

МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ
И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
Северо-Кавказский филиал
ордена Трудового Красного Знамени федерального государственного
бюджетного образовательного учреждения высшего образования
«Московский технический университет связи и информатики»

УТВЕРЖДАЮ
Зам. директора по УР
Н.А. Андреева
« 31 » 03 2025 г.

Б1.О.28 Организационное и правовое обеспечение информационной безопасности рабочая программа дисциплины

Кафедра: Информационная безопасность
Направление подготовки: 10.03.01 Информационная безопасность
Профиль: Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)
Формы обучения: очная

Распределение часов дисциплины по семестрам (для очной формы обучения (ОФО))

Вид учебной работы	ОФО	
	ЗЕ	часов/
Общая трудоемкость дисциплины, в том числе (по семестрам, курсам):	3	108/3
Контактная работа, в том числе (по семестрам, курсам):		64/3
Лекции		32/3
Лабораторных работ		
Практических занятий		32/3
Семинаров		
Самостоятельная работа		44/3
Контроль		
Число контрольных работ (по курсам)		
Число КР (по семестрам, курсам)		
Число КП (по семестрам, курсам)		
Число зачетов с разбивкой по семестрам		1/3
Число экзаменов с разбивкой по семестрам		

Программу составил:
Доцент кафедры ИБ, к.пол.н. Жуковский Д.А.

Рабочая программа дисциплины
«Организационное и правовое обеспечение информационной безопасности»

Разработана в соответствии с ФГОС ВО:
направления подготовки **10.03.01 «Информационная безопасность»**, утвержденным приказом Министерства науки и высшего образования Российской Федерации от 17 ноября 2020 г. N 1427.

Составлена на основании учебного плана
направления **10.03.01 Информационная безопасность, профиля «Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)»**, одобренного Учёным советом СКФ МТУСИ, протокол № 8 от 31.03.2025г., и утвержденного директором СКФ МТУСИ 31.03.2025 г.

Рассмотрена и одобрена на заседании кафедры
«Информационная безопасность»

Протокол от «31» 03 2025 г. № 8

И.о.зав. кафедрой  А.Г.Жуковский

1. Цели изучения дисциплины

Целями изучения дисциплины «Организационное и правовое обеспечение информационной безопасности» является изучение организационно-правовых основ обеспечения информационной безопасности в современных телекоммуникационных системах, а также содействие формированию научного мировоззрения и развитию системного мышления..

2. Планируемые результаты обучения

Изучение дисциплины направлено на формирование у обучающегося способности решать профессиональные задачи в соответствии с *эксплуатационной деятельностью*.

Результатом освоения дисциплины являются сформированные у обучающегося следующие компетенции:

УК-10. Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности
Знать:
- формы проявления экстремизма, терроризма, коррупционного поведения в различных сферах общественной жизни, антикоррупционные законодательные акты; - сущность коррупционного поведения и его взаимосвязь с социальными, экономическими, политическими и иными условиями.
Уметь:
- применять правовые нормы противодействия экстремизму, терроризму и коррупционному поведению; - анализировать, толковать и правильно применять правовые нормы о противодействии экстремизму, терроризму и коррупционному поведению
Владеть:
- навыками работы с антикоррупционными нормативами; - навыками работы с законодательными и другими нормативными правовыми актами
ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности
Знать:
- особенности применения нормативных и правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации; - требования нормативных правовых актов и нормативных и методических документов, регламентирующих деятельность по защите информации
Уметь:
- решать задачи профессиональной деятельности на основе применения нормативных и правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации; - анализировать нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации
Владеть:
- навыками решения конкретных задач по защите информации на основе применения нормативных и правовых актов, нормативных и методических документов; - навыками выделения основной содержательной информации в нормативных и правовых актах

3. Место дисциплины в структуре образовательной программы

Требования к предварительной подготовке обучающегося (предшествующие дисциплины, модули, темы):	
1	Б1.О.10 «Гражданское социально-ответственное поведение»
Последующие дисциплины и практики, для которых освоение данной дисциплины необходимо:	
1	Б1.О.39 «Обеспечение безопасности персональных данных в информационных системах»

4. Структура и содержание дисциплины

4.1 Очная форма обучения, 4 года (всего 108 часа, 64 часов контактной работы)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компетенции	УМИО
1	2	3	4	5	6
Курс 2, Семестр 3					
Модуль 1 – Правовое обеспечение информационной деятельности – 54 (32+22) часов					
1.1	Информационные отношения, как объект правового регулирования. Законодательство РФ в области информационной безопасности. Структура информационной сферы и характеристика ее элементов. Виды информации. Конституционные гарантии прав на информацию и механизм их реализации. Понятие и структура информационной безопасности.	Лек.	8	УК-10	Л1.1 Л1.2 Л2.1
1.2	Правовой режим защиты государственной тайны. Правовое обеспечение защиты государственной тайны. Контроль и надзор за обеспечением защиты государственной тайны.	Лек.	8	УК-10	Л1.3 Л2.3
1.3	Законодательство РФ в области информационной безопасности	ПЗ	6	УК-10	Л1.1 Л1.2 Л2.1 Л2.2
1.4	Правовые режимы защиты информации конфиденциального характера. Государственное регулирование деятельности в области защиты информации.	ПЗ	6	УК-10	Л1.1 Л1.2 Л2.1
1.5	Правовая охрана результатов интеллектуальной деятельности. Преступления в сфере компьютерной информации	ПЗ	4	УК-10	Л1.1 Л1.2 Л2.1
1.6	Законодательство РФ в области информационной безопасности. Изучение положений о государственном лицензировании деятельности в области защиты информации. Защита компьютерной информации. Технические каналы утечки компьютерной информации. Защита информации от утечки по техническим каналам	СРС	22	УК-10	Л1.1 Л1.2 Л2.2
Модуль 2. Организационное обеспечение информационной безопасности 54 (32+22) часов					
2.1	Понятие организационной защиты информации.	Лек.	8	ОПК-5	Л1.1

	Направления, принципы и условия организационной защиты информации. Подходы и требования к организации системы защиты информации.				Л1.2 Л2.3
2.2	Основные понятия организации безопасности в области защиты информации	Лек.	8	ОПК-5	Л1.1 Л1.2 Л2.3
2.3	Понятие допуска к государственной тайне	ПЗ	4	ОПК-5	Л1.1 Л1.2 Л2.3
2.4	Порядок и особенности допуска к государственной тайне отдельных категорий граждан	ПЗ	4	ОПК-5	Л3.1
2.5	Изучение положений о сертификации средств защиты информации по требованиям безопасности информации. Система сертификации средств криптографической защиты информации.	ПЗ	4	ОПК-5	Л3.1
2.6	Основы мониторинга оборудования инфокоммуникационных технологий и систем связи с целью оценки соответствия их состояния требованиям технических регламентов, международных и национальных стандартов и иных нормативных документов.	ПЗ	2	ОПК-5	Л1.1 Л1.2 Л2.3
2.7	Методы, силы и средства, используемые для организации защиты информации.	ПЗ	2	ОПК-5	Л1.1 Л1.2 Л2.3
2.8	Преступления в сфере компьютерной информации. Классификация компьютерных преступлений. Криминалистические особенности расследования компьютерных преступлений. Международные стандарты и соглашения в области безопасности информационных технологий.	СРС	22	ОПК-5	Л1.1 Л1.2 Л2.3
	Зачет			УК-10 ОПК-5	Л1.1 Л1.2 Л2.1 Л2.2 Л2.3 Л3.1
Итого – 72 часа					

5. Учебно-методическое и информационное обеспечение дисциплины

5.1. Рекомендуемая литература				
5.1.1. Основная литература				
Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л 1.1	А.Р. Газизов	Организационное и правовое обеспечение информационной безопасности : учебное пособие	Ростов-на-Дону: Донской государственный технический университет, 2017. — 156 с. — ISBN 978-5-7890-1384-7	Э1

