БЕЗОПАСНОСТЬ

СРЕДСТВА ЗАЩИТЫ

от утечки информации по техническим каналам

Ольга Такташова
Специалист по комплексной защите информации

В последние годы понятие «защита информации» становится знакомым всё более широким слоям общества. Из сферы государственных интересов оно распространилось и в сферу интересов коммерческих предприятий, учреждений и частных лиц.

Однако простые обыватели чаще всего под защитой информацией понимают обеспечение безопасности данных в компьютерных системах от различного рода злонамеренных действий третьих лиц, не подозревая даже о существовании обширного набора методов и средств для защиты информации, циркулирующей в помещениях. Проще говоря, для противодействия подслушиванию, подглядыванию и прочим, более хитроумным и технически сложным способам выведать то, что находится за закрытыми дверями.

Деятельность по технической защите информации складывается, прежде всего, из деятельности по обнаружению технических каналов утечки информации и комплекса мероприятий, направленных на исключение возможности возникновения таких каналов.

По природе своего возникновения каналы утечки можно разделить на специально организованные и возникающие естественным путём.

В первом случае, злоумышленник, как правило, использует для получения информации специальные технические средства, которые он может внедрить на объект. Это могут быть так называемые закладные устройства – «жучки», которые передают информацию по радиоэфиру, в инфракрасном (ИК) диапазоне, по телефонным линиям связи, электросети, а также скрытно установленные видеокамеры или диктофоны. Для получения информации без захода в контролируемое помещение применяют направленные и «лазерные» микрофоны, стетоскопы, средства высокочастотного навязывания и др.

Каналы утечки информации второго типа возникают вследствие конструктивных особенностей средств обработки информации (оргтехники), электробытовых приборов, систем громкоговорящей связи и т.п. Злоумышленник, используя специальную высокочувствительную аппаратуру, может выделить информационные сигналы из побочных электромагнитных излучений и наводок, создаваемых этими средствами.

Любые мероприятия по защите информации, прежде всего, начинаются с выявления каналов утечки информации и обнаружения внедрённых закладных устройств, проще говоря – с «чистки» помещения.

Для обнаружения каналов утечки информации существует целый

БЕЗОПАСНОСТЬ

Миниатюрный индикатор поля – частотомер SEL SP-71/M «Оберег».

Нелинейный локатор с непрерывным излучением SEL SP-61/M «Катран»

Устройство обнаружения видеокамер «Алмаз»

арсенал технических средств: от простых, обращение с которыми под силу новичку, до сложных профессиональных систем, требующих специальных знаний и навыков.

Всех их можно условно разделить на 3 типа:

1. Обнаруживающие технические средства съёма («закладки») по их излучениям в радиоэфире, проводных цепях и т.д. в режиме передачи информации.

2. Обнаруживающие непосредственно сами устройства съёма информации, замаскированные в предметах интерьера, строительных элементах и т. д., находящиеся как в активном (рабочем), так и пассивном (выключенном) состоянии.

3. Обнаруживающие опасные информативные сигналы и наводки, возникающие при работе офисной и бытовой техники и вспомогательных технических средств.

Простейшими устройствами первого типа являются индикаторы поля, которые обнаруживают радиозакладки по превышению уровня их излучения над общим радиофоном. Достоинством таких устройств является лёгкость и простота использования, быстрое определение местонахождения радиоизлучающих устройств. Но в условиях сильных радиопомех, например, вблизи от станций сотовой связи, теле- и радиоретрансляторов и тому подобных источников радиоизлучения, индикаторы поля малоэффективны. Для повышения эффективности поиска используются индикаторы поля с применением обратной акустической связи («акустозавязкой»), с определением частоты излучения, селекцией цифровой и аналоговой передачи. Представителями данного типа устройств являются детектор поля ST 006, миниатюрный индикатор поля – частотомер SEL SP-71/M «Оберег».

Более совершенными и точными при поиске радиозакладок являются сканирующие и скоростные приёмники, спектроанализаторы. Единственным их недостатком является длительное время поиска (при переборе радиочастот). Для увеличения эффективности и скорости обнаружения на их основе создаются программно-аппаратные комплексы радиомониторинга с использованием банка данных «почерка» различных радиозакладок. Представителями данного класса устройств являются скоростной приёмник-коррелятор SEL SP-81 «Оракул», многофункциональный поисковый прибор ST 031 «Пиранья», спектральный коррелятор Oscor. Причём последние два являются многофункциональными приборами, позволяющими обнаруживать не только радиоизлучение, но и излучение в ИК диапазоне, электромагнитные и виброакустические сигналы. Также они могут служить и для проверки любых проводных линий (телефонных линий, сети электропитания и т. п.).

Все вышеперечисленные устройства позволяют находить только работающие и излучающие технические средства съёма информации. Но существует целый класс закладок, которые накапливают информацию и передают её в эфир за очень короткий промежуток времени или же включаются дистанционно по команде. Поэтому для их обнаружения применяются устройства второго отмеченного нами типа. К ним относятся нелинейные локаторы, металлоискатели и переносные рентгеновские установки.

Нелинейные локаторы обнаруживают полупроводниковые элементы, из которых состоит большинство радиоэлектронных средств съёма информации. При облучении области пространства, в котором размещены полупроводники, высокочастотной электромагнитной волной в отражённой волне появляются вторая и третья гармоники этой частоты. Выпускаются нелинейные локаторы с импульсным зондирующим сигналом (например, «Люкс», NR-900EM), с непрерывным излучением (SEL SP-61/M «Катран») и с сочетанием обеих типов излучения («Лорнет», ORION).

Многофункциональный поисковый прибор ST 031 «Пиранья»

Для специальной проверки вычислительной и оргтехники, а также для проверки элементов строительных конструкций применяются рентгеновские установки.

Отдельной категорией поисковой техники являются устройства обнаружения видеокамер. Их можно разделить на 2 основные группы. Приборы первой группы обнаруживают оптику видеокамер при их подсветке ИК лазером («Алмаз», «Чистильщик»). Приборы второй группы осуществляют поиск видеокамер по характерным для них электромагнитным излучениям (IRIS, SEL SP-101 «Аркан»).

Для исследования побочных электромагнитных излучений и оценки возможности утечки информации за счет виброакустических и акусто-электрических преобразований применяют специальные программно-аппаратные комплексы. К таким средствам относятся, например, система «Сигурд», комплексы «Навигатор» и «СПРУТ». Такие системы контроля защиты информации довольно дорогостоящи и используются в основном только специализированными подразделениями и фирмами.

После поисковых мероприятий и определения каналов утечки информации помещение оборудуют средствами пассивной и активной защиты. К пассивным относятся различные фильтры, специальные плёнки на окна, звукоизолирующие и экранирующие материалы. При невозможности или недостаточности пассивных мер применяются генераторы помех: в радиодиапазоне, виброакустические генераторы, постановщики ИК и оптических помех, генераторы шума по электросети и телефонным линиям, подавители сотовой связи, средств магнитной записи. Как правило, активные средства защиты быстро и легко устанавливаются в любое, даже неподготовленное помещение. А средства пассивной защиты требуют закладывать их еще на этапе проектирования и строительства.

В любом случае техническая защита информации – это деятельность, требующая принятия хорошо продуманных решений. Недостаточно просто купить и установить устройства, закрывающие, на ваш взгляд, все возможные каналы утечки. Прежде чем приступать к защитным мероприятиям следует произвести условное моделирование потенциального противника, сделать примерную оценку его технических, экономических и прочих возможностей. Это поможет выстроить оптимальную систему защиты и избежать ненужных материальных затрат. Безусловно, для грамотного проведения такой оценки, а также для определения существующих каналов утечки информации и подбора целесообразных средств защиты нужны специалисты, причем обладающие не только практическим опытом, но и необходимыми лицензиями на осуществление такой деятельности.