**МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ,
СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»
(СПбГУТ)**

Санкт-Петербургский колледж телекоммуникаций им. Э.Т. Кренкеля

УТВЕРЖДАЮ
Заместитель директора
по учебной работе
_____ Н.В. Калинина
17 марта 2022 г

СПбГУТ))) Документ подписан простой электронной подписью

Сертификат: 008a56eb36a1808f06
Владелец: Машков Георгий Михайлович
Действителен с 07.05.2022 по 06.05.2027

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ПРАКТИЧЕСКИХ РАБОТ

по учебной дисциплине
ОП.04. ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

по специальности
10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

среднего профессионального образования

Санкт-Петербург
2022

ОП.04. Основы информационной безопасности. Методические указания по выполнению практических работ.

Составил: Кривоносова Н.В. – Санкт-Петербург, 2022.

Методические указания содержат описания практических занятий, предусмотренных рабочей программой Основы информационной безопасности. Каждая работа рассчитана на 2 академических часа, общий объём составляет 18 часов. Методические указания предназначены для обучающихся очной формы обучения по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем.

Рассмотрено и одобрено предметной (цикловой) комиссией информационной безопасности телекоммуникационных систем Санкт-Петербургского колледжа телекоммуникаций им. Э.Т. Кренкеля.

СОДЕРЖАНИЕ

Практическое занятие 1.

РАБОТА С ДОКУМЕНТАМИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РФ ПО ОПРЕДЕЛЕНИЮ ОБЪЕКТОВ ЗАЩИТЫ И КЛАССИФИКАЦИИ ТАЙН

1. Цель работы: изучить правовые основы российского законодательства в сфере информационной безопасности.

2. Задачи работы:

– изучить нормативно-правовые документы

Студент должен:

Уметь:

- классифицировать защищаемую информацию по видам тайны и степеням секретности;
- классифицировать основные угрозы безопасности информации.

Знать:

- сущность и понятие информационной безопасности, характеристику ее составляющих;
- место информационной безопасности в системе национальной безопасности страны;
- виды, источники и носители защищаемой информации;

ПК:

- ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно – телекоммуникационных систем и сетей.

3. Подготовка к работе

Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1.

Подготовить бланк отчета.

4. Задание

Изучить основные правовые документы об информационной безопасности, составить словарь основных терминов.

5. Порядок выполнения работы

Изучить следующие нормативно-правовые документы (список не является окончательным):

• Конституция Российской Федерации

• Доктрина информационной безопасности (2016)стратегия национальной безопасности Российской Федерации (2015)

• Федеральные законы:

- о 390-ФЗ О безопасности (2010)
- о 5485-1 О государственной тайне (1993)
- о 149-ФЗ Об информации, информационных технологиях и о защите информации (2006)
- о 152-ФЗ О персональных данных (2006)
- о 184-ФЗ О техническом регулировании (2002)
- о 98-ФЗ О коммерческой тайне (2004)
- о 63-ФЗ Об электронной подписи (2011)

Выделить понятия, относящиеся к сфере информационной безопасности, составить словарь важных терминов.

6. Содержание отчета

1. название и цель работы;
2. перечень осваиваемых компетенций;
3. задание;
4. ход выполнения работ;
5. выводы по работе;

6. ответы на контрольные вопросы.

7. Контрольные вопросы к защите

1. Что называют правовыми основами обеспечения информационной безопасности в России?.
2. Сколько статей в разделе «Преступления в сфере компьютерной информации» уголовного кодекса РФ?
3. Какой документ определяет на международном уровне пределы вмешательства в частную жизнь со стороны государства и других субъектов?.

Приложение 1

Краткие сведения из теории

Правовыми основами обеспечения информационной безопасности в России называют некоторые правовые документы, содержащие базовые понятия сферы безопасности. В данной иерархии важнейшим документом является Конституция Российской Федерации. Так как все нормативно-правовые документы должны подчиняться ей, как основному закону Российской Федерации. Также во внимания принимаются общепризнанные принципы и нормы международного права, международные договоры Российской Федерации, федеральные конституционные законы, федеральные законы, а также нормативные правовые акты Президента Российской Федерации и Правительства Российской Федерации.

Приложение 2

Самостоятельная работа к практическому занятию

«Работа с документами в области информационной безопасности РФ по определению объектов защиты и классификации тайн»

Самостоятельная работа по теме занятия включает в себя:

- изучение теоретического материала лекционных занятий, учебной литературы, Интернет-ресурсов, раздела «Краткие сведения из теории» настоящего описания ПЗ;
- выполнение практических заданий.

Практическое занятие 2. ОПРЕДЕЛЕНИЕ ОБЪЕКТОВ ЗАЩИТЫ НА ТИПОВОМ ОБЪЕКТЕ ИНФОРМАТИЗАЦИИ

1. **Цель работы**: научиться определять объекты защиты на типовом объекте информатизации
2. **Задачи работы:**

– изучить примеры должностных инструкций;
– изучить руководящие документы Гостехкомиссии РФ№
– изучить классификацию информации ограниченного доступа;
– для своего варианта задания по аналогии с примером:
– определить назначение и структуру объекта информатизации;
– перечислить физические лица, имеющие доступ к ресурсам и (или) в помещения, в которых располагаются ТС ИС;
– перечислить компоненты ИС;
– перечислить информацию, обрабатываемую ИС;
– сделать выводы по определению объектов защиты.

Студент должен:
Уметь:

- классифицировать защищаемую информацию по видам тайны и степеням секретности;
- классифицировать основные угрозы безопасности информации.

Знать:

- сущность и понятие информационной безопасности, характеристику ее составляющих;
- место информационной безопасности в системе национальной безопасности страны;
- виды, источники и носители защищаемой информации;

ПК:

- ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно – телекоммуникационных систем и сетей.

3. **Подготовка к работе**

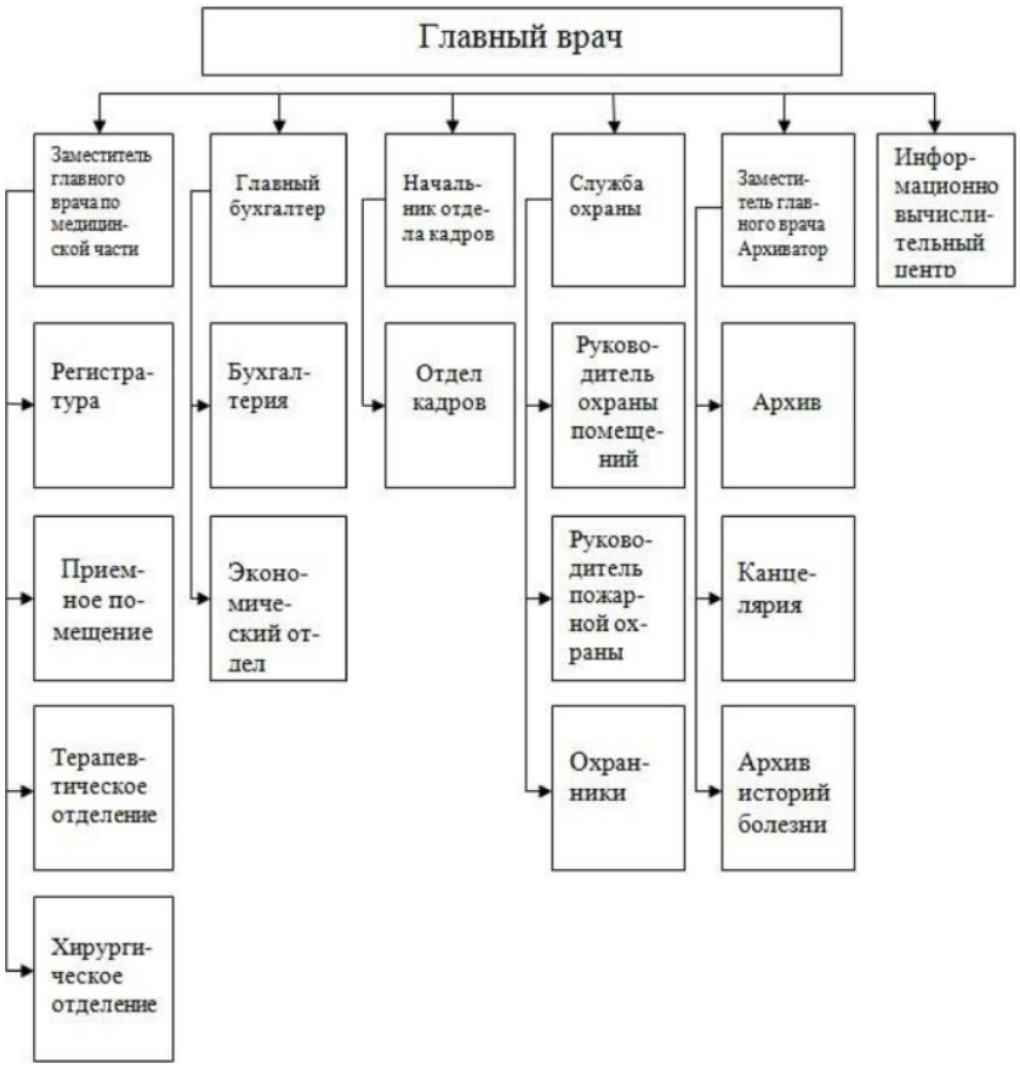
Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1.
Подготовить бланк отчета.

