Тема 11. Мероприятия организации инженерно-технической защиты информации

Занятие 1. Организация защиты информации от утечки по техническим каналам на предприятии

Учебные вопросы:

- Введение
- Организация защиты информации от утечки по техническим каналам
- Этапы организации работ по защите информации от утечки по техническим каналам
- Заключение

Литература

- Хорев А. А. Организация защиты информации от утечки по техническим каналам. Журнал "Специальная Техника" №3 2006.
- Хорев А.А. Способы и средства защиты информации: Учеб. пособие. – М.: МО РФ, 2000.
- Бузов Г. А. и д.р. Защита от утечки информации по техническим каналам. М.: Горячая линия-Телеком, 2005.
- Халяпин Д.Б. Защита информации. Вас подслушивают? Защищайтесь. – М.: НОУ ШО Баярд, 2004.
- Торокин А.А. Основы инженерно-технической защиты информации. – М.: Гелиус, 2005.

Первый учебный вопрос: Организация защиты информации от утечки по техническим каналам

- Защита конфиденциальной информации от утечки по техническим каналам основана на выполнении комплекса организационных и технических мероприятий, составляющих систему технической защиты информации на защищаемом объекте (СТЗИ), и должна быть дифференцированной в зависимости от установленной категории объекта информатизации или защищаемого помещения, где: - организационные мероприятия по защите информации от утечки по техническим каналам основываются на учете ряда рекомендаций при выборе помещений для установки технических средств обработки конфиденциальной информации (ТСОИ) и ведения конфиденциальных переговоров, введении ограничений на используемые ТСОИ, вспомогательные технические средства и системы (ВТСС) и их размещение, а также введении определенного режима доступа сотрудников предприятия (организации, фирмы) на объекты информатизации и в выделенные помещения;

  - технические мероприятия по защите информации от утечки по техническим каналам основываются на применении технических средств защиты и реализации специальных проектных и конструкторских решений.

Основы организации технической защиты

Технические мероприятия по ЗИ от ТКУИ основываются на применении тех. средств защиты и реализации спец. проектных и конструкторских решений.

Техническая ЗИ осуществляется подразделениями по ЗИ (службами безопасности) или отдельными специалистами. Для разработки мер по ЗИ могут привлекаться сторонние организации, имеющие лицензии ФСТЭК или ФСБ России.

Для ЗИ рекомендуется использовать сертифицированные по требованиям безопасности информации технические средства защиты.

Перечень необходимых мер ЗИ определяется по результатам специального обследования объекта защиты, сертификационных испытаний и специальных исследований технических средств или каналов утечки.

Уровень технической ЗИ должен соответствовать соотношению затрат на организацию ЗИ и величины ущерба.

Защищаемые объекты должны быть аттестованы по требованиям безопасности информации в соответствии с нормативными документами ФСТЭК России на соответствие установленным нормам и требованиям по ЗИ (аттестат соответствия).

Ответственность за обеспечение требований по технической ЗИ возлагается на руководителей организаций, эксплуатирующих защищаемые объекты.

В целях своевременного выявления и предотвращения утечки информации по техническим каналам должен осуществляться контроль состояния и эффективности ЗИ.

Организация работ по ЗИ возлагается на руководителей подразделений, эксплуатирующих защищаемые объекты, а контроль за обеспечением ЗИ - на руководителей подразделений по защите информации (служб безопасности).

Установка технических средств обработки конфиденциальной информации, а также средств защиты информации должна выполняться в соответствии с техническим проектом или техническим решением.

Организационные документы создания СТЗИ

- Порядок организации на предприятии работ по созданию и эксплуатации объектов информатизации и защищаемых помещений определяется на предприятии в разрабатываемом «Руководстве по защите информации» или специальном «Положении о порядке организации и проведения на предприятии работ по ЗИ, которое определяет:
- порядок определения защищаемой информации;
- порядок привлечения подразделений предприятия, специалистов сторонних организаций к разработке и эксплуатации СЗИ объекта информатизации;
- порядок взаимодействия всех занятых сил;
- порядок разработки, ввода в действие и эксплуатации объекта информатизации;
- ответственность должностных лиц.

