Министерство образования и молодежной политики Свердловской области
государственное автономное профессиональное образовательное учреждение
Свердловской области
«Уральский радиотехнический колледж им. А.С. Попова»

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.03 Организационно – правовое обеспечение информационной безопасности

для специальности среднего профессионального образования

10.02.03 Информационная безопасность автоматизированных систем

программы базовой подготовки

2020 г.

Рабочая программа учебной дисциплины разработана на основе Федерального государственного образовательного стандарта специальности среднего профессионального образования 10.02.03 Информационная безопасность автоматизированных систем

УТВЕРЖДАЮ
Заместитель директора
по учебной работе
_____ Д.В. Колесников
«30» _____06____ 2020 г.

Рекомендована цикловой методической комиссией
«Электронных вычислительных машин»
Протокол от «29»___06____ 2020 г. №__6__
Председатель ЦМК _____Ю.Г. Котова

Разработчик:

Терентьева Ольга Арсеньевна, преподаватель УРТК им. А. С. Попова

Рецензент:

Уймин А. Г., преподаватель УРТК им. А. С. Попова

СОДЕРЖАНИЕ

1. ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.03 Организационно-правовое обеспечение информационной безопасности

1.1. Область применения программы

Рабочая программа учебной дисциплины является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности СПО 10.02.03 Информационная безопасность автоматизированных систем

1.2. Место дисциплины в структуре основной профессиональной образовательной программы: общепрофессиональная дисциплина профессионального цикла

Дисциплина способствует формированию следующих общих и профессиональных компетенций:

- ОК 1. Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности;

- ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество;

- ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.

- ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития;

- ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности;

- ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации;

- ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности;

- ОК 12. Производить инсталляцию и настройку автоматизированных информационных систем, выполнять в автоматизированных информационных системах регламентные работы по обновлению, техническому сопровождению и восстановлению при отказах;

- ПК 1.4. Организовывать мероприятия по охране труда и технике безопасности в процессе эксплуатации автоматизированных систем и средств защиты информации в них;

- ПК 1.5. Вести техническую документацию, связанную с эксплуатацией средств технической защиты и контроля информации в автоматизированных системах;

- ПК 2.4. Участвовать в обеспечении учета, обработки, хранения и передачи конфиденциальной информации;

- ПК 2.6. Применять нормативные правовые акты, нормативно-методические документы по обеспечению информационной безопасности программно-аппаратными средствами;

- ПК 3.5. Применять нормативные правовые акты, нормативно-методические документы по обеспечению информационной безопасности инженерно-техническими средствами.

1.3. Цели и задачи дисциплины – требования к результатам освоения дисциплины

В результате освоения дисциплины обучающийся должен уметь:

-осуществлять организационное и правовое обеспечение информационной безопасности телекоммуникационных систем в рамках должностных обязанностей техника по защите информации;

-применять нормативные правовые акты и нормативные методические документы в области защиты информации;

-выявлять каналы утечки информации на объекте защиты;

-контролировать соблюдение персоналом требований режима защиты информации;

-оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации;

-защищать свои права в соответствии с трудовым законодательством.

В результате освоения дисциплины обучающийся должен 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 государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны;

-правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации;

-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).

1.4. Количество часов на освоение программы дисциплины:

максимальной учебной нагрузки обучающегося - 96 часов, в том числе:

- обязательной аудиторной учебной нагрузки обучающегося - 64 часа;
- самостоятельной работы обучающегося - 32 часа.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	***Объем часов***
Максимальная учебная нагрузка (всего)	96
Обязательная аудиторная учебная нагрузка (всего)	64
в том числе:	
практические занятия	20
Самостоятельная работа обучающегося (всего)	32
в том числе:	
Домашняя работа: оформление результатов практических работ, поиск и анализ информации по вопросам правового регулирования организации и применения наемного труда	32
Итоговая аттестация в форме дифференцированного зачета	

2.2. Тематический план и содержание учебной дисциплины ОП.03 Организационно-правовое обеспечение информационной безопасности»