4. **Задание**

Задание 1. Построение структуры подразделений объекта защиты, характеристика назначения объекта и решаемых задач. Определение функционально-отраслевой принадлежности объекта.

Структура подразделений объекта может быть представлена в виде схемы или таблицы. Под организационной структурой предприятия понимаются состав, соподчиненность, взаимодействие и распределение работ по подразделениям и органам управления, между которыми устанавливаются определенные отношения по поводу реализации властных полномочий, потоков команд и информации. Организационная структура объекта построена по линейно-функциональному признаку.

В качестве примера рассмотрим объект информатизации больница. Руководителем является главный врач. В подчинении у главного врача находятся заместитель по медицинской части, заместитель по экономическим вопросам, главный бухгалтер, начальник отдела кадров, заместитель главного врача архиватор и информационно вычислительный центр и служба охраны, включающая в себя руководителя охраны помещений, руководителя пожарной охраны и штат охранников. Главный врач контролирует работу управлений, которым подчинены различные отделы. Каждый отдел подчиняется начальнику отдела. Организационная структура объекта показана на рисунке.



Далее необходимо перечислить решаемые задачи и направления деятельности, осуществляемой на объекте. Привести описание ведущихся на объекте работ, дать характеристику операций, выполняемых на объекте и условий их выполнения. Сформулировать назначение объекта.

Определение функционально-отраслевой принадлежности объекта. По назначению все объекты информатизации делятся на:

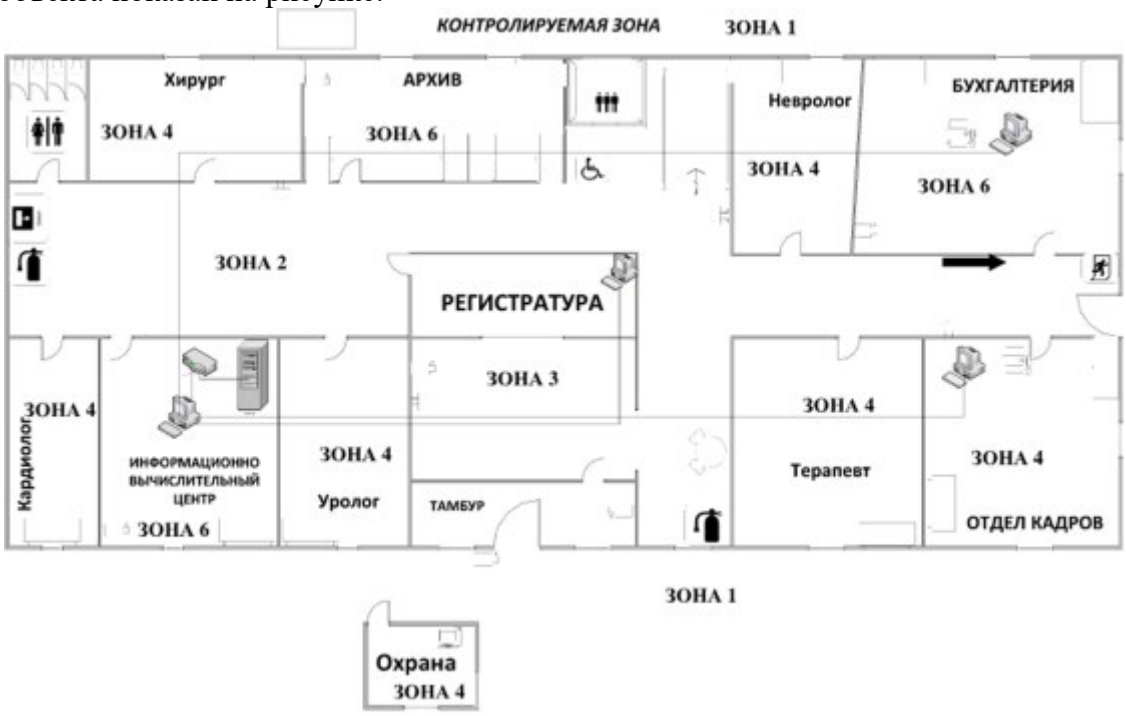
- - производственные;
- - строительные;
- - транспортные;
- - топливно-энергетического комплекса;
- - оборонно-промышленного комплекса;
- - социального назначения;
- - культурного назначения.

Определить к какому типу относится заданный объект. Определить виды и масштабы возможного ущерба в результате нарушения безопасности. Определить категорию заданного объекта по уровню важности в соответствии с ГОСТ Р 50776-95 (МЭК 60839-1-4:1989)

Задание 2. Построение плана объекта

Построение плана объекта. Определение защищаемых зон на плане. Построить план объекта, с помощью принятых стандартом условных обозначений показать все объекты защиты.

Определить категории защищаемых зон. Определить структуру контролируемых зон. Пример плана объекта показан на рисунке:



На данном объекте показаны несколько зон системы безопасности, которые имеют структуру вложенных зон. В целях физической защиты объектов на базе построения зоны безопасности предприятия имеется система доступа и управления, которая также позволяет минимизировать возможность возникновения угроз. Многозональность обеспечивает дифференцированный санкционированный доступ различных категорий сотрудников и посетителей к различным составляющим объекта путем разделения его пространства на контролируемые зоны.

Определить категории контролируемых зон, заполнить таблицу по данным исследуемого объекта защиты:

Категория	Наименование зоны	Функциональное назначение зоны объекта	Условия доступа сотрудников	Условия доступа посетителей	Наличие охраны
I	Свободная	Заполнить по данному объекту	Свободный	Свободный	Есть
II	Наблюдаемая	Заполнить	Свободный	Свободный	Есть
Ш	Регистрационная	Заполнить	Свободный	Свободный с регистрацией по удостоверениям личности	Есть
IV	Режимная	Заполнить	По служебн. удостоверениям или	По разовым пропускам	Усиленная охрана

			идентификаци онным картам		
V	Усиленной защиты	Заполнить	По спецдоку-ментам	По спецпро-пускам	Усиленная охрана
VI	Высшей защиты	Заполнить	По спецдоку-ментам	По спецпро-пускам	Усиленная охрана

5. Содержание отчета

1. название и цель работы;
2. перечень осваиваемых компетенций;
3. задание;
4. исходные данные по заданию/варианту;
5. ход выполнения работ;
6. выводы по работе;
7. ответы на контрольные вопросы.

6. Контрольные вопросы к защите

1. Что такое уязвимость и угроза ИБ?
2. Что такое риск информационной безопасности, для чего оценивать риски?
3. Что такое объект защиты информации? Приведите примеры.

Приложение 1

Краткие сведения из теории

Защита информации должна быть системной, включающей в себя различные взаимосвязанные компоненты. Важнейшим из этих компонентов являются объекты защиты, ибо от их состава зависят и методы, и средства защиты и состав мероприятий.

Объект защиты информации - информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с поставленной целью защиты информации.

В соответствии с данным определением можно классифицировать объекты защиты в соответствии с рисунком 1

В качестве объекта защиты часто рассматривается объект информатизации. Объект информатизации - совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров. ФСТЭК в своих руководящих документах трактует данное понятие несколько иначе.

Под объектами информатизации, аттестуемыми по требованиям безопасности информации, понимаются автоматизированные системы различного уровня и назначения, системы связи, отображения и размножения вместе с помещениями, в которых они установлены, предназначенные для обработки и передачи информации, подлежащей защите, а также сами помещения, предназначенные для ведения конфиденциальных переговоров.

В отношении любого объекта информатизации справедливы следующие утверждения:

1. Объект информатизации создан ради осуществления какой-то деятельности - основной деятельности.
2. Информационные технологии на объекте информатизации служат для реализации целей основной деятельности.
3. Состояние объекта информатизации динамически меняется под влиянием внешних и внутренних факторов.

