

*Стремление узнать чужие секреты, будь то частные или профессиональные, и непременно скрыть свои собственные заложено, видимо, в самой природе человека. Люди веками подслушивали и подглядывали за своими соседями, врагами, друзьями и конкурентами. Для этого не гнушались любыми средствами – от подкупа до хитроумных технологий.*

*Текст: Валерия СОКОЛОВА, фото: Елизавета ПАШКОВА*

## За мной следят, или «Шпионские штучки» для обывателей

**Например, секретная система связи банкирского дома Ротшильдов во время Первой мировой войны работала быстрее, чем связь государств-участников войны. Банк Ротшильда в Лондоне получал доклады с полей сражений раньше, чем они поступали премьер-министру по официальным каналам.**

Шпионские скандалы то и дело про- скальзывают в сегодняшних публи- кациях СМИ, чего стоил один только приемопередатчик, замаскированный под камень британскими спецслужба- ми в московском парке. Разведыва- тельные управления ведь для того и создавались, чтобы на государствен-

ном уровне заниматься военным или промышленным шпионажем, а также отслеживать и анализировать все то важное, что происходит в нашем не- спокойном мире каждый день.

Практически в каждом фильме зна- менитой бондианы британский супе-

рагент пользуется разнообразными миниатюрными фотоаппаратами в часах, кольцах и биноклях. Не стоит думать, что подобные устройства су- ществуют лишь в кино или доступны лишь секретным спецслужбам.

Типичная история не только для России, но и для современного Калининграда. Один бизнесмен объявил о грядущих переменах в компании и введении в действие поэтапного плана, позволяющего изменить подход к продажам, уве- личить производительность труда и в итоге продать товар дешевле, чем конкуренты. Все переговоры он вел исключительно в собственном ка- бинете, предусмотрительно вклю- чив громкую музыку.

Однако в решающий момент вы- яснилось, что его прямой конкурент подготовил контратаку. О том, как это могло произойти и что нужно знать, чтобы уберечь себя и свой бизнес от нежелательного вторжения, рас- сказал на очередной встрече Клуба ИТ-директоров Калининградского



региона Дмитрий КРИКУН, генеральный директор группы компаний «Интеллект-Холдинг».

В 90-х гг. на рынках Калининграда можно было найти последние военные разработки в области тайной слежки. После развала СССР огромному числу НИИ, прежде работавших на военную промышленность, пришлось выйти на открытый рынок. В то время из-под полы могли достать разработку, стоившую десятки тысяч долларов, позволяющую прослушивать разговоры, находясь за сотни метров от объекта. В настоящее время подобной практики давно уже нет, ведь наказание не только за продажу, но и за покупку шпионской техники предусмотрено весьма суровое.

Самым известным устройством прослушки является жучок (или закладка), позволяющий записывать звуки в помещении и затем либо передавать их тем или иным способом хозяину, либо хранить информацию до изъятия. Жучки могут работать как от батареек, так и от сети, записывать все подряд или быть активированными по сигналу или даже голосом подслушиваемого.

Более продвинутым способом разведки считается установка миниатюрных видеокамер высокого разрешения, вмонтированных в интерьер или предметы обихода. Они также могут периодически отсылать информацию или хранить ее до изъятия. Обнаружить подобную закладку, особенно спрятанную и находящуюся в режиме ожидания, очень непросто. Для этого потребуется изучить все поверхности кабинета с помощью специального сканера – нелинейного локатора. Устройство посылает волны на потенциальные жучки и ждет отклика. Однако такой же отклик может дать и другое электронное устройство, и даже ржавчина.

Другим способом, позволяющим избавиться от прослушки, является установка широкополосных или узкополосных генераторов помех. Достаточно поставить устройство, внешне похожее на магнитофон со множеством антенн, в кабинет ди-