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся, курсовая работ (проект) *(если предусмотрены)*	Объем часов	Уровень освоения
1	2	3	4
Раздел 1. Организационное и правовое обеспечение информационной безопасности автоматизированных и телекоммуникационных систем		**14**	
Тема 1.1. Принципы и методы защиты информации	**Содержание учебного материала**	2	
	1 Введение. Классификация методов обеспечения информационной безопасности. Организационные, правовые, программно-технические, формальные и неформальные средства защиты информации.		2
	2 Принципы и методы организационно-правовой защиты информации.		2
	3 Взаимосвязь мер противодействия угрозам безопасности: правовых, организационных, технологических, физических и технических.		3
	Практические занятия	2	
	1 Классификация методов обеспечения информационной безопасности.		
	Самостоятельная работа обучающихся: подготовка к защите практической работы	2	
Тема 1.2. Организационно-правовое обеспечение информационной безопасности	**Содержание учебного материала**	4	
	1 Организационные и правовые методы защиты информации		2
	2 Лицензирование деятельности предприятий в области защиты информации		3
	3 Сертификация средств защиты информации		3
	4 Аттестация объектов информатизации по требованиям безопасности информации.		3
	5 Деятельность Федеральной службы технического и экспортного контроля (ФСТЭК России), Федеральной службы безопасности (ФСБ) в области информационной безопасности		2
	Практические занятия	2	
	1 Применение организационно-правовых и технических мер по противодействию угрозе безопасности информации		
	Самостоятельная работа обучающихся: Изучение взаимосвязи мер противодействия угрозам безопасности. Подготовка к защите практической работы	2	
Раздел 2.Нормативные правовые акты и нормативные методические документы в области информационной безопасности и защиты информации		**50**	

1	2		3	4
Тема 2.1. Законодательные акты в области информационной безопасности и защиты информации	**Содержание учебного материала**		4	
	1	Доктрина информационной безопасности Российской Федерации. Концепция национальной безопасности Российской Федерации		1
	2	Конституция Российской Федерации		1
	3	Закон РФ «О безопасности»		1
	4	Федеральный закон "Об информации, информационных технологиях и о защите информации"		3
	5	Закон РФ «О государственной тайне»		3
	6	Федеральный закон «О коммерческой тайне»		3
	7	Федеральный закон «О персональных данных»		2
	8	Федеральный закон «О техническом регулировании»		1
	9	Федеральный закон «Об обеспечении единства измерений»		1
	10	Федеральный закон «Об электронной подписи»		1
	11	Федеральный закон «О связи»		1
	12	Федеральный закон «О лицензировании отдельных видов деятельности»		2
	13	Федеральный закон «Об органах Федеральной Службы Безопасности в Российской Федерации»		2
	Практические занятия		2	
	1	Классификация информации, подлежащей защите		
	Самостоятельная работа обучающихся Анализ динамики уровня информатизации общества. Изучение понятий и терминов, закрепленных в законодательных актах в области информационной безопасности и защиты информации. Подготовка к защите практической работы		2	
Тема 2.2. Нормативные правовые акты президента Российской Федерации в области информационной безопасности и защиты информации	**Содержание учебного материала**		2	
	1	Указ президента «Об основах государственной политики в сфере информатизации»		1
	2	Указ президента "Вопросы Межведомственной комиссии по защите государственной тайны"		2
	3	Указ президента «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена"		2
	4	Указ президента "Об утверждении перечня сведений конфиденциального характера"		3
	5	Указ Президента "Об утверждении перечня сведений, отнесенных к государственной тайне"		3
	6	Указ президента "Вопросы Федеральной службы безопасности Российской Федерации"		3
	7	Указ президента "Вопросы федеральной службы по техническому и экспортному контролю"		3
	Практические занятия		2	
	1	Организация работы по определению состава, засекречиванию и рассекречиванию конфиденциальной информации		
	Самостоятельная работа обучающихся Изучение терминов и понятий, закрепленных в нормативных правовых актах президента Российской Федерации в области информационной безопасности и защиты информации. Оформление отчета по практической работ. Подготовка к защите практической работы.		2	