Защищаемыми объектами информатизации в соответствии с СТР-К (Специальные требования и рекомендации по технической защите конфиденциальной информации, утвержденные приказом Гостехкомиссии России от 30.08.2002 № 282) являются:

- средства и системы информатизации (средства вычислительной техники,

автоматизированные системы различного уровня и назначения на базе средств вычислительной техники, в том числе информационно-вычислительные комплексы, сети и системы, средства и системы связи и передачи данных, технические средства приема, передачи и обработки информации (телефонии, звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение), используемые для обработки конфиденциальной информации (Основные технические средства и системы - ОТСС);

- технические средства и системы, не обрабатывающие непосредственно конфиденциальную информацию, но размещенные в помещениях, где она обрабатывается/циркулирует (вспомогательные технические средства - ВТСС);
- защищаемые помещения.

Приложение 2

Самостоятельная работа к практическому занятию

«Определение объектов защиты на типовом объекте информатизации»

Самостоятельная работа по теме занятия включает в себя:

- изучение теоретического материала лекционных занятий, учебной литературы, Интернет-ресурсов, раздела «Краткие сведения из теории» настоящего описания ПЗ;
- выполнение практических заданий.

Практические задания для самостоятельного выполнения:

- В соответствии с вариантом определите для вашей организации 5 наиболее важных объектов защиты, свой выбор обоснуйте.
- Для каждого объекта защиты определите ценность (от 1 до 5), обоснуйте ваш выбор.
- Для каждого объекта защиты подберите по 1 возможной уязвимости.
- Для каждой уязвимости подберите по возможной угрозе.
- Проанализировав всё уязвимости и угрозы дайте оценку риска каждой угрозы (низкий, средний, высокий). Ответ обоснуйте.

  Варианты:

  1. Отделение коммерческого банка
  2. Поликлиника
  3. Колледж
  4. Офис страховой компании
  5. Рекрутинговое агентство
  6. Интернет-магазин
  7. Центр оказания государственных услуг
  8. Отделение полиции
  9. Аудиторская компания
  10. Дизайнерская фирма
  11. Офис Интернет-провайдера
  12. Офис адвоката
  13. Компания по разработке ПО для сторонних организаций
  14. Агентство недвижимости
  15. Туристическое агентство
  16. Офис благотворительного фонда
  17. Издательство
  18. Консалтинговая фирма
  19. Рекламное агентство
  20. Отделение налоговой службы
  21. Офис нотариуса
  22. Бюро перевода (документов)
  23. Научно проектное предприятие
  24. Брачное агентство
  25. Редакция газеты
  26. Гостиница
  27. Праздничное агентство
  28. Городской архив
  29. Диспетчерская служба такси
  30. Железнодорожная касса

Вопросы для самопроверки самостоятельной работы и вопросы для защиты ПЗ

- Что такое объект информатизации, приведите примеры?
- Что такое источник угрозы, приведите примеры.

Практическое занятие 3. КЛАССИФИКАЦИЯ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ ПО ВИДАМ ТАЙНЫ И СТЕПЕНЯМ КОНФИДЕНЦИАЛЬНОСТИ

1. **Цель работы**: научиться классифицировать защищаемую информацию по конфиденциальности

2. **Задачи работы:**
- определить категории лиц, имеющих доступ к защищаемой информации и ресурсам;
- классифицировать защищаемую информацию по конфиденциальности

Студент должен:
Уметь:
- классифицировать основные угрозы безопасности информации.

Знать:
- сущность и понятие информационной безопасности, характеристику ее составляющих;
- место информационной безопасности в системе национальной безопасности страны;
- виды, источники и носители защищаемой информации;

ПК:
- ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно – телекоммуникационных систем и сетей.

3. **Подготовка к работе**
Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1.
Подготовить бланк отчета.

3. Задание

Используя документы «Должностные инструкции», определить наличие информации с ограниченным доступом для каждой должности. Определить конфиденциальность информации и принадлежность её к определенному виду тайны. Результаты исследований поместить в таблицу:

Должность	Документ	Реквизиты документов	Конфиденциальная информация. Вид тайны.	Закон, на основании которого у информации статус конфиденциальной
Начальник отдела кадров	Анкета По должностной инструкции	Фамилия Имя Отчество	Персональные данные Коммерческая тайна	Ст11ФЗ «Об информации, информатизации и защите информации»

7. Содержание отчета
1. название и цель работы;
2. перечень осваиваемых компетенций;
3. задание;
4. исходные данные по заданию/варианту;
5. ход выполнения работ;
6. выводы по работе;
7. ответы на контрольные вопросы.

8. Контрольные вопросы к защите

1. Понятие угрозы безопасности информации.
2. Системная классификация угроз безопасности информации.
3. Каналы несанкционированного доступа к информации.

Приложение 1

Краткие сведения из теории

Обрабатываемая в ИС информация включает в себя:

- открытую (общедоступную) информацию;
- информацию ограниченного доступа (персональные данные).

Персональные данные, обрабатываемые в типовой ИС, могут включать в себя:

- персональные данные сотрудников:

1. биографические данные;
2. опознавательные данные;
3. личные характеристики;
4. сведения о семейном положении;
5. сведения о финансовом положении;
6. сведения об образовании;
7. сведения о профессиональных навыках;
8. сведения о состоянии здоровья;

- персональные данные иных субъектов, в том числе:

1. информация о гражданах (персональные данные);
2. персональные данные о гражданах в их заявлениях и жалобах;
3. сведения, содержащиеся в записях актов гражданского состояния;
4. сведения о населении, содержащиеся в переписных листах;
5. иные персональные данные.

Таким образом, в типовых ИС обрабатываются персональные данные следующих категорий:

- *категория 1* - персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;
- *категория 2* - персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1;

категория 3 - персональные данные, позволяющие идентифицировать субъекта персональных данных.

Информация составляет СЛУЖЕБНУЮ или КОММЕРЧЕСКУЮ ТАЙНУ в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании, и обладатель информации принимает меры к охране ее конфиденциальности. Сведения, которые не могу составлять СЛУЖЕБНУЮ или КОММЕРЧЕСКУЮ ТАЙНУ, определяются законом и иными правовыми актами.

Коммерческая тайна - управленческая, производственная, научно-техническая, финансовая, экономическая, торговая и иная документированная информация, используемая для достижения целей предпринимательской деятельности (получение прибыли, предотвращение ущерба и упущенной выгоды, получение добросовестного преимущества над конкурентами), которую предприниматель относит к конфиденциальной.

Конфиденциальная информация - документированная информация, правовой режим которой установлен специальными нормами действующего законодательства в области государственной, коммерческой, промышленной и другой общественной деятельности.

Указом Президента Российской Федерации от 6 марта 1997 года № 188 утвержден перечень сведений конфиденциального характера:

1. Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.

2. Сведения, составляющие тайну следствия и судопроизводства.

3. Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна).

4. Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее).

5. Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна).

6. Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

Предварительный Перечень сведений, составляющих служебную или коммерческую тайну, формируется под руководством начальников структурных подразделений организации в соответствии с указаниями начальника службы безопасности (заместителя по режиму) и Положением о порядке и методических указаниях по его формированию.

При разработке предварительного Перечня в структурных подразделениях должны руководствоваться:

• Конституцией Российской Федерации, принятой 12 декабря 1993 года;

• Законом Российской Федерации «О государственной тайне» № 5485-1 от 21.07.93;

• Федеральным законом Российской Федерации «Об информации, информатизации и защите информации» № 24-ФЗ от 20.02.95;

• Указом Президента Российской Федерации «Об утверждении Перечня сведений, отнесенных к государственной тайне» № 1203 от 30.11.95;

• Указом Президента Российской Федерации «Об утверждении Перечня сведений конфиденциального характера» № 188 от 06.03.97;

• Постановлением Правительства Российской Федерации «О Перечне сведений, которые не могут составлять коммерческую тайну» № 35 от 05.12.91;

• анализом характера возможного ущерба в случае несанкционированного распространения сведений конфиденциального характера;

• анализом преимуществ и недостатков для работы с открытым и закрытым (внутренним) применением таких сведений.

Примерный перечень сведений, составляющих служебную или коммерческую тайну организации:

Сведения о структуре и масштабах производства, производственных мощностях, типе и размещении оборудования, запасах сырья, материалов, комплектующих и готовой продукции.

Сведения о применяемых оригинальных методах управления организацией. Сведения о подготовке, принятии и исполнении отдельных решений руководства организации по коммерческим, организационным, научно-техническим и иным вопросам.

Сведения о планах расширения или свертывания производства различных видов продукции и их технико-экономических обоснованиях. Также сведения о планах инвестиций, закупок и продаж.

Сведения о фактах проведения, целях, предмете и результатах совещаний и заседаний органов управления организации.