Второй учебный вопрос: Этапы организации работ по защите информации от утечки по техническим каналам

- Первый этап (подготовительный, предпроектный);
- Второй этап (проектирование СТЗИ);
- Третий этап (этап ввода в эксплуатацию защищаемого объекта и системы технической защиты информации).

Подготовительный этап создания системы технической защиты информации

На первом этапе проводится специальное обследование защищаемых объектов, разрабатывается аналитическое обоснование необходимости создания СТЗИ и техническое (частное техническое) задание на ее создание.

При проведении специального обследования защищаемых объектов для анализа возможных технических каналов утечки на объекте изучаются:

- план (в масштабе) прилегающей к зданию местности в радиусе до 150 - 300 м с указанием (по возможности) принадлежности зданий и границы КЗ;
- поэтажные планы здания с указанием всех помещений и характеристиками их стен, перекрытий, материалов отделки, типов дверей и окон;
- план-схема инженерных коммуникаций всего здания, включая систему вентиляции;
- план-схема системы заземления объекта с указанием места расположения заземлителя;
- план-схема системы электропитания здания с указанием места расположения разделительного трансформатора (подстанции), всех щитов и разводных коробок;
- план-схема прокладки телефонных линий связи с указанием мест расположения распределительных коробок и установки телефонных аппаратов;
- план-схема систем охранной и пожарной сигнализации с указанием мест установки и типов датчиков, а также распределительных коробок.

Аналитическое обоснование необходимости создания СТЗИ

- определяется перечень сведений, подлежащих защите;
- проводится категорирование сведений конфиденциального характера;
- определяется перечень лиц, допущенных до сведений конфиденциального характера, подлежащих защите;
- определяется степень участия персонала в обработке информации, характер их взаимодействия между собой и со службой безопасности;
- разрабатывается матрица допуска персонала к сведениям конфиденциального характера, подлежащих защите;
- определяется (уточняется) модель вероятного злоумышленника;
- проводятся классификация и категорирование объектов информатизации и защищаемых помещений;
- проводится обоснование необходимости привлечения специализированных организаций, имеющих необходимые лицензии для проектирования и внедрения СТЗИ;
- проводится оценка материальных, трудовых и финансовых затрат на разработку и внедрение СТЗИ;
- определяются ориентировочные сроки разработки и внедрения СТЗИ.

Категории важности информации (в зависимости от величины ущерба)

- **1 категория** – информация, утечка которой может привести к потере экономической или финансовой самостоятельности предприятия или потери ее репутации (потери доверия потребителей, смежников, поставщиков и т.п.);
- **2 категория** – информация, утечка которой может привести к существенному экономическому ущербу или снижению ее репутации;
- **3 категория** – информация, утечка разглашение которой может нанести экономический ущерб предприятию.

Категории важности информации (в зависимости от распространения информации

- **первая группа (1)** – конфиденциальная информация, которая циркулирует только на предприятии и не предназначенная для передачи другой стороне;
- **вторая группа (2)** – конфиденциальная информация, которая предполагается к передаче другой стороне или получаемая от другой стороны.

Уровни конфиденциальности информации

Величина ущерба (негативных последствий), который может быть нанесен при разглашении конкретной информации	Уровень конфиденциальности информации	
	информация, не подлежащая передаче другим предприятиям (организациям)	информация, предназначенная для передачи другим предприятиям (организациям) или полученная от них
Утечка информации может привести к потере экономической или финансовой самостоятельности предприятия или потери ее репутации	1.1	1.2
Утечка информации может привести к существенному экономическому ущербу или снижению репутации предприятия	2.1	2.2
Утечка информации может нанести экономический ущерб предприятию	3.1	3.2

Режимы доступа к сведениям, составляющим коммерческую тайну

- *Режим 1 – обеспечивает доступ ко всему перечню сведений конфиденциального характера. Устанавливается руководящему составу предприятия;*
- *Режим 2 – обеспечивает доступ к сведениям при выполнении конкретных видов деятельности (финансовая, производственная, кадры, безопасность и т.п.). Устанавливается для руководящего состава отделов и служб;*
- *Режим 3 – обеспечивает доступ к определенному перечню сведений при выполнении конкретных видов деятельности. Устанавливается для сотрудников - специалистов конкретного отдела (службы) в соответствии с должностными обязанностями.*