1	2		3	4
Тема 2.3. Постановления правительства Российской Федерации в области информационной безопасности	**Содержание учебного материала**		4	
	1	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		3
	2	Положение о сертификации средств защиты информации		3
	3	Об организации лицензирования отдельных видов деятельности		3
	4	Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти		2
	5	О лицензировании деятельности по технической защите конфиденциальной информации		2
	6	Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных		2
	7	Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами		3
	8	Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных		3
	Практические занятия		4	
	1	Определение типа угроз безопасности персональных данных, актуальных для информационной системы и установление уровня защищенности		
	2	Правила лицензирования деятельности организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну		
	Самостоятельная работа обучающихся Изучение правил лицензирования 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. Оформление отчетного материала по практическим работам.		4	

1	2		3	4
Тема 2.4. Нормативные и методические документы по технической защите информации	**Содержание учебного материала**		6	
	1	Приказ ФСТЭК №58 от 5.02.2010г. "Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных"		2
	2	Приказ ФСТЭК, ФСБ, Мининформсвязи России от 13.02.2008г. №55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных»		3
	3	"Административный регламент ФСТЭК по исполнению государственной функции по лицензированию деятельности по технической защите конфиденциальной информации" от 28.08.2007 №181		1
	4	Приказ ФСТЭК России 11 февраля 2013 г. N 17 "Об утверждении требований к защите информации, не составляющей государственную тайны, содержащейся в государственных информационных системах"		2
	5	Руководящий документ ФСТЭК России «Средства вычислительной техники Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации»		1
	6	Типовые требования ФСБ по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных		1
	7	Методические рекомендации ФСБ по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных		1
	8	Административный регламент ФСТЭК по исполнению государственной функции по лицензированию деятельности по разработке и (или) производству средств защиты конфиденциальной информации		2
	9	Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная заместителем директора ФСТЭК России 15 февраля 2008		3
	10	Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная заместителем директора ФСЭК России 14 февраля 2008		3
	Практические занятия		4	
	1	Выявление каналов утечки информации на объекте защиты.		
	2	Определение актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных		
	Самостоятельная работа обучающихся Изучение терминов и понятий, закрепленных в нормативных и методических документах по технической защите информации. Оформление отчетного материала по практическим работам. Подготовка к защите.		6	

1	2		3	4
Тема 2.5. Основные национальные стандарты в области защиты информации	**Содержание учебного материала**		2	
	1	ГОСТ Р 50922-2006. Защита информации. Основные термины и определения		1
	2	ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью.		1
	3	ГОСТ Р ИСО 7498-2-99 Государственный стандарт Российской Федерации. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель		1
	4	ГОСТ Р 51241-98 Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний.		1
	5	ГОСТ Р 50.1.053- 2005 Информационные технологии, основные термины и определения в области технической защиты информации		1
	Самостоятельная работа обучающихся Изучение стандартов в области защиты информации		2	
Тема 2.6. Международные стандарты по оценке безопасности информационных технологий	**Содержание учебного материала**		2	
	1	Общие критерии оценки безопасности информационных технологий международной организации по стандартизации (ИСО) информационных технологий.		1
	2	Стандарт ITSEC (Критерии Оценки Защищенности Информационных Технологий)		1
	Самостоятельная работа обучающихся Анализ требований стандартов ITSEC (Критерии Оценки Защищенности Информационных Технологий)		2	
Раздел 3 Организационно-правовое обеспечение информационной безопасности в организации			**30**	