Сведения о кругообороте средств организации, финансовых операциях, состоянии банковских счетов организации и проводимых операциях, об уровне доходов организации, о состоянии кредита организации (пассивы и активы). Главная книга организации.

Сведения о применяемых организацией оригинальных методах изучения рынка (маркетинга). Сведения о результатах изучения рынка, содержащие оценки состояния и перспектив развития рыночной коньюктуры. Сведения о рыночной стратегии организации, о

применяемых организацией оригинальных методах осуществления продаж, об эффективности служебной или коммерческой деятельности организации.

Обобщенные сведения о внутренних и зарубежных заказчиках, подрядчиках, поставщиках, потребителях, покупателях, компаньонах, спонсорах, посредниках, клиентах и других партнерах, состоящих в деловых отношениях с организацией.

Обобщенные сведения о внутренних и зарубежных предприятиях как потенциальных конкурентах в деятельности организации, оценке качества деловых отношений с конкурирующими предприятиями в различных сферах деловой активности.

Сведения о подготовке, проведении и результатах переговоров с деловыми партнерами организации.

Сведения об условиях конфиденциальности, из которых можно установить порядок соглашения и другие обязательства организации с партнерами (клиентами, контрагентами).

Сведения о методах расчета, структуре, уровне реальных цен на продукцию и размеры скидок.

Сведения о подготовке к участию в торгах и аукционах, результатах приобретения или продажи на них товаров.

Сведения о целях, задачах, программах перспективных научных исследований. Ключевые идеи научных разработок, точные значения конструкционных характеристик, создаваемых изделий и оптимальных параметров разрабатываемых технологических процессов (размеры, объемы, конфигурация, процентное содержание компонентов, температура, давление, время и т. д.). Аналитические и графические зависимости, отражающие найденные закономерности и взаимосвязи, данные об условиях экспериментов и оборудовании, на котором они проводились. Сведения о материалах, из которых изготовлены отдельные детали, об особенностях конструкторско-технологического, художественно-технического решения изделия, дающие положительный экономический эффект.

Сведения о методах защиты от подделки товарных и фирменных знаков, о состоянии парка ПЭВМ и программного обеспечения.

Сведения об особенностях используемых и разрабатываемых технологий и специфике их применения, об условиях их производства и транспортировке продукции.

Сведения о порядке и состоянии организации защиты служебной или коммерческой тайны, о порядке и состоянии организации охраны, системы сигнализации, пропускном режиме.

Сведения, составляющие служебную или коммерческую тайну организаций, предприятий-партнеров и передаваемые ими в пользование на доверительной основе.

Приложение 2

Самостоятельная работа к практическому занятию
«Классификация защищаемой информации по видам тайны и степеням конфиденциальности»

Самостоятельная работа по теме занятия включает в себя:

- изучение теоретического материала лекционных занятий, учебной литературы, Интернет-ресурсов, раздела «Краткие сведения из теории» настоящего описания ПЗ;
- выполнение практических заданий.

Вопросы для самопроверки самостоятельной работы и вопросы для защиты ПЗ

- Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи.
- Понятие конфиденциальной информации.
- Виды конфиденциальной информации.
- Принципы засекречивания данных.

Практическое занятие 4.

РАБОТА С ДОКУМЕНТАМИ КЛАССИФИКАЦИИ УГРОЗ И МЕТОДОВ ОПРЕДЕЛЕНИЯ УЯЗВИМОСТЕЙ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

1. Цель работы: научиться определять уязвимости объекта информатизации на основе изучения предметной области

2. Задачи работы:

− Изучить предметную область
− Определить уязвимости
− Классифицировать определенные уязвимости

Студент должен:

Уметь:

- классифицировать защищаемую информацию по видам тайны и степеням секретности;
- классифицировать основные угрозы безопасности информации.

Знать:

- сущность и понятие информационной безопасности, характеристику ее составляющих;
- место информационной безопасности в системе национальной безопасности страны;
- виды, источники и носители защищаемой информации;
- источники угроз безопасности информации и меры по их предотвращению;
- факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах;
- жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи;
- современные средства и способы обеспечения информационной безопасности;
- основные методики анализа угроз и рисков информационной безопасности;

ПК:

- ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно – телекоммуникационных систем и сетей.

3. Подготовка к работе

Составьте таблицу, содержащую причины нарушения целостности информации и мер предосторожности, применяемых для защиты информации от потери целостности.

4. Задание

Описать информационную систему железной дороги, выбранный из таблицы 1 в соответствии с предпоследней цифрой шифра.

Таблица 1

Варианты информационных объектов железной дороги

Цифра шифра	Информационный объект	Цифра шифра	Информационный объект
0	Испытательный центр объектов железнодорожного транспорта	5	Отдел управления сети связи
1	Транспортно-логистический центр	6	Служба сигнализации и связи
2	Служба организации труда и заработной платы	7	Главный расчетный информационный центр
3	Служба информационных технологий	8	Служба безопасности движения поездов
4	Служба бухгалтерского учета	9	Финансово-экономическая служба

5. Порядок выполнения работы

1 Конкретизировать род деятельности ИО, определить ее штат, структуру административного управления.

2 Категорировать информацию, с которой работают в данном ИО исходяиз его рода деятельности.

3 Составить список необходимого оборудования для нормальной работы компании, включая, при необходимости, и бытовую технику.

4 Оценить свойства и стоимость информационных активов ИО. Работу выполнять в виде таблицы 2.

Стоимость актива определять в зависимости отего сво

5 йств по таблице 3.

6 Определить не менее пяти угроз для выбранных активов, их источников и методов борьбы с ними, которые могут быть реализованы по отношению к информации, создаваемой, хранящейся и обрабатываемой на информационном объекте. Работу выполнять в виде таблицы 4.

Таблица 2 - Перечень активов информационного объекта

Тип актива	Свойства информационного актива			Стоимость актива
	целостность	доступность	конфиденциальность	

Таблица 3 – **Определение стоимости актива в зависимости от его свойств**

Стоимость актива,	Свойства актива		
	целостность	доступность	конфиденциальность
	–	–	–

Таблица 4 – **Определение угроз, их источников и методов борьбы с данными угрозами**

Уязвимость	Наименование угрозы	Источник угрозы	Возможный результат при реализации угрозы, какие активы могут быть повреждены

6. Содержание отчета

a. Цель работы.
b. Результаты выполнения задания.
c. Описание информационного объекта.
d. Таблица перечня информационного объекта
e. Таблица угроз, их источников и методов борьбы с данными угрозами для информационного объекта.
f. Вывод по работе.

7. Контрольные вопросы к защите

a. Чем информационная система отличается от информационного объекта?
b. Что принято называть угрозой информационной безопасности?
c. Какова классификация методов защиты информации, в том числе по характеру проводимых мероприятий?
d. Какова классификация угроз информационной безопасности?
e. Что понимается под термином «информационный объект»?
f. Что представляет собой угроза права собственности?

Приложение 1

Краткие сведения из теории

На этапе описания информационной системы (ИС) необходимо указать цели ее создания, границы, информационные ресурсы, требования в области информационной безопасности (ИБ) и компонентов управления информационной системой и режимом ИБ.

Описание рекомендуется делать в соответствии со следующим планом:

- аппаратные средства ИС, их конфигурация;

- используемое программное обеспечение (ПО);
- интерфейсы системы, то есть внешние и внутренние связи с позиции информационной технологии;
- типы данных и информации;
- персонал, работающий в данной ИС (обязанности);
- миссия данной ИС (основные цели);
- критичные типы данных и информационные процессы;
- функциональные требования к ИС;
- категории пользователей системы и обслуживающего персонала;
- формальные требования в области ИБ, применимые к данной ИС (законодательство, ведомственные стандарты и т. д.);
- архитектура подсистемы ИБ;
- топология локальной сети;
- программно-технические средства обеспечения ИБ;
- входные и выходные потоки данных;
- система управления в данной ИС (должностные инструкции, система планирования в сфере обеспечения ИБ);
- существующая система управления в области ИБ (резервное копирование, процедуры реагирования на нештатные ситуации, инструкции по ИБ, контроль поддержания режима ИБ и т. д.);
- организация физической безопасности;
- управление и контроль внешней по отношению к ИС средой (климатическими параметрами, электропитанием, защитой от затоплений, агрессивной среды и т. д.).

