**Федеральное агентство связи**

**Ордена Трудового Красного Знамени**

**Федеральное государственное бюджетное образовательное учреждение высшего образования**

**«Московский технический университет связи и информатики»**

Кафедра «Математической кибернетики и информационных технологий»

**Отчет по лабораторной работе №5**

по дисциплине «Основы информационной безопасности» на тему:

«ОРГАНИЗАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ»

Вариант №10

Выполнили: студенты группы БВТ2001

Смирнов Денис, Игорь Разумов, Дмитрий Диденков и Вера Ильинская

Проверила:

Магомедова Д.И.

Москва

2021

**Оглавление**

[1 Цель работы 3](#_Toc56204906)

[2 Ход работы 3](#_Toc56204907)

[2.1 Постановка задачи 3](#_Toc56204908)

[3 Ответы на контрольные вопросы 4](#_Toc56204910)

[4 Вывод 12](#_Toc56204910)

**1 Цель работы**

Закрепление теоретических знаний в области правового обеспечения информационной безопасности. Тема: Изучение особенностей аттестации помещений по требованиям безопасности информации.

**2 Ход работы**

1. Изучить литературу и учебные материалы по теме (Конституция РФ, Доктрина информационной безопасности РФ и федеральные законы в области информационной безопасности, правовые режимы защиты информации).

2. Ответить на контрольные вопросы.

3. Оформить отчет, содержащий краткую информацию по контрольным вопросам.

4. Защитить практическую работу преподавателю (защита в виде опроса).

**2.1 Постановка задачи**

В нашем варианте нам требовалось изучить особенности аттестации помещений по требованиям безопасности информации, освоить связанную с этим материалом литературу и законодательную базу, а также оформить отчёт, содержащий краткую информацию по контрольным вопросам.

**Вариант 10**

**Тема:** Изучение особенностей аттестации помещений по требованиям безопасности информации.

**Вопрос 1.**

Аттестация объектов информатизации по требованиям безопасности информации – это комплекс организационно-технических мероприятий, в результате которых посредством специального документа - "Аттестата соответствия" подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных ФСТЭК России (Федеральная служба по техническому и экспортному контролю России).

**Вопрос 2.**

Виды аттестации помещений по требованиям безопасности

информации:

* Обязательная аттестация – процедура аттестации, которая должна быть проведена в обязательном порядке для определённого вида объектов информатизации.
* Добровольная аттестация - процедура аттестации, которая проводится в соответствии с установленными требованиями по защите информации по решению владельца объекта информатизации. В пример таких объектов можно привести:

1. Объекты информации, обрабатывающие коммерческую тайну;
2. Информационные системы персональных данных;
3. Прочие объекты информации, предназначенные для обработки информации ограниченного доступа.

**Вопрос 3.**

Обязательной аттестации подлежат помещения (объекты информации), которые:

1. Предназначены для обработки информации, содержащей сведения, составляющие государственную тайну;
2. Управляют экологически опасными объектами;
3. Предназначены для ведения секретных переговоров;
4. Обрабатывают служебную тайну;
5. Предназначены для ведения конфиденциальных переговоров;
6. Обрабатывают персональные данные.

**Вопрос 4.**

Порядок проведения аттестации помещений по требованиям

безопасности информации включает следующие действия:

1. Подача и рассмотрение заявки на аттестацию. Заявка имеет установленную форму, с которой можно ознакомиться в "Положении об аттестации объектов информатизации по требованиям безопасности". Заявитель направляет заявку в орган по аттестации, который в месячный срок рассматривает заявку, выбирает схему аттестации и согласовывает ее с заявителем.
2. Предварительное ознакомление с аттестуемым объектом - производится в случае недостаточности предоставленных заявителем данных до начала аттестационных испытаний;
3. Испытание в испытательных лабораториях несертифицированных средств и систем защиты информации, используемых на аттестуемом объекте.
4. Разработка и согласование программы и методики аттестационных испытаний. Этот шаг является результатом рассмотрения исходных данных и предварительного ознакомления с аттестуемым объектом. Орган по аттестации (отраслевые и региональные предприятия, учреждения и организации, специальные центры ФСТЭК России, аккредитованные ФСТЭК России и получившие от него лицензию на проведение аттестации объектов информатизации) определяет перечень работ и их продолжительность, методику испытаний, состав аттестационной комиссии, необходимость использования контрольной аппаратуры и тестовых средств или участия испытательных лабораторий. Программа аттестационных испытаний согласовывается с заявителем.
5. Заключение договоров на аттестацию. Результатом предыдущих четырех этапов становится заключение договора между заявителем и органом по аттестации, заключением договоров между органом по аттестации и привлекаемыми экспертами и оформлением предписания о допуске аттестационной комиссии к проведению аттестации.
6. Проведение аттестационных испытаний объекта информатизации. В ходе аттестационных испытаний выполняется следующее:

* Анализ организационной структуры объекта информатизации, информационных потоков, состава и структуры комплекса технических средств и программного обеспечения, системы защиты информации на объекте, разработанной документации и ее соответствия требованиям нормативной документации по защите информации;
* Определяется правильность категорирования объектов ЭВТ (электронно-вычислительная техника) и классификации при аттестации АС (автоматизированных систем), выбора и применения сертифицированных и несертифицированных средств и систем защиты информации;
* Проводятся испытания несертифицированных средств и систем защиты информации на аттестуемом объекте или анализ результатов их испытаний в испытательных центрах (лабораториях) по сертификации;
* Проверяется уровень подготовки кадров и распределение ответственности персонала за обеспечение выполнения требований по безопасности информации;
* Проводятся комплексные аттестационные испытания объекта информатизации в реальных условиях эксплуатации путем проверки фактического выполнения установленных требований на различных этапах технологического процесса обработки защищаемой информации;
* Оформляются протоколы испытаний и заключение по результатам аттестации с конкретными рекомендациями по устранению допущенных нарушений, приведению системы защиты объекта информатизации в соответствие с установленными требованиями и совершенствованию этой системы, а также рекомендациями по контролю за функционированием объекта информатизации.

К заключению прилагаются протоколы испытаний, подтверждающие полученные при испытаниях результаты и обосновывающие приведенный в заключении вывод. Заключение и протоколы испытаний подлежат утверждению органом по аттестации.

1. Оформление, регистрация и выдача "Аттестата соответствия" (если заключение по результатам аттестации утверждено). В случае же, если заявитель не согласен с отказом в выдаче "Аттестата соответствия", он может подать апелляцию. Апелляция рассматривается в срок, не превышающий один месяц с привлечением заинтересованных сторон.

**Вопрос 5.**

Для проведения испытаний заявитель представляет органу по аттестации следующие исходные данные и документацию:

* Приемо-сдаточную документацию на объект информатизации;
* Акты категорирования выделенных помещений и объектов информатизации;
* Инструкции по эксплуатации средств защиты информации;
* Технический паспорт на аттестуемый объект;
* Документы на эксплуатацию (сертификаты соответствия требованиям безопасности информации) ТСОИ (технического средства обработки информации)
* Сертификаты соответствия требованиям безопасности информации на ВТСС (вспомогательные технические средства и системы);
* Сертификаты соответствия требованиям безопасности информации на технические средства защиты информации;
* Акты на проведенные скрытые работы;
* Протоколы измерения звукоизоляции выделенных помещений и эффективности экранирования сооружений и кабин (если они проводились);
* Протоколы измерения величины сопротивления заземления;
* Протоколы измерения реального затухания информационных сигналов до мест возможного размещения средств разведки;
* Данные по уровню подготовки кадров, обеспечивающих защиту информации;
* Данные о техническом обеспечении средствами контроля эффективности защиты информации и их метрологической поверке;
* Нормативную и методическую документацию по защите информации и контролю эффективности защиты.

