**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.08. ОРГАНИЗАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

по специальности

10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

среднего профессионального образования

Санкт-Петербург
2022

Организационно-правовое обеспечение информационной безопасности. Методические указания по выполнению практических работ.

Составители: Амирова А.П., Кривоносова Н.В. – Санкт-Петербург, 2022.

Методические указания содержат описания практических занятий, предусмотренных рабочей программой Организационно-правовое обеспечение информационной безопасности. Каждая работа рассчитана на 2 академических часа, общий объём составляет 30 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 НОРМАТИВНЫМИ ДОКУМЕНТАМИ

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

2. Задачи работы:

- изучить основные документы в области информационной безопасности

Студент должен:

Уметь:

- осуществлять организационное обеспечение информационной безопасности автоматизированных (информационных) систем в рамках должностных обязанностей техника по защите информации;
- применять нормативные правовые акты и нормативные методические документы в области защиты информации;
- контролировать соблюдение персоналом требований по защите информации при ее обработке с использованием средств вычислительной техники;
- оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации;
- защищать свои права в соответствии с трудовым законодательством

Знать:

- основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области;
- правовые основы организации защиты информации, содержащей сведения, составляющие государственную тайну и информации конфиденциального характера, задачи органов защиты государственной тайны;
- нормативные документы в области обеспечения защиты информации ограниченного доступа;
- организацию ремонтного обслуживания аппаратуры и средств защиты информации;
- принципы и методы организационной защиты информации, организационное обеспечение информационной безопасности в организации;
- правовое положение субъектов правоотношений в сфере профессиональной деятельности (включая предпринимательскую деятельность);
- нормативные методические документы, регламентирующие порядок выполнения мероприятий по защите информации, обрабатываемой в автоматизированной (информационной) системе;
- законодательные и нормативные правовые акты, регламентирующие трудовые правоотношения.

ПК:

- ПК 1.4. Осуществлять контроль функционирования информационно – телекоммуникационных систем и сетей.
- ПК 3.2. Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации, используемых в информационно – телекоммуникационных системах и сетях.

3. Подготовка к работе

Подготовить тетрадь под словарь.

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:
- 390-ФЗ О безопасности (2010)
- 5485-1 О государственной тайне (1993)
- 149-ФЗ Об информации, информационных технологиях и о защите информации (2006)
- 152-ФЗ О персональных данных (2006)
- 184-ФЗ О техническом регулировании (2002)
- 98-ФЗ О коммерческой тайне (2004)
- 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 такое федеральный закон?
2. Что такое доктрина ИБ?
3. Что такое нормативно-правовой документ?

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 нормативными документами»

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.

ЗАЩИТА ИНФОРМАЦИИ, СОДЕРЖАЩЕЙСЯ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ОБЩЕГО ПОЛЬЗОВАНИЯ

1. Цель работы: знать и разбираться в защите информации

2. Задачи работы:

- иметь знания о защите информации в системах общего пользования

Студент должен:

Уметь:

- осуществлять организационное обеспечение информационной безопасности автоматизированных (информационных) систем в рамках должностных обязанностей техника по защите информации;

Знать:

- основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области;

ПК:

- ПК 1.4. Осуществлять контроль функционирования информационно – телекоммуникационных систем и сетей.
- ПК 3.2. Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации, используемых в информационно – телекоммуникационных системах и сетях.

3. Подготовка к работе

Повторить факторы, влияющие на организацию системы защиты информации, методы защиты информации, цели и задачи защиты информации.

4. Задание

Выполнить задания 1-5, включающие в себя информацию о защите информации

5. Порядок выполнения работы

- **Задание 1**

Основные цели и защиты информации

- **Задание 2**

Факторы, влияющие на организацию системы защиты информации

- **Задание 3**

Дестабилизирующее воздействие

- **Задание 4**

Требования безопасности информационной системы

- **Задание 5**

Основные методы защиты информации

6. 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.

Приложение 1

Краткие сведения из теории

Дестабилизирующее воздействие - негативное воздействие на компьютерную систему, реализуемое использованием реализации угрозы ИБ, в результате чего происходит нарушение конфиденциальности информации, её уничтожение, блокирование, модификация.

Причины со стороны людей:

1. непосредственное воздействие на носитель информации
2. несанкционированное распространение информации
3. вывод из строя тех. Средств
4. нарушение режима работы тех. средств и технологий обработки информации
5. вывод из строя и нарушение работы систем обеспечения функционирования

Причины со стороны тех. средств:

1. тех. Поломка
2. возгорание
3. природные явления
4. выход из строя систем обеспечения функционирования

Причины со стороны тех. средств

1. выход из строя
2. создание ПЭМИН

Причины со стороны систем обеспечения функционирования тех. средств

1. выход систем из строя
2. нарушение режимов работы

Причины со стороны природных явлений

1. землетрясение
2. наводнение
3. тайфун

Методы дестабилизирующего воздействия

1. НСД (получение доступа с использованием перебора паролей)
2. использование известных ошибок в ПО
3. DOS-атаки
4. внедрение программно-аппаратных закладок

В качестве защиты могут быть использованы:

1. межсетевые экраны
2. антивирус
3. система обнуружения вторжений
4. Honey Pot - запуск на отд. сервере, включ в ЛВС с ЗИ (это как?) - система начинает фиксировать любые действия дестабилизирующего воздействия (заманив хакера)
5. криптосредства
6. использование организационных мероприятий

Практическое занятие 3.

ВЫБОР ФУНКЦИЙ И ЗАДАЧ ОРГАНОВ ИСПОЛНИТЕЛЬНОЙ ВЛАСТИ, УПОЛНОМОЧЕННЫХ В ОБЛАСТИ ИБ

1. **Цель работы**: изучить структуру органов власти по защите информации, взаимодействие органов обеспечения информационной безопасности, функции каждого из участников этого процесса
2. **Задачи работы:**

– первая часть занятия проводится в виде опроса и рассмотрения структуры органов власти по защите информации.

– вторая часть занятия проводится в виде выполнения РГЗ.

Студент должен:

Уметь:

- осуществлять организационное обеспечение информационной безопасности автоматизированных (информационных) систем в рамках должностных обязанностей техника по защите информации;
- применять нормативные правовые акты и нормативные методические документы в области защиты информации;
- контролировать соблюдение персоналом требований по защите информации при ее обработке с использованием средств вычислительной техники;
- оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации;
- защищать свои права в соответствии с трудовым законодательством

Знать:

- основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области;
- правовые основы организации защиты информации, содержащей сведения, составляющие государственную тайну и информации конфиденциального характера, задачи органов защиты государственной тайны;
- нормативные документы в области обеспечения защиты информации ограниченного доступа;

ПК:

- ПК 1.4. Осуществлять контроль функционирования информационно – телекоммуникационных систем и сетей.
- ПК 3.2. Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации, используемых в информационно – телекоммуникационных системах и сетях.

3. **Подготовка к работе**

повторить информацию о видах информации

4. **Задание**

научиться выявлять виды информации ограниченного доступа на предприятии и относить к одной из групп конфиденциальности либо секретности

5. **Порядок выполнения работы**

- Проанализировать информационные активы выбранного вами предприятия: Укажите месторасположение информационных активов по отделам
- Перечень информационных активов при построении системы защиты информации можно представить в виде отношения сведений S={si} и уровня их конфиденциальности A={ak}, где i – номер оцениваемого сведения, а k – упорядоченное множество значений лингвистической переменной

- «категория закрытой информации» = { <Открытая, несекретная информация (ОИ)>, <Персональные данные (ПДн)>, <Коммерческая тайна (КТ)>, <Служебная тайна (СТ)>, <Секретно (С)>, <Совершенно секретно (СС)>, <Особой важности (ОВ)>, <Для служебного пользования (ДСП)> , ….}.
- Отразите взаимосвязи между информационными активами и критериями их безопасности.
- Изучите технологический процесс обработки и хранения информации, физических условий и условий окружающей среды на выбранном предприятии: – внешние подключения с другими системами – протоколы взаимодействия; – хранение информации – файловая организация и архивация; – накопление информации – каналы, носители, накопители, обмен информации, фактографическая информация, репликация, архивация, обновления, предоставление информации разным категориям пользователей; – способ предоставления информации – сайты, почта и вывод на печать, мобильные пользователи, требования в работе с документированной информацией – средства обработки и передачи информации, технические и программные средства ВТ, средства и линии связи, предоставляющие возможности как для перемещения (передачи, копирования) информации между различными областями памяти и информационными носителями, различными средствами обработки, определенными для АС, так и по выводу информации из установленной для нее сферы обращения.