Активы организации – все, что имеет ценность для организации в интересах достижения целей деятельности и находится в ее распоряжении. К активам организации могут относиться:

- информационные активы, в том числе различные виды информации, циркулирующие в информационной системе (служебная, управляющая, аналитическая, деловая и т. д.) на всех этапах жизненного цикла (генерация, хранение, обработка, передача, уничтожение);
- выпускаемая продукция и/или оказываемые услуги;
- аппаратура: процессоры, модули, клавиатуры, терминалы, рабочие станции, персональные компьютеры, принтеры, дисководы, коммуникационные линии, терминальные серверы, маршрутизаторы;
- программное обеспечение: исходные тексты, объектные модули, утилиты, диагностические программы, операционные системы, коммуникационные программы;
- данные: обрабатываемые, непосредственно доступные, архивированные, сохраненные в виде резервной копии, регистрационные журналы, базы данных, передаваемые по коммуникационным линиям;
- пользователи, обслуживающий персонал;
- документация: по программам, по аппаратуре, системная, по административным процедурам;
- расходные материалы: бумага, формы, красящая лента, магнитные носители.

Для системы, находящейся в стадии проектирования, и для уже существующей системы характер описания и степень подробности ответов будут разными. В первом случае (стадия проектирования) достаточно указать общие требования в области ИБ.

Анализ угроз информационной безопасности.

Под у г р о з о й информационной безопасности объекта понимаются возможные воздействия на него, приводящие к ущербу.

И с т о ч н и к у г р о з ы – это потенциальные антропогенные, техногенные или стихийные носители угрозы безопасности.

У я з в и м о с т ь о б ъ е к т а – это присущие объекту причины, приводящие к нарушению безопасности информации на объекте.

А т а к а – это возможные последствия реализации угрозы при взаимодействии источника угрозы через имеющиеся уязвимости. Атака – это всегда пара «источник – уязвимость», реализующая угрозу и приводящая к ущербу.

К настоящему времени известно большое количество угроз информационной безопасности. Рассмотрим их к л а с с и ф и к а ц и ю по различным классификационным признакам.

По виду:

− физической и логической целостности (уничтожение или искажение информации). Угроза целостности – несанкционированное изменение, искажение, уничтожение информации;

− конфиденциальности (несанкционированное получение). Угроза конфиденциальности – нарушение свойства информации быть известной толь- ко определенным субъектам;

− доступности. Угроза доступности (отказ в обслуживании) – нарушение работоспособности объекта, доступ к которому получил злоумышленник;

− права собственности.

По характеру:

− случайные (отказы, сбои, ошибки, стихийные явления). Случайные угрозы обусловлены недостаточной надежностью аппаратуры и программных продуктов, недопустимым уровнем внешних воздействий, ошибками персонала. Методы оценки воздействия этих угроз рассматриваются, как правило, в теории надежности, программировании, инженерной психологии;

− преднамеренные (злоумышленные действия людей). Преднамеренные угрозы связаны с действиями людей (работники спецслужб либо самого объекта, хакеры). Для несанкционированного доступа к информации вы- числительной системы злоумышленник может воспользоваться штатными каналами доступа, если по отношению к ним не предприняты никакие меры защиты, либо нештатными каналами доступа, к которым принято относить:

- побочное электромагнитное излучение информации с аппаратуры системы;
- побочные наводки информации по сети электропитания и заземления;
- побочные наводки информации на вспомогательных коммуникациях;
- подключение к внешним каналам связи.

По источникам:

− человек;

− технические устройства;

− программное обеспечение;

− внешняя среда (состояние атмосферы, побочные шумы, сигналы и наводки).

Угроза, как следует из определения, – это опасность причинения ущерба, то есть в этом определении проявляется жесткая связь технических проблем с юридической категорией, каковой является «ущерб».

Угрозами безопасности информации являются нарушения при обеспечении:

− конфиденциальности;

− доступности;

− целостности.

Конфиденциальность информации – это свойство информации быть известной только аутентифицированным законным ее владельцам или пользователям.

Доступность информации – это свойство информации быть доступной для аутентифицированных законных ее владельцев или пользователей. Нарушения при обеспечении доступности:

- блокирование информации;
- уничтожение информации и средств ее обработки.

Целостность информации – это свойство информации быть неизмен- ной в семантическом смысле при воздействии на нее случайных или пред- намеренных искажений или разрушающих воздействий. Нарушения при обеспечении целостности:

- модификация (искажение) информации;
- отрицание подлинности информации;
- навязывание ложной информации.

Все методы защиты информации по характеру проводимых действий можно разделить:

- на законодательные (правовые);

- организационные;
- технические;
- комплексные.

Для обеспечения защиты объектов информационной безопасности должны быть соответствующие правовые акты, устанавливающие порядок защиты и ответственность за его нарушение. Законы должны давать ответы на следующие вопросы: что такое информация, кому она принадлежит, как может с ней поступать собственник, что является посягательством на его права, как он имеет право защищаться, какую ответственность несет нарушитель прав собственника информации.

Установленные в законах нормы реализуются через комплекс организационных мер, проводимых, прежде всего, государством, ответственным за выполнение законов, и собственниками информации. К таким мерам относятся издание подзаконных актов, регулирующих конкретные вопросы по защите информации (положения, инструкции, стандарты и т. д.), и государственное регулирование сферы через систему лицензирования, сертификации, аттестации.

Поскольку в настоящее время основное количество информации генерируется, обрабатывается, передается и хранится с помощью технических средств, то для конкретной ее защиты в информационных объектах необходимы технические устройства. В силу многообразия технических средств нападения приходится использовать обширный арсенал технических средств защиты. Наибольший положительный эффект достигается в том случае, когда все перечисленные способы применяются совместно, т. е. комплексно.

Приложение 2

Самостоятельная работа к практическому занятию
«Работа с документами классификации угроз и методов определения уязвимостей объектов информатизации»

Самостоятельная работа по теме занятия включает в себя:

- изучение теоретического материала лекционных занятий, учебной литературы, Интернет-ресурсов, раздела «Краткие сведения из теории» настоящего описания ПЗ;
- выполнение практических заданий.

Практическое занятие 5.
ОПРЕДЕЛЕНИЕ УГРОЗ ОБЪЕКТА ИНФОРМАТИЗАЦИИ И ИХ КЛАССИФИКАЦИЯ

1. **Цель работы**: определение угроз объекта информатизации и их классификация.
2. **Задачи работы:**

– Научиться определять и классифицировать угрозы информационной безопасности объекта

Студент должен:

Уметь:

- классифицировать защищаемую информацию по видам тайны и степеням секретности;
- классифицировать основные угрозы безопасности информации.

Знать:

- сущность и понятие информационной безопасности, характеристику ее составляющих;
- место информационной безопасности в системе национальной безопасности страны;
- виды, источники и носители защищаемой информации;
- источники угроз безопасности информации и меры по их предотвращению;
- факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах;
- жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи;
- современные средства и способы обеспечения информационной безопасности;
- основные методики анализа угроз и рисков информационной безопасности;

ПК:

- ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно – телекоммуникационных систем и сетей.

3. **Подготовка к работе**

Изучить текст документа «Доктрина информационной безопасности». Заполнить таблицы.

4. **Задание**

1. Заполнить таблицы на основе Доктрины

Таблица 1. Классификация угроз информационной безопасности РФ по общей направленности

Угрозы информационной безопасности РФ			
Угрозы конституционным правам и свободам, общественному сознанию личности	Угрозы информационному обеспечению государственной политики	Угрозы развитию Отечества	Угрозы безопасности информационных и телекоммуникационных средств и систем
(содержание)	(содержание)	(содержание)	(содержание)

Таблица 2. Источники угроз информационной безопасности

Источники угроз информационной безопасности	
Внешние источники	Внутренние источники
(содержание)	(содержание)

2.Составить перечень угроз для заданного объекта информатизации. Заполнить таблицу.

Таблица 1. Перечень угроз

Номер угрозы	Источник угрозы	Среда распространения	Носитель информации

3.Провести анализ потенциальных каналов утечки на указанном объекте. Составить перечень каналов утечки информации на защищаемом объекте с указанием места расположения по образцу таблицы 1.

Таблица 1. Перечень потенциальных каналов утечки информации

Каналы утечки информации с объекта защиты			Место расположения
1	Оптический канал	Окно со стороны проспекта	каб. № 1
		Окно со стороны проспекта	каб. № 2
		Окно со стороны проспекта	каб. № 3
2	Радиоэлектронный канал	Стоянка автотранспорта на просп.	указать
		Система часофикации	указать
		Телефон	указать
		Розетки	указать
		ПК	указать
		Воздушная линия электропередачи	указать
		Система оповещения	указать
		Система пожарной сигнализации	указать
3	Акустический канал	Теплопровод подземный	указать
		Водопровод подземный	указать
		Стены помещения	указать
		Батареи	указать
		Окна контролируемого помещения	указать
4	Материально-вещественный канал	Документы на бумажных носителях	указать
		Персонал предприятия	указать
		Производственные отходы	указать

3.Построить модель угроз и комплексную модель каналов утечки информации для заданного объекта. Заполнить таблицы.

