Технологии

Жук в тарелке

Российские компании учатся противостоять шпионажу

Влад Гринкевич

Негласная добыча информации при помощи технических средств становится весьма распространенным инструментом конкурентной борьбы во всем мире. Россия в этом смысле не исключение: в нашей стране за 2000 – 2001 годы объем продаж устройств для шпионажа увеличился вдвое. Такими же темпами росли продажи устройств, позволяющих защититься от шпионажа.

На российском рынке средств шпионажа большинство игроков действуют «в тени»: средства для похищения информации легально доступны лишь силовым структурам. Все негосударственные компании, которые пользуются шпионской техникой, делают это незаконно. В то же время рынок средств защиты от шпионажа абсолютно легален. Несмотря на разницу в правовом статусе, два рынка взаимосвязаны. С технологической точки зрения второй рынок представляет собой производное от первого: на всякий яд находится противоядие, против всякой технологии «атаки» разрабатывается технология защиты.

Покупайте российское!

По словам Ивана Белоуса, генерального директора компании «Сюртель» (одного из крупных российских производителей специальных средств), в течение 2000 – 2001 годов продажи продукции в легальном секторе средств защиты выросли вдвое. Белоус считает, что на теневом рынке средств похищения информации наблюдается та же картина. Оценить емкость рынка трудно: производители «шпионской» техники уверяют, что статистику продаж на рынке средств технической защиты в РФ аналитические агентства не ведут. Компании занимаются исследованием рынка «для служебного пользования» и делиться данными с прессой не хотят.

Техника для похищения и защиты информации хлынула на российский рынок сразу после распада СССР. Вплоть до 1998 года, когда был принят закон «Об использовании специальных технических средств в оперативно- розыскной деятельности», оборот подобной продукции практически не регулировался. На рынке преобладали зарубежные спецсредства. Сейчас ситуация иная: 70% рынка занимает отечественная техника, которая намного дешевле зарубежных аналогов. Ее производят частные компании, отпочковавшиеся от государственных НИИ. По словам Владимира Надеждина, директора питерской

компании «Смерш Техникс» (специализируется на производстве устройств обнаружения и подавления диктофонов), средства получения информации сегодня официально выпускают около 50 компаний, 40 из которых базируются в Москве. Многие из них одновременно разрабатывают и средства защиты.

И стекла имеют уши

Производители уверяют, что хорошие средства «атаки» большинству коммерческих структур недоступны. «Они используют относительно простую технику, часто кустарного производства, которую при желании можно купить даже на Митинском рынке», – уверяет Иван Белоус. В основном это всевозможные «жучки» – миниатюрные микрофоны с радиопередатчиками и средства для прослушивания проводных телефонов.

По данным «Сюртель», до 60% продаж средств защиты приходится на обнаружители и подавители микрофонов, а также на технику, защищающую телефонные линии. Кустарный «жучок» (работает в открытом FM-диапазоне и легко засекается сканером) стоит от $50 до $300. Фирменный «жучок» использует закрытые каналы передачи, его трудно обнаружить поисковой техникой, поэтому и стоит такая аппаратура до $1,5 тыс.

Более «продвинутым» прибором считается статоскоп – «жучок» с вибродатчиком в качестве микрофона. Датчик ставится на твердые предметы и считывает звуковые волны. Статоскоп может устанавливаться не только внутри прослушиваемого помещения, но и вне его. В качестве микрофона в статоскопе может также использоваться лазерный луч, направленный на предметы, способные действовать как мембраны, – стекла, зеркала, посуду. Приемником отраженного смодулированного луча служит объектив с большим фокусным расстоянием. Стоит такая «игрушка» около $15 тыс. Подслушать разговор, не приближаясь к объекту, можно и с помощью узконаправленнных микрофонов. Подобные микрофоны усиливают нужный сигнал и отсекают посторонние шумы. Улавливать звук они могут с расстояния около 1 км.