Классификация защищаемых объектов

Задача технической защиты информации	Установленный класс защиты
Полное скрытие информационных сигналов, которые возникают при обработке информации или ведении переговоров (скрытие факта обработки конфиденциальной информации на объекте)	А
Скрытие параметров информационных сигналов, которые возникают при обработке информации или ведении переговоров, по которым возможно восстановление конфиденциальной информации (скрытие информации, обрабатываемой на объекте)	Б

Категорирование защищаемых объектов информатизации и защищаемых помещений

- Категорирование защищаемых объектов информатизации и защищаемых помещений проводится комиссиями, назначенными руководителями предприятий, в ведении которых они находятся.
- В состав комиссий, включаются представители подразделений, ответственных за обеспечение безопасности информации, и представители подразделений, эксплуатирующих защищаемые объекты.

Порядок категоривания защищаемых объектов

- определяются объекты информатизации и защищаемые помещения, подлежащие защите
- определяется уровень конфиденциальности информации, обрабатываемой ТСПИ или обсуждаемой в выделенном помещении, и производится оценка стоимости ущерба, вследствие ее утечки;
- для каждого объекта защиты устанавливается класс защиты (А или Б) и определяются потенциальные ТКУИ и специальные технические средства, которые могут использоваться для перехвата информации;
- определяется рациональный состав средств защиты, а также разрабатываются организационные мероприятия по закрытию конкретного ТКУИ для каждого объекта защиты;
- для информации, отнесенной к конфиденциальной и предоставленной другой стороной, определяется достаточность мер, принятых по ее защите;
- проводится оценка стоимости мероприятий по закрытию конкретного ТКУИ для каждого объекта защиты;
- с учетом оценки возможностей вероятного злоумышленника по использованию для перехвата информации тех или иных технических средств разведки, а также с учетом стоимост закрытия каждого канала утечки информации и стоимости ущерба, который может быть нанесен предприятию вследствие ее утечки, определяется целесообразность закрытия тех или иных технических каналов утечки информации;
- после принятия решения о том, какие ТКУИ необходимо закрывать, устанавливается категория объекта информатизации или защищаемого помещения.

Результаты работы комиссии оформляются актом, который утверждается должностным лицом, назначившим комиссию.

Потенциальные ТКУИ, обрабатываемой ТСПИ

Технические каналы утечки информации	Специальные технические средства, используемые для перехвата информации
Электромагнитный	Средства поиска ПЭМИН, установленные в близлежащих строениях и транспортных средствах, находящихся за границей контролируемой зоны
Электрический	Средства поиска ПЭМИН, подключаемые к линиям электропитания ТСПИ, соединительным линиям ВТСС, посторонним проводникам, цепям заземления ТСПИ за пределами контролируемой зоны
Высокочастотное облучение ТСПИ	Аппаратура “высокочастотного облучения”, установленная в ближайших строениях или смежных помещениях, находящихся за пределами контролируемой зоны
Внедрение в ТСПИ электронных устройств перехвата информации	Аппаратные закладки модульного типа, устанавливаемые в системный блок или периферийные устройства в процессе сборки, эксплуатации и ремонта ПЭВМ: аппаратные закладки для перехвата изображений, выводимых на экран монитора, устанавливаемые в мониторы ПЭВМ; аппаратные закладки для перехвата информации, вводимой с клавиатуры ПЭВМ, устанавливаемые в клавиатуру; аппаратные закладки для перехвата информации, выводимой на печать, устанавливаемые в принтер; аппаратные закладки для перехвата информации, записываемой на жесткий диск ПЭВМ, устанавливаемые в системный блок. Аппаратные закладки, скрытно внедряемые в блоки, узлы, платы и отдельные элементы схем ПЭВМ на стадии их изготовления