Таблица 1. Модель угроз защищаемого объекта

№ элемента	Цена информации	Путь проникновения	Оценка реальности	Величина угрозы	Ранг угрозы

Таблица 2. Комплексная модель каналов утечки

№ п/п	Цена информации	Источник сигнала	Путь утечки	Вид канала	Оценка реальности	Величина угрозы/ранг

5. Содержание отчета

1. название и цель работы;
2. перечень осваиваемых компетенций;
3. задание;
4. ход выполнения работ;
5. выводы по работе;
6. ответы на контрольные вопросы.

6. Контрольные вопросы к защите

1. Понятие угрозы безопасности информации.
2. Системная классификация угроз безопасности информации.
3. Угрозы информационной безопасности РФ.
4. Источники угроз информационной безопасности РФ.
5. Содержание угроз информационной безопасности РФ.
6. Каналы и методы несанкционированного доступа к информации
7. Уязвимости. Методы оценки уязвимости информации

Приложение 1

Самостоятельная работа к практическому занятию

«Определение угроз объекта информатизации и их классификация»

Самостоятельная работа по теме занятия включает в себя:

- изучение теоретического материала лекционных занятий, учебной литературы, Интернет-ресурсов, раздела «Краткие сведения из теории» настоящего описания ПЗ;
- выполнение практических заданий.

Практическое занятие 6.

РАБОТА В СПРАВОЧНО-ПРАВОВОЙ СИСТЕМЕ С НОРМАТИВНЫМИ И ПРАВОВЫМИ ДОКУМЕНТАМИ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РФ

1. **Цель работы**: научиться работать в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности.
2. **Задачи работы:**

− Изучить краткие сведения из теории;
− Выполнить задания на определение ключевых направлений защиты информации

Студент должен:

Уметь:

- классифицировать защищаемую информацию по видам тайны и степеням секретности;
- классифицировать основные угрозы безопасности информации.

Знать:

- сущность и понятие информационной безопасности, характеристику ее составляющих;
- место информационной безопасности в системе национальной безопасности страны;
- виды, источники и носители защищаемой информации;
- источники угроз безопасности информации и меры по их предотвращению;
- факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах;
- жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи;
- современные средства и способы обеспечения информационной безопасности;
- основные методики анализа угроз и рисков информационной безопасности;

ПК:

- ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно – телекоммуникационных систем и сетей.

3. **Подготовка к работе**

Изучить часть 4 Гражданского кодекса РФ. Дать развернутый ответ на поставленные вопросы. Необходимо обосновать свой ответ, указав наименование соответствующего нормативного документа, его статью и пункт статьи, на которые следует опираться.

4. **Задание**

Задача 1 Гражданин Иванов предложил гражданам Шаталову и Моисееву идею создания информационно-справочной системы «Альбомы рок-музыкантов» в среде программирования Delphi 6.0, лицензионная версия которой была приобретена Моисеевым. Граждане Шаталов и Моисеев создали такую систему и зарегистрировали свое авторство на нее без участия гражданина Иванова. Имеет ли место в данной ситуации нарушение авторского права гражданина Иванова?

Задача 2 Гражданин Алексеев создал инструментальное программное средство для работы с трехмерной компьютерной графикой под названием – «Alex 3D» и зарегистрировал на него свои права. 20.09.2006 этот гражданин заключил договор с компанией «Moscow Technology и передал свои имущественные права на распространение своего программного продукта сроком на один год (т.е. до 19.09.2007). После заключения договора компания «Moscow Technology» распространила версию программы "Alex 3D" с предварительной модификацией данного программного продукта без ведома автора. Имеет ли место в данной ситуации нарушение авторского права гражданина Алексеева?

Задача 3 Гражданин Серебренников разработал в соавторстве с гражданином Семеновым информационно-справочную систему «Энциклопедия. Животные Крайнего севера».

Финансовую поддержку программных разработок вышеупомянутым гражданам оказал гражданин Андреев. Граждане Серебренников и Семенов 13.05.06 оформили свое авторство на данную информационную систему. В марте 2006 г. данный программный продукт был выпущен под авторством гражданина Андреева. Имеет ли место в данной ситуации нарушение авторского права граждан Серебренникова и Семенова?

Задача 4 Будет ли удовлетворен судебный иск студента Максимкина к студенту Федорову в том, что последний нарушил авторское право, выдавая идею Максимкина получить более эффективный алгоритм сортировки массива на основе линейной и пузырьковой сортировки за свою?

Задача 5 Гражданин В. А. Мельников, автор и правообладатель электронной энциклопедии «Вокруг света», планировал сотрудничать с компанией «Видеотех», занимающейся тиражированием программных продуктов. Экземпляр электронной энциклопедии был передан в компанию для ознакомления. При этом договор о передаче компании «Видеотех» имущественных прав на программу составлен не был. В. А. Мельников предъявил судебный иск к компании «Видеотех», которая осуществила выпуск данного программного продукта. Какое решение вынесет суд и почему?

Задача 6 Гражданин М. А. Петров, автор и правообладатель информационно-справочной системы «Энциклопедия. Легковые автомобили от А до Я», 19.04.2007 подписал договор с компанией «Мир программ» о передаче имущественного права на выпуск своей системы. Первые экземпляры программы должны были поступить в продажу не раньше 17.06.2007. Однако 25.05.2007 года гражданин Петров обнаружил экземпляры своего программного продукта в одном из ларьков. Имеется ли несоответствие, связанное с нарушением информационной безопасности?

Задача 7 Гражданин П. А. Сергеев зарегистрировал созданную им информационную систему «Растения Омской области» под своим именем 17.05.2007. Его авторское право на созданную им информационную систему будет действовать до 17.05.2057. Имеется ли несоответствие, связанное с нарушением информационной безопасности?

Задача 8 Гражданка И. П. Лукашина решила зарегистрировать свое авторское право на созданную ею базу данных и осуществила это следующим образом: © 2006 Лукашина Ирина. Имеется ли несоответствие, связанное с нарушением информационной безопасности?

Задача 9 Гражданин В. П. Чумаков зарегистрировал свое авторское право на созданную им операционную систему «New System». Однако гражданину Чумакову не принадлежит право модификации созданного им программного продукта. Имеется ли несоответствие, связанное с нарушением информационной безопасности?

5. Содержание отчета

1. название и цель работы;
2. перечень осваиваемых компетенций;
3. задание;
4. описание решения задач;
5. ход выполнения работ;
6. выводы по работе;
7. ответы на контрольные вопросы.

6. Контрольные вопросы к защите

1. Законодательные акты в области защиты информации.
2. Российские и международные стандарты, определяющие требования к защите информации.

Приложение 1

Самостоятельная работа к практическому занятию

«Работа в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности РФ»

Самостоятельная работа по теме занятия включает в себя:

- изучение теоретического материала лекционных занятий, учебной литературы, Интернет-ресурсов, раздела «Краткие сведения из теории» настоящего описания ПЗ;
- выполнение практических заданий.

Практическое занятие 7.

РАБОТА В СПРАВОЧНО-ПРАВОВОЙ СИСТЕМЕ С НОРМАТИВНЫМИ И ПРАВОВЫМИ ДОКУМЕНТАМИ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МЕЖДУНАРОДНОГО СТАТУСА

3. Цель работы: : научиться работать в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности.

4. Задачи работы:

− Изучить краткие сведения из теории;

− Выполнить задания на определение ключевых направлений защиты информации

1. Студент должен:

Уметь:

- классифицировать защищаемую информацию по видам тайны и степеням секретности;
- классифицировать основные угрозы безопасности информации.

Знать:

- сущность и понятие информационной безопасности, характеристику ее составляющих;
- место информационной безопасности в системе национальной безопасности страны;
- виды, источники и носители защищаемой информации;
- источники угроз безопасности информации и меры по их предотвращению;
- факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах;
- жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи;
- современные средства и способы обеспечения информационной безопасности;
- основные методики анализа угроз и рисков информационной безопасности;

ПК:

- ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно – телекоммуникационных систем и сетей.

3. Подготовка к работе

Изучить содержания ст. 272, 273, 274 УК РФ. Дать развернутый ответ на поставленные вопросы. Необходимо обосновать свой ответ, указав наименование соответствующего нормативного документа, его статью и пункт статьи, на которые следует опираться.