Л 1.2	М.А. Полтавцева	Организационные и правовые аспекты информационной безопасности. Учебное пособие	СПб.: Университет ИТМО, 2016. - 169 с.	Э2
5.1.2. Дополнительная литература				
	Авторы, составители	Заглавие	Издательство, год	Кол.
Л 2.1	С.А. Нестеров	Основы информационной безопасности: учебное пособие	СПб.: Санкт-Петербургский политех. ун-т Петра Великого, 2014. - 322 с.	Э3
Л 2.2	Н.Н. Куняев, А.С. Дёмушкин, А.Г. Фабричнов, Т.В., Т.В. Кондрашева	Конфиденциальное делопроизводство и защищенный электронный документооборот : Учебник	М.: Логос, 2016. - 500 с	Э4
Л 2.3	А.Н. Кубанков, Н.Н. Куняев.	Система обеспечения информационной безопасности Российской Федерации: организационно-правовой аспект: Учебное пособие	М.: Всерос. гос. университет юстиции (РПА Минюста России), 2014. - 78 с.	Э5
5.1.3. Учебно-методическое обеспечение				
	Авторы, составители	Заглавие	Издательство, год	Кол.
Л 3.1	М.Е. Рубанова, Н.Н. Портенко, В.В. Масляков	Правоведение. Учебное пособие	Саратов : РЕАВИЗ, 2023. — 284 с.	Э6
5.2. Электронные образовательные ресурсы				
Э1	https://www.iprbookshop.ru/117813.html			
Э2	https://www.iprbookshop.ru/147727.html			
Э3	http://www.iprbookshop.ru/43960			
Э4	http://www.iprbookshop.ru/66416.html			
Э5	http://www.iprbookshop.ru/47262.html			
Э6	https://www.iprbookshop.ru/153841.html			
5.3 Информационно-справочные системы и профессиональные базы данных				
5.3.1	Консультант Плюс – https://www.consultant.ru/			
5.3.2	Гарант – https://www.garant.ru/			
5.3.2	Консорциум Кодекс – https://docs.cntd.ru/			
5.3.3	Научная электронная библиотека – https://www.elibrary.ru/			
5.3.4	Профессиональная база данных: Федеральный портал «Российское образование»: [Электронный ресурс] – Режим доступа: http://www.edu.ru/ (открытый доступ)			
5.3.5	Профессиональная база данных: Федеральный центр информационно-образовательных ресурсов: [Электронный ресурс] – Режим доступа: http://fcior.edu.ru/ (открытый доступ)			
5.4 Программное обеспечение				
СКФ МТУСИ обеспечен необходимым комплектом лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства:				
П.1	MS Power Point, MS Word			
П.2	Пакет Libre Office			

6. Материально-техническое обеспечение дисциплины

6.1 МТО лекционных занятий	
1	Лекционная аудитория, оснащенная интерактивной доской, проектором, ПК (ноутбуком), экраном
6.2 МТО лабораторных работ и практических занятий	
1	Учебные аудитории, оборудованные компьютерной техникой, с возможностью подключения к сети «Интернет», и обеспечением доступа в электронную информационно-образовательную среду СКФ МТУСИ
6.3 МТО рубежных контролей, зачетов, экзаменов	
1	Учебные аудитории, оборудованные компьютерной техникой с возможностью выхода в локальную сеть Филиала и Интернет
6.4 МТО самостоятельной работы обучающихся	
1	Помещение для самостоятельной работы обучающихся оснащено компьютерной техникой с возможностью подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду СКФ МТУСИ

7. Оценочные материалы

Оценочные материалы и перечень видов оценочных средств текущего контроля и промежуточной аттестации представлены в Приложении 1 к рабочей программе дисциплины.

8. Методические рекомендации для обучающихся по освоению дисциплины

Методические рекомендации по освоению дисциплины представлены в Приложении 2 к рабочей программе дисциплины.

9. Особенности реализации дисциплины (модуля) при обучении инвалидов и лиц с ограниченными возможностями здоровья

Рабочая программа дисциплины (модуля) при необходимости может быть адаптирована для обучения (в том числе с применением дистанционных образовательных технологий) лиц с ограниченными возможностями здоровья, инвалидов. Для этого требуется заявление обучающихся, являющихся лицами с ограниченными возможностями здоровья, инвалидами, или их законных представителей и рекомендации психолого-медико-педагогической комиссии. При обучении лиц с ограниченными возможностями здоровья учитываются их индивидуальные психофизические особенности. Обучение инвалидов осуществляется также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

Для лиц с нарушением слуха возможно предоставление учебной информации в визуальной форме (краткий конспект лекций; тексты заданий, напечатанные увеличенным шрифтом), на аудиторных занятиях допускается присутствие ассистента, а также сурдопереводчиков и тифлосурдопереводчиков.

Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет практические задания.

Доклад (реферат) также может быть представлен в письменной форме, при этом требования к содержанию остаются теми же, а требования к качеству изложения материала (понятность, качество речи, взаимодействие с аудиторией и т. д.) заменяются на соответствующие требования, предъявляемые к письменным работам (качество оформления текста и списка литературы, грамотность, наличие иллюстрационных материалов и т.д.).

Промежуточная аттестация для лиц с нарушениями слуха проводится в письменной форме, при этом используются общие критерии оценивания. При необходимости время подготовки к ответу может быть увеличено.

Для лиц с нарушением зрения допускается аудиальное предоставление информации, а также использование на аудиторных занятиях звукозаписывающих устройств (диктофонов и т.д.). Допускается присутствие на занятиях ассистента (помощника), оказывающего обучающимся необходимую техническую помощь.

Текущий контроль успеваемости осуществляется в устной форме.

При проведении промежуточной аттестации для лиц с нарушением зрения тестирование может быть заменено на устное собеседование по вопросам.

Для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, на аудиторных занятиях, а также при проведении процедур текущего контроля успеваемости и промежуточной аттестации могут быть предоставлены необходимые технические средства (персональный компьютер, ноутбук или другой гаджет); допускается присутствие ассистента (ассистентов), оказывающего обучающимся необходимую техническую помощь (занять рабочее место, передвигаться по аудитории, прочитать задание, оформить ответ, общаться с преподавателем).

10. Дополнения и изменения в Рабочей программе

Лист актуализации рабочей программы дисциплины «Б1.О.28 Организационное и правовое обеспечение информационной безопасности» для использования в 20___/20___ учебном году

Утверждаю

Зам. директора по УР _____
«___» _____ 20___ г.

Направление: 10.03.01 Информационная безопасность

Профиль: Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)

Форма обучения: очная

(Возможны следующие варианты):

- а) Рабочая программа действует без изменений.
- б) В рабочую программу вносятся следующие изменения:
 - 1)
 - 2)
 - 3)

Разработчик (и): _____
(ФИО, ученая степень, ученое звание)

«___» _____ 20___ г.

Рабочая программа пересмотрена и одобрена на заседании кафедры ИБ

Протокол № _____ от «___» _____ 20___ г.

Заведующий кафедрой _____

Оценочные материалы для проведения текущего контроля и промежуточной аттестации по дисциплине

1. Оценочные материалы для проведения промежуточной аттестации по дисциплине

1.1 Шкала оценивания компетенций

Шкала оценивания компетенций		
Оценка	Уровень освоения компетенции	Критерии оценивания
«Отлично»	Высокий уровень	Обучающийся показывает всестороннее, систематическое и глубокое знание основного и дополнительного учебного материала, умеет свободно выполнять задания, предусмотренные программой; усвоил основную и знаком с дополнительной рекомендованной литературой; может объяснить взаимосвязь основных понятий дисциплины в их значении для последующей профессиональной деятельности; проявляет творческие способности в понимании, изложении и использовании учебного материала.
«Хорошо»	Повышенный уровень	Обучающийся показывает достаточный уровень знаний в пределах основного учебного материала, без существенных ошибок выполняет предусмотренные в программе задания; усвоил основную литературу, рекомендованную в программе; способен объяснить взаимосвязь основных понятий дисциплины при дополнительных вопросах преподавателя. Допускает не существенные погрешности в ответах, устраняет их без помощи преподавателя.
«Удовлетворительно»	Пороговый уровень	Обучающийся показывает знания основного учебного материала в минимальном объеме, необходимом для дальнейшей учебы; справляется с выполнением заданий, предусмотренных программой, допуская при этом большое количество не принципиальных ошибок; знаком с основной литературой, рекомендованной программой. Допускает существенные погрешности в ответах, но обладает необходимыми знаниями для их устранения под руководством преподавателя.
«Неудовлетворительно»	Минимальный уровень не достигнут	Обучающийся обнаруживает пробелы в знаниях основного учебного материала, допускает принципиальные ошибки в выполнении предусмотренных программой

