Однако профессиональное сообщество осталось разочарованным этим беззубым законом, так как он действует только на бумаге. Согласно результатам исследования «Защита персональных данных по закону», проведенного в начале 2007 года аналитическим центром InfoWatch, 94% из 300 опрошенных специалистов по информационной безопасности заявили, что России было просто необходимо этот нормативный акт. В то же время лишь 6% выразили уверенность в том, что данный закон будет работать.

Алексей Доля

Shift in Pentagon's security-privacy balance?

Меняет ли Пентагон баланс в соотношении «безопасность—конфиденциальность»?

Alexandra Marks

Александра Маркс

В переводе TALON означает «Предупреждение угрозы и местное наблюдение». Это база данных о потенциальных угрозах против военных баз США как на территории США, так и за рубежом, о которых гражданские лица и военнослужащие докладывают в военную разведку. Для предотвращения этих угроз предполагалась организация своего рода военных патрулей в окрестностях баз. В 2005 году СМН сообщили, что в распоряжении TALON находится огромный архив материалов о местных пациентах и студентах, выступающих против службы в армии. Именно тогда активист антивоенного движения Кот Хордински обнаружил, что его группа

упоминается в файлах Пентагона как представляющая угрозу. «Нам стало жутковато, когда мы узнали, что наши имена фигурируют в базе данных Пентагона. Это нас действительно задело за живое», — говорит студент университета Калифорния в Санта-Крус. Все это заставило господина Хордински и его группу не только активизировать антивоенную деятельность, но и разоблачить Пентагон и рассказать общественности о базе данных, содержащей информацию о гражданах США. С помощью Американского союза гражданских свобод (ACLU) и десятков других пацифистских организаций они накопили столько доказательств, что заставили министерство обороны опубликовать тысячи страниц записей, которые оно собирало об антивоенных активистах. За этим последо-

вало расследование конгресса. Пентагон также был обвинен в нарушении закона о разведывательной деятельности и своих собственных инструкций.

В декабре 2005 года министерство обороны осуществило собственную проверку базы данных TALON. Вскоре после этого оно объявило, что уничтожило «много информации», которая, как и предполагалось, хранилась ненадлежащим образом. В отчете инспектора министерства обороны, опубликованном в июне этого года, говорится, что более 5000 из 13 000 документов в базе данных были уничтожены в апреле 2007 года. Источник в Пентагоне, попросивший не называть его имя, сообщил, что после вознившего шума предоставление информации по системе TALON также прекратилось. Все эти факторы

вынудили Пентагон на прошлой неделе объявить, что в сентябре он закроет программу, но будет продолжать противостоять потенциальным угрозам в отношении военных и правоохранительных органов. «Смысла в предоставлении информации практически не стало», — считает пресс-секретарь Пентагона майор Патрик Райдер. Майор Райдер отказался комментировать, сыграла ли обеспокоенность гражданскими свободами определенную роль в принятии решения, однако добавил: «Гражданские свободы всегда волнуют департамент».

ACLU настаивает на том, что упоминаемая Пентагоном причина закрытия базы данных неуместна. «Люди начинают с опаской верить в то, что ситуация меняется», — говорит руководитель программы

национальной безопасности в ACLU Джамил Джаффер. — Однако следует посмотреть на TALON в контексте многих других разведывательных программ, которые в последние пять лет были запущены. Мы находимся в странной ситуации, когда, с одной стороны, правительство требует как можно больше информации о людях, а с другой — создает трудности для людей в получении информации, необходимой для того, чтобы оценить законность действий правительства».

«Конституция разрешает использовать самые агрессивные методы при условии, что, ведя эту борьбу, мы не нарушаем наши свободы и демократию», — говорит Брюс Фейн, официальный представитель управления юстиции, возглавляемого президентом

Рейганом, который сейчас является председателем «Американской программы свободы» — консервативной группы, защищающей гражданские свободы.

Опыт научил Хордински, который эмигрировал сюда из Польши в возрасте восьми лет, тому, как важно быть бдительным в борьбе за права человека. «Я никогда не думал, что в этой стране может произойти что-нибудь подобное», — рассказывает он. — Это грустно и странным образом напоминает мне истории о коммунизме, о которых я слышал в детстве. Я бы не хотел сравнивать сегодняшнюю ситуацию с тем временем, однако оно много говорит о состоянии нашей страны, и об этом мы можем говорить сколько угодно».

Перевела Тамила Джоджуа