6. 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.

7. Контрольные вопросы к защите

- Какие виды тайн бывают?
- Какие органы исполнительной власти есть в России?

Приложение 1

Краткие сведения из теории

Информация может храниться в различных формах, включая такие как цифровая форма (например, файлы с данными, сохраненные на электронных или оптических носителях), материальная форма (например, на бумаге), а также в нематериальном виде в форме знаний служащих. Информация ограниченного доступа на предприятии отражена в активах предприятия. Актив – это что-либо, что имеет ценность для организации

Практическое занятие 4.
РАЗРАБОТКА БАЗОВОГО БЛОКА ДОКУМЕНТОВ ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИСПДН СОСТАВЛЕНИЕ ПЕРЕЧНЯ ПДН

1. **Цель работы**: является теоретическая и практическая подготовка студентов в области изучения задач определения модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных, научиться работать с нормативными документами по защите персональных данных.

2. **Задачи работы:**
   - использовать документ «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России 15.02.2008 г. ДСП.»

Студент должен:
Уметь:
- осуществлять организационное обеспечение информационной безопасности автоматизированных (информационных) систем в рамках должностных обязанностей техника по защите информации;

Знать:
- основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области;
- правовые основы организации защиты информации, содержащей сведения, составляющие государственную тайну и информации конфиденциального характера, задачи органов защиты государственной тайны;

ПК:
- ПК 1.4. Осуществлять контроль функционирования информационно – телекоммуникационных систем и сетей.
- ПК 3.2. Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации, используемых в информационно – телекоммуникационных системах и сетях.

3. **Подготовка к работе**
   изучить документы
   - «Алгоритм действий оператора ПДн по созданию системы защиты ИСПДн».

   - Акт Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

4. **Задание**
   1. Изучить документ «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных». ФСТЭК России от 15.02.2008 г.
   2. На основании документа «Базовая модель угроз» определяют Модель вероятного нарушителя путём сбора всех возможных категорий нарушителей.
   3. На основании документа «Базовая модель угроз», пп. 6.1-6.6 определить перечень угроз безопасности для конкретной структуры ИСПДн, указанной в Приложении 1 данной методики в пункте таблицы, соответствующему порядковому номеру студента в списке преподавателя.

5. Порядок выполнения работы

Студенты выполняют следующие задания: Изучают категории нарушителей, описанные в документе ФСТЭК России «Базовая модель». Для конкретной информационной системы определяют перечень вероятных нарушителей ИСПДн с учетом всех исключений. Результаты записывают в таблицу (см. таблицу 2). Изучают модели безопасности, описанные в документе ФСТЭК России «Базовая модель». Составляют перечень всех возможных угроз по документу ФСТЭК России «Базовая модель». Результаты записывают в таблицу 3, представленную в виде примера.

6. 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.

7. Контрольные вопросы к защите

- Что такое модель угроз?
- Что такое персональные данные?
- Что такое угроза персональных данных?

Приложение 1

Краткие сведения из теории

Персональные данные (ПДн)– это любая информация о людях. Это могут быть персональные данные сотрудников, данные пациентов (если речь идет о медучреждении), данные граждан (если речь идет о госучреждении) и т.д.

БПДн – безопасность персональных данных.

ПО - программное обеспечение.

Модель угроз (безопасности информации) – физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать 2 уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Информационная система персональных данных (ИСПДн) – это совокупность программных и технических средств (компьютеры, принтеры, сканеры, коммутационное оборудование и т.д.) на которых обрабатываются персональные данные.

АРМ - автоматизированное рабочее место

МИО – международный информационный обмен.

ИСПДн-С - информационная система, обрабатывающая специальные категории персональных данных, если в ней обрабатываются персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных;

ИСПДн-О – информационная система, обрабатывающая общедоступные персональные данные, если в ней обрабатываются персональные данные субъектов персональных данных, полученные только из общедоступных источников персональных данных, созданных в соответствии со статьей 8 Федерального закона "О персональных данных".

ИСПДн-Б - информационная система, обрабатывающая биометрические персональные данные, если в ней обрабатываются сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных, и не обрабатываются сведения, относящиеся к специальным категориям персональных данных.

ИСПДн-И - информационная система, обрабатывающая иные категории персональных данных, если в ней не обрабатываются персональные данные специальные, общедоступные и биометрические.

Практическое занятие 5.

СОСТАВЛЕНИЕ ПЕРЕЧНЯ ЗАЩИЩАЕМЫХ РЕСУРСОВ ПДН

1. Цель работы: рассмотрение основных и наиболее важных моментов при разработке политики «Обработка персональных данных в организации» для выбранной организации в соответствии с требованиями законодательства о ПДн

2. Задачи работы:

- определить принципы, порядок и условия обработки персональных данных (ПДн) абонентов, работников организации и иных лиц, чьи ПДн обрабатываются организацией, а также третьими лицами по поручению организацииСтудент должен:

Уметь:

- осуществлять организационное обеспечение информационной безопасности автоматизированных (информационных) систем в рамках должностных обязанностей техника по защите информации;
- применять нормативные правовые акты и нормативные методические документы в области защиты информации;
- контролировать соблюдение персоналом требований по защите информации при ее обработке с использованием средств вычислительной техники;
- оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации;
- защищать свои права в соответствии с трудовым законодательством

Знать:

- основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области;
- правовые основы организации защиты информации, содержащей сведения, составляющие государственную тайну и информации конфиденциального характера, задачи органов защиты государственной тайны;
- нормативные документы в области обеспечения защиты информации ограниченного доступа;
- организацию ремонтного обслуживания аппаратуры и средств защиты информации;
- принципы и методы организационной защиты информации, организационное обеспечение информационной безопасности в организации;
- правовое положение субъектов правоотношений в сфере профессиональной деятельности (включая предпринимательскую деятельность);
- нормативные методические документы, регламентирующие порядок выполнения мероприятий по защите информации, обрабатываемой в автоматизированной (информационной) системе;
- законодательные и нормативные правовые акты, регламентирующие трудовые правоотношения.

ПК:

- ПК 1.4. Осуществлять контроль функционирования информационно – телекоммуникационных систем и сетей.
- ПК 3.2. Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации, используемых в информационно – телекоммуникационных системах и сетях.

3. Подготовка к работе

Повторите основные свойства и особенности защиты персональных данных

4. Задание

- Внимательно изучите теоритические сведения о перечне защищаемых ресурсов ПДн.
- Рассмотрите основные принципы работы с ПДн.

5. Порядок выполнения работы

Изучите:

- При каких случаях допускается обработка ПДн в организации.
- С какими целями выполняется обработка ПДн в организации.
- Кем может осуществляться обработка данных.
- Как достигается обеспечение безопасности ПДн.
- Типовую форму ПДн.
- Что такое автоматизированная система и неавтоматизированная обработка.