Потенциальные технические каналы утечки речевой информации

Технические каналы утечки информации	Специальные технические средства, используемые для перехвата информации
Прямой акустический (через щели, окна, двери, технологические проемы, вентиляционные каналы и т. д.)	направленные микрофоны, установленные в близлежащих строениях и транспортных средствах, находящихся за границей контролируемой зоны; специальные высокочувствительные микрофоны, установленные в воздуховодах или в смежных помещениях, принадлежащих другим организациям; электронные устройства перехвата речевой информации с датчиками микрофонного типа, установленные в воздуховодах, при условии неконтролируемого доступа к ним посторонних лиц; прослушивание разговоров, ведущихся в выделенном помещении, без применения технических средств посторонними лицами (посетителями, техническим персоналом) при их нахождении в коридорах и смежных с выделенным помещениях (непреднамеренное прослушивание)
Акустовибрационный (через ограждающие конструкции, трубы инженерных коммуникаций и т.д.)	электронные стетоскопы, установленные в смежных помещениях, принадлежащих другим организациям; электронные устройства перехвата речевой информации с датчиками контактного типа, установленные на инженерно-технических коммуникациях (трубы водоснабжения, отопления, канализации, воздуховоды и т.п.) и внешних ограждающих конструкциях (стены, потолки, полы, двери, оконные рамы и т.п.) выделенного помещения, при условии неконтролируемого доступа к ним посторонних лиц

Потенциальные технические каналы утечки речевой информации

Акустооптический (через оконные стекла)	лазерные акустические локационные системы, установленные в близлежащих строениях и транспортных средствах, находящихся за границей контролируемой зоны
Акустоэлектрический (через соединительные линии ВТСС)	специальные низкочастотные усилители, подключаемые к соединительным линиям ВТСС, обладающим “микрофонным” эффектом, за пределами контролируемой зоны; аппаратура “высокочастотного навязывания”, подключаемая к соединительным линиям ВТСС, обладающим “микрофонным” эффектом, за пределами контролируемой зоны
Акустоэлектромагнитный (параметрический)	специальные радиоприемные устройства, установленные в близлежащих строениях и транспортных средствах, находящихся за границей контролируемой зоны, перехватывающие ПЭМИ на частотах работы высокочастотных генераторов, входящих в состав ВТСС, обладающих “микрофонным” эффектом; аппаратура “высокочастотного облучения”, установленная в ближайших строениях или смежных помещениях, находящихся за пределами контролируемой зоны

Категории объектов информатизации и защищаемых помещений

Задача технической защиты информации	Закрываемые технические каналы утечки информации	Установленная категория объекта защиты
Полное скрытие информационных сигналов, возникающих при обработке информации техническим средством или ведении переговоров (скрытие факта обработки конфиденциальной информации на объекте)	все потенциальные технические каналы утечки информации	1
Скрытие параметров информационных сигналов, возникающих при обработке информации техническим средством или ведении переговоров, по которым возможно восстановление конфиденциальной информации (скрытие информации, обрабатываемой на объекте)	все потенциальные технические каналы утечки информации	2
Скрытие параметров информационных сигналов, возникающих при обработке информации техническим средством или ведении переговоров, по которым возможно восстановление конфиденциальной информации (скрытие информации, обрабатываемой на объекте)	наиболее опасные технические каналы утечки информации	3

Содержание аналитического обоснования

- перечень сведений конфиденциального характера с указанием их уровня конфиденциальности;
- перечень сотрудников предприятия, допущенных до конфиденциальной информации, с указанием их режима доступа, а при необходимости и матрицы доступа;
- информационную характеристику и организационную структуру объектов защиты;
- перечень объектов информатизации, подлежащих защите, с указанием их категорий;
- перечень защищаемых помещений, подлежащих защите, с указанием их категорий;
- перечень и характеристику технических средств обработки конфиденциальной информации с указанием их места установки;
- перечень и характеристику ВТСС с указанием их места установки;
- предполагаемый уровень оснащения вероятного злоумышленника;
- ТКУИ, подлежащие закрытию (устранению);
- организационные мероприятия по закрытию технических каналов утечки информации;
- перечень и характеристику предлагаемых к использованию технических средств защиты информации с указанием их места установки;
- методы и порядок контроля эффективности защиты информации;
- обоснование необходимости привлечения специализированных организаций, имеющих необходимые лицензии на право проведения работ по защите информации, для проектирования;
- оценку материальных, трудовых и финансовых затрат на разработку и внедрение СТЗИ;
- ориентировочные сроки разработки и внедрения СТЗИ;
- перечень мероприятий по обеспечению конфиденциальности информации на стадии проектирования СТЗИ.

- Пояснительная записка подписывается руководителем группы (комиссии), проводившей аналитическое обоснование, согласовывается с руководителем службы безопасности и утверждается руководителем предприятия.

Техническое задание (ТЗ) на разработку СТЗИ

- общие положения;
- обоснование разработки;
- исходные данные объекта защиты в техническом, программном, информационном и организационном аспектах;
- ссылку на нормативно-методические документы, с учетом которых будет разрабатываться и приниматься в эксплуатацию СТЗИ;
- конкретные требования к СТЗИ;
- перечень предполагаемых к использованию технических средств защиты информации;
- состав, содержание и сроки проведения работ по этапам разработки и внедрения;
- перечень подрядных организаций - исполнителей различных видов работ;
- перечень предъявляемой заказчику научно-технической продукции и документации.

- Техническое задание на проектирование СТЗИ защищаемого объекта оформляется отдельным документом, согласовывается с проектной организацией, службой (специалистом) безопасности организации-заказчика в части достаточности мер по технической защите информации и утверждается заказчиком.

Технический проект СТЗИ

- титульный лист;
- пояснительную записку, содержащую информационную характеристику и организационную структуру объекта защиты, сведения об организационных и технических мероприятиях по ЗИ от утечки по ТКУИ;
- перечень ОИ, подлежащих защите, с указанием мест их расположения и установленной категории защиты;
- перечень защищаемых помещений, подлежащих защите, с указанием мест их расположения и установленной категории защиты;
- перечень устанавливаемых ТСПИ с указанием наличия сертификата и мест их установки;
- перечень устанавливаемых ВТСС с указанием наличия сертификата и мест их установки;
- перечень устанавливаемых ТСЗ информации с указанием наличия сертификата и мест их установки;
- схему (в масштабе) с указанием плана здания, в котором расположены защищаемые объекты, границ контролируемой зоны, трансформаторной подстанции, заземляющего устройства, трасс прокладки инженерных коммуникаций, линий электропитания, связи, пожарной и охранной сигнализации, мест установки разделительных устройств и т.п.;
- технологические поэтажные планы здания (в масштабе) с указанием мест расположения объектов информатизации и защищаемых помещений, характеристик их стен, перекрытий, материалов отделки, типов дверей и окон;
- планы объектов информатизации (в масштабе) с указанием мест установки ТСПИ, ВТСС и прокладки их соединительных линий, а также трасс прокладки инженерных коммуникаций и посторонних проводников;
- план-схему инженерных коммуникаций всего здания, включая систему вентиляции;
- план-схему системы заземления объекта, с указанием места расположения заземлителя;
- план-схему системы электропитания здания с указанием места расположения разделительного трансформатора (подстанции), всех щитов и разводных коробок;
- план-схему прокладки телефонных линий связи с указанием мест расположения распределительных коробок и установки телефонных аппаратов;
- план-схему систем охранной и пожарной сигнализации с указанием мест установки и типов датчиков, а также распределительных коробок;
- схемы систем активной защиты (если они предусмотрены техническими заданием на проектирование);
- инструкции и руководства по эксплуатации технических средств защиты для пользователей и ответственных за обеспечение безопасности информации на объекте информатизации.

Рекомендации для разработки технического проекта

- в защищаемых помещениях необходимо устанавливать сертифицированные ТСПИ и ВТСС;
- для размещения ТСПИ целесообразно выбирать подвальные и полуподвальные помещения (они обладают экранирующими свойствами);
- кабинеты руководителей организации, а также особо важные защищаемые помещения рекомендуется располагать на верхних этажах (за исключением последнего) со стороны, менее опасной с точки зрения ведения разведки;
- необходимо предусмотреть подвод всех коммуникаций (водоснабжение, отопление, канализация, телефония, электросеть и т.д.) к зданию в одном месте. Вводы коммуникаций в здание целесообразно сразу ввести в щитовое помещение и обеспечить закрытие его входа и установку сигнализации или охраны;
- в случае если разделительный трансформатор (трансформаторная подстанция), от которой осуществляется электропитание защищаемых технических средств и защищаемых помещений, расположен за пределами КЗ, необходимо предусмотреть отключение от низковольтных шин подстанции, от которых осуществляется питание защищаемых объектов, потребителей, находящихся за контролируемой зоной;
- электросиловые кабели рекомендуется прокладывать от общего силового щита по принципу вертикальной разводки на этажи с горизонтальной поэтажной разводкой и с установкой на каждом этаже своего силового щитка. Аналогичным образом должны прокладываться соединительные кабели вспомогательных технических средств, в том числе кабели систем связи;
- число вводов коммуникаций в зону защищаемых помещений должно быть минимальным и соответствовать числу коммуникаций. Незадействованные посторонние проводники, проходящие через защищаемые помещения, а также кабели (линии) незадействованных вспомогательных технических средств должны быть демонтированы;
- прокладка информационных цепей, а также цепей питания и заземления защищаемых технических средств должна планироваться таким образом, чтобы был исключен или уменьшен до допустимых пределов их параллельный пробег с различными посторонними проводниками, имеющими выход за пределы контролируемой зоны;
- для заземления технических средств (в том числе вспомогательных), установленных в выделенных помещениях, необходимо предусмотреть отдельный собственный контур заземления, расположенный в пределах контролируемой зоны. Если это невозможно, необходимо предусмотреть линейное зашумление системы заземления объекта;
- необходимо исключить выходы посторонних проводников (различных трубопроводов, воздухопроводов, металлоконструкций здания и т.п.), в которых присутствуют наведенные информативные сигналы, за пределы контролируемой зоны. Если это невозможно, необходимо предусмотреть линейное зашумление посторонних проводников;

Рекомендации (продолжение)

- прокладку трубопроводов и коммуникаций горизонтальной разводки рекомендуется осуществлять открытым способом или за фальшпанелями, допускающими их демонтаж и осмотр;
- в местах выхода трубопроводов технических коммуникаций за пределы выделенных помещений рекомендуется устанавливать гибкие виброизолирующие вставки с заполнением пространства между ними и строительной конструкцией раствором на всю толщину конструкции. В случае невозможности установки вставок потребуется оборудование трубопроводов системой вибрационного зашумления;
- необходимо предусматривать прокладку вертикальных стояков коммуникаций различного назначения вне пределов зоны выделенных помещений;
- ограждающие конструкции выделенных помещений, смежные с другими помещениями организации, не должны иметь проемы, ниши, а также сквозные каналы для прокладки коммуникаций;
- систему приточно-вытяжной вентиляции и воздухообмена зоны выделенных помещений целесообразно сделать отдельной, она не должна быть связана с системой вентиляции других помещений организации и иметь свой отдельный забор и выброс воздуха;
- короба системы вентиляции рекомендуется выполнять из неметаллических материалов. Внешняя поверхность коробов вентиляционной системы, выходящих из выделенной зоны или отдельных важных помещений, должна предусматривать их отделку звукопоглощающим материалом. В местах выхода коробов вентиляционных систем из выделенных помещений рекомендуется установить мягкие виброизолирующие вставки из гибкого материала, например брезента или плотной ткани. Выходы вентиляционных каналов за пределами зоны выделенных помещений должны быть закрыты металлической сеткой;
- в помещениях, оборудованных системой звукоусиления, целесообразно применять облицовку внутренних поверхностей ограждающих конструкций звукопоглощающими материалами;
- дверные проемы в особо важных помещениях необходимо оборудовать тамбурами;
- декоративные панели отопительных батарей должны быть съемными для осмотра;
- в особо важных выделенных помещениях не рекомендуется использование подвесных потолков, особенно неразборной конструкции;
- для остекления особо важных выделенных помещений рекомендуется применение солнцезащитных и теплозащитных стеклопакетов;
- полы особо важных выделенных помещений целесообразно делать без плинтусов;
- в выделенных помещениях не рекомендуется применять светильники люминесцентного освещения. Светильники с лампами накаливания следует выбирать на полное сетевое напряжение без применения трансформаторов и выпрямителей.