		заданий, не знаком с рекомендованной литературой, не может исправить допущенные ошибки. Как правило, оценка «неудовлетворительно» ставится обучающимся, которые не могут продолжить обучение или приступить к профессиональной деятельности по окончании вуза без дополнительных занятий по соответствующей дисциплине.
--	--	---

1.2 Показатели, критерии и шкалы оценивания компетенций

Показатели компетенции	Критерии оценивания	Шкала оценивания
УК-10: Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному у поведению и противодействовать им в профессиональной деятельности		
Знать:		
- формы проявления экстремизма, терроризма, коррупционного поведения в различных сферах общественной жизни, антикоррупционные законодательные акты	Контрольная работа	Модуль 1 0÷5 «Неудовлетворительно» - 0-2 «Удовлетворительно» - 3 «Хорошо» - 4 «Отлично» - 5
- сущность коррупционного поведения и его взаимосвязь с социальными, экономическими, политическими и иными условиями	Контрольная работа	Модуль 2 0÷5 «Неудовлетворительно» - 0-2 «Удовлетворительно» - 3 «Хорошо» - 4 «Отлично» - 5
Уметь:		
- применять правовые нормы противодействия экстремизму, терроризму и коррупционному поведению	Практические занятия 1	Модуль 1 0÷10 «Неудовлетворительно» - 0-2 «Удовлетворительно» - 3-5 «Хорошо» - 6-8 «Отлично» - 9-10
- анализировать, толковать и правильно применять правовые нормы о противодействии экстремизму, терроризму и коррупционному поведению	Практические занятия 2	Модуль 2 0÷10 «Неудовлетворительно» - 0-2 «Удовлетворительно» - 3-5 «Хорошо» - 6-8 «Отлично» - 9-10
Владеть:		
- навыками работы с антикоррупционными нормативами	Практические занятия 3	Модуль 1 0÷10 «Неудовлетворительно» - 0-3 «Удовлетворительно» - 4-6 «Хорошо» - 7-8 «Отлично» - 9-10
- навыками работы с законодательными и другими нормативными правовыми актами	Практические занятия 3	Модуль 2 0÷10 «Неудовлетворительно» - 0-3 «Удовлетворительно» - 4-6

		«Хорошо» - 7-8 «Отлично» - 9-10
ОПК-5: Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности		
Знать:		
- особенности применения нормативных и правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации	Контрольная работа	Модуль 1 0÷5 «Неудовлетворительно» - 0-2 «Удовлетворительно» - 3 «Хорошо» - 4 «Отлично» - 5
- требования нормативных правовых актов и нормативных и методических документов, регламентирующих деятельность по защите информации	Контрольная работа	Модуль 2 0÷5 «Неудовлетворительно» - 0-2 «Удовлетворительно» - 3 «Хорошо» - 4 «Отлично» - 5
Уметь:		
- решать задачи профессиональной деятельности на основе применения нормативных и правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации	Практические занятия 4	Модуль 1 0÷10 «Неудовлетворительно» - 0-2 «Удовлетворительно» - 3-5 «Хорошо» - 6-8 «Отлично» - 9-10
- анализировать нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	Практические занятия 5	Модуль 2 0÷10 «Неудовлетворительно» - 0-3 «Удовлетворительно» - 4-6 «Хорошо» - 7-8 «Отлично» - 9-10
Владеть:		
- навыками решения конкретных задач по защите информации на основе применения нормативных и правовых актов, нормативных и методических документов	Практические занятия 6	Модуль 1 0÷10 «Неудовлетворительно» - 0-3 «Удовлетворительно» - 4-6 «Хорошо» - 7-8 «Отлично» - 9-10
- навыками выделения основной содержательной информации в нормативных и правовых актах	Практические занятия 7-8	Модуль 2 0÷10 «Неудовлетворительно» - 0-3 «Удовлетворительно» - 4-6 «Хорошо» - 7-8 «Отлично» - 9-10
	Зачет	0-100 «Не зачтено» - 0-40 «Зачтено» - 41-60

1.3 Оценочные материалы: типовые контрольные задания, иные материалы

1.3.1 Оценочные материалы текущего контроля для очной формы обучения

Данная дисциплина формирует у обучающегося 2 компетенции, которые связаны, взаимодействуют между собой и объективно оценить каждую в отдельности при ответе обучающегося на контрольный вопрос или при выполнении практического или лабораторного задания достаточно сложно. Предлагается считать, что вклад 2-х компетенций в общую оценку при ответе на вопрос примерно одинаков.

Модуль 1 (50 баллов):

Модуль содержит 2 лекционных, 3 практических занятий. Знание лекционного материала оценивается по контрольной работе, состоящей из двух вопросов, максимальное количество баллов за контрольную работу составляет 10. За практические занятия обучающийся получает максимум 40 баллов. Общее максимальное количество баллов за модуль 1 составляет 50.

Вопросы для контрольной работы (УК-10):

1. Какие методы защиты лежат в основе комплексной системы информационной безопасности любого объекта.
2. С принятием каких законов началось формирование законодательства в информационной сфере?
3. Признаки и объекты профессиональной тайны?
4. Какие сведения относятся к служебной тайне?
5. Правовой статус службы безопасности.

Практическое занятие 1.

1. Какие общественные отношения являются предметом правового регулирования в информационной сфере?
2. Какова структура информационного законодательства РФ?
3. Какой закон установил принципы правового регулирования отношений, в информационной сфере?
4. Какие документы составляют правовую базу в информационной сфере?
5. На каком законе РФ основывается система защиты государственных секретов?
6. Какую информацию относят к сведениям, составляющим государственную тайну?
7. Назовите степени секретности, установленные для сведений, составляющих государственную тайну?
8. На каких принципах основан порядок засекречивания сведений, составляющих государственную тайну?
9. Кем установлен порядок рассекречивания и продления сроков засекречивания архивных документов?
10. Кем устанавливаются формы сертификата и знака соответствия?

Практическое занятие 2.

1. Виды материальных носителей сведений.
2. Определение и виды конкурентной разведки.
3. Какие сведения не могут составлять коммерческую тайну?
4. Какие грифы конфиденциальности может использовать предприятие для обозначения степени важности коммерческой информации?
5. Какие виды деятельности в области защиты информации подлежат лицензированию?
6. Порядок лицензирования, срок действия лицензии?
7. Организационная структура системы сертификации в области защиты конфиденциальной информации?
8. При каких организациях созданы системы сертификации в РФ?

9. Порядок и требования при осуществлении сертификации средств защиты информации?

10. В каких случаях сертификация носит добровольный характер?

Практическое занятие 3.

1. Назначение службы защиты информации.
2. Место службы защиты информации в системе безопасности предприятия.
3. Служба защиты информации как составная часть системы защиты.
4. Служба защиты информации как орган управления защитой информации.
5. Служба защиты информации как координатор деятельности по обеспечению безопасности информации.
6. Статус службы защиты информации в структуре предприятия.

Модуль 2: (50 баллов):

Модуль содержит 2 лекционных, 4 практических занятий. Знание лекционного материала оценивается по контрольной работе, состоящей из двух вопросов, максимальное количество баллов за контрольную работу составляет 10. За практические занятия обучающийся получает максимум 40 баллов. Общее максимальное количество баллов за модуль 1 составляет 50.

Вопросы для контрольной работы (ОПК-5):

1. Процедурные меры обеспечения информационной безопасности включают?
2. Управление персоналом при обеспечении информационной безопасности предполагает?
3. Физическая защита при обеспечении информационной безопасности предполагает?
4. Поддержание работоспособности при обеспечении информационной безопасности предполагает?
5. Реагирование на нарушения режима безопасности предполагает?
6. Планирование восстановительных работ включает?
7. Этапность планирования восстановительных работ?
8. Идентификация – это процесс ...? Аутентификация предполагает ...?