**Вопрос 6.**

Содержание заключения аттестационной проверки помещения:

* Состав аттестационной комиссии (группы);
* Дату проведения аттестации;
* Перечень руководящих документов, в соответствии с которыми проводилась аттестация;
* Перечень документов по защите информации в выделенном помещении, представленных аттестационной комиссии;
* Характеристику выделенного помещения (назначение, местоположение, условия размещения и т.д.);
* Перечень вспомогательных технических средств и систем (ВТСС), установленных на объекте информатизации;
* Перечень технических средств защиты информации, установленных в выделенном помещении;
* Характеристику организационных мероприятий по защите информации;
* Виды работ, проводимых в ходе аттестации;
* Перечень использованной в ходе инструментальной проверки (аттестационных испытаний) аппаратуры (перечисляется вся используемая аппаратура контроля по оцениваемым каналам и ее заводские номера);
* Результаты анализа документации по защите информации в выделенном помещении. Вывод о соответствии (несоответствии) разработанной документации по защите информации требованиям нормативно-методических документов ФСТЭК РФ;
* Оценку правильности категорирования выделенного помещения;
* Оценку уровня подготовки кадров и распределения ответственности за выполнение требований по защите информации;
* Результаты специального обследования выделенного помещения;
* Условия расположения выделенного помещения относительно границы контролируемой зоны, характеристику смежных с ним помещений, минимальное расстояние до границы контролируемой зоны;
* Характеристику вспомогательных технических средств и систем, соединительные линии которых выходят за пределы контролируемой зоны (наименование, тип, назначение и т.п.). Указывается длина соединительных линий от ВТСС до возможных мест подключения к ним средств перехвата информации, находящихся за пределами контролируемой зоны. Перечисляются технические средства защиты ВТСС с указанием их мест установки. При наличии сертификатов соответствия на средства защиты ВТСС указывается срок их действия. Вывод о соответствии (несоответствии) реального состава ВТСС, средств их защиты указанному в техническом паспорте на выделенное помещение и представленных исходных данных. Вывод о состоянии и сохранности печатей и пломб на ВТСС (в случае выявления перечисляются технические средства, подвергавшиеся несанкционированному вскрытию);
* Характеристику системы электропитания выделенного помещения (описывается схема электропитания выделенного помещения, указываются номера и места расположения трансформаторной подстанции, электрощитовой, распределительных щитов, от которых осуществляется розеточной и осветительной сетей электропитания выделенного помещения и их расположение относительно границы контролируемой зоны);
* Перечень инженерных коммуникаций, выходящих за пределы контролируемой зоны. Указывается их длина от выделенного помещения до мест возможного подключения средств перехвата информации, расположенных за пределами контролируемой зоны. Указывается наличие (отсутствие) специальных вставок в инженерных коммуникациях;
* Результаты акустовибрационных измерений:
* коэффициенты звукоизоляции ограждающих конструкций (окон, дверей, стен, пола, потолка) выделенного помещения в октавных полосах частот и словесная разборчивость речи W в местах возможного подключения средств перехвата информации с датчиками микрофонного типа;
* коэффициенты виброизоляции ограждающих конструкций выделенного помещения, а также различных элементов инженерно-технических систем, включая их коммуникации, в октавных полосах частот и словесная разборчивость речи W в местах в местах возможного подключения средств перехвата информации с датчиками контактного типа;
* вывод о соответствии (несоответствии) эффективности защиты выделенного помещения от утечки информации по прямым акустическим, акустовибрационным и акустооптическим каналам требованиям нормативно-методических документов ФСТЭК РФ;
* Результаты проведения испытаний системы виброакустической маскировки (СВАМ) выделенного помещения (при ее использовании):
* словесная разборчивость речи W в местах возможного подключения средств перехвата информации с датчиками микрофонного типа;
* словесная разборчивость речи W в местах в местах возможного подключения средств перехвата информации с датчиками контактного типа;
* вывод о соответствии (несоответствии) эффективности защиты выделенного помещения от утечки информации по прямым акустическим, акустовибрационным и акустооптическим каналам при использовании СВАМ требованиям нормативно-методических документов ФСТЭК РФ;
* измеряемые уровни информационных сигналов на выходе ВТСС, возникающих вследствие акустоэлектрического преобразования акустических сигналов элементами ВТСС, в октавных полосах частот со среднегеометрическими частотами 250, 500, 1000, 2000, 4000 Гц;
* Результаты акустоэлектрических измерений:
* словесная разборчивость речи W в соединительных линиях ВТСС, имеющих в своем составе элементы, обладающие микрофонным эффектом;
* проведения испытаний средств защиты ВТСС;
* вывод о соответствии (несоответствии) эффективности защиты ВТСС от утечки информации по акустоэлектрическим каналам требованиям нормативно-методических документов ФСТЭК РФ;
* Недостатки, выявленные в ходе аттестации;
* Общий вывод о соответствии (несоответствии) эффективности защиты выделенного помещения требованиям нормативно-методических документов ФСТЭК РФ, о возможности (невозможности) выдачи «Аттеста­та соответствия» и разрешения ведения переговоров соответствующего уровня конфиденциальности (секретности).

