Спецтехника: рыночные аспекты

И.П. Белоус,
эксперт

Для большинства профильных организаций 2002 г. прошел под знаком борьбы с терроризмом и с пониманием того, что спецслужбам не справиться с этой задачей без применения специальных технических средств (СТС), без развития и обновления средств контроля и защиты информации.

Использование конфиденциальных сведений, полученных несанкционированным путем, наносит материальный и иной вред как государственным, коммерческим организациям, так и физическим лицам. Зачастую полученные именно таким путем сведения используются для подготовки преступлений и террористических актов.

Проблема современности

В силу недостаточной информированности большинство российских граждан и организаций не видит для себя особо острой задачи обеспечения информационной безопасности. Более того, деятельность в данной области ограничена относительно узким кругом специалистов и фирм, предлагающих в этом секторе рынка свои услуги и технические средства. Между тем такая проблема существует и с развитием информационных технологий становится все более и более актуальной.

Любая информация, не носящая массового характера и предназначенная для ограниченного круга лиц, попадая в руки злоумышленника, может быть использована им во вред. Даже если содержание информации, на первый взгляд, может носить безобидный характер, злоумышленник может использовать буквально все: от сведений чисто бытового характера до информации, содержащей служебную и коммерческую тайну.

Масштабность мероприятий по защите информации должна зависеть прежде всего от оценки упущенной выгоды и размеров ущерба, который может нанести технический шпионаж. Многие, надеясь на авось, обращаются к специалистам только после ощутимых финансовых потерь. В этот момент перед потерпевшими встает ряд сложных, требующих разрешения проблем. Во-первых, это выбор предприятия или фирмы, которые, с одной стороны, должны гарантировать конфиденциальность при ведении своей деятельности, с другой – эффективно решать поставленные задачи, используя как технические, так и организационные методы. Во-вторых, это выбор необходимых технических средств. Рассмотрим второй аспект более подробно.

Оптимальная конфигурация

В настоящее время на рынке предлагается огромное количество устройств, способных в той или иной степени решать проблемы информационной безопасности. Степень их эффективности (как и ценовые характеристики) колеблется в очень широком диапазоне. Поэтому, прежде чем приступить к формированию парка необходимых технических средств, необходимо произвести условное моделирование потенциального противника, то есть того, от кого должна быть установлена защита, сделать примерную оценку его технических и интеллектуальных возможностей в данной области безопасности. Такая оценка поможет оптимально сконфигурировать создаваемую систему информационной безопасности и избежать необоснованных материальных затрат. Комплексный подход был бы неполон без обзора рынка специальной техники контроля информации (СТКИ).

Технические средства контроля информации

Рынок СТКИ в силу ограниченного законом круга потребителей достаточно узок и закрыт. Сегодня на этом сегменте рынка работают около 70 российских компаний, имеющих лицензию ФСБ на разработку, производство и поставку специальных технических средств (СТС). Наиболее успешно работают фирмы, установившие прямые контакты с потребителями СТС – субъектами оперативно-розыскной деятельности (ОРД). Таких фирм на рынке не более десяти, и в основном они находятся в московском регионе.

За последний год государство существенно увеличило финансирование силовых структур для закупок СТКИ, были выделены средства и на разработку новой техники. Это явилось толчком к оживлению деятельности на рынке СТС государственных НИИ и производственных предприятий, которые за долгое время недостаточного финансирования и отсутствия притока молодых кадров зачастую утратили свой инженерно-научный потенциал.

Сегодня наблюдается тенденция ведения совместных разработок в области СТКИ между государственными и коммерческими предприятиями и организациями или же разработок техники частной фирмой в интересах субъекта оперативно-розыскной деятельности. Такое сотрудничество выгодно обеим сторонам и позволяет государственным спецслужбам получать технику на уровне лучших мировых образцов или даже превосходящую их по многим параметрам, но существенно дешевле.

Рыночная классификация

Современный уровень развития элементной базы и технологий позволяет осуществлять контроль (технический съем) информации самыми разнообразными способами и приемами, но классифицировать СТКИ удобней всего по методу получения конфиденциальной информации:

- средства акустического контроля (от простейших проводных до направленных и лазерных радиомикрофонов);
- средства контроля и перехвата информации на технических каналах связи (от ТЛФ-закладок и съемников до комплексов по контролю сотовой и пейджинговой связи);
- средства для скрытого визуального наблюдения, фото- и видеосъемки (от видеозакладок и специальной оптики до тепловизоров и приборов ночного видения);
- средства перехвата информации, обрабатываемой на компьютерах и в компьютерных сетях (от программных закладок и вирусов до средств контроля монитора по его излучению);
- средства накопления, регистрации и обработки накопленной информации (от диктофонов до многоканальных комплексов записи и автоматизированных систем работы с базами данных).

