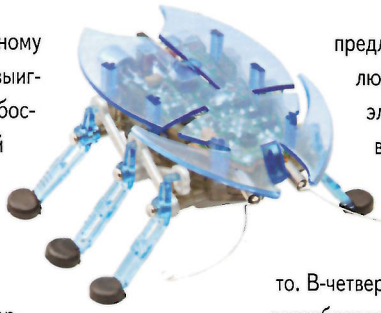
Закладочные устройства («жучки») и как с ними бороться

Геннадий БУЗОВ,
заведующий лабораторией защиты информации от утечки по техническим каналам учебного центра «ИНФОРМЗАЩИТА», кандидат военных наук, доцент



Переход нашего государства к рыночным отношениям привел к активному проявлению конкурентной борьбы между фирмами. Для того чтобы выиграть в этой борьбе, руководитель должен принимать грамотные и обоснованные решения, направленные как на управление повседневной деятельностью фирмы, так и нацеленные на перспективы развития. Для этого он должен иметь необходимую информацию, именно достоверная и своевременно полученная информация составляет основу для принятия управленческих решений.

Поэтому любые серьезные мероприятия начинаются со сбора информации. В условиях непланового развития экономики единственным регулирующим принципом, как мы знаем, является соотношение спроса и предложения, следовательно, любая фирма стремится знать, что творится в сфере ее интересов. То есть хочет иметь весь объем интересующей ее информации. Такую информацию можно получить различными методами. Например, можно анализировать легальные данные из различных общедоступных источников. Однако для этого необходимо иметь как минимум толкового аналитика. Можно пойти и по другому, более простому, но незаконному пути: получать информацию непосредственно от руководителей конкурирующих фирм.

В настоящее время речевая информация была и остается основной для получения исходных данных для принятия решения, и ее цена достаточно высока. Следовательно, заинтересованные лица пытаются получить эти сведения зачастую незаконным путем и для этой цели используют закладочные устройства (ЗУ).

В последнее время у большинства обывателей появилось расхожее мнение, что применение ЗУ в условиях развития компьютерной техники и всемирной электронной паутины – вчерашний день, однако это не так, и тому есть ряд подтверждений. Во-первых, в условиях рыночной экономики спрос рождает предложение, а в интернете предлагается множество подслушивающих устройств на любой вкус и карман. Во-вторых, за последние годы электронные устройства существенно уменьшились в размерах, энергопотреблении и стоимости. В-третьих, внедрение технических средств для негласного и незаконного получения речевой информации достаточно просто. В-четвертых, если данный вопрос не актуален, то для чего потребовалось вводить в Уголовный кодекс РФ новую статью с ужесточением наказания с 3 до 4 лет лишения свободы, а именно: «Ст.138.1. УК Незаконный оборот специальных технических средств, предназначенных для негласного получения информации (введена Федеральным законом от 7.12.2011 № 420-ФЗ). Незаконные производство, приобретение и (или) сбыт 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, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового, либо лишением свободы на срок до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового».

Все вышеизложенное позволяет сделать выводы о том, что проблема защиты от незаконного получения информации ограниченного пользования с помощью различного рода ЗУ является актуальной и в настоящее время. Учитывая, что история нашего существования в условиях рыночной экономики – это история непрерывного раздела и передела рынков, борьбы за влияние и получение прибыли во многих областях экономики, конкуренция с течением времени лишь набирает обороты. Поэтому многие предприниматели самого различного уровня вправе опасаться возможного применения средств прослушивания как стороны конкурентов (а иногда и партнеров по бизнесу), так в ряде случаев и со стороны криминальных структур. В настоящее время ЗУ могут быть закамуфлированы в различные бытовые приборы и оборудование, такие как часы, компьютерные мыши, флешки, различные модели, письменные приборы, калькуляторы и т. д. В качестве примера можно привести настенные часы с ЗУ, обнаруженные на одной из фирм (рис. 1).

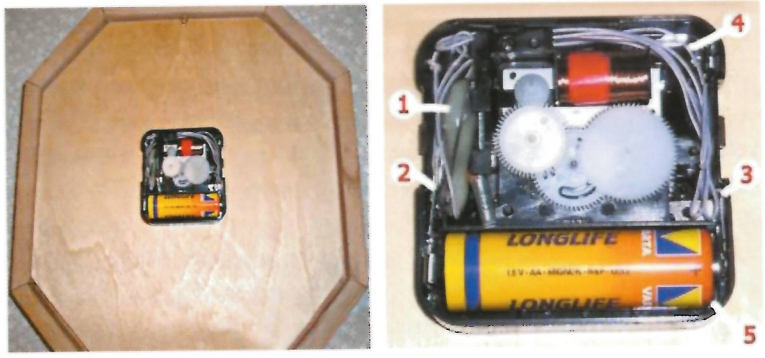


Рис. 1. Радиомикрофон, закамуфлированный в часовом механизме

Таким образом, напрашивается вывод о том, что выявление ЗУ является актуальной проблемой для большинства серьезных фирм. А если существует проблема, то необходимо найти и законные пути для ее решения. Наше законодательство обязывает при оказании услуг по выявлению незаконно установленных СТС иметь лицензию ФСБ на данный вид деятельности и в то же время разрешает выполнять поисковые работы без лицензии, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя. Об этом свидетельствует ряд законодательных актов: ФЗ 04.05.2011 № 99 «О лицензировании отдельных видов деятельности» – статья 12; постановление правительства Российской Федерации от 16 апреля 2012 г. № 314 «Об утверждении Положения о лицензировании деятельности по выявлению электронных устройств, предназначенных для негласного получения информации (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)».

Таким образом, мы получили официальное разрешение на выявление ЗУ без получения лицензии при защите своих интересов, однако о том, как это сделать самим, нигде не написано. Методики по выявлению ЗУ, даже при защите информации конфиденциального характера, имеют гриф «Секретно» и предназначены только для лицензиатов.

Итак, я надеюсь, что все изложенное позволит большинству сделать правильные выводы о том, что спасение утопающих дело рук самих утопающих, тем более что государство своими законодательными актами разрешает решать задачи по выявлению незаконно установленных СТС своими силами и без лицензии. И, как правило, здесь возникает ряд вопросов, а именно:

1. Что вы собираетесь выявлять?
2. Как выявлять?
3. Кто этим будет заниматься?

Что вы собираетесь выявлять? В любом случае подготовка к специальной проверке начинается с выявления и анализа возможных угроз вашей информации. Для этого необходимо:

- проанализировать информацию, циркулирующую на вашем предприятии, с целью выявления той, которая может заинтересовать потенциальных противников, быть востребована и реализована на рынке;
- попытаться определить, кто заинтересован в получении этих сведений;
- кого противник может использовать для получения этих сведений.

Затем необходимо оценить возможности вероятного противника с целью выявления потребительских свойств и технических характеристик ЗУ, которые он может применить.

Полученная информация позволит спланировать мероприятия по выявлению ЗУ и требуемое для этого оборудование.

Как выявлять? В любом случае выявление ЗУ в помещениях, в которых, по вашим предположениям, они могли быть установлены, начинается с визуального осмотра помещения и выявления подозрительных мест и предметов, в первую очередь недавно появившихся, в которых могут находиться ЗУ.

«Единственное, чем можно найти закладку, – это пара хорошо натренированных человеческих глаз и комплект намозоленных и опытных рук.

Электронное измерительное оборудование используется только для того, чтобы подсказывать поисковику, где смотреть. Нет волшебных черных коробочек, которые находят закладки». Джеймс Аткинсон James M. Atkinson, GranitelslandGroup.

Однако не всегда одним лишь визуальным осмотром можно выявить скрытно установленные и закамуфлированные ЗУ. Поэтому для гарантированного выявления необходимо использовать поисковое оборудование.

Оптимальный комплект такого оборудования состоит из аппаратно-программного комплекса; сканирующего приемника; индикаторов поля; оптических обнаружителей видеокамер. В качестве дополнительного оборудования можно рекомендовать нелинейный локатор и комплект инструментов.

Кто этим будет заниматься? Ответ на этот вопрос зависит от многих факторов и прежде всего от цели поиска. Если вы хотите действительно обезопасить себя от возможной утечки важной для вас информации, то для проведения поисковых мероприятий целесообразно в штате фирмы иметь подготовленных специалистов, так как профилактическую проверку с целью выявления возможно внедренных ЗУ необходимо проводить регулярно. Если вас не интересует результат, а волнует формальная сторона вопроса, то для проведения проверки можно пригласить фирму, имеющую лицензию ФСБ на ее проведение.

В статье были рассмотрены вопросы реальности применения различного рода ЗУ для получения информации конфиденциального характера и дан краткий анализ законности и подходов к проведению поисковых работ с целью выявления ЗУ. Вопросы методики поиска и применения специального оборудования – это тема для специального изучения.