Прослушать телефонный разговор недоброжелатель может, подключившись к телефонной линии. Некоторые устройства позволяют делать это бесконтактно. Поселившийся в телефоне «жук» способен переправлять подслушанную информацию прямо по телефонной линии. Принять этот сигнал можно на любом участке до ближайшей АТС. Точно так же ведут себя «жучки», спрятанные в электроприборах и розетках. Их сигнал передается по линиям электропроводки, а принять его можно из ближайшей розетки. Кроме того, при определенной доработке в «жука» превращается сам телефон – некоторые его детали способны преобразовывать звуковой сигнал и посылать его по линии.

Говорит и показывает циферблат

Другим «модным» направлением, по словам Белоуса, является видеошпионаж.

Средств для этого предостаточно. Видеокамеры с объективами диаметром около 0,5 мм могут монтироваться в очках, пуговицах и т.д. Они соединяются с передатчиком (размером с сигаретную пачку), который транслирует «репортаж» на несколько сот метров. Такие приборы, в частности, производит «Сюртель».

Возможности шпионской техники становятся все шире благодаря использованию цифровых технологий. На выставке Comdex Fall 2001 в Лас-Вегасе компания Sony представила цифровую видеокамеру, встроенную в наручные часы. Камера оснащена небольшим поворотным объективом, микрофоном и цветным дисплеем, позволяющим просмотреть отснятые сюжеты. Самый изощренный метод технической разведки – сканирование побочных излучений электронных приборов. По излучению компьютерного монитора можно определить, что сейчас на нем изображено. Этот метод, равно как и перехват и расшифровка сигналов мобильного телефона цифровых стандартов, большинству частных структур недоступен. «Такие технологии находятся «на вооружении» у государственных спецслужб и крупнейших корпораций – по уровню оснащения и подготовки их службы безопасности не уступают государственным силовым структурам», – говорит директор «Сюртель».

Портрет врага

Средства борьбы со шпионской техникой доступны всем желающим. Эти устройства делятся на две группы: средства обнаружения и средства защиты. Компании-производители предлагают клиентам широкий спектр подобных устройств – от портативных индикаторов электромагнитных полей (их делают в виде ручек, портмоне или пейджеров) до сложных измерительных комплексов, способных оценивать степень защищенности помещения от акустических и виброакустических «жучков».

Нина Калинина, исполнительный директор компании «Маском» (один из крупных производителей и дистрибуторов средств защиты), считает, что одной лишь покупкой специального оборудования безопасности не обеспечишь. «Многие компании понимают, что информацию необходимо защищать, но плохо представляют себе, как это делать. Зачастую средства защиты применяются ими наугад или по совету знакомых. Между тем этот вопрос необходимо решать комплексно: сначала нужно составить портрет противника и лишь после этого разрабатывать концепцию защиты», – говорит Калинина. Это мнение разделяет и Владимир Надеждин из «Смерш Техникс»: «Разработка концепции защиты – наиболее трудоемкий этап».

Производители часто оказывают услуги по обследованию помещений и определению возможных каналов утечки. В Москве такая «чистка», с выездом специальной бригады, стоит от $20 до $30 за каждый обследованный квадратный метр площади. В зависимости от результатов проверки предлагаются различные варианты защиты. Чаще всего специалисты рекомендуют оснастить помещения генераторами помех и устройствами для экранирования (защита от электромагнитных излучений и от подслушивания, производимого при помощи акустических приборов).

По словам Ивана Белоуса, минимальный защитный набор (включает в себя средства акустической и эфирной защиты, а также защиту телефона) для

комнаты площадью 30 кв. м стоит около $3 тыс. Защита от диктофонов увеличит стоимость вдвое. Владимир Надеждин сообщил «Ко», что комплексная защита одной комнаты переговоров может стоить до $50 тыс.

Нина Калинина говорит, что покупка компаниями поискового и защитного оборудования на сумму $50 тыс. уже не редкость. «Многие нефтяные, металлургические или машиностроительные компании тратят на приобретение поискового оборудования по $100 тыс. – $200 тыс.», – сообщила она.

Наиболее крупные корпорации закладывают комплексную систему безопасности в проект здания еще на стадии разработки архитектурного решения офиса. Комплексные системы ведут постоянный мониторинг помещения. Они могут, к примеру, засечь человека с «жучком» и отслеживать его передвижения внутри здания. Стоимость систем комплексной безопасности здания измеряется сотнями тысяч долларов.