Практическое занятие 4.

1. Правовая защита фирменного наименования, товарных знаков, знаков обслуживания и наименования мест происхождения товаров?
2. Особенности расследования компьютерных преступлений?
3. Какие задачи решаются судебно-бухгалтерской и программно-технической экспертизами при проведении следственных действий?
4. Существующая классификация компьютерных преступлений?
5. Методы и приемы предупреждения компьютерных преступлений?
6. В каких документах представлены нормы правового обеспечения защиты информации в автоматизированных системах?
7. Что представляет собой документ «Политика безопасности»?
8. Какие документы необходимо представить для присвоения класса защищенности в автоматизированных системах?
9. Выполнение каких правил безопасности обеспечивается путем реализации «Политики безопасности»?

Практическое занятие 5.

1. Принципы и порядок создания системы физической защиты объекта?
2. Целями и задачами проведения анализа уязвимости являются?

3. Основными этапами стадии концептуального проекта являются?
4. Основными угрозами безопасности, которые могут привести к утрате корпоративных ресурсов предприятия являются?
5. Этапы оценки уязвимости существующей системы физической защиты объекта?
6. Система физической защиты объекта?
7. Методы физической защиты объектов?
8. Типовая структура физической защиты объекта?
9. Охрана с помощью технических средств?

Практическое занятие 6.

1. Характеристика методов с применением специализированных аппаратных средств?
2. Характеристика методов основанных на анализе биометрических характеристик пользователя?
3. Разграничение доступа предполагает...?
4. Протоколирование и аудит предполагает...?
5. Цели реализация протоколирования и аудита?
6. Криптографическое преобразование данных предполагает...?
7. Режим секретности это?
8. Режим секретности по содержанию включает в себя?

Практическое занятие 7.

1. Принципы управления службой защиты информации.
2. Понятие и сущность методов управления.
3. Система методов управления.
4. Административно-правовые методы управления.
5. Экономические методы управления.
6. Социально-психологические методы управления.
7. Взаимосвязь методов управления.
8. Необходимость комплексного и системного применения методов управления службой защиты информации.

Практическое занятие 8.

1. Состав и содержание управленческих функций.
2. Технология управления службой защиты информации.
3. Значение управленческих решений.
4. Цели планирования.
5. Виды планирования, их назначение.
6. Содержание и структура планов.
7. Технология планирования..

1.3.2 Вопросы, выносимые на зачет по дисциплине «Организационное и правовое обеспечение информационной безопасности» (УК-10, ОПК-5) (промежуточная аттестация)

1. Информация как объект правового регулирования.
2. Государственная система защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам.
3. Государственная тайна. Порядок допуска должностных лиц и граждан Российской Федерации к государственной тайне.
4. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа.
5. Оценка соответствия объектов информатизации требованиям безопасности информации.

6. Классификация автоматизированных систем и требования по защите информации.
7. Специальные защитные знаки.
8. Лицензирования и сертификации в области технической защите конфиденциальной информации.
9. Система сертификации средств защиты информации о требованиях безопасности информации.
10. Ключевые системы информационной инфраструктуры.
11. Правовой режим обеспечения безопасности персональных данных.
12. Особенности обработки персональных данных осуществляемой без использования средств автоматизации.
13. Особенности обеспечения безопасности персональных данных операторами, являющимися государственными либо муниципальными органами.
14. Особенности обработки биометрических персональных данных.
15. Правовой режим обеспечения безопасности государственных и муниципальных систем.
16. Режим защиты коммерческой тайны.
17. Системы управления (менеджмента) информационной безопасности. Принципы построения.
18. "Планирование" системы управления (менеджмента) информационной безопасности.
19. "Внедрение" системы управления (менеджмента) информационной безопасности.
20. "Мониторинг и анализ" и "Сопровождение и совершенствование" системы управления (менеджмента) информационной безопасности.
21. Управление рисками информационной безопасности. Методы обработки рисков информационной безопасности.
22. Управление непрерывностью бизнеса.
23. Последовательность формирования и введения в строй системы экономической безопасности (СЭБ)
24. Процесс управления рисками. Идентификация и способы контроля рисков,
25. Производственный менеджмент и безопасность
26. Несчастные случаи, связанные с производством
27. Действия при возникновении несчастного случая на производстве
28. Концепции экологической безопасности
29. Менеджмент коммерческой безопасности
30. Сущность и содержание организации как самоуправляемой системы,
31. Внутренняя и внешняя среда фирмы
32. Этапы создания самоуправляемой организации
33. Структура, численность и состав СБО
34. Совет безопасности предприятия и его задачи
35. Основные задачи СБ предприятия
36. Руководящие документы по деятельности СБ
37. Основные функции и задачи отделения режима и охраны
38. Основными функциями и задачи оперативного отделения
39. Основные функции отделения маркетинговой разведки
40. Основные функции информационно-аналитического отделения

2. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Порядок и методика проведения текущего контроля и промежуточной аттестации.

Предусмотрены следующие виды контроля:

- текущий контроль по каждому модулю – в форме написания контрольной работы для оценки теоретических знаний;
- текущий контроль по каждому модулю – в форме отчетов по лабораторным работам и практическим занятиям для оценки практических навыков;
- промежуточная аттестация по дисциплине – в форме зачета.

Текущий контроль успеваемости в форме защиты практических проводится в два этапа:

- 1-й этап: допуск к выполнению практической работы – проводится в форме письменной «летучки» (5-10 мин) с целью контроля знаний обучающихся теоретической части лабораторной работы и готовности к выполнению практических исследований;
- 2-й этап выполняется по окончании каждой практической работы (практического занятия) в форме индивидуального собеседования по выполненным исследованиям или расчетам. Проводится с целью контроля закрепления теоретической части материала и степени отработки обучающимся практических навыков исследования на аппаратуре.

С целью повышения качества обучения за счет побуждения обучающихся к активной текущей учебной работе, четкого и оперативного контроля всего хода учебного процесса, снижения роли случайных и субъективных факторов при оценивании учебной деятельности обучающихся в образовательном процессе реализована модульно-рейтинговая система.

Правила ее использования прописаны в «Положении об МРС».

Набранные обучающимся баллы в рамках текущего контроля переводятся в оценку на зачете в соответствии со следующей шкалой:

- «не зачтено» - от 0 до 40 от максимального количества баллов;
- «зачтено» - от 41 до 100 максимального количества баллов.

Соотношения максимального количества баллов, полученных обучающимся по блокам модулей, показаны в Таблице 1.

Таблица 1 - Распределение баллов по модулям дисциплины «Организационное и правовое обеспечение информационной безопасности»

Модуль	Всего баллов (Максимальное значение)	Теоретический блок (Контрольная работа)	Практический блок
Модуль 1	50	10	40
Модуль 2	50	10	40
Зачет	41-100		

На зачете производится оценка тех компетенций, которые должны быть в той или иной форме освоены в процессе изучения. Рекомендуются формировать вопросы в билетах таким образом, чтобы преподаватель смог оценить все компетенции данной дисциплины.

3 Промежуточная аттестация

Промежуточная аттестация проводится в форме зачета. Зачет проводится по расписанию в устном виде по билетам к зачету. Результаты аттестации заносятся в ведомость и зачетную книжку обучающегося.

Образец билета к зачету

	МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»	Утверждаю Зав. кафедрой «ИБ» _____ Жуковский А.Г. «___» _____ 20__ г.
Направление подготовки: 11.03.01 Информационная безопасность Курсы: 2 Дисциплина: Организационное и правовое обеспечение информационной безопасности		
Билет №1 1. Режим защиты коммерческой тайны. 2. Особенности обработки персональных данных осуществляемой без использования средств автоматизации. Доцент каф. «ИБ» _____ Жуковский Д.А. «___» _____ 20__ г.		

Один комплект отпечатанных билетов к зачету, подписанных преподавателем кафедры и утвержденных заведующим кафедрой хранится у заведующего кафедрой, другой комплект – у преподавателя, ведущего дисциплину.

4 Тестовые задания по дисциплине «Организационное и правовое обеспечение информационной безопасности»

Тестовые задания позволяют оценить уровень сформированности 2-х компетенций УК-10 и ОПК-5.

Задания распределены по блокам в соответствии с уровнем сложности. Каждый блок содержит номер задания, и текст задания.

Базовый уровень содержит примерно 50 % заданий.

Он формируется из заданий с выбором одного или нескольких верных ответов из предложенных или воспроизведения фактического материала (терминология, факты, классификация, параметры и др.);

Повышенный уровень в среднем составляет 35 % заданий.

В нем используются задания на сопоставление, сравнение, установление последовательности;

Высокий уровень в среднем составляют – 15 % заданий.

В задании используются: решения нетиповых задач, алгоритмы, доказательства, задания с развернутым ответом – определения, перечисление, изображение схемы, структуры и др.

Количество заданий по каждой компетенции равно 20. Всего 40 заданий.

Один комплект тестовых вопросов с указанием правильных ответов хранится у заведующего кафедрой, другой комплект – у преподавателя, ведущего дисциплину.

УК-10. Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности

БЛОК А (базовый уровень) – Задание с выбором одного или нескольких верных ответов из предложенных

Инструкция по тестам Блока А: Прочитайте текст и выберите один или несколько правильных ответов

№ задания	Дисциплина	Тексты заданий
1	Б1.О.28 Организационное и правовое обеспечение информационной безопасности	Свойство информации, определяющее ее достаточность для принятия решения называется: 1) достоверность 2) адекватность 3) полнота 4) доступность
2	Б1.О.28 Организационное и правовое обеспечение информационной безопасности	Глобальная компьютерная сеть – это: 1) множество компьютеров, связанных каналами передачи информации и находящихся в пределах одного помещения, здания 2) совокупность хост-компьютеров и файл-серверов 3) совокупность локальных сетей и компьютеров, расположенных на больших расстояниях и соединенных с помощью каналов связи в единую систему 4) информационная система с гиперсвязями
3	Б1.О.28 Организационное и правовое обеспечение информационной безопасности	Информационное законодательство – это: 1) совокупность норм права, регулирующих общественные отношения в информационной сфере 2) совокупность норм права, регулирующих гражданские отношения в информационной сфере 3) совокупность норм права, регулирующих административные отношения в информационной сфере
4	Б1.О.28 Организационное и правовое обеспечение	Государственные органы разрабатывают и совершенствуют законодательное регулирование в сфере информационной безопасности с целью: 1) поддержки отечественных производителей средств защиты информации

№ задания	Дисциплина	Тексты заданий
	информационной безопасности	2) обеспечения защиты государственных информационных ресурсов 3) увеличения объема информации, циркулирующей в информационных сетях 4) защиты интересов правообладателей
5	Б1.О.28 Организационное и правовое обеспечение информационной безопасности	Структура информационного законодательства строится исходя из принципа: 1) Верховенства закона 2) Справедливости 3) Неравенства
6	Б1.О.28 Организационное и правовое обеспечение информационной безопасности	Конфиденциальность информации: 1) обязательное требование не сохранять такую информацию третьим лицам без согласия ее обладателя 2) обязательное требование не удалять такую информацию третьим лицам без согласия ее обладателя 3) обязательное требование не передавать такую информацию третьим лицам без согласия ее обладателя
7	Б1.О.28 Организационное и правовое обеспечение информационной безопасности	Документированная информация - это: 1) зафиксированная на материальном носителе информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель 2) информация без реквизитов, позволяющих определить такую информацию или ее материальный носитель 3) информация на жестком диске
8	Б1.О.28 Организационное и правовое обеспечение информационной безопасности	Информационные ресурсы принято классифицировать по: 1) принадлежности и доступности 2) принадлежности и надежности 3) доступности и информативности
9	Б1.О.28 Организационное и правовое обеспечение информационной безопасности	Обладателем информации может быть: 1) Российская Федерация, субъект Российской Федерации, муниципальное образование 2) физическое лицо, юридическое лицо, Российская Федерация, субъект Российской Федерации, муниципальное образование 3) физическое лицо, юридическое лицо
10	Б1.О.28 Организационное и правовое обеспечение информационной безопасности	Информация в зависимости от категории доступа к ней подразделяется: 1) общедоступную информацию и информацию ограниченного доступа 2) закрытую информацию и информацию ограниченного доступа 3) частично доступную информацию и информацию ограниченного доступа

БЛОК Б (повышенный уровень) – Задание закрытого типа на установление соответствия

Инструкция: Прочитайте текст и установите соответствие

№ задания	Дисциплина	Тексты заданий
11	Б1.О.28 Организационное и правовое обеспечение информационной безопасности	Предметом правового регулирования в информационной сфере являются: 1) создание и распространение информации 2) реализация права на поиск, получение, передачу и потребление информации 3) создание и применение информационных систем и технологий 4) создание и применение средств информационной безопасности 5) формирование информационных ресурсов Какие понятия им соответствуют? А. Регулируются Федеральным законом от 27.07.2006 №149-ФЗ (ред. от 24.06.2025) «Об информации, информационных технологиях и о защите информации». Б. Закреплено в статье 29 Конституции РФ. Согласно ей, каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом.

№ задания	Дисциплина	Тексты заданий
		В. Это возможность создания совокупности взаимосвязанных компонентов, которые работают вместе для сбора, обработки, хранения и передачи информации. Г. Включает, например, защиту устройств и личных данных (персональная безопасность), защиту внутренних сетей и серверов (корпоративная безопасность), защиту ключевых инфраструктур (государственная безопасность). Д. Процесс создания данных, организованных для получения достоверной информации в разных областях знаний и практической деятельности. Информационные ресурсы — это знания, подготовленные людьми для социального использования в обществе и зафиксированные на материальном носителе.
12	Б1.О.28 Организационное и правовое обеспечение информационной безопасности	В зависимости от порядка распространения информация подразделяется: 1) свободно распространяемую 2) предоставляемую по соглашению 3) распространяемую в соответствии с федеральными законами 4) распространение которой в РФ ограничивается или запрещается Какие примеры им соответствуют? А. Информация, накапливаемая в открытых фондах библиотек, музеев, а также в государственных, муниципальных и иных информационных системах; Б. Это могут быть сведения об общем размере инвестиций, сумме займа, количестве и качестве планируемых рабочих мест, ожидаемых налоговых поступлениях и другие. В. Информация, направленная на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды. Г. Информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению.
13	Б1.О.28 Организационное и правовое обеспечение информационной безопасности	Система защиты государственных секретов основывается на Законе РФ Закон РФ от 21.07.93 N 5485-І Редакция от 08.08.2024 — Действует с 08.08.2024. В настоящем Законе используются следующие основные понятия: 1) государственная тайна (ГТ) 2) носители сведений, составляющих государственную тайну 3) система защиты государственной тайны Какие понятия им соответствуют? А. Материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов. Б. Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации. В. Совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну, и их носителей, а также мероприятий, проводимых в этих целях.
14	Б1.О.28 Организационное и правовое обеспечение информационной безопасности	Устанавливаются три степени секретности сведений, составляющих государственную тайну, и соответствующие грифы секретности для носителей указанных сведений: 1) особой важности 2) совершенно секретно 3) секретно Какие понятия им соответствуют? А. Это степень секретности сведений, которые, согласно закону «О государственной тайне», относятся к военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-розыскной деятельности. Б. Один из грифов секретности, который обозначает сведения, распространение которых может нанести ущерб интересам ведомства или отрасли экономики Российской Федерации в одной или нескольких областях.

№ задания	Дисциплина	Тексты заданий
		В. Означает, что документ предназначен для прочтения руководящими работниками организации, рядовые сотрудники его не читают. Содержание текста достаточно важно, его распространение может нанести значительный ущерб.

БЛОК Б (повышенный уровень) – Задание закрытого типа на установление последовательности

Инструкция: Прочитайте текст и установите правильную последовательность

№ задания	Дисциплина	Тексты заданий
15	Б1.О.28 Организационное и правовое обеспечение информационной безопасности	Расставьте в правильной последовательности этапы нанесения реквизитов на носители сведений, составляющих государственную тайну: 1) о степени секретности сведений со ссылкой на соответствующий пункт перечня сведений, подлежащих засекречиванию 2) об органе государственной власти, о предприятии, об учреждении, организации, осуществивших засекречивание носителя 3) о дате или условии рассекречивания сведений 4) о регистрационном номере
16	Б1.О.28 Организационное и правовое обеспечение информационной безопасности	Расставьте в правильной последовательности этапы, связанные с охраной конфиденциальности информации в рамках трудовых отношений. Работодатель обязан: 1) создать работнику необходимые условия для соблюдения им установленного работодателем режима коммерческой тайны 2) ознакомить под расписку работника с установленным работодателем режимом коммерческой тайны и с мерами ответственности за его нарушение 3) ознакомить под расписку работника с перечнем информации, составляющей коммерческую тайну
17	Б1.О.28 Организационное и правовое обеспечение информационной безопасности	Расставьте в правильной последовательности этапы допуска к сведениям, составляющим государственную тайну, предполагает: 1) проведение проверочных мероприятий в отношении лица, получающего допуск 2) ознакомление лица, получающего допуск, с соответствующими нормами законодательства 3) получение согласия на временное ограничение прав от лица, получающего допуск

БЛОК В (высокий уровень) – Задание открытого типа с развернутым ответом

Инструкция: Прочитайте текст и запишите обоснованный ответ

№ задания	Дисциплина	Тексты заданий
18	Б1.О.28 Организационное и правовое обеспечение информационной безопасности	Впишите пропущенное словосочетание. В российском законодательстве предусмотрена ответственность за коммерческий подкуп. Согласно ч. 1 ст. 204 УК РФ, это _____ лицу, выполняющему управленческие функции в коммерческой или иной организации, денег, ценных бумаг, иного имущества, а равно незаконное оказание ему услуг имущественного характера за совершение действий (бездействия) в интересах дающего в связи с занимаемым этим лицом служебным положением
19	Б1.О.28 Организационное и правовое обеспечение информационной безопасности	Впишите пропущенное слово. На результаты интеллектуальной деятельности и приравненные к ним средства _____ признаются интеллектуальные права, которые включают исключительное право, являющееся имущественным правом, а в случаях, предусмотренных настоящим Кодексом, также личные неимущественные права и иные права (право следования, право доступа и другие).
20	Б1.О.28 Организационное и правовое	Впишите пропущенное словосочетание. Импорт, тиражирование, продажа, а также иное введение в гражданский оборот экземпляров программ без разрешения их правообладателей является _____

№ задания	Дисциплина	Тексты заданий
	обеспечение информационной безопасности	нарушителем _____. Суд может наложить арест на все экземпляры произведения, в отношении которых предполагается, что они являются контрафактными, а также на материалы и оборудование, используемые или предназначенные для их изготовления или воспроизведения.

Система оценивания выполнения тестовых заданий по компетенции УК-10

Номер задания	Указания по оцениванию	Результат оценивания (баллы, полученные за выполнение задания/характеристика правильности ответа)
Задания 1-10	Задания с выбором одного или нескольких верных ответов из предложенных считается верным, если правильно указана цифра или цифры, означающие верные ответы.	Совпадение с верным ответом оценивается 1 баллом; неверный ответ или его отсутствие - 0 баллов.
Задания 11-14	Задания закрытого типа на установление соответствия считается верным, если правильно установлены все соответствия (позиции из одного столбца верно сопоставлены с позициями другого)	Полное совпадение с верным ответом оценивается 1 баллом; неверный ответ или его отсутствие - 0 баллов.
Задания 15-17	Задания закрытого типа на установление последовательности считается верным, если правильно указана вся последовательность цифр	Полное совпадение с верным ответом оценивается 1 баллом; если допущены ошибки или ответ отсутствует - 0 баллов.
Задания 18-20	Задание открытого типа с развернутым ответом считается верным, если ответ совпадает с эталонным по содержанию и полноте.	Полный правильный ответ на задание оценивается 1 баллом. Если в ответе используются перечисления, то различный порядок следования правильных ответов в перечислении не считается ошибкой. Если допущена ошибка, ответ не полный, неправильный или отсутствует - 0 баллов.

ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности

БЛОК А (базовый уровень) – Задание с выбором одного или нескольких верных ответов из предложенных

Инструкция по тестам Блока А: Прочитайте текст и выберите один или несколько правильных ответов

№ задания	Дисциплина	Тексты заданий
1	Б1.О.28 Организационное и правовое обеспечение информационной безопасности	Профессиональная тайна – это: 1) защищаемая по закону информация, доверенная лицу в силу исполнения им своих профессиональных обязанностей, не связанных с государственной и муниципальной службой 2) защищаемая по закону информация, доверенная лицу в силу исполнения им своих профессиональных обязанностей, связанных с государственной и муниципальной службой 3) защищаемая по закону информация, доверенная лицу в силу исполнения им своих профессиональных обязанностей, не связанных с государственной службой
2	Б1.О.28 Организационное и правовое обеспечение информационной безопасности	Общедоступные персональные данные - это: 1) персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или в соответствии с федеральными законами 2) персональные данные, доступ неограниченного круга лиц к которым предоставлен с без согласия субъекта персональных данных или в соответствии с федеральными законами 3) персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или в соответствии с системой муниципальных правовых актов
3	Б1.О.28 Организационное и правовое обеспечение информационной безопасности	Федеральный орган, который выполняет специальные и контрольные функции по обеспечению государственной безопасности, связанной с критической информационной инфраструктурой, вопросами государственной тайны, противодействием иностранной технической разведке - это: 1) ФСТЭК ☐ 2) СВР ☐ 3) ФСБ ☐
4	Б1.О.28 Организационное и правовое обеспечение информационной безопасности	Техническими средствами защиты авторских прав признаются: 1) любые технологии, технические устройства или их компоненты, контролирующие доступ к произведению, предотвращающие либо ограничивающие осуществление действий, которые разрешены автором или иным правообладателем в отношении произведения 2) особые технологии, из определенного перечня средств, контролирующие доступ к произведению, предотвращающие либо ограничивающие осуществление действий, которые не разрешены автором или иным правообладателем в отношении произведения 3) любые технологии, технические устройства или их компоненты, контролирующие доступ к произведению, предотвращающие либо ограничивающие осуществление действий, которые не разрешены автором или иным правообладателем в отношении произведения
5	Б1.О.28 Организационное и правовое обеспечение информационной безопасности	Лицензия – это: документ, дающий право на осуществление указанного вида деятельности в течении определенного времени: 1) документ, дающий право на осуществление указанного вида деятельности в течении одного года 2) документ, дающий право на осуществление указанного вида деятельности в течение неопределенного времени 3) документ, дающий право на осуществление указанного вида деятельности в течении определенного времени

№ задания	Дисциплина	Тексты заданий
6	Б1.О.28 Организационное и правовое обеспечение информационной безопасности	Контроль за обеспечением защиты ГТ осуществляют: 1) Президент и Правительство РФ; 2) Президент; 3) Правительство РФ; 4) Государственная дума
7	Б1.О.28 Организационное и правовое обеспечение информационной безопасности	К конфиденциальной информации не относится: 1) Коммерческая тайна 2) Персональные данные о гражданах 3) Государственная тайна 4) Ноу-хау
8	Б1.О.28 Организационное и правовое обеспечение информационной безопасности	Государственные информационные ресурсы не могут принадлежать: 1) физическим лицам 2) коммерческим предприятиям 3) негосударственным учреждениям 4) всем перечисленным субъектам
9	Б1.О.28 Организационное и правовое обеспечение информационной безопасности	Патентное право – это: 1) форма правовой защиты в отношении изобретений во всех областях человеческой деятельности 2) форма правовой защиты в отношении музыкальных произведений 3) форма правовой защиты в отношении графических изображений
10	Б1.О.28 Организационное и правовое обеспечение информационной безопасности	Авторское право на произведение возникает в силу: 1) факта огласки 2) факта его передачи 3) факта его создания

БЛОК Б (повышенный уровень) – Задание закрытого типа на установление соответствия
Инструкция: Прочитайте текст и установите соответствие

№ задания	Дисциплина	Тексты заданий
11	Б1.О.28 Организационное и правовое обеспечение информационной безопасности	Профессиональная тайна – защищаемая по закону информация, доверенная лицу в силу исполнения им своих профессиональных обязанностей, не связанных с государственной и муниципальной службой и не являющаяся государственной или коммерческой тайной, распространение которой может нанести ущерб интересам лица, доверившего эти сведения. В соответствии с данным определением можно выделить следующие объекты профессиональной тайны: 1) врачебная тайна 2) тайна связи 3) нотариальная тайна 4) адвокатская тайна 5) тайна усыновления 6) тайна страхования 7) тайна исповеди А) сведения, доверенные священнослужителю гражданином Б) сведения о страхователе, застрахованном лице и выгодоприобретателе В) сведения об усыновлении ребенка усыновителем Г) сведения, сообщенные адвокату гражданином в связи с оказанием юридической помощи Д) сведения, доверенные нотариусу в связи с совершением нотариальных действий Е) тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений Ё) информация, содержащая: результаты обследования лица, сведения о факте

№ задания	Дисциплина	Тексты заданий
12	Б1.О.28 Организационное и правовое обеспечение информационной безопасности	обращения за медицинской помощью, иные сведения о состоянии здоровья Организационно-техническими методами обеспечения информационной безопасности РФ являются: 1) создание и совершенствование системы обеспечения информационной безопасности РФ 2) разработка и совершенствование средств защиты информации 3) сертификация средств защиты информации, и лицензирование деятельности в области защиты информации Установите соответствие методов их описанию: А) система обеспечения информационной безопасности - совокупность сил обеспечения информационной безопасности, осуществляющих скоординированную и спланированную деятельность, и используемых ими средств обеспечения информационной безопасности Б) выбор наиболее эффективных способов и методов защиты информации В) этот документ свидетельствует о том, что устройства соответствуют установленным стандартам и могут эффективно использоваться по назначению
13	Б1.О.28 Организационное и правовое обеспечение информационной безопасности	Несанкционированный доступ и перехват информации (QA) включает в себя следующие виды компьютерных преступлений: 1) QAH 2) QAI 3) QAT Установите соответствие обозначений их содержанию: А. Кража времени: незаконное использование компьютерной системы или сети с намерением неуплаты. Б. Перехват (interception): перехват при помощи технических средств, без права на то. Перехват информации осуществляется либо прямо через внешние коммуникационные каналы системы, либо путем непосредственного подключения к линиям периферийных устройств. При этом объектами непосредственного подслушивания являются кабельные и проводные системы, наземные микроволновые системы, системы спутниковой связи, а также специальные системы правительственной связи. К данному виду компьютерных преступлений также относится электромагнитный перехват (electromagnetic pickup). Современные технические средства позволяют получать информацию без непосредственного подключения к компьютерной системе: ее перехват осуществляется за счет излучения центрального процессора, дисплея, коммуникационных каналов, принтера и т.д. Все это можно осуществлять, находясь на достаточном удалении от объекта перехвата. В. Компьютерный абсордаж (хакинг - hacking): неправомерный доступ в компьютер или сеть. Этот вид компьютерных преступлений обычно используется хакерами для проникновения в чужие информационные сети.
14	Б1.О.28 Организационное и правовое обеспечение информационной безопасности	Для характеристики методов несанкционированного доступа и перехвата информации используется следующая терминология: 1) "Жучок" (bugging) 2) "Откачивание данных" (data leakage) 3) "Уборка мусора" (scavenging) 4) метод следования "За дураком" (piggybacking) 5) метод "За хвост" (between the lines entry) 6) метод "Неспешного выбора" (browsing) 7) метод "Поиск бреши" (trapdoor entry) 8) метод "Люк" (trapdoor) 9) метод "Маскарад" (masquerading) 10) метод "Мистификация" (spoofing) Установите соответствие терминов их содержанию: А. Используется при случайном подключении "чужой" системы. Злоумышленник, формируя правдоподобные отклики, может поддерживать заблуждение ошибочно подключившегося пользователя в течение какого-то промежутка времени и получать некоторую полезную для него информацию, например коды пользователя. Б. Злоумышленник с использованием необходимых средств проникает в

№ задания	Дисциплина	Тексты заданий
		компьютерную систему, выдавая себя за законного пользователя. В. В найденной "бреши" программа "разрывается" и туда вставляется определенное число команд. По мере необходимости "люк" открывается, а встроенные команды автоматически осуществляют свою задачу. Г. Используются ошибки или неудачи в логике построения программы. Обнаруженные бреши могут эксплуатироваться неоднократно. Д. Несанкционированный доступ к базам данных и файлам законного пользователя осуществляется путем нахождения слабых мест в защите систем. Однажды обнаружив их, злоумышленник может спокойно читать и анализировать содержащуюся в системе информацию, копировать ее, возвращаться к ней по мере необходимости. Е. Можно подключаться к линии связи законного пользователя и, догадавшись, когда последний заканчивает активный режим, осуществлять доступ к системе. Ё. Если набрать в руки различные предметы, связанные с работой на компьютере, и прохаживаться с деловым видом около запертой двери, где находится терминал, то, дождавшись законного пользователя, можно пройти в дверь помещения вместе с ним. Ж. Поиск данных, оставленных пользователем после работы на компьютере. Этот способ имеет две разновидности - физическую и электронную. В физическом варианте он может сводиться к осмотру мусорных корзин и сбору брошенных в них распечаток, деловой переписки и т.д. Электронный вариант требует исследования данных, оставленных в памяти машины. З. Отражает возможность сбора информации, необходимой для получения основных данных, в частности о технологии ее прохождения в системе. И. Характеризует установку микрофона в компьютере с целью перехвата разговоров обслуживающего персонала.

БЛОК Б (повышенный уровень) – Задание закрытого типа на установление последовательности

Инструкция: Прочитайте текст и установите правильную последовательность

№ задания	Дисциплина	Тексты заданий
15	Б1.О.28 Организационное и правовое обеспечение информационной безопасности	Для характеристики преступления могут использоваться до пяти кодов, расположенных в порядке убывания значимости совершенного. Расставьте в последовательном порядке убывания значимости совершенного: 1. QF - Компьютерное мошенничество 2. QD - Изменение компьютерных данных 3. QA - Несанкционированный доступ и перехват 4. QR - Незаконное копирование 5. QS - Компьютерный саботаж 6. QZ - Прочие компьютерные преступления
16	Б1.О.28 Организационное и правовое обеспечение информационной безопасности	Расставьте в последовательном порядке этапы процесса следственных действий обязательных для первоначального этапа расследования: 1. Назначение комплексной судебно-бухгалтерской и программно-технической экспертизы с привлечением специалистов правоохранительных органов, специалистов в области средств компьютерной техники, по ведению банковского учета с использованием средств компьютерной техники, документообороту, организации бухучета и отчетности, специалистов по обеспечению безопасности информации в компьютерных системах. 2. Исследование: журналов сбойных ситуаций, рабочего времени ЭВМ, по передачи смен операторами; средств защиты и контроля банковских компьютерных систем, регистрирующих пользователей, моменты включения (активации) системы либо подключение к ним абонентов с определенным индексом или без такового; протоколов вечернего решения, представляющих собой копию действий операторов, отображенную на бумажном носителе в ходе вечерней обработки информации, которая проводится по истечении каждого операционного дня; контрольных чисел файлов; всего программного обеспечения ЭВМ; "прошитых" микросхем постоянно запоминающих устройств, микропроцессоров и их схемного исследования. 3. Получение и анализ технических указаний по обработке ежедневной

№ задания	Дисциплина	Тексты заданий
		бухгалтерской информации с перечнем выходящих форм. 4. Допрос лиц из числа инженеров - программистов, занимавшихся разработкой программного обеспечения и его сопровождением, специалистов отвечающих за защиту информации и специалистов электронщиков, занимающихся эксплуатацией и ремонтом вычислительной техники. 5. Назначение комплексной судебно-бухгалтерской и программно-технической экспертизы с привлечением специалистов правоохранительных органов, специалистов в области средств компьютерной техники, по ведению банковского учета с использованием средств компьютерной техники, документообороту, организации бухучета и отчетности, специалистов по обеспечению безопасности информации в компьютерных системах. Проведение обыска в служебном помещении, на рабочем месте подозреваемого с целью обнаружения и изъятия физических носителей машинной информации и других документов, имеющих или возможно имеющих отношение к несанкционированному отношению программного обеспечения или носящих иные следы подготовки к хищению денежных средств.
17	Б1.О.28 Организационное и правовое обеспечение информационной безопасности	Расставьте в последовательном порядке нормативно-правовое обеспечение информационной безопасности: 1. Политика ИБ 2. Частные политики информационной безопасности 3. Инструкции информационной безопасности 4. Регламенты информационной безопасности

БЛОК В (высокий уровень) – Задание открытого типа с развернутым ответом

Инструкция: Прочитайте текст и запишите обоснованный ответ

№ задания	Дисциплина	Тексты заданий
18	Б1.О.28 Организационное и правовое обеспечение информационной безопасности	Дополните фразу. Электронный документ – это документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по _____ сетям или обработки в информационных системах
19	Б1.О.28 Организационное и правовое обеспечение информационной безопасности	Дополните фразу. Гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных – это _____ информационной системы.
20	Б1.О.28 Организационное и правовое обеспечение информационной безопасности	Дополните фразу. Архивные документы включаются в состав _____ фонда на основании экспертизы ценности документов. Решение принимается Центральной экспертно-проверочной комиссией Федерального архивного агентства. В фонде хранятся документы государственной, муниципальной и частной собственности. Архивные документы, находящиеся в государственной и муниципальной собственности, не подлежат приватизации и не могут находиться в хозяйственном обороте.

Система оценивания выполнения тестовых заданий по компетенции ОПК-5

Номер задания	Указания по оцениванию	Результат оценивания (баллы, полученные за выполнение задания/характеристика правильности ответа)
Задания 1-10	Задания с выбором одного или нескольких верных ответов из предложенных считается верным, если правильно указана цифра или цифры, означающие верные ответы.	Совпадение с верным ответом оценивается 1 баллом; неверный ответ или его отсутствие - 0 баллов.
Задания 11-14	Задания закрытого типа на установление соответствия считается верным, если правильно установлены все соответствия (позиции из одного столбца верно сопоставлены с позициями другого)	Полное совпадение с верным ответом оценивается 1 баллом; неверный ответ или его отсутствие - 0 баллов.
Задания 15-17	Задания закрытого типа на установление последовательности считается верным, если правильно указана вся последовательность цифр	Полное совпадение с верным ответом оценивается 1 баллом; если допущены ошибки или ответ отсутствует- 0 баллов.
Задания 18-20	Задание открытого типа с развернутым ответом считается верным, если ответ совпадает с эталонным по содержанию и полноте.	Полный правильный ответ на задание оценивается 1 баллом. Если в ответе используются перечисления, то различный порядок следования правильных ответов в перечислении не считается ошибкой. Если допущена ошибка, ответ не полный, неправильный или отсутствует - 0 баллов.

Методические рекомендации по освоению дисциплины

1. Методические рекомендации преподавателю

Перед началом изучения дисциплины преподаватель должен ознакомить обучающихся с рабочей программой и оценочными материалами по дисциплине, с видами учебной и самостоятельной работы, перечнем литературы и интернет-ресурсов, с формами текущей и промежуточной аттестации, с критериями оценки качества знаний для итоговой оценки по дисциплине.

При проведении лекций, преподаватель:

- 1) формулирует тему и цель занятия, объявляет учебные вопросы;
- 2) излагает основные теоретические положения;
- 3) с помощью технических средств обучения и/или под запись дает определения основных понятий, расчетных формул;
- 4) проводит примеры из отечественного и зарубежного опыта, дает текущие статистические данные для наглядного и образного представления изучаемого материала;
- 5) в конце занятия выдает вопросы для самостоятельного изучения.

На практических занятиях в учебной аудитории обучающийся консультируется с преподавателем, определяет наиболее эффективные методы решения поставленных задач. Если какая-то часть заданий практического занятия остается не выполненной, обучающийся может продолжить их выполнение во время внеаудиторной самостоятельной работы.

Для оценки полученных знаний и освоения учебного материала по каждому разделу и в целом по дисциплине преподаватель использует формы текущего контроля и промежуточной аттестации обучающихся.

2. Методические рекомендации обучающимся

Приступая к изучению новой учебной дисциплины, обучающиеся должны ознакомиться с рабочей программой, оценочными материалами, учебной, научной и методической литературой, имеющейся в ЭИОС СКФ МТУСИ,

Глубина усвоения дисциплины зависит от активной и систематической работы обучающегося на лекциях и практических занятиях, а также в ходе самостоятельной работы, по изучению рекомендованной литературы.

2.1 Методические указания для обучающихся по лекционным занятиям

Важно сосредоточить внимание на содержании лекции. Это поможет лучше воспринимать учебный материал и уяснить взаимосвязь проблем по всей дисциплине.

Основное содержание лекции целесообразнее записывать в тетради в виде ключевых фраз, понятий, тезисов, обобщений, схем, опорных выводов. Необходимо обращать внимание на термины, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации. Желательно оставлять в конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющей материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

С целью уяснения теоретических положений, разрешения спорных ситуаций необходимо задавать преподавателю уточняющие вопросы. Для закрепления содержания лекции в памяти, необходимо во время самостоятельной работы внимательно прочесть свой конспект и дополнить его записями из учебников и рекомендованной литературы.

Конспектирование читаемых лекций и их последующая доработка способствует более глубокому усвоению знаний, и поэтому являются важной формой учебной деятельности обучающихся.

2.3 Методические указания для обучающихся по подготовке к практическим занятиям

Целью практических занятий является закрепление теоретических знаний, полученных при изучении дисциплины.

При подготовке к практическому занятию целесообразно выполнить следующие рекомендации:

- изучить основную литературу; ознакомиться с дополнительной литературой, новыми публикациями в периодических изданиях: журналах, газетах и т.д.;
- при необходимости доработать конспект лекций. При этом учесть рекомендации преподавателя и требования учебной программы.

При выполнении практических занятий основным методом обучения является самостоятельная работа обучающегося под управлением преподавателя. На них пополняются теоретические знания обучающихся, их умение творчески мыслить, анализировать, обобщать изученный материал, проверяется отношение обучающихся к будущей профессиональной деятельности.

Вопросы, не рассмотренные на лекциях и практических занятиях, должны быть изучены обучающимися в ходе самостоятельной работы. Контроль самостоятельной работы обучающихся над учебной программой курса осуществляется в ходе занятий методом посредством тестирования. В ходе самостоятельной работы каждый обучающийся обязан прочитать основную и по возможности дополнительную литературу по изучаемой теме, дополнить конспекты лекций недостающим материалом, выписками из рекомендованных первоисточников. Выделить непонятные термины, найти их значение в энциклопедических словарях.

Для подготовки к практическим занятиям обучающиеся могут воспользоваться электронно-библиотечными системами. Также обучающиеся могут взять на дом необходимую литературу на абонементе библиотеки Филиала или воспользоваться читальными залами.

Оценка выполненной работы осуществляется преподавателем комплексно: по результатам выполнения заданий, устному сообщению и оформлению работы.

После подведения итогов занятия обучающийся обязан устранить недостатки, отмеченные преподавателем при оценке его работы.

3. Методические рекомендации для обучающихся по самостоятельной работе

Самостоятельная работа обучающихся является составной частью учебной работы и имеет целью закрепление и углубление полученных знаний и навыков, поиск и приобретение новых знаний, в том числе с использованием автоматизированных обучающих курсов (систем), а также выполнение учебных заданий, подготовку к предстоящим занятиям, зачетам и экзаменам.

Самостоятельная работа во внеаудиторное время включает в себя:

- повторение лекционного материала;
- подготовки к практическим занятиям;
- изучения учебной и научной литературы;
- решения задач, выданных на практических занятиях;
- подготовки к тестированию;
- выделение наиболее сложных и проблемных вопросов по изучаемой теме, получение разъяснений и рекомