В большинстве индустриально развитых стран информация является первоосновой всех аспектов развития общества. Из-за этого значение информационной сферы в обеспечении безопасности жизнедеятельности общества все возрастает. Через нее реализуется значительная часть угроз не только национальной безопасности государства, но и экономическому благополучию учреждений и предприятий. Главная цель мер, предпринимаемых на уровне управления организацией, - сформировать программу работ в области информационной безопасности и обеспечить ее выполнение, выделяя необходимые ресурсы и постоянно контролируя состояние дел. Традиционно вопросы защиты информации в различных организациях решались посредством контроля физического доступа сотрудников к определенным информационным ресурсам (архивам, документам, хранилищам, компьютерам, принтерам, базам данных). С появлением информационных технологий и сетевых информационных систем такой подход стал невозможен, поскольку нельзя обеспечить физический контроль над каналами связи как внутри, так и особенно вне организации.

Промышленный шпионаж — форма недобросовестной конкуренции, при которой осуществляется незаконное получение, использование, разглашение информации, составляющей коммерческую, служебную или иную охраняемую законом тайну с целью получение преимуществ при осуществлении предпринимательской деятельности, а равно получения материальной выгоды.

Промышленный шпионаж остаётся, и будет оставаться мощным инструментом государственных разведок, предназначение которых — прямое нарушение законов иностранных государств в интересах и по поручению своей страны.

К средствам получения секретов относятся различные технические системы. Если у нас пока основными владельцами разведывательных технических средств являются специальные государственные органы (службы), то на Западе они находятся в пользовании и частных лиц. Это позволяет предпринимателям широко использовать средства электронной разведки в получении необходимой информации. Снятие ее с телефонных переговоров, ЭВМ, помещений, где ведутся секретные беседы, и т.д. Применение тех или иных средств зависит от информации, которую намеревается получить субъект. Один вид информации может быть похищен, другой прослушан, третий - сфотографирован или сделаны

зарисовки, четвертый записан на магнитофон, пятый - снят кинокамерой и т.д. Иногда используется комплекс специальных мер по её получению. В зависимости от вида получения информации принимаются соответствующие меры защиты.

Все приборы, предназначенные для поиска технических средств по принципу их действия, можно разделить на три больших класса:

- устройства поиска активного типа, то есть такие, которые сами воздействуют на объект и исследуют сигнал отклика. К приборам этого типа обычно относят: нелинейные локаторы; рентгенометры; магнитно-резонансные локаторы; акустические корректоры.
- устройства поиска пассивного типа. К ним относятся: металлоискатели; тепловизоры; устройства поиска по электромагнитному излучению; устройства поиска аномальных параметров телефонной линии; устройства поиска аномалий магнитного поля.
- комплексы, выполненные на основе высокочувствительных сканеров реализующие сразу несколько поисковых функций. Они в состоянии проводить круглосуточный автоматический мониторинг эфира, анализировать основные характеристики и направления пойманных сигналов, умея засечь не только излучение радиозакладки, но и работу ретрансляционных передатчиков.

В заключение можно сделать вывод, что тематики разработок на рынке промышленного шпионажа охватывают практически все стороны жизни общества, безусловно, ориентируясь на наиболее финансово-выгодные. Спектр предлагаемых услуг широк: от примитивных радиопередатчиков до современных аппаратно-промышленных комплексов ведения разведки. Конечно, у нас нет еще крупных фирм, производящих технику подобного рода, нет и такого разнообразия ее моделей, как на Западе, но техника отечественных производителей вполне может конкурировать с аналогичной западной, а иногда она лучше и дешевле. Естественно, речь идет о сравнении техники, которая имеется в открытой продаже. Аппаратура же, используемая спецслужбами (ее лучшие образцы), намного превосходит по своим возможностям технику, используемую коммерческими организациями.

Все это связано с достаточным риском ценности разного рода информации, разглашение которой может привести к серьезным потерям в различных областях (административной, научно-технической, коммерческой и т.д.).

Надежная защита информации в разрабатываемых и функционирующих системах обработки данных может быть эффективной, если она будет надежной на всех

объектах и во всех элементах системы, которые могут быть подвергнуты угрозам. В связи с этим для создания средств защиты важно определить природу угроз, формы и пути их возможного проявления и осуществления, перечень объектов и элементов, которые, с одной стороны, могут быть подвергнуты (косвенно или непосредственно) угрозам с целью нарушения защищенности информации, а с другой – могут быть достаточно четко локализованы для организации эффективной защиты информации.