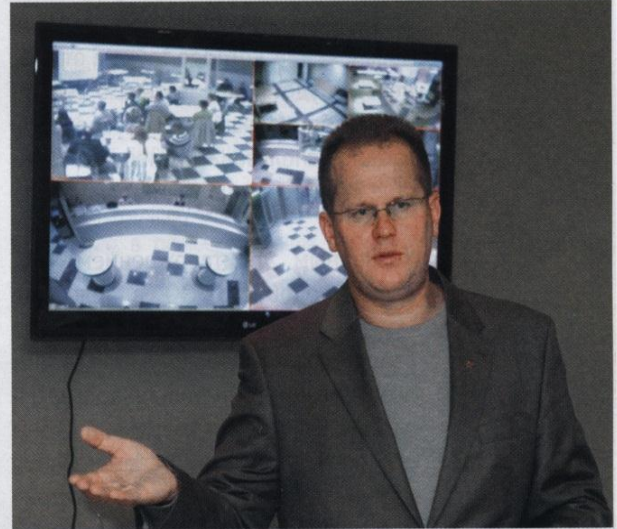
ректора, и в эфире будут слышны одни лишь помехи. Однако подобные устройства обладают существенным недостатком – из-за сильного излучения все, кто длительное время находится вблизи, чувствуют недомогание. Поэтому рекомендуется пользоваться такими генераторами помех только во время важных переговоров.

Чтобы обнаружить закладку (жучок), необязательно пользоваться сложными устройствами, достаточно не оставлять посетителей одних в кабинете, пускать только тех, кому доверяете, и периодически проверять классические места установки закладок – оборотные стороны столешниц и стульев. Не забывайте, что миниатюрные диктофоны и видеокамеры могут скрываться в самых безобидных на вид предметах – авторучках, зажигалках и ежедневниках.

Довольно экзотическим способом слежки является снятие виброакустических волн с поверхности оконных стекол. Для этого нужно направить лазерный луч, улавливающий колебания, на окно комнаты, откуда будет производиться съем информации, определить угол отражения и поймать его обратно. В идеале будут слышны все звуки внутри помещения, однако у этого способа есть и существенный недостаток – необходимо отсутствие сторонних акустических помех и колебаний окон от общественного транспорта.

Тем не менее, чтобы обезопасить себя от такого способа тайного слежения, ведь дальность действия луча может достигать до километра, достаточно периодически приоткрывать окно в помещении. Угол отражения от оконного стекла изменится, и потребуется много времени, чтобы снова поймать обратный луч.

Классическим приемом слежки является перехват телефонных переговоров. Для этого на линию устанавливается специальный трансмиттер, активирующийся во время телефонного разговора. Источником питания может служить сама телефонная линия. Для локализации перехватчика



потребуется специальные устройства, анализирующие работу телефонных линий компании.

Более простым способом записи телефонных разговоров является монтаж диктофона прямо в телефонную трубку. В случае с мобильными телефонами злоумышленнику достаточно взять его на 30 секунд, чтобы установить шпионское программное обеспечение, которое тайком от владельца будет передавать всю информацию, проходящую через телефон, и заодно использовать телефон в качестве круглосуточного диктофона.

Косвенным подтверждением наличия подобного ПО в телефоне может служить слишком быстро разряжающийся аккумулятор и подозрительная активность подсветки экрана. Если вы не уверены в своем мобильном телефоне, рекомендуется вынимать батарейку во время встреч или использовать так называемый акустический сейф. Внешне устройство похоже на обычный чехол для телефона или подставку, однако вну-

три находится сканер, блокирующий несанкционированную активацию каналов сотовой связи в режиме доступа к микрофону мобильного телефона.

В качестве способа противодействия всевозможным подслушивающим и подсматривающим устройствам применяются сложные системы анализа частот каналов и блокировки подозрительных. Однако многие считают, что достаточно включить громкую музыку, и никто не сможет подслушать их разговор.

Это распространенное заблуждение. Существуют устройства, позволяющие разделять голоса и стороннюю музыку. Для этого достаточно иметь запись зашумленного разговора и оригинал музыкальной записи. Песня просто вычитается из аудиодорожки, и на выходе слышна речь без каких-либо помех. Поэтому самый простой и эффективный способ защитить тайну переговоров – включить запись вашего собственного голоса с каким-либо оригинальным текстом. ○

#### **ДЛЯ СПРАВКИ:**

**Статья 138 УК РФ.  
Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений**

**Незаконные производство, сбыт или приобретение специальных технических средств, предназначенных для негласного получения информации, наказываются штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.**

**А также ограничением свободы на срок до трех лет, либо лишением свободы на срок до трех лет с лишением права занимать определенные должности.**