6. Содержание отчета

1. Название, цель работы
2. Изучение и знание теоритического материала
3. Ответы на вопросы
4. Выводы по работе

7. Контрольные вопросы к защите

1. Что такое безопасность персональных данных?
2. Что такое автоматизированная система и неавтоматизированная обработка?
3. Что такое перечень ресурсов?

Приложение 1

Краткие сведения из теории

Абонент – физическое или юридическое лицо, с которым заключен Договор о предоставлении услуг связи;

Персональные данные (ПДн) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных); **Биометрические персональные данные –** сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных;

Оператор персональных данных – государственный орган, муниципальный орган, юридическое или физическое 13 лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц; Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

Информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

Трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу;

Вопросы для самопроверки самостоятельной работы и вопросы для защиты ПЗ

Практическое занятие 6.
КЛАССИФИКАЦИЯ ИСПДН

1. **Цель работы**: освоение навыков в области тайны защиты информации, изучение политики безопасности.
2. **Задачи работы:**
   - классифицировать защищаемую информацию по конфиденциальности;
   - определить категории лиц, имеющих доступ к защищаемой информации и ресурсам.

Студент должен:
Уметь:

- осуществлять организационное обеспечение информационной безопасности автоматизированных (информационных) систем в рамках должностных обязанностей техника по защите информации;
- применять нормативные правовые акты и нормативные методические документы в области защиты информации;
- контролировать соблюдение персоналом требований по защите информации при ее обработке с использованием средств вычислительной техники;
- оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации;
- защищать свои права в соответствии с трудовым законодательством

Знать:

- основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области;
- правовые основы организации защиты информации, содержащей сведения, составляющие государственную тайну и информации конфиденциального характера, задачи органов защиты государственной тайны;
- нормативные документы в области обеспечения защиты информации ограниченного доступа;
- организацию ремонтного обслуживания аппаратуры и средств защиты информации;
- принципы и методы организационной защиты информации, организационное обеспечение информационной безопасности в организации;
- правовое положение субъектов правоотношений в сфере профессиональной деятельности (включая предпринимательскую деятельность);
- нормативные методические документы, регламентирующие порядок выполнения мероприятий по защите информации, обрабатываемой в автоматизированной (информационной) системе;
- законодательные и нормативные правовые акты, регламентирующие трудовые правоотношения.

ПК:

- ПК 1.4. Осуществлять контроль функционирования информационно – телекоммуникационных систем и сетей.
- ПК 3.2. Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации, используемых в информационно – телекоммуникационных системах и сетях.

3. **Подготовка к работе**

Перед началом работы рекомендуется ознакомиться с теоритическими сведениями: о государственной тайне, коммерческой тайне, персональными данными, базами данных.

4. **Задание**

1) Повторить теоретические вопросы о категорировании информации
2) 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 3. Перечень законов по информационной безопасности приведён в Приложении 1.
3) Ответьте на вопросы по теоретическому материалу.

5. Порядок выполнения работы

1) Изучите теоритическую часть
2) Заполните таблицу по примеру (Таб.3)
3) Ответить те на вопросы по теоретическому материалу.

Таблица 3.

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»

6. Содержание отчета

- Название, цель работы, ход выполнения работы
- Выполнение теоритической части работы
- Выполнение практической части работы, в том числе задание – 2.
- Выводы по работе.

7. Контрольные вопросы к защите

- Конфиденциальная информация это?
- Нормативно-правовые акты?
- Законодательные акты?

Приложение 1

Краткие сведения из теории

Абонентский пункт (АП) - автоматизированная система, подключаемая к Сети с помощью коммуникационного оборудования и прёдназначенная для работы абонента Сети.

Защищаемые помещения (ЗП) - помещения (служебные кабинеты, актовые, конференц-залы и т.д.), специально предназначенные для проведения конфиденциальных мероприятий (совещаний, обсуждений, конференций, переговоров и т.п.).

Контролируемая зона (КЗ) - это пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание сотрудников и посетителей организации, а также транспортных средств.

Информация с ограниченным доступом	Нормативные и законодательные акты
Государственная тайна	Закон РФ «О государственной тайне», ст. 275, 276, 283, 284 УК РФ
Конфиденциальная информация	Ст. 10 ФЗ «Об информации, информатизации и защите информации»
Персональные данные	Ст. 11 ФЗ «Об информации, информатизации и защите информации»
Личная и семейная тайна	Ст. 23 Конституции Российской Федерации, ст. 11 ФЗ «Об информации, информатизации и защите информации», ст. 150 Гражданского кодекса Российской Федерации, ст. 137 УК РФ
Служебная тайна	Ст. 139 Гражданского кодекса Российской Федерации, ст. 155, 311 УК РФ
Служебная информация	Ст. 31 ФЗ «О рынке ценных бумаг»
Коммерческая тайна	Ст. 139 Гражданского кодекса Российской Федерации, ст. 183 УК РФ
Сведения о сущности изобретения («ноу-хау»)	Указ Президента Российской Федерации № 188 от 6.03.1997 г. «Об утверждении перечня сведений конфиденциального характера»
Тайна следствия и судопроизводства	Указ Президента Российской Федерации № 188 от 6.03.1997 г. «Об утверждении перечня сведений конфиденциального характера», ст. 310 УК РФ
Тайна связи	Ст. 63 ФЗ «О связи», ст. 11 ФЗ «Об информации, информатизации и защите информации», ст. 138 УК РФ
Тайна страхования	Ст. 946 Гражданского кодекса Российской Федерации
Тайна усыновления	Ст. 139 Семейного кодекса Российской Федерации, ст. 155 УК РФ
Тайна исповеди	Ст. 3 ФЗ «О свободе совести и религиозных объединениях»
Банковская тайна	Ст. 857 Гражданского кодекса Российской Федерации, ст. 26 ФЗ «О внесении изменений и дополнений в Закон РСФСР "О банках и банковской деятельности в РСФСР"», ст. 183 УК РФ
Нотариальная тайна	Ст. 16, 29 Основ законодательства Российской Федерации о нотариате, ст. 202 УК РФ
Адвокатская тайна	Закон РФ «Об адвокатской деятельности и адвокатуре в Российской Федерации»
Врачебная тайна	Ст. 161 Основ законодательства Российской Федерации об охране здоровья граждан, ст. 14 Закона Российской Федерации «О трансплантации органов и (или) тканей человека»

Практическое занятие 7.

РАБОТА С ПРАВОВОЙ ДОКУМЕНТАЦИИ ПО ЛИЦЕНЗИРОВАНИЮ ДЕЯТЕЛЬНОСТИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1. Цель работы: освоить порядок классификации автоматизированных систем в защищенном исполнении и методы правовой защиты информации ограниченного доступа, обрабатываемой в них.

2. Задачи работы:

- понять принципы работы с докуминтацией по лтцензированию деятельностт в области информационной безопасности.Вспомнить теоретический материал по теме.

Студент должен:

Уметь:

- осуществлять организационное обеспечение информационной безопасности автоматизированных (информационных) систем в рамках должностных обязанностей техника по защите информации;
- применять нормативные правовые акты и нормативные методические документы в области защиты информации;
- контролировать соблюдение персоналом требований по защите информации при ее обработке с использованием средств вычислительной техники;
- оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации;
- защищать свои права в соответствии с трудовым законодательством

Знать:

- основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области;
- правовые основы организации защиты информации, содержащей сведения, составляющие государственную тайну и информации конфиденциального характера, задачи органов защиты государственной тайны;
- нормативные документы в области обеспечения защиты информации ограниченного доступа;
- организацию ремонтного обслуживания аппаратуры и средств защиты информации;
- принципы и методы организационной защиты информации, организационное обеспечение информационной безопасности в организации;
- правовое положение субъектов правоотношений в сфере профессиональной деятельности (включая предпринимательскую деятельность);
- нормативные методические документы, регламентирующие порядок выполнения мероприятий по защите информации, обрабатываемой в автоматизированной (информационной) системе;
- законодательные и нормативные правовые акты, регламентирующие трудовые правоотношения.