1	2		3	4
Тема 3.1 Нормативно-методическое и документационное обеспечение информационной безопасности юридического лица любой формы собственности	**Содержание учебного материала**		8	2
	1	Обеспечение защищенности информационной среды организации на единой концептуальной и методической основе (комплексная согласованность, целенаправленность и планомерность)		
	2	Нормативно-методическое и документационное обеспечение информационной безопасности юридического лица любой формы собственности		3
	3	Классификация внутренних документов организации по обеспечению своей информационной безопасности		2
	4	Документирование системы взглядов на проблему обеспечения информационной безопасности организации. Документы первого уровня. Концепция информационной безопасности организации.		2
	5	Документирование анализа рисков на основе инвентаризации и классификации информационных ресурсов. Документы второго уровня. Политики информационной безопасности организации		2
	6	Документы третьего уровня. Стандарты информационной безопасности организации.		2
	7	Документы четвертого уровня, содержащие свидетельства выполненной деятельности по обеспечению информационной безопасности		2
	8	Применение нормативных правовых актов и нормативных методических документов в области защиты информации		3
	10	Оформление документации по регламентации мероприятий и оказанию услуг в области защиты информации		3
	Практические занятия		2	
	1	Анализ политики информационной безопасности		
	Самостоятельная работа обучающихся Изучение документационного обеспечения информационной безопасности юридического лица любой формы собственности. Оформление отчетного материала по практической работе.		4	
Тема 3.2. Организация работы по соблюдению требований режима защиты информации	Содержание учебного материала		8	3
	1	Правовое положение субъектов правоотношений в сфере профессиональной деятельности (включая предпринимательскую деятельность)		
	2	Правовые нормы допуска лиц к сведениям, составляющих государственную тайну		3
	3	Организация работы по выявлению утечки информации на объекте защиты		2
	4	Контролирование соблюдения персоналом требований режима защиты информации		3
	5	Контроль за косвенными каналами утечки информации на объекте защиты		2
	6	Контроль за прямыми каналами утечки информации на объекте защиты		2
	7	Организация ремонтного обслуживания аппаратуры		2
	8	Организация ремонтного обслуживания средств защиты информации		3
	9	Обязанности и ответственность работников, трудовая деятельность которых связана с обеспечением информационной безопасности		3
	10	Способы защиты прав работников, деятельность которых связана с информационной безопасностью автоматизированных систем, в соответствии с трудовым законодательством		3
	Практические занятия		2	
	1	Оформление допуска лиц к сведениям, составляющих государственную тайну		
	Самостоятельная работа обучающихся Оформление отчетных материалов по практической работе. Подготовка к зачетному занятию.		6	

1	2	3	4
Зачетное занятие		**2**	
	Всего:	**96**	

Для характеристики уровня освоения учебного материала используются следующие обозначения:
1. – ознакомительный (узнавание ранее изученных объектов, свойств);
2. – репродуктивный (выполнение деятельности по образцу, инструкции или под руководством)
3. – продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач)

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально-техническому обеспечению

Реализация рабочей программы дисциплины требует наличия учебного кабинета, совмещенного с другими дисциплинами, а также мастерской «Кибербезопасность».

Оборудование учебного кабинета:

1. Персональные компьютеры с лицензионным программным обеспечением и выходом в Интернет.
2. Проекционное мультимедиа оборудование
3. Мебель с числом посадочных мест, не менее списочной численности учебной группы.
4. Доска, мел или маркеры
5. Методические указания к выполнению практических и самостоятельных работ

Оборудование мастерской «Кибербезопасность»:

- ПЭВМ в сборе (i7/32Gb MEM/ 256Gb + 1Tb nvme SSD/ Nvidia Qadro 1000 / Intel 4x1Gb/s Lan Card/ 27” Monitor)
- Epson EB-2247U
- Экран для проектора Lumien Master Picture 191x300 Matte White FiberGlass
- Рабочее место в сборе:
  - стол (ШхД) 1200x750;
  - рама задняя длинная;
  - перфопанель – 4;
  - набор держателей;
  - электроблок на 8 розеток;
  - полка приборная длинная;
  - светильник светодиодный – 2 шт;
  - кронштейн для монитора;
  - полка для системного блока;
  - стул тканевый с металлической крестовиной;
  - металлические колеса для стула;
  - набор подлокотников.
- Стол для преподавателя
- Стулья для брифинг зоны
- Стол для брифинг зоны (переговорный)
- Вешалка
- Корзина для мусора
- Корзина для бахил

3.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1) Новиков, В.К. Организационно-правовые основы информационной безопасности (защиты информации). Юридическая ответственность за правонарушения в области информационной безопасности (защиты информации) [Электронный ресурс] : учебное пособие / В.К. Новиков. — Электрон. дан. — Москва : Горячая линия-Телеком, 2017. — 176 с. — Режим доступа: https://e.lanbook.com/book/111084. — Загл. с экрана.