Рекомендации на этапе ввода в эксплуатацию системы технической защиты информации

- организацию охраны и физической защиты помещений объекта информатизации и защищаемых помещений, исключающих несанкционированный доступ к ТСПИ, их хищение и нарушение работоспособности, хищение носителей информации;
- при проведении реконструкции объекта должен быть организован контроль и учет лиц и транспортных средств, прибывших и покинувших территорию проводимых работ;
- рекомендуется организовать допуск строителей на территорию и в здание по временным пропускам или ежедневным спискам;
- копии строительных чертежей, особенно поэтажных планов помещений, схем линий электропитания, связи, систем охранной и пожарной сигнализации и т.п. должны быть учтены, а их число ограничено. По окончании монтажных работ копии чертежей, планов, схем и т.п. подлежат уничтожению установленным порядком;
- необходимо обеспечить хранение комплектующих и строительных материалов на складе под охраной;
- не рекомендуется допускать случаев проведения монтажных операций и отделочных работ, выполняемых одиночными рабочими, особенно в ночное время;
- на этапе отделочных работ необходимо обеспечить ночную охрану здания.

Мероприятиям по организации контроля ввода в эксплуатацию

- перед монтажом необходимо обеспечить скрытную проверку всех монтируемых конструкций, особенно установочного оборудования, на наличие разного рода меток и отличий их друг от друга, а также закладных устройств;
- необходимо организовать периодический осмотр зон выделенных помещений в вечернее или в нерабочее время при отсутствии в нем строителей в цельях выявления подозрительных участков и мест;
- организовать контроль за ходом всех видов строительных работ на территории и в здании. Основная функция контроля заключается в подтверждении правильности технологии строительно-монтажных работ и соответствия их техническому проекту;
- организовать осмотр мест и участков конструкций, которые по технологии подлежат закрытию другими конструкциями. Такой контроль может быть организован легально под легендой необходимости проверки качества монтажа и материалов или скрытно;
- необходимо тщательно проверять соответствие монтажных схем и количество прокладываемых проводов техническому проекту. Особое внимание необходимо уделять этапу ввода проводных коммуникаций и кабелей в зону выделенных помещений. Все прокладываемые резервные провода и кабели необходимо нанести на план-схему с указанием мест их начала и окончания.

Технический паспорт на объект защиты

- пояснительная записка, содержащая информационную характеристику и организационную структуру объекта защиты, сведения об организационных и технических мероприятиях по защите информации от утечки по техническим каналам;
- перечень объектов информатизации, подлежащих защите, с указанием мест их расположения и установленной категории защиты;
- перечень защищамых помещений, подлежащих защите, с указанием мест их расположения и установленной категории защиты;
- перечень устанавливаемых ТСПИ с указанием наличия сертификата (предписания на эксплуатацию) и мест их установки;
- перечень устанавливаемых ВТСС с указанием наличия сертификата и мест их установки;
- перечень устанавливаемых технических средств защиты информации с указанием наличия сертификата и мест их установки;
- схему (в масштабе) с указанием плана здания, в котором расположены защищаемые объекты, границ контролируемой зоны, трансформаторной подстанции, заземляющего устройства, трасс прокладки инженерных коммуникаций, линий электропитания, связи, пожарной и охранной сигнализации, мест установки разделительных устройств и т.п.;
- технологические поэтажные планы здания (в масштабе) с указанием мест расположения объектов информатизации и выделенных помещений, характеристик их стен, перекрытий, материалов отделки, типов дверей и окон;
- планы объектов информатизации (в масштабе) с указанием мест установки ТСПИ, ВТСС и прокладки их соединительных линий, а также трасс прокладки инженерных коммуникаций и посторонних проводников;
- план-схему инженерных коммуникаций всего здания, включая систему вентиляции;
- план-схему системы заземления объекта, с указанием места расположения заземлителя;
- план-схему системы электропитания здания с указанием места расположения разделительного трансформатора (подстанции), всех щитов и разводных коробок;
- план-схему прокладки телефонных линий связи с указанием мест расположения распределительных коробок и установки телефонных аппаратов;
- план-схему систем охранной и пожарной сигнализации с указанием мест установки и типов датчиков, а также распределительных коробок;
- схемы систем активной защиты (если они предусмотрены).