ПК:

- ПК 1.4. Осуществлять контроль функционирования информационно – телекоммуникационных систем и сетей.
- ПК 3.2. Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации, используемых в информационно – телекоммуникационных системах и сетях.

3. Подготовка к работе

Стоит воспользоваться литературой по теме:

Законы РФ:

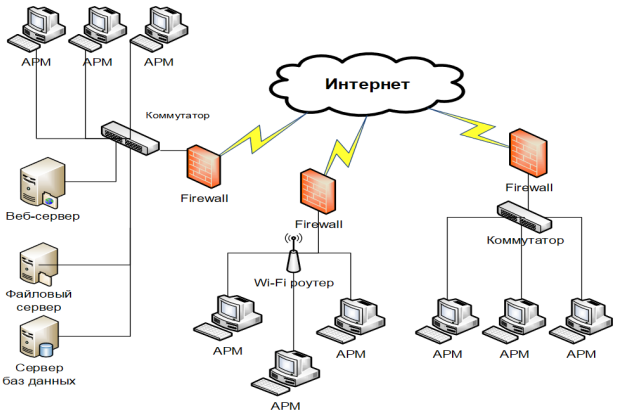
- "О государственной тайне" № 5485-1 от21.07.93;
- "О сертификации продукции и услуг" № 5485-1 от 10.06.93;
- "О защите прав потребителей" № 2300-1 от 07.02.92,
- "Об информации, информатизации и защите информации" № 24-ФЗ от 20.02.95;
- "О стандартизации" № 5154-1 от 10.06.93.
- "О федеральных органах правительственной связи и информации" № 4524-1 от 19.02.93.

Постановления Правительства РФ:

- "О лицензировании отдельных видов деятельности" № 1418 от 24.12.94;
- "О лицензировании деятельности предприятий..." № 333 от 15.04.95;
- "О сертификации средств ЗИ" № 608 от 26.06.95.

4. Задание

Разработать структурную схему АС для предприятия / организации /
Пример структурной схемы АС приведен на рисунке 2.3



5. Порядок выполнения работы

прописать последовательность выполнения работы, формулы, таблицы, графики

6. 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.

7. Контрольные вопросы к защите

1. РД «Автоматизированные системы. Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по
защите информации» от 30 марта 1992 г.
2. РД «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации» от 30
марта 1992 г.
3. Что представляет собой документ «Политика безопасности»?
4. Выполнение каких правил безопасности обеспечивается путем реализации «Политики безопасности»?
5. В каких документах представлены нормы правового обеспечения защиты информации в АС?

6. Какие документы необходимо представить для присвоения класса защищенности?
7. Какие классификационные признаки являются определяющими при установлении класса АС?
8. Сколько классов АС существует и чем они различаются?
9. От чего зависит выбор класса защищенности СВТ для АС, создаваемых на базе защищенных СВТ?
10. Где указаны требования к безопасности компьютерных сетей в РФ?

Практическое занятие 8.

РАБОТА С НОРМАТИВНОЙ ДОКУМЕНТАЦИИ ПО ЛИЦЕНЗИРОВАНИЮ ДЕЯТЕЛЬНОСТИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1. **Цель работы**: закрепление теоретических знаний по вопросам государственного лицензирования деятельности в области защиты информации
2. **Задачи работы:**
   - понять принципы работы с докуминтацией по лицензированию деятельности в области информационной безопасности.Вспомнить теоретический материал по теме.

Студент должен:

Уметь:

- осуществлять организационное обеспечение информационной безопасности автоматизированных (информационных) систем в рамках должностных обязанностей техника по защите информации;
- применять нормативные правовые акты и нормативные методические документы в области защиты информации;
- контролировать соблюдение персоналом требований по защите информации при ее обработке с использованием средств вычислительной техники;
- оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации;
- защищать свои права в соответствии с трудовым законодательством

Знать:

- основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области;
- правовые основы организации защиты информации, содержащей сведения, составляющие государственную тайну и информации конфиденциального характера, задачи органов защиты государственной тайны;
- нормативные документы в области обеспечения защиты информации ограниченного доступа;
- организацию ремонтного обслуживания аппаратуры и средств защиты информации;
- принципы и методы организационной защиты информации, организационное обеспечение информационной безопасности в организации;
- правовое положение субъектов правоотношений в сфере профессиональной деятельности (включая предпринимательскую деятельность);
- нормативные методические документы, регламентирующие порядок выполнения мероприятий по защите информации, обрабатываемой в автоматизированной (информационной) системе;
- законодательные и нормативные правовые акты, регламентирующие трудовые правоотношения.

ПК:

- ПК 1.4. Осуществлять контроль функционирования информационно – телекоммуникационных систем и сетей.
- ПК 3.2. Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации, используемых в информационно – телекоммуникационных системах и сетях.

3. **Подготовка к работе**

изучить учебные материалы темы №2 «Государственное лицензирование деятельности в области защиты информации», используя литературу [1, с.45-55; 2-8], а также конспект лекций.

При подготовке к практическому занятию студентам рекомендуется ответить на контрольные вопросы:

- Сформулируйте основные понятия, принятые в сфере государственного лицензирования в области защиты информации.
- Организационная структура системы государственного лицензирования в области защиты информации.
- Функции государственных органов по лицензированию в области защиты информации.
- Функции лицензионных центров по лицензированию в области защиты информации.
- Права и обязанности лицензиатов.
- Порядок проведения лицензирования и контроля за деятельностью лицензиатов.
- Назовите случаи приостановления или прекращения действия лицензии.
- В каких случаях предприятию отказывают в выдаче лицензии?
- Какие документы предоставляются для получения лицензии?
- Каковы особенности лицензирования деятельности по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах?
- Какие средства относятся к шифровальным?
- Каковы особенности лицензирования видов деятельности, связанных с шифровальными (криптографическими) средствами?
- Назовите лицензионные требования и условия при распространении шифровальных (криптографических) средств.
- Назовите лицензионные требования и условия при осуществлении разработки, производства шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем.
- Назовите лицензионные требования и условия при предоставлении услуг в области шифрования информации.
- Назовите лицензионные требования и условия при осуществлении деятельности по техническому обслуживанию шифровальных (криптографических) средств.

4. Задание

1. Изучить материал по теме «Работа с нормативной документацией по лицензированию деятельности в области информационной безопасности»
2. Воспользоваться литературой:

- Снытников А.А. Лицензирование и сертификация в области защиты информации. – М.: Гелиос АРВ, 2003.
- О лицензировании отдельных видов деятельности: Федеральный закон от 08.08.2001 г. № 128-ФЗ.
- О государственном лицензировании деятельности в области защиты информации: Утв. решением Государственной технической комиссии при Президенте Российской Федерации и Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 27 апреля 1994 г. №10 (с изменениями и дополнениями от 24 июня 1997 г. №60).
- О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны: Постановление Правительства Российской Федерации от 15 апреля 1995 г. №333.

- Об организации лицензирования отдельных видов деятельности: Постановление Правительства Российской Федерации от 26 января 2006 г. №45.
- О лицензировании деятельности по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах: Постановление Правительства Российской Федерации от 22 октября 2007 г. №689.
- О лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами: Постановление Правительства Российской Федерации от 29 декабря 2007 г. №957.
- О лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации: Постановление Правительства Российской Федерации от 31 августа 2006 г. №532.

5. Порядок выполнения работы

1. Прочитать предложенную выше литературу.
2. Проанализировать прочитанный материал.
3. Так же важно изучить основыные термины по теме.