Из всей вышеперечисленной техники основная часть относится к специальным техническим средствам негласного получения информации (СТС НПИ), оборот которых строго регламентируется нормативными актами, а их несанкционированное применение может привести к уголовной ответственности.

Немалую же часть составляет техника так называемого двойного назначения, являющаяся составной частью СТС НПИ, но

в отдельном виде к таковой не относящаяся. К такой технике можно отнести проводные микрофоны, многоканальные магнитофоны, малогабаритные диктофоны и видеомагнитофоны (в том числе бескинематические), сверхминиатюрные видеокамеры и т.д.

Анализ рынка СТКИ показывает, что на данный момент существует огромный выбор технических средств, предназначенных для различных способов добывания информации. Они разработаны с использованием новейших цифровых технологий и исполнены в виде, затрудняющем их обнаружение поисковыми средствами.

Все вышеперечисленное делает задачу по обнаружению и блокированию каналов несанкционированного доступа и утечки информации исключительно сложной с технической и организационной сторон. Следует отметить, что проблема информационной безопасности должна решаться комплексно, а бессистемное приобретение отдельных технических средств, как правило, приводит к неэффективным финансовым затратам с минимальными результатами. Поэтому не следует делать никаких приобретений без серьезной консультации со специалистами. Более того, практика некомплексного подхода к обеспечению информационной безопасности дискредитирует саму возможность решения проблемы защиты информации.

Специальная техника защиты информации

В целом комплексная защита информации – сложный и многообразный процесс. Для того, чтобы составить для себя ясное представление об этом, систематизируем методы защиты и увяжем их в составе комплексного мероприятия.

Во-первых, сразу необходимо отметить, что информация охраняется государством, и защита ее включает в себя нормативно-правовые, организационные и технические средства. В свою очередь, технические средства можно разделить на технику защиты информации в помещениях и каналах (сетях) связи (ТЗИ) и технику обнаружения каналов утечки информации и выявления электронных устройств несанкционированного съема информации.

С учетом принятого постановления Правительства РФ № 290 от 30 апреля 2002 г. ТЗИ можно классифицировать по степени важности защищаемой информации на технику защиты конфиденциальной информации и технику, применяемую для защиты информации, относящейся к государственной тайне. В отдельный класс можно выделить технику (обычно это программно-аппаратные комплексы) для оценки защищенности объектов информатизации и исследования ПЭМИН.

Рынок средств ТЗИ достаточно широк и стремительно развивается. В отличие от рынка СТС НСИ, в нем активно участвуют зарубежные производители, особенно в сегменте измерительной и поисковой техники. Постоянно растет и круг потребителей такого оборудования. Этому способствует и то, что после кризиса 1998 г. парк такой техники несколько лет не обновлялся, и теперь предприятия и организации наверстывают упущенное, заполняя образовавшийся пробел. Можно отметить и то, что в последнее время значительный интерес к российской технике и технологиям проявляют зарубежные фирмы.

Номенклатура средств ТЗИ

Рынок средств технической защиты информации достаточно насыщен, и здесь реально подобрать наиболее подходящий и приемлемый по цене комплект техники, эффективно и реально обеспечивающий информационную безопасность, для любого потребителя (субъекта или объекта информатизации). Так, для выявления различных каналов утечки информации и оценки возможности применения их потенциальным противником можно использовать, например, индикаторы поля (или индикаторы радиоизлучения), являющиеся наиболее простыми поисковыми средствами. Основной принцип их работы состоит в выявлении абсолютного максимума уровня излучения в помещении. Некоторые индикаторы могут работать в сторожевом режиме и определять

Таблица 1

Комбинированные поисковые приборы российского производства

Приборы и их характеристики		D008	ST-031/031P "Пиранья"	ST-032	ПКУ-6М
Индикатор поля	диапазон частот, МГц	50–1500	30–2500	30-2500	–
	чувствительность, не хуже, мВ	2	10	4	–
Анализатор-приемник проводных линий	диапазон частот, МГц	0,05–7	0,1–15	0,05–9	0,02– 24,5
Детектор инфракрасных излучений	спектральный диапазон, нм	–	770–1000	770–1000	770–1000
	угол поля зрения, град	–	30	30	30
Детектор магнитного поля	диапазон частот, кГц	–	0,3–5	0,5–300	Не нормируется
Виброакустический приемник	чувствительность, не хуже, Вхс^2/м	–	1	1	Не нормируется
Акустическоий приемник	чувствительность, не хуже, мВ/П	–	5	5	0,2–20 кГц