4. Задание

Задача 1 Бывший сотрудник химико-биологического предприятия вместе со своим приятелем программистом скопировали конфиденциальную информацию: состав ингредиентов, их пропорции и формулу нового лекарственного препарата – с целью продажи этой информации конкурирующей организации. Можно ли квалифицировать действия лица (группы лиц) в описанной ситуации как противоправные?

Задача 2 П.П. Андреев, сотрудник одного из филиалов ИТ-банка, внедрил в компьютерную банковскую систему вирус, уничтожающий исполняемые файлы (файлы с расширением *.exe. В результате внедрения этого вируса было уничтожено 40 % банковских программных приложений, что принесло банку материальный ущерб размере 750 000 рублей. Можно ли квалифицировать действия лица (группы лиц) в описанной ситуации как противоправные?

Задача 3 Сотрудник Научно-исследовательского института приборостроения скопировал схемы, чертежи и графики прибора с целью продажи этой информации зарубежной фирме производителю. Можно ли квалифицировать действия лица (группы лиц) в описанной ситуации как противоправные?

Задача 4 Решение в пользу какой стороны и почему вынесет суд при предъявлении владельцем фирмы «Электронная галерея» И. С. Дубцовым судебного иска к продавцу этой же фирмы, если по вине последнего произошло электрическое замыкание и было повреждено значительное количество компьютерной техники?

Задача 5 Будет ли привлечена к уголовной ответственности главный бухгалтер, торговой сети «Оптпром» С.Н. Вульф, если ее действия повлекли уничтожение компьютерной информации в базах данных вышеуказанной торговой сети и после ревизии предприятие было оштрафовано на 350 000 рублей?

Задача 6 Будет ли удовлетворен иск компании «Интермедиа» о привлечении к уголовной в ответственности гражданина Р.И. Сизова и выплате им фирме денежной компенсации, если он внедрил в компьютерную сеть компании программу, действие которой заключается в уничтожении исполняемых файлов в какой-либо компьютерной сети. Функционирование данной программы принесло убытки различным организациям на общую сумму 670 000 рублей.

Задача 7 За несанкционированный доступ и копирование компьютерной информации суд приговорил гражданина РФ В. А. Лютикова к 5 годам лишения свободы. Найдите и исправьте несоответствие в предложенной ситуации, если оно имеет место.

Задача 8 По вине оператора по набору данных М. Л. Плехановой, работавшей с компьютерной системой бухгалтерских платежей, торговая сеть «Антиквар» понесла денежные убытки в размере 1 850 000 рублей. М. Е. Плехановой было предъявлен обвинение по ст. 273 УК РФ. Найдите и исправьте несоответствие в предложенной ситуации, если оно имеет место.

Задача 9 Студентам технического университета за доступ к компьютерной системе службы внутренних дел и копирование части файлов данной системы было предъявлено обвинение по ст. 272, п. 1 УК РФ. Найдите и исправьте несоответствие в предложенной ситуации, если оно имеет место.

Задача 10 Н.А. Симонова, сотрудница отдела продаж косметической компании «Макияж», за распитие кофейного напитка в непосредственной близости от ЭВМ была наказана исправительными работами сроком на 15 суток. Найдите и исправьте несоответствие в предложенной ситуации, если оно имеет место.

Задача 11 Оператор ПК торговой сети «Вернисаж» Д. С. Ермилов был обвинен по ст. 272, п. 1 УК РФ за изменение данных в поле «Адрес» в базе данных клиентских платежей. Эту модификацию он произвел по просьбе самой клиентки в связи с изменением ее места жительства. Найдите и исправьте несоответствие в предложенной ситуации, если оно имеет место.

Задача 12 За распространение программы, действие которой заключается в уничтожении текстовых файлов в какой-либо компьютерной сети, студент III курса авиационного техникума был наказан судом штрафом в размере 100 минимальных размеров оплаты труда. Найдите и исправьте несоответствие в предложенной ситуации, если оно имеет место.

Задача 13 За несанкционированный доступ к компьютерной информации в файлах химико-биологического исследовательского центра «New Life» и ее модификацию гражданку РФ А. С. Иванову суд приговорил к 8 месяцам исправительных работ. Найдите и исправьте несоответствие в предложенной ситуации, если оно имеет место.

Задача 14 За нарушение работы с компьютерной системой бухгалтерских платежей авиакомпании «Небеса» сотруднице вышеупомянутой организации Т. В. Бариновой, действия которой привели к модификации компьютерных данных и принесли авиакомпании «Сибирь» денежные убытки в размере 150 000 рублей, было предъявлено обвинение по ст. 274 УК РФ. Найдите и исправьте несоответствие в предложенной ситуации, если оно имеет место.

5. Содержание отчета

1. название и цель работы;
2. перечень осваиваемых компетенций;
3. задание;
4. решение кейсов;
5. ход выполнения работ;

6. выводы по работе;
7. ответы на контрольные вопросы.

6. Контрольные вопросы к защите

1. Система сертификации РФ в области защиты информации.
2. Основные правила и документы системы сертификации РФ в области защиты информации.

Приложение 1

Самостоятельная работа к практическому занятию

«Работа в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности международного статуса»

Самостоятельная работа по теме занятия включает в себя:

- изучение теоретического материала лекционных занятий, учебной литературы, Интернет-ресурсов, раздела «Краткие сведения из теории» настоящего описания ПЗ;
- выполнение практических заданий.

Практическое занятие 8.
ВЫБОР МЕР ЗАЩИТЫ ИНФОРМАЦИИ ДЛЯ АВТОМАТИЗИРОВАННОГО РАБОЧЕГО МЕСТА

1. Цель работы: выбор мер защиты информации для автоматизированного рабочего места.

2. Задачи работы:

− Изучить средства защиты АРМ;

− Составить классификацию средств защиты АРМ.

Студент должен:

Уметь:

- классифицировать защищаемую информацию по видам тайны и степеням секретности;
- классифицировать основные угрозы безопасности информации.

Знать:

- сущность и понятие информационной безопасности, характеристику ее составляющих;
- место информационной безопасности в системе национальной безопасности страны;
- виды, источники и носители защищаемой информации;
- источники угроз безопасности информации и меры по их предотвращению;
- факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах;
- жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи;
- современные средства и способы обеспечения информационной безопасности;
- основные методики анализа угроз и рисков информационной безопасности;

ПК:

- ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно – телекоммуникационных систем и сетей.

3. Подготовка к работе

Подготовить табличные данные по организации защиты информации на АРМ

4. Задание

Задание 1. Построить функциональную структуру СФЗ заданного объекта. Разработать модель мероприятий физической защиты объекта в соответствии с моделями угроз и каналов утечки информации на заданном объекте.

В процессе организационных мероприятий необходимо определить:

а) контролируемую зону (зоны);

б) выделить из эксплуатируемых технических средств технические средства, используемые для передачи, обработки и хранения конфиденциальной информации (ОТСС);

в) выявить в контролируемой зоне (зонах) вспомогательные технические средства и системы (ВТСС).

Задание 2. Составить план организационно-технических мероприятий по образцу таблицы 1.

Таблица 1. План организационно-технических мероприятий

№ п\п	Демаскирующий признак	Мероприятия по уменьшению (ослаблению) демаскирующих признаков
I. Организационные мероприятия		
1	Прибытие сотрудников на службу в форменной одежде	1. Прибытие сотрудников на службу в форменной одежде другого ведомства. 2. Проведение совещаний и переподготовки сотрудников других ведомств
2	Перемещение сотрудников	1. Разграничение доступа сотрудников в различные помещения. 2. Организация пропускного режима
3	Готовая продукция	1. Разграничение доступа сотрудников в склад при вывозе продукции за пределы предприятия
4	Отходы производства	1. Сбор и утилизация отходов производства. 2. Уничтожение отходов делопроизводства
II. Технические мероприятия		
1	Излучение ПЭВМ	1. Организация работы системы зашумления. 2. Установка в ПЭВМ генераторов зашумления. 3. Персонификация доступа в систему. 4. Программная защита системы ПЭВМ. 5. Плановые (внеплановые) проверки ПЭВМ
2	Телефонная связь	1. Организация работы внутренней АТС. 2. Запись переговоров сотрудников по телефонам. 3. Закрытие каналов связи
3	Строительные конструкции здания	1. Нанесение на стекла пленки поглощающей ИК-излучение. 2. Установка системы виброакустического зашумления стекол и строительных конструкций. 3. Специальная проверка персонала обслуживающего смежные помещения

Задание 3. Подготовить план внедрения на предприятии конфиденциального делопроизводства, используя следующую методику:

– первый этап – определение перечня сведений конфиденциального характера и документов, содержащих конфиденциальные сведения. Разделение сведений на несколько групп по степени конфиденциальности (например: строго конфиденциальные, конфиденциальные, для служебного пользования);

– второй этап - утверждение перечня сведений конфиденциального характера у руководства, а также определение порядка и сроков переутверждения данного перечня, а также снижение и снятие грифа конфиденциальности;

– третий этап – определение правил конфиденциального бумажного делопроизводства на основе общего бумажного делопроизводства;

– четвертый этап – определение порядка допуска сотрудников к сведениям конфиденциального характера;

– пятый этап – заключение договоров о нераспространении конфиденциальных сведений между сотрудниками, которые будут допущены к работе с конфиденциальной информацией и руководством организации;

– шестой этап – создание необходимых нормативных документов (инструкций, должностных обязанностей и т.д.);

– седьмой этап – доведение нормативных документов до сотрудников в рамках функциональных обязанностей;

– восьмой этап – создание механизмов контроля за соблюдением конфиденциального делопроизводства;

– девятый этап – создание механизма ответственности за нарушение правил конфиденциального делопроизводства.