2) Петренко, В.И. Защита персональных данных в информационных системах. Практикум [Электронный ресурс] : учебное пособие / В.И. Петренко, И.В. Мандрица. — Электрон. дан. — Санкт-Петербург : Лань, 2019. — 108 с. — Режим доступа: https://e.lanbook.com/book/111916. — Загл. с экрана.

Дополнительные источники:

1. Программно-аппаратные средства защиты информации [Электронный ресурс] : учебное пособие / Л.Х. Мифтахова [и др.]. — Электрон. дан. — Санкт-Петербург : ИЦ Интермедия, 2018. — 408 с. — Режим доступа: https://e.lanbook.com/book/103200. — Загл. с экрана.

2. Ю.А.Родичев. Нормативная база и стандарты в области информационной безопасности. Учебное пособие - СПб.: Питер, 2017г. – 256стр.

3. Федеральный закон «О лицензировании отдельных видов деятельности» от 04.05.2011 N 99-ФЗ (ред. от 13.07.2015, с изм. от 30.12.2015).

4. Федеральный закон «Об электронной подписи» от 06.04.2011 N 63-ФЗ (ред. от 28.06.2014).

5. Федеральный закон «О связи» от 07.07.2003 N 126-ФЗ (ред. от 13.07.2015)

6. Кодекс Российской Федерации «Об административных правонарушениях» Федеральный закон от 30 декабря 2001 №195-ФЗ.

7. Уголовный кодекса Российской Федерации. Федеральный закон Российской Федерации от 13 июня 1996 №63-ФЗ .

8. Основы информационной безопасности : учеб. пособие / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов .— М.: Горячая линия – Телеком, 2011.

9. Доктрина информационной безопасности РФ. Утверждена президентом РФ 09.09.2000. – М.: Межд. Изд. «Информациология», 2000.

10. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 N 6-ФКЗ, от 30.12.2008 N 7-ФКЗ, от 05.02.2014 N 2-ФКЗ, от 21.07.2014 N 11-ФКЗ)

11. Федеральный закон Российской Федерации от 27 июля 2006 г №149-ФЗ «Об информации, информационных технологиях и о защите информации».

12. Федеральный закон Российской Федерации от 21 июля 1993 № 5485-1 « О государственной тайне».

13. Федеральный закон от 29.07.2004 N 98-ФЗ (ред. от 12.03.2014) "О коммерческой тайне".

14. Федеральный закон от 03.04.1995 N 40-ФЗ (ред. от 22.12.2014) "О Федеральной службе безопасности".

15. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 21.07.2014) "О персональных данных" (с изм. и доп., вступ. в силу с 01.09.2015).

16. Трудовой Кодекс Российской Федерации: Федеральный закон РФ от 30 декабря 2001 №197-ФЗ.

17. Указ Президента Российской Федерации от 20 января 1994 г. N 170 "Об основах государственной политики в сфере информатизации" (с изменениями и дополнениями).

18. Указ Президента Российской Федерации от 6 октября 2004 г. N 1286 Вопросы Межведомственной комиссии по защите государственной тайны.

19. Указ Президента Российской Федерации "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена" от 17 марта 2008 г. N 351.

20. Указ Президента Российской Федерации «Об утверждении перечня сведений конфиденциального характера" от 6 марта 1997 г. № 188.

21. Указ Президента Российской Федерации «Об утверждении перечня сведений, отнесенных к государственной тайне" от 30 ноября 1995 г. N 1203.