6. 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.

7. Контрольные вопросы к защите

1. Организационная структура системы государственного лицензирования в области защиты информации.
2. Общий порядок проведения лицензирования в области защиты информации.
3. Контроль за деятельностью лицензиатов.
4. Изучение перечня видов деятельности предприятий в области защиты информации, подлежащих лицензированию.

Практическое занятие 9.
ПОДГОТОВКА ДОКУМЕНТОВ К ПОЛУЧЕНИЮ ЛИЦЕНЗИИ

1. Цель работы: **:** подготовка документов к получению лицензии

2. Задачи работы:

-повторить теоретический материал по теме
- подготовить документы к получению лицензии.

Студент должен:
Уметь:

- осуществлять организационное обеспечение информационной безопасности автоматизированных (информационных) систем в рамках должностных обязанностей техника по защите информации;
- применять нормативные правовые акты и нормативные методические документы в области защиты информации;
- контролировать соблюдение персоналом требований по защите информации при ее обработке с использованием средств вычислительной техники;
- оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации;
- защищать свои права в соответствии с трудовым законодательством

Знать:

- основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области;
- правовые основы организации защиты информации, содержащей сведения, составляющие государственную тайну и информации конфиденциального характера, задачи органов защиты государственной тайны;
- нормативные документы в области обеспечения защиты информации ограниченного доступа;
- организацию ремонтного обслуживания аппаратуры и средств защиты информации;
- принципы и методы организационной защиты информации, организационное обеспечение информационной безопасности в организации;
- правовое положение субъектов правоотношений в сфере профессиональной деятельности (включая предпринимательскую деятельность);
- нормативные методические документы, регламентирующие порядок выполнения мероприятий по защите информации, обрабатываемой в автоматизированной (информационной) системе;
- законодательные и нормативные правовые акты, регламентирующие трудовые правоотношения.

ПК:

- ПК 1.4. Осуществлять контроль функционирования информационно – телекоммуникационных систем и сетей.
- ПК 3.2. Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации, используемых в информационно – телекоммуникационных системах и сетях.

3. Подготовка к работе

При подготовке к практическому занятию студентам рекомендуется повторить материал
1. Организационная структура системы государственного лицензирования в области защиты информации.
2. Общий порядок проведения лицензирования в области защиты информации.

3. Контроль за деятельностью лицензиатов.
4. Изучение перечня видов деятельности предприятий в области защиты информации, подлежащих
лицензированию.
5. Функции государственных органов по лицензированию в области защиты информации.
6. Назовите случаи приостановления или прекращения действия лицензии.

4. Задание

- Используя справочно-правовые системы ознакомиться с нормативно-правовыми актами, регулирующими лицензирование отдельных видов предпринимательской деятельности (найти минимум 3 вида деятельности).
- Используя открытые источники, в том числе интернет-источники, выяснить расценки на лицензии
конкретных видов деятельности.
- Составить заявление о предоставлении лицензии на деятельность по технической защите конфиденциальной информации юридическому лицу.
• Предварительно ознакомьтесь с деятельность, связанной с технической защитой конфиденциальной
информации, выбрать для заявления какой-то конкретный вид деятельности.
• Оформить заявление в соответствии с требованиями (или воспользовавшись образцом)

5. Порядок выполнения работы

1. Прочитать предложенную литературу.
2. Проанализировать прочитанный материал.
3. Так же важно изучить основные термины по теме.
4. Выполнить практическое задание.

6. 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.

7. Контрольные вопросы к защите

1. Что такое лицензия?
2. Что таоке техническая защита?
3. Для чего нужна лицензия в области защиты информации

Практическое занятие 10.
ПОДГОТОВКА ОБЪЕКТА К АТТЕСТАЦИИ. ИЗУЧЕНИЕ ТИПОВЫХ ФОРМ ДОКУМЕНТОВ

1. Цель работы: записать цель работы с учетом умений соответствующих рабочей программе учебной дисциплины (профессионального модуля)

2. Задачи работы:

- сформировать систему объектов информатизации по требованиям безопасности информации.
- определять виды аттестации объектов информатизации по требованиям безопасности информации.

Студент должен:
Уметь:

- осуществлять организационное обеспечение информационной безопасности автоматизированных (информационных) систем в рамках должностных обязанностей техника по защите информации;
- применять нормативные правовые акты и нормативные методические документы в области защиты информации;
- контролировать соблюдение персоналом требований по защите информации при ее обработке с использованием средств вычислительной техники;
- оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации;
- защищать свои права в соответствии с трудовым законодательством

Знать:

- основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области;
- правовые основы организации защиты информации, содержащей сведения, составляющие государственную тайну и информации конфиденциального характера, задачи органов защиты государственной тайны;
- нормативные документы в области обеспечения защиты информации ограниченного доступа;
- организацию ремонтного обслуживания аппаратуры и средств защиты информации;
- принципы и методы организационной защиты информации, организационное обеспечение информационной безопасности в организации;
- правовое положение субъектов правоотношений в сфере профессиональной деятельности (включая предпринимательскую деятельность);
- нормативные методические документы, регламентирующие порядок выполнения мероприятий по защите информации, обрабатываемой в автоматизированной (информационной) системе;
- законодательные и нормативные правовые акты, регламентирующие трудовые правоотношения.

ПК:

- ПК 1.4. Осуществлять контроль функционирования информационно – телекоммуникационных систем и сетей.
- ПК 3.2. Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации, используемых в информационно – телекоммуникационных системах и сетях.

3. Подготовка к работе

Изучить

1. Функции ФСТЭК и органов по аттестации в области аттестации объектов информатизации по требованиям безопасности информации.
2. Функции испытательных центров (лабораторий) и заявителей по аттестации объектов информатизации по требованиям безопасности информации.
3. Порядок проведения аттестации и контроля.

4. Задание

- Приведите объекты информатизации, которые подлежат обязательной аттестации.
- Опишите порядок проведения аттестации объектов информатизации по требованиям безопасности информации.
- Приведите сведения, на основании которых разрабатывается программа

аттестационных испытаний.

- Перечислите сведения об объекте, представленные в техническом паспорте объекта информатизации.
- Перечислите виды аттестации помещений по требованиям безопасности информации.

5. Порядок выполнения работы

Ознакомьтесь с "Положением об аттестации объектов информатизации по требованиям безопасности". Составьте заявление на аттестацию объекта информатизации по требованиям безопасности. Аналогично предыдущим работам подберите себе объект информатизации для аттестации и для него составьте заявление на аттестацию.

6. 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.

7. Контрольные вопросы к защите

Ознакомьтесь с "Положением об аттестации объектов информатизации по требованиям безопасности". Что такое аттестация? Каковы функции ФСТЭК?

Практическое занятие 11. ПОДГОТОВКА ДОКУМЕНТОВ К АТТЕСТАЦИИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

1. **Цель работы**: закрепить теоретических знаний по вопросам аттестации объектов информатизации
2. **Задачи работы:**
   - Закрепление теоретических знаний по теме аттестации объектов информатизации по требованиям безопасности информации.
   - Закрепление теоретических знаний по теме государственного лицензирования деятельности в области защиты информации.

Студент должен:

Уметь:

- осуществлять организационное обеспечение информационной безопасности автоматизированных (информационных) систем в рамках должностных обязанностей техника по защите информации;
- применять нормативные правовые акты и нормативные методические документы в области защиты информации;
- контролировать соблюдение персоналом требований по защите информации при ее обработке с использованием средств вычислительной техники;
- оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации;
- защищать свои права в соответствии с трудовым законодательством

Знать:

- основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области;
- правовые основы организации защиты информации, содержащей сведения, составляющие государственную тайну и информации конфиденциального характера, задачи органов защиты государственной тайны;
- нормативные документы в области обеспечения защиты информации ограниченного доступа;
- организацию ремонтного обслуживания аппаратуры и средств защиты информации;
- принципы и методы организационной защиты информации, организационное обеспечение информационной безопасности в организации;
- правовое положение субъектов правоотношений в сфере профессиональной деятельности (включая предпринимательскую деятельность);
- нормативные методические документы, регламентирующие порядок выполнения мероприятий по защите информации, обрабатываемой в автоматизированной (информационной) системе;
- законодательные и нормативные правовые акты, регламентирующие трудовые правоотношения.