В случае если эффективность защиты объекта информатизации или выделенного помещения не соответствует требованиям нормативно-методических документов ФСТЭК РФ, то формулируются предложения по устранению выявленных в ходе аттестации нарушений, сроки и условия представления для повторной аттестации объекта информатизации или выделенного помещения.

**Вопрос 7.**

Содержание протокола аттестационных испытаний помещения:

* Вид испытаний;
* Объект испытаний;
* Дату и время проведения испытаний;
* Место проведения испытаний;
* Перечень использованной в ходе испытаний аппаратуры (наименование, тип, заводской номер, номер свидетельства о поверке и срок его действия);
* Перечень нормативно-методических документов, в соответствии с которыми проводились испытания;
* Методику проведения испытания (краткое описание);
* Результаты измерений;
* Результаты расчетов;
* Выводы по результатам испытаний.

**Вопрос 8.**

Содержание аттестата соответствия на объект информатизации:

* Регистрационный номер;
* Дату выдачи;
* Срок действия;
* Наименование, адрес и местоположение объекта информатизации (выделенного помещения);
* Категорию объекта информатизации (выделенного помещения);
* Класс защищенности автоматизированной системы;
* Разрешенный гриф конфиденциальности (секретности) информации, обрабатываемой на объекте информатизации (обсуждаемой в выделенном помещении);
* Организационную структуру объекта информатизации и вывод об уровне подготовки специалистов по защите информации;
* Номера и даты утверждения программы и методики, в соответствии с которыми проводились аттестационные испытания;
* Перечень руководящих документов, в соответствии с которыми проводилась аттестация;
* Номер и дата утверждения заключения по результатам аттестационных испытаний;
* Состав комплекса технических средств обработки информации ограниченного доступа (с указанием категории, заводских номеров, модели, изготовителя, номеров сертификатов соответствия и мест установки), перечень вспомогательных технических средств и систем (с указанием заводских номеров, модели, изготовителя, номеров сертификатов соответствия и мест установки), перечень технических средств защиты информации (с указанием заводских номеров, модели, изготовителя, номеров сертификатов соответствия и мест установки), а также схемы их размещения в помещениях и относительно границ контролируемой зоны, перечень используемых программных средств;
* Организационные мероприятия, при проведении которых разрешается обработка информации ограниченного доступа;
* Перечень действий, которые запрещаются при эксплуатации объекта информатизации (выделенного помещения);
* Список лиц, на которых возлагается обеспечение требований по защите информации и контроль за эффективностью реализованных мер и средств защиты информации.

**4. Вывод**

В результате проделанной работы нам удалось изучить литературу и учебные материалы по теме (Конституция РФ, Доктрина информационной безопасности РФ и федеральные законы в области информационной безопасности, правовые режимы защиты информации), а также другую связанную с этим законодательную базу, что позволило нам освоить особенности аттестации помещений по требованиям безопасности информации.