Обикновено се приема, че при подозрение за рисково състояние на офис по отношение на изтичането на информация, то същото се отнася за автомобила и дома на управителя на фирмата или организацията. **Подслушвателни устройства** обикновено се поставят в автомобила, къщата на шефа и понякога в офиса.

Защитата от СРС може да бъде пасивна (състояща се в откриване и локализация на техническите средства), активна - чрез създаване на смущения, или комбинирана. Използват се следните похвати за откриване на подслушвателни устроиства:

- оглед на обекта (помещението);
- контрол на радиоизлъчванията на електронните прибори чрез индикатори на полета;
- контрол на радиоефира чрез специални широколентови радиоприемници;
- проверка на телефонните линии чрез специални прибори;
- проверка на отсъствието на сигнали по електрозахранващата мрежа 220 V.

Най-надеждната защита на речевата информация става чрез създаване на акустични шумове, чрез генератори на "бял шум". Най-перспективно е използването на генератори на "речеподобни" шумове.

Лицензираните частни фирми, които се занимават със защита от СРС (те извършват т.нар. TSCM услуги), не са много.

Защитата срещу "социалното инженерство" по същество е контраразузнавателна дейност на фирмените служби за сигурност. В нея влизат дейности като вербуване на секретни сътрудници на службата, събиране на оперативна информация и др.

Ако персоналният компютър се използва само от един човек, важно е да се предотврати несанкционираният достъп до него от други лица във времето, когато в него се намира защитавана информация и да се осигури защита на данните върху информационни носители от обир. В персоналния компютър изчислителни ресурси са оперативната памет, процесорът, вградените твърди или гъвкави магнитни дискове, клавиатурата, дисплеят, принтерът, периферните устройства. Защитата на оперативната памет и

процесора предполага контрол за появяването в оперативната памет на така наречените резидентни програми, защита на системните данни, изчистване на остатъци от секретна информация в неизползваемите области на паметта. Достатъчно е да се използва програма за тестване на оперативната памет, която да контролира състава на резидентните програми и тяхното разположение. Ако персоналният компютър се използва от група лица, то освен това може да възникне необходимост да се предотврати несанкционираният достъп на тези ползватели до информацията на другите лица от групата. Освен това във всички случаи трябва да се защити информацията от повреждане в резултат на грешки в програмата и оборудването и заразяване на компютъра с вируси. Провеждането обаче на защитни мероприятия е задължително за всички ползватели на компютъра без изключение и не се отнася непосредствено към проблема за защитата на информацията от конкурентите.

За осигуряване на защита на автономен компютър чрез пароли трябва да има:

а) парола за BIOS;

б) пароли за отделните файлове;

в) защитени с пароли архивни ZIP файлове.

Обаче, ако в първия случай крадец открадне целия компютър или само хард диска, достатъчно е да изключи батерията, която захранва CMOS паметта, за да игнорира паролата.

Прост и евтин метод за защита на потребителско ниво е унищожаване на файлове. Това става чрез програми за физическо изтриване на файловете от диска.

Добро правило е след използване на лазерен принтер за отпечатване на чувствителна информация, след последния отпечатан лист да се пуснат "за печат" един-два празни листа.