ПК:

- ПК 1.4. Осуществлять контроль функционирования информационно – телекоммуникационных систем и сетей.
- ПК 3.2. Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации, используемых в информационно – телекоммуникационных системах и сетях.

3. **Подготовка к работе**

1. Воспользоваться литературой:

ГОСТ Р 50922-2006. Защита информации. Основные термины и определения; Рекомендации по стандартизации Р 50.1.056-2005. Техническая защита информации. Основные термины и определения; Постановление Правительства Российской Федерации от 03.02.2012 No 79 «О лицензировании деятельности по технической защите конфиденциальной информации»; Федеральный закон от 04.05.2011 No 99-ФЗ «О лицензировании отдельных видов деятельности»

4. Задание

1. Изучить материал по теме : Подготовка документов к аттестации объектов информатизации.
2. Подготовить реферат:

Темы рефератов:

1. Лицензирование деятельности в области защиты государственной тайны.
2. Особенности лицензирования деятельности в области защиты информации, составляющей государственную тайну.
3. Общий порядок проведения лицензирования в области защиты информации.
4. Система сертификации средств защиты информации по требованиям безопасности информации.
5. Система сертификации средств криптографической защиты информации.
6. Виды аттестации помещений по требованиям безопасности информации.

5. Порядок выполнения работы

1. Прочитать предложенную выше литературу.
2. Проанализировать прочитанный материал.
3. Подготовить реферат на одну из предложенных тем.

6. 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.

7. Контрольные вопросы к защите

1. Перечень видов деятельности, на осуществление которых требуется лицензия.
2. Органы, уполномоченные на ведение лицензионной деятельности.
3. Основные принципы, организационная структура и порядок проведения аттестации.
4. Какие объекты информатизации подлежат обязательной аттестации.
5. Основные принципы, организационная структура системы аттестации объектов информатизации по требованиям безопасности информации. Орган по аттестации. Порядок проведения аттестации, а также контроля и надзора за аттестацией и эксплуатацией аттестованных объектов информатизации. Правовой статус аттестата соответствия. Подача апелляции.

Практическое занятие 12.
ПОДГОТОВКИ ДОКУМЕНТОВ К СЕРТИФИКАЦИИ

1. Цель работы: ознакомиться с правилами проведения сертификации информационно – программных средств

2. Задачи работы:

− научиться сертифицировать информацию

Студент должен:
Уметь:

- осуществлять организационное обеспечение информационной безопасности автоматизированных (информационных) систем в рамках должностных обязанностей техника по защите информации;
- применять нормативные правовые акты и нормативные методические документы в области защиты информации;
- контролировать соблюдение персоналом требований по защите информации при ее обработке с использованием средств вычислительной техники;
- оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации;
- защищать свои права в соответствии с трудовым законодательством

Знать:

- основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области;
- правовые основы организации защиты информации, содержащей сведения, составляющие государственную тайну и информации конфиденциального характера, задачи органов защиты государственной тайны;
- нормативные документы в области обеспечения защиты информации ограниченного доступа;
- организацию ремонтного обслуживания аппаратуры и средств защиты информации;
- принципы и методы организационной защиты информации, организационное обеспечение информационной безопасности в организации;
- правовое положение субъектов правоотношений в сфере профессиональной деятельности (включая предпринимательскую деятельность);
- нормативные методические документы, регламентирующие порядок выполнения мероприятий по защите информации, обрабатываемой в автоматизированной (информационной) системе;
- законодательные и нормативные правовые акты, регламентирующие трудовые правоотношения.

ПК:

- ПК 1.4. Осуществлять контроль функционирования информационно – телекоммуникационных систем и сетей.
- ПК 3.2. Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации, используемых в информационно – телекоммуникационных системах и сетях.

3. Подготовка к работе

По конспекту лекций, материалу, данному в приложении и указанной литературе изучить правила проведения сертификации информационно – программных средств. Ответить на контрольные вопросы.

4. Задание

Изучить порядок проведения сертификации информационно – программных средств. Разработать порядок проведения сертификации информационно – программных средств для своего варианта. Заполнить форму заявки на проведение сертификации продукции. Составить отчет по форме о проделанной работе.

5. Порядок выполнения работы

Получить допуск к работе. Выполнить задание.

6. 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.

7. Контрольные вопросы к защите

1. Что такое сертификация?
2. Какой орган проводит сертификацию предприятия?

Приложение 1

Краткие сведения из теории

Сертификация продукции – вид деятельности по оценке соответствия продукции стандартам, регламентам, техническим условиям и другой документации. В России действуют различные виды сертификации, то есть системы подтверждения качества. Наиболее востребованной является сертификация ГОСТ Р. Сертификация ГОСТ Р включает в себя систему добровольной и обязательной сертификации. Добровольное подтверждение соответствия осуществляется в форме добровольной сертификации.

Практическое занятие 13.
ВЫПОЛНЕНИЕ АНАЛИЗА ПРЕДПРИЯТИЯ НА ПРЕДМЕТ ДЕЯТЕЛЬНОСТИ

1. **Цель работы**: научиться анализировать предприятия на предмет деятельности
2. **Задачи работы:**
   - проводить анализ предприятия на предмет деятельности и уметь решать таблицы

Студент должен:

Уметь:

- осуществлять организационное обеспечение информационной безопасности автоматизированных (информационных) систем в рамках должностных обязанностей техника по защите информации;
- применять нормативные правовые акты и нормативные методические документы в области защиты информации;
- контролировать соблюдение персоналом требований по защите информации при ее обработке с использованием средств вычислительной техники;
- оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации;
- защищать свои права в соответствии с трудовым законодательством

Знать:

- основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области;
- правовые основы организации защиты информации, содержащей сведения, составляющие государственную тайну и информации конфиденциального характера, задачи органов защиты государственной тайны;
- нормативные документы в области обеспечения защиты информации ограниченного доступа;
- организацию ремонтного обслуживания аппаратуры и средств защиты информации;
- принципы и методы организационной защиты информации, организационное обеспечение информационной безопасности в организации;
- правовое положение субъектов правоотношений в сфере профессиональной деятельности (включая предпринимательскую деятельность);
- нормативные методические документы, регламентирующие порядок выполнения мероприятий по защите информации, обрабатываемой в автоматизированной (информационной) системе;
- законодательные и нормативные правовые акты, регламентирующие трудовые правоотношения.

ПК:

- ПК 1.4. Осуществлять контроль функционирования информационно – телекоммуникационных систем и сетей.
- ПК 3.2. Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации, используемых в информационно – телекоммуникационных системах и сетях.

3. Подготовка к работе

Показатели организационно-технического уровня:

1. Показатели состояния уровня техники и технологии:
- Показатели научно-технического уровня производства;
- Показатели уровня технологии производства.
2. Показатели организационного уровня производства:

- Показатели организации производства;
- Показатели уровня управления предприятием;
- Показатели уровня организации и фонда оплаты труда;
- Показатели социальных условий работы коллектива.

4. Задание

Решать и составлять таблицы

- Показатели организационно-технического уровня и методику их расчета.
- Осуществлять расчет технико-экономических показателей и их анализ.

5. Порядок выполнения работы

1. Определить показатели степени механизации, автоматизации производства 2. Провести анализ длительности и структуры производственного цикла, коэффициент непрерывности

6. 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.

