4.4. Оценка возможностей средств технической разведки осуществляется с использова нормативных документов ФСТЭК России.

4.5. Оценка возможности НСД к информации в средствах вычислительной техники и автоматизированных системах осуществляется с использованием следующих руководящих документов ФСТЭК России:

Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации;

Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации;

Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по технической защите конфиденциальной информации.

НСД к информации и специальные воздействия на нее реально возможны, если не выполняются требования перечисленных выше документов, дифференцированные в зависимости от степени конфиденциальности обрабатываемой информации, уровня полномочий пользователей по доступу к конфиденциальной информации и режимов обработки данных в автоматизированных системах.

5. Организационные и технические мероприятия по технической защите конфиденциальной информации

5.1. Разработка мер, и обеспечение защиты конфиденциальной информации осуществляются при проведении таких работ. Разработка мер защиты информации может осуществляться также сторонними предприятиями, имеющими соответствующие лицензии ФСТЭК России и ФСБ России на право осуществления соответствующих работ.

5.2. Для защиты конфиденциальной информации, используются сертифицированные по требованиям безопасности технические средства защиты.

5.3. Ответственность за обеспечение требований по технической защите конфиденциальной информации возлагается на руководителя.

5.5. Техническая защита информации в защищаемых помещениях.

К основным мероприятиям по технической защите конфиденциальной информации в ЗП относятся:

5.5.1. Определение перечня ЗП по результатам анализа циркулирующей в них конфиденциальной информации и условий ее обмена (обработки).

5.5.2. Назначение сотрудников, ответственных за выполнение требований по технической защите конфиденциальной информации. 5.5.3. Разработка частных инструкций по обеспечению безопасности информации в ЗП.

5.5.4. Обеспечение эффективного контроля за доступом.

5.5.5. Инструктирование сотрудников, работающих на ПЭВМ, других технических средств обработки информации, средств связи с соблюдением требований по технической защите конфиденциальной информации.

5.5.6. Проведение в ЗП обязательных визуальных проверок на наличие внедренных закладных устройств, в том числе осуществление контроля всех посторонних предметов, подарков, сувениров и прочих предметов, оставляемых в ЗП.

5.5.7. Исключение неконтролируемого доступа к линиям связи.

5.5.8. Осуществление сотрудниками, ответственными за безопасность информации, контроля за проведением всех монтажных и ремонтных работ в выделенных и смежных с ними помещениях, а также в коридорах.

5.5.9. Обеспечение требуемого уровня звукоизоляции входных дверей и окон.

5.5.10. Демонтирование или заземление (с обеих сторон) лишних (незадействованных) проводников и кабелей.

5.5.13. Техническая защита информации в средствах вычислительной техники (СВТ) от несанкционированного доступа должна обеспечиваться путем выполнения необходимых организационных мер защиты, установки сертифицированных программных и аппаратно-технических средств защиты информации от НСД, защиты каналов связи, предназначенных для передачи конфиденциальной информации, защиты информации от воздействия программ-закладок и компьютерных вирусов.

5.6. Организация и проведение работ по антивирусной защите информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, при ее обработке техническими средствами определяются настоящим документом, действующими государственными стандартами и другими нормативными и методическими документами.

Организации антивирусной защиты информации на объектах информатизации достигается путём:

установки и применения средств антивирусной защиты информации;

обновления баз данных средств антивирусной защиты информации;

действий должностных лиц при обнаружении заражения информационно-вычислительных ресурсов программными вирусами.

5.7.1. Организация работ по антивирусной защите информации возлагается на руководителя, а методическое руководство и контроль над эффективностью предусмотренных мер защиты информации на специалиста по обслуживанию вычислительной техники.

5.7.2. Защита информации от воздействия программных вирусов на объектах информатизации должна осуществляться посредством применения средств антивирусной защиты. Порядок применения средств антивирусной защиты устанавливается с учетом следующих требований:

обязательный входной контроль на отсутствие программных вирусов всех поступающих на объект информатизации носителей информации, информационных массивов, программных средств общего и специального назначения;

периодическая проверка пользователями жестких магнитных дисков (не реже одного раза в неделю) и обязательная проверка используемых в работе носителей информации перед началом работы с ними на отсутствие программных вирусов;

внеплановая проверка носителей информации на отсутствие программных вирусов в случае подозрения на наличие программного вируса;

восстановление работоспособности программных средств и информационных массивов в случае их повреждения программными вирусами.

5.7.3. К использованию допускается только лицензированные, сертифицированные антивирусные средства.

5.7.4. Порядок применения средств антивирусной защиты во всех случаях устанавливается с учетом следующих требований:

Входной антивирусный контроль всей поступающей на внешних носителях информации и программных средств любого назначения.

Входной антивирусный контроль всей информации поступающей с электронной почтой;

Входной антивирусный контроль всей поступающей информации из сети Internet;

Выходной антивирусный контроль всей исходящей информации на любых внешних носителях и/или передаваемой по локальной сети на другие рабочие станции/сервера, а так же передача информации посредством электронной почты;

Периодическая антивирусная проверка на отсутствие компьютерных вирусов на жестких дисках рабочих станций и серверов;

Обязательная антивирусная проверка используемых в работе внешних носителей информации;

Обеспечение получения обновлений антивирусных программ в автоматическом режиме, включая обновления вирусных баз и непосредственно новых версий программ;

Внеплановая антивирусная проверка внешних носителей и жестких дисков на отсутствие компьютерных вирусов в случае подозрения на наличие компьютерного вируса;

Восстановление работоспособности программных и аппаратных средств, а так же непосредственно информации в случае их повреждения компьютерными вирусами.