22. Указ президента Российской Федерации "Вопросы Федеральной службы безопасности Российской Федерации» от 11 июля 2003 года №960.

23. Указ президента Российской Федерации "Вопросы федеральной службы по техническому и экспортному контролю" от 16 августа 2004 г. № 1085 (с изменениями и дополнениями от 22 марта 2005 г. № 330; от 20 июля 2005 г. №846; от 30 ноября 2006 г. № 1321).

24. Постановление правительства РФ «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» от 15 апреля 1995 г. № 333.

25. Постановление правительства РФ Положение о сертификации средств защиты информации от 26 июня 1995 г. № 608 (с изменениями и дополнениями от 23 апреля 1996 г. № 509; от 29 марта 1999 г. № 342; от 17 декабря 2004 г. № 808).

26. Постановление правительства РФ О лицензировании деятельности по технической защите конфиденциальной информации от 3 февраля 2012 г. №79.

27. Постановление правительства РФ Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах от 17.11.2007 № 781.

28. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная заместителем директора ФСТЭК России 15 февраля 2008.

29. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная заместителем директора ФСЭК России 14 февраля 2008.

30. Типовые требования ФСБ по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных.

31. Методические рекомендации ФСБ по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных.

32. Постановление Правительства Российской Федерации от 01 ноября 2012 г.№1119 «Требования к защите персональных данных при их обработке в информационных системах персональных данных».

33. Шаньгин, В.Ф. Информационная безопасность [Электронный ресурс] : учеб. пособие — Электрон. дан. — Москва : ДМК Пресс, 2014. — 702 с. — Режим доступа: https://e.lanbook.com/book/50578. — Загл. с экрана.

34. С.Г. Баричев., В.В.Гончаров., Р.Е. Серов Основы современной криптографии. 3-издание. – 2011.

35. Мельников В.П. Информационная безопасность и защита информации: учебное пособие. - М.: Издательский центр «Академия», 2007.

Интернет ресурсы

1. zakonprost.ru/koap;
2. http://www. fstec.ru
3. http://www. ittec.ru
4. http://www. fsb.ru
5. http://dehack.ru/zak_akt

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в процессе проведения практических занятий, тестирования.

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
1	**2**
В результате изучения дисциплины обучающийся **должен уметь**:	
Осуществлять организационное и правовое обеспечение информационной безопасности телекоммуникационных систем в рамках должностных обязанностей техника по защите информации	Проверка умений в процессе выполнения заданий на практических занятиях, дифференцированный зачет
Применять нормативные правовые акты и нормативные методические документы в области защиты информации	Проверка умений в процессе выполнения заданий на практических занятиях, дифференцированный зачет
Выявлять каналы утечки информации на объекте защиты	Проверка умений в процессе выполнения заданий на практических занятиях
Контролировать соблюдение персоналом требований режима защиты информации	Проверка умений в процессе выполнения заданий на практических занятиях, дифференцированный зачет
Оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации	Проверка умений в процессе выполнения заданий на практических занятиях, внеаудиторной самостоятельной работе, дифференцированный зачет
Защищать свои права в соответствии с трудовым законодательством	Проверка умений в процессе выполнения заданий на практических занятиях, дифференцированный зачет
В результате изучения дисциплины обучающийся **должен 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	Опрос, внеаудиторная самостоятельная работа, дифференцированный зачет
Правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны	Опрос, внеаудиторная самостоятельная работа, дифференцированный зачет
Правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации	Опрос, защита практических работ, дифференцированный зачет
Организацию ремонтного обслуживания аппаратуры и средств защиты информации	Опрос, дифференцированный зачет

1	2
Принципы и методы организационной защиты информации, организационное обеспечение информационной безопасности в организации	Опрос, внеаудиторная самостоятельная работа, дифференцированный зачет
Правовое положение субъектов правоотношений в сфере профессиональной деятельности (включая предпринимательскую деятельность)	Опрос, внеаудиторная самостоятельная работа, дифференцированный зачет