7. Контрольные вопросы к защите

- Что такое технико-экономические показатели?
- Что такое организационно-технический уровень?

Приложение 1

Краткие сведения из теории

Для оценки уровня механизации и автоматизации машины и оборудования условно делят на группы (см.табл.8.1)

Таблица 8.1

машины ручного управления	1
простые машины частично механизированные	2а
простые машины полностью механизированные	2в
машины частично автоматизированные	3а
машины полностью автоматизированные	3в
машины автоматизированные и программируемые	4
гибкие и автоматизированные и программируемые системы	5

Практическое занятие 14.
СОСТАВЛЕНИЕ КРИТЕРИЕВ ВИДА ДЕЯТЕЛЬНОСТИ ПРЕДПРИЯТИЯ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1. Цель работы: освоение способов анализа рисков информационной безопасности. Составление критериев вида деятельности предприятия в области информационной безопасности

2. Задачи работы:

- научиться выявлять риски информационной безопаснос
- получить знания на тему: организационно-функциональная структура предприятия.
- идентифицировать и оценить информационные активы
- научиться оценивать уязвимость активов

Студент должен:

Уметь:

- осуществлять организационное обеспечение информационной безопасности автоматизированных (информационных) систем в рамках должностных обязанностей техника по защите информации;
- применять нормативные правовые акты и нормативные методические документы в области защиты информации;
- контролировать соблюдение персоналом требований по защите информации при ее обработке с использованием средств вычислительной техники;
- оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации;
- защищать свои права в соответствии с трудовым законодательством

Знать:

- основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области;
- правовые основы организации защиты информации, содержащей сведения, составляющие государственную тайну и информации конфиденциального характера, задачи органов защиты государственной тайны;
- нормативные документы в области обеспечения защиты информации ограниченного доступа;
- организацию ремонтного обслуживания аппаратуры и средств защиты информации;
- принципы и методы организационной защиты информации, организационное обеспечение информационной безопасности в организации;
- правовое положение субъектов правоотношений в сфере профессиональной деятельности (включая предпринимательскую деятельность);
- нормативные методические документы, регламентирующие порядок выполнения мероприятий по защите информации, обрабатываемой в автоматизированной (информационной) системе;
- законодательные и нормативные правовые акты, регламентирующие трудовые правоотношения.

ПК:

- ПК 1.4. Осуществлять контроль функционирования информационно – телекоммуникационных систем и сетей.
- ПК 3.2. Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации, используемых в информационно – телекоммуникационных системах и сетях.

3. Подготовка к работе

В качестве основных компонентов предметной области (в различных сочетаниях) рассматриваются:

- предприятие, фирма, объединение, государственное учреждение и т.д., функционирование которого предусматривает проведение мероприятий по обеспечению информационной безопасности (обеспечению конфиденциальности, целостности и доступности информации);
- система защиты информации предприятия, функционирование которой не в полной мере обеспечивает адекватное реагирование на угрозы информационной безопасности;
- отдельный вид деятельности по обеспечению информационной безопасности, рассматриваемый, как бизнес-процесс, требующий оптимизации.

Стоит вспомнить :

Схему общей организационно-функциональной структуры предприятия, которая бы отражала содержание аппарата управления и объекта управления на предприятии, основные административные и функциональные подразделения предприятия. Схема должна носить целостный характер.В организационной структуре должна соблюдаться логичность представления должностей и подразделений. Например, на втором уровне подчиненности указываются либо должности руководителей, либо названия подразделений.

Риск – комбинация вероятности события и его последствий, (другими словами, риск – это математической ожидание ущерба информационным активам компании). Тем не менее, результат оценивания риска может быть представлен как в форме количественного показателя (тыс. рублей), так и виде качественного: **приемлемый** риск или **неприемлемый** риск. Важно, чтобы управление рисками информационной безопасности осуществлялось четко и последовательно во всей организации.

Информационный актив является компонентом или частью общей системы, в которую организация напрямую вкладывает средства, и который, соответственно, требует защиты со стороны организации. При идентификации активов следует иметь в виду, что всякая система информационных технологий включает в себя не только информацию – сведения, данные, независимо от формы их представления, но и аппаратные средства, программное обеспечение и т.д. Могут существовать следующие типы активов:

- информация/данные (например, файлы, содержащие информацию о платежах или продукте);
- аппаратные средства (например, компьютеры, принтеры);
- программное обеспечение, включая прикладные программы (например, программы обработки текстов, программы целевого назначения);
- оборудование для обеспечения связи (например, телефоны, медные и оптоволоконные кабели);
- программно-аппаратные средства (например, гибкие магнитные диски, CD-ROM, программируемые ROM);
- документы (например, контракты);
- фонды (например, в банковских автоматах);
- продукция организации;
- услуги (например, информационные, вычислительные услуги);
- конфиденциальность и доверие при оказании услуг (например, услуг по совершению платежей);
- - оборудование, обеспечивающее необходимые условия работы;
- - персонал организации;
- - престиж (имидж) организации.

На этапе подготовки к практическому занятию студенты должны, используя литературу углубить свои знания по методам оценки уязвимости информации. Необходимо провести идентификацию уязвимостей окружающей среды, организации, процедур, персонала, менеджмента, администрации, аппаратных средств, программного обеспечения или аппаратуры связи, которые могли бы быть использованы источником угроз для нанесения ущерба активам и деловой деятельности организации, осуществляемой с их использованием.

4. Задание

1. Изучить материал по теме „ Методика оценки уязвимости информации“
2. Воспользоваться литературой: 1. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах: Учебное пособие для вузов. – 3-е издание. – М.: Горячая линия-Телеком, 2005.

5. Порядок выполнения работы

1. Прочитать предложенную выше литературу.
2. Проанализировать прочитанный материал.
3. Так же важно изучить основыные термины по теме.

6. 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.

7. Контрольные вопросы к защите

1. Дайте определения безопасности информации, уязвимости информации, защищенности информации, угрозам безопасности информации, защите информации.Перечислите источники угроз безопасности информации.
2. Охарактеризуйте основные принципы системной классификации угроз безопасности информации.
3. Поясните суть методики оценки уязвимости информации

Приложение 1

Краткие сведения из теории

Показатель эффективности представляет собой количественную (реже качественную) меру, позволяющую вынести суждение об эффективности функционирования системы защиты информации (дать оценку эффективности процесса). При выборе и/или формировании показателя эффективности следует помнить о том, вне зависимости от содержания процесса, показатель должен иметь ясный физический смысл, то есть размерность показателя должна наглядно отражать сущность оцениваемого процесса, виды расходуемых ресурсов, а также однозначно характеризовать выходной продукт процесса

Выбранная или сформированная количественная мера должна обеспечивать сравнимость результатов. Так, например, показатели, характеризующие скорость обработки информации в зависимости от рассматриваемых программно-аппаратных средств, могут иметь вид: **Мбайт/сек**и**Мбит/сек**, а выходная характеристика одного и того же процесса в зависимости от выбора продолжительности отчетного периода, может иметь размерность:**количество документов/месяц**,**количество документов/квартал**,**количество документов/год**. Очевидно, что сравнение численных значений показателей, имеющих разную размерность недопустимо.

Результаты ранжирования активов

Наименование актива	**Ценность актива (ранг)**
Информационный актив №1	**1**
Физический актив № 3	**1**
…	…
Информационный актив №3	**4**
Актив программного обеспечения №2	**5**
Физический актив №4	**5**

угроза – это потенциальная причина инцидента, который может нанести ущерб системе или организации, а инцидент, (**инцидент информационной безопасности)** – это любое непредвиденное или нежелательное событие, которое может нарушить деятельность организации или информационную безопасность

Практическое занятие 15.
СОСТАВЛЕНИЕ ТРУДОВОГО ДОГОВОРА СОТРУДНИКА СЛУЖБЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1. **Цель работы**: Разработка должностных инструкций для лиц, ответственных за обеспечение информационной безопасности.
2. **Задачи работы:**

- узнать о требованиях к составлению трудового договора для сотрудника службы информационной безопасности.