Задание 4. Составить план реализации мероприятий по защите информации, учитывая критические ресурсы и информационную инфраструктуру. К критическим ресурсам следует отнести:

– персонал;
– информационную структуру;
– физическую инфраструктуру.

К информационной инфраструктуре следует отнести:

– компьютеры;
– программы и данные;
– информационные сервисы;
– документацию.

5. Содержание отчета

1. название и цель работы;
2. перечень осваиваемых компетенций;
3. задание;
4. выполненные задания;
5. выводы по работе;
6. ответы на контрольные вопросы.

6. Контрольные вопросы к защите

1. Основные механизмы защиты информации.
2. Система защиты информации.
3. Меры защиты информации, реализуемые в автоматизированных (информационных) системах.
4. Программные и программно-аппаратные средства защиты информации.
5. Инженерная защита и техническая охрана объектов информатизации.
6. Организационно-распорядительная защита информации. Работа с кадрами и внутриобъектовый режим. Принципы построения организационно-распорядительной системы.

Приложение 1

Самостоятельная работа к практическому занятию

«Выбор мер защиты информации для автоматизированного рабочего места»

Самостоятельная работа по теме занятия включает в себя:

- изучение теоретического материала лекционных занятий, учебной литературы, Интернет-ресурсов, раздела «Краткие сведения из теории» настоящего описания ПЗ;
- выполнение практических заданий.

Практическое занятие 9.
СОСТАВЛЕНИЕ ПАСПОРТА ЗАЩИЩЕННОГО АВТОМАТИЗИРОВАННОГО РАБОЧЕГО МЕСТА

1. **Цель работы**: научиться планировать рабочее место персонала
2. **Задачи работы:**

− Изучить теоретические сведения;
− Составить паспорт АРМ.

Студент должен:
Уметь:

- классифицировать защищаемую информацию по видам тайны и степеням секретности;
- классифицировать основные угрозы безопасности информации.

Знать:

- сущность и понятие информационной безопасности, характеристику ее составляющих;
- место информационной безопасности в системе национальной безопасности страны;
- виды, источники и носители защищаемой информации;
- источники угроз безопасности информации и меры по их предотвращению;
- факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах;
- жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи;
- современные средства и способы обеспечения информационной безопасности;
- основные методики анализа угроз и рисков информационной безопасности;

ПК:

- ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно – телекоммуникационных систем и сетей.

3. **Подготовка к работе**

Изучить краткие сведения из теории

4. **Задание**

1) На основе требований к рабочему месту и примера паспорта рабочего места (см. пример ниже) разработать паспорт рабочего места менеджера;

2) обосновать оснащение рабочего места согласно должностным инструкциям.

5. **Порядок выполнения работы**

Выполнить задание по примеру:

1 Назначение и общая характеристика рабочего места:
- предприятие ООО «Название»;
- структурное подразделение
– руководство;
- рабочее место директора;
- категория персонала
– руководитель;
- адрес.

2 Планировка рабочего места директора предприятия.

3. Функции и задачи управления:
3.1 управление стратегией развития;
3.2 организация системы управления;
3.3 управление персоналом и социальным развитием;
3.4 управление экономическим развитием;

3.5 управление финансами и бухгалтерским учетом;
3.6 управление трудом и зарплатой;
3.7 управление маркетингом и сбытом;
3.8 управление внешнеэкономической деятельностью.
4. Регламентирующая документация:
4.1 устав предприятия;
4.2 договор учредителей;
4.3 философия предприятия;
4.4 правило внутреннего трудового распорядка;
4.5 положение об оплате труда;
4.6 штатное расписание;
4.7 положение о подразделениях;
4.8 контракт директора;
4.9 должностная инструкция директора;
4.10 регламенты предприятия.
5. Мебель и оборудование: -
рабочий стол 120×80см – 3 шт.;
- стол для компьютера 80×80 см – 1 шт.;
- уголок R 80 см – 1 шт.;
- книжный шкаф – 1 шт.;
- кресло директора – 1 шт.;
- кресло для посетителей –3 шт.;
- стулья кабинетные –10 шт.;
- сейф металлический – 1 шт.
6. Технические средства:
- персональный компьютер – 1 шт.;
- коммутатор внутренней связи – 1 шт.;
- телефонный аппарат (факс) - 1 шт.;
- письменная доска – 1 шт.;
- кондиционер бытовой – 1 шт.;
- множительный аппарат «XEROX» - 1 шт.;
- канцелярский набор «Органайзер» - 1 шт.;
- папки деловые – 20 шт.
7. Загрузка рабочего места:
- нормативная общая трудоемкость;
- трудоемкость выполнения основных функций;
- производственные командировки;
- отпуска и регламентируемые перерывы;
- норма управляемости;
- коэффициент равновесия загрузки.
8. Условия труда:
- общая площадь – 30м2 ;
- площадь на 1 сотрудника во время освещения – 2м2 ;
- санитарные условия – нормальные;
- норма освещенности – 200Лк;
- средняя температура 20°С;
- уровень влажности – до 50%;
- уровень шума – не более 50 дб.;
- цвет помещения – светло-серый.
9. Оплата труда:
- должностной оклад;

- премия;
- ежегодная премия (бонус).

10. Охрана труда и техника безопасности:
- инструкция по охране труда;
- инструкция по эксплуатации технических средств;
- инструкция по электробезопасности;
- фирменная одежда (костюм, ботинки, рубашка, галстук);
- рабочая одежда для посещения объектов (халат, каска, сапоги, очки);
- средства индивидуальной защиты (газовый пистолет, электрошок).

11. Социальные льготы:
- персональный автомобиль ;
- очередной отпуск – 28 календарных дней;
- дополнительный оплачиваемый отпуск – 6 дней в году;
- творческий день – 1 раз в месяц.

12. Критерии эффективности труда:
- рост чистой прибыли (процент к предыдущему году);
- снижение затрат на 1 рубль продукции;
- рост объемов производства (тыс. руб., процент к предыдущему году);
- снижение текучести рабочих кадров (в процентах);
- рост качества продукции (снижение процента брака)

5. Содержание отчета

1. название и цель работы;
2. перечень осваиваемых компетенций;
3. задание;
4. ход выполнения работ;
5. выводы по работе;
6. ответы на контрольные вопросы.

6. Контрольные вопросы к защите

1. Требования к защищенному АРМ
2. Составление паспорта защищенного АРМ

Приложение 1

Краткие сведения из теории

Паспорт (типовой проект) рабочего места рабочих и служащих включает следующие разделы:

1) назначение и общие характеристики;
2) планировка рабочего места;
3) мебель, оборудование и технические средства;
4) функциональные обязанности (основные элементы работы);
5) методы и приемы труда;
6) условия труда;
7) оплата труда;
8) организация обслуживания;
9) регламентирующая документация;
10) загрузка рабочего места (нормирование);
11) охрана труда и техника безопасности.

Методика разработки паспорта рабочего места включает такие этапы, как:

1) анализ литературы, типовых проектов рабочих мест, посещение передовых офисов;

2) расчет потребности в площадях, оборудовании, технических средствах, разработка технического задания на типовые рабочие места для подразделений;

3) разработка технического проекта, заказ мебели и оборудования, проведение ремонта помещений, монтаж мебели, разработка регламентирующих документов;

4) внедрение паспорта рабочего места.

Приложение 2

Самостоятельная работа к практическому занятию

«Составление паспорта защищенного автоматизированного рабочего места»

Самостоятельная работа по теме занятия включает в себя:

- изучение теоретического материала лекционных занятий, учебной литературы, Интернет-ресурсов, раздела «Краткие сведения из теории» настоящего описания ПЗ;
- выполнение практических заданий.