Таблица 2

Нелинейные локаторы российского производства

Характеристики	Катран SP-61/M	Родник–2ЗК	Онега–23	HP- 900EM
Вид излучения	Непрерывный	Импульсный/непрерывный	Импульсный	Импульсный
Частота излучения, МГц	891–897	980–1020	910	900
Анализируемая гармоника	2 и 3	2 и 3	2 и 3	2 и 3
Мощность излучения, Вт	2	2	80	150
Чувствительность, дБ	-127	-145	-120	-129
Диапазон регулировки чувствительности, дБ	–	45	42	50
Диапазон регулировки мощности	80 мВт, 160 мВт, 600 мВт , 2 Вт	20	–	8
Питание, В	220 /12	220 /12	220 /12	220 /12
Время работы от аккумулятора, ч	3	4	2?3	2?4
Вес комплекта, кг	4	6	5	8

частоту излучения. Но они ограничены малым радиусом действия.

К следующей группе можно отнести специальные радиоприемные устройства (сканирующие или панорамные приемники, спектроанализаторы). Наиболее эффективно их использование в составе программно-аппаратных комплексов радиоконтроля, позволяющих автоматизировать процесс поиска и проводить измерения для оценки ПЭМИН. Особую группу занимают здесь многофункциональные и универсальные приборы, выполненные в виде единого устройства и позволяющие проводить поиск как по радиоэфиру, так и в проводных линиях, в акустическом и ИК-диапазонах.

Наименее представлены в современной номенклатуре поисковой техники, но необходимы и важны, с точки зрения специалистов, устройства для проверки телефонных линий и других проводных коммуникаций – анализаторы линий (в том числе и сетей питания).

Поисковая техника

Одной из наиболее сложных задач в поисковых мероприятиях является обнаружение пассивных или внедренных в конструктивные элементы помещений закладных устройств. Для их поиска применяются нелинейные локаторы, по сути представляющие малогабаритную радиолокационную станцию. Принцип действия их основан на преобразовании зондирующего луча при попадании его на полупроводниковый переход в кратные гармоники.

При проведении поисковых работ используют и досмотровые средства. К их числу относятся портативные рентгенотелевизионные комплексы, различные эндоскопы, металлодетекторы и прочее вспомогательное оборудование (например, специализированные наборы инструментов, досмотровые зеркала и т. д.). Проведение поисковых мероприятий является неотъемлемой частью работ по защите информации, но при этом не следует забывать собственно о технических средствах защиты информации.

Для обеспечения защиты какого-либо объекта (здания, помещения, линии связи) требуется использование набора средств ТЗИ, обеспечивающих защиту информации от утечки по каждому из возможных каналов. Не существует одного прибора, обеспечивающего полную и всестороннюю защиту. Каждый прибор обеспечивает контроль и закрытие конкретных каналов и в соответствии с установленными правилами должен быть сертифицирован.

Новые тенденции развития спецтехники контроля и защиты информации

В настоящее время наблюдается рост предложений новых образцов специальной техники контроля и защиты информации. Более подробно они представлены на страницах данного каталога.

Применение новых цифровых технологий позволило уменьшить цифровые диктофоны до размеров, позволяющих камуфлировать их практически в любой даже самый малогабаритный предмет. Дальнейшим их развитием станет беспроводной дистанционный сброс информации в другой накопитель на большое расстояние за короткое время.

На рынке появились сверхминиатюрные видеокамеры – меньше одного кубического сантиметра. А появление миниатюрных цифровых магнитофонов, размером не больше пачки сигарет, со временем качественной записи в несколько часов позволяет существенно расширить применение систем видеорегистрации.

Для передачи звука и видеоизображения все чаще применяются цифровые каналы. Использование цифровых методов закрытия информации находит все большее применение в телекоммуникационных сетях связи. Происходит автоматизация и миниатюризация приборов по поиску электронных закладных устройств и измерений ПЭМИН. Появляется новый класс приборов, предназначенных для применения индивидуальными потребителями.

Нелинейные локаторы для поисковых мероприятий становятся доступней по цене и проще в использовании.

Задача борьбы с терроризмом и переоснащение силовых структур специальной техникой останется актуальной и в 2003 г. Следовательно, ожидается дальнейшее развитие рынка СТЗИ, появление новых разработок и нетрадиционных решений. ■