Студент должен:

Уметь:

- осуществлять организационное обеспечение информационной безопасности автоматизированных (информационных) систем в рамках должностных обязанностей техника по защите информации;
- применять нормативные правовые акты и нормативные методические документы в области защиты информации;
- контролировать соблюдение персоналом требований по защите информации при ее обработке с использованием средств вычислительной техники;
- оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации;
- защищать свои права в соответствии с трудовым законодательством

Знать:

- основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области;
- правовые основы организации защиты информации, содержащей сведения, составляющие государственную тайну и информации конфиденциального характера, задачи органов защиты государственной тайны;
- нормативные документы в области обеспечения защиты информации ограниченного доступа;
- организацию ремонтного обслуживания аппаратуры и средств защиты информации;
- принципы и методы организационной защиты информации, организационное обеспечение информационной безопасности в организации;
- правовое положение субъектов правоотношений в сфере профессиональной деятельности (включая предпринимательскую деятельность);
- нормативные методические документы, регламентирующие порядок выполнения мероприятий по защите информации, обрабатываемой в автоматизированной (информационной) системе;
- законодательные и нормативные правовые акты, регламентирующие трудовые правоотношения.

ПК:

- ПК 1.4. Осуществлять контроль функционирования информационно – телекоммуникационных систем и сетей.
- ПК 3.2. Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации, используемых в информационно – телекоммуникационных системах и сетях.

3. **Подготовка к работе**

Стоит узнать:

Основными задачами службы безопасности предприятия являются:

- обеспечение безопасности производственно-торговой деятельности и защиты информации и сведений, являющихся коммерческой тайной;
- организация работы по правовой, организационной и инженерно-технической (физической, аппаратной, программной и математической) защите коммерческой тайны;
- организация специального делопроизводства, исключающего несанкционированное получение сведений, являющихся коммерческой тайной;
- предотвращение необоснованного допуска и доступа к сведениям и работам, составляющим коммерческую тайну;
- выявление и локализации возможных каналов утечки конфиденциальной информации в процессе повседневной производственной деятельности и в экстремальных (аварийных, пожарных и др.) ситуациях;
- обеспечение режима безопасности при проведении всех видов деятельности, включая различные встречи, переговоры, совещания, заседания, связанные с деловым сотрудничеством как на национальном, так и на международном уровне;
- обеспечение охраны зданий, помещений, оборудования, продукции и технических средств обеспечения производственной деятельности;
- обеспечение личной безопасности руководства и ведущих сотрудников и специалистов;
- оценка маркетинговых ситуаций и неправомерных действий злоумышленников и конкурентов.

Служба безопасности предприятия выполняет следующие общие функции:

- организует и обеспечивает пропускной и внутриобъектовый режим в зданиях и помещениях, порядок несения службы охраны, контролирует соблюдение требований режима сотрудниками, смежниками, партнерами и посетителями;
- руководит работами по правовому и организационному регулированию отношений по защите коммерческой тайны;
- участвует в разработке основополагающих документов с целью закрепления в них требований обеспечения безопасности и защиты коммерческой тайны, в частности, Устава, Коллективного договора, Правил внутреннего трудового распорядка, Положений о подразделениях, а также трудовых договоров, соглашений, подрядов, должностных инструкций и обязанностей руководства, специалистов, рабочих и служащих;
- разрабатывает и осуществляет совместно с другими подразделениями мероприятия по обеспечению работы с документами, содержащими сведения, являющиеся коммерческой тайной, при всех видах работ организует и контролирует выполнение требований «ИНСТРУКЦИИ по защите коммерческой тайны»;
- изучает все стороны коммерческой, производственной, финансовой и другой деятельности для выявления и закрытия возможных каналов утечки конфиденциальной информации, ведет учет и анализ нарушений режима безопасности, накапливает и анализирует данные о злоумышленных устремлениях конкурентов и других организаций, о деятельности предприятия и его клиентов, партнеров, смежников;
- организует и проводит служебные расследования по фактам разглашения сведений, утрат документов и других нарушений безопасности предприятия; разрабатывает, ведет, обновляет и пополняет «Перечень сведений, составляющих коммерческую тайну» и другие нормативные акты, регламентирующие порядок обеспечения безопасности и защиты информации;
- обеспечивает строгое выполнение требований нормативных документов по защите коммерческой тайны;

- осуществляет руководство службами и подразделениями безопасности подведомственных предприятий, организаций, учреждений и других в части оговоренных в договорах условиях по защите коммерческой тайны;
- организует и регулярно проводит учебу сотрудников предприятия и службы безопасности по всем направлениям защиты коммерческой тайны, добиваясь, чтобы к защите коммерческих секретов был осознанный подход;
- ведет учет сейфов, металлических шкафов, специальных хранилищ и других помещений, в которых разрешено постоянное или временное хранение конфиденциальных документов;
- ведет учет выделенных для конфиденциальной работы помещений, технических средств в них, обладающих потенциальными каналами утечки информации;
- поддерживает контакты с правоохранительными органами и службами безопасности соседних предприятий в интересах изучения криминогенной обстановки в районе.

4. Задание

1. Изучить учебный материал по данной теме
2. Изучить общие положения, должностные обязанности, права, ответственность сотрудников СБ
3. Разработать должностные инструкции для лиц, ответственных за обеспечение информационной безопасности.

5. Порядок выполнения работы

1. Воспользоваться литературой для изучения материала по теме.

2. Проанализировав прочитанный материал, составить трудовой договор для сотрудника СБ.

6. 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.

Приложение 1

Краткие сведения из теории

Для защиты коммерческих секретов предприятия создают собственные службы безопасности, важной предпосылкой создания которых является разработка их структуры, состава, положений о подразделениях и должностных инструкций для руководящего состава и сотрудников.

Структура службы информационной безопасности

В структуру службы безопасности могут входить:

- директор (заместитель директора) или руководитель, непосредственно подчиненный главе фирмы;
- заместитель начальника службы безопасности — на некоторых предприятиях он руководит физической, а иногда и технической службами охраны;
- аналитик;
- юрист;
- специалисты в области обеспечения безопасности, экономической разведки, промышленной контрразведки;
- технические специалисты, умеющие применять специальную технику для защиты помещений;
- сотрудники физической охраны и пропускного режима (по найму), но подчиненные руководителю службы безопасности).

Условно сотрудников службы информационной безопасности можно разделить по функциональным обязанностям:

Сотрудник группы безопасности. В его обязанности входит обеспечение контроля за защитой наборов данных и программ, помощь пользователям и организация общей поддержки групп управления защитой и менеджмента в своей зоне ответственности. При децентрализованном управлении каждая подсистема ИС имеет своего сотрудника группы безопасности.

Администратор безопасности системы. В его обязанности входит ежемесячное опубликование нововведений в области защиты, новых стандартов, а также контроль за выполнением планов непрерывной работы и восстановления (при необходимости) и за хранением резервных копий.

Администратор безопасности данных. В его обязанности входит реализация и изменение средств защиты данных, контроль за состоянием защиты наборов данных, ужесточение защиты в случае необходимости, а также координирование работы с другими администраторами.

Руководитель группы. В его обязанности входит разработка и поддержка эффективных мер защиты при обработке информации для обеспечения сохранности данных, оборудования и программного обеспечения; контроль за выполнением плана восстановления и общее руководство административными группами в подсистемах ИС (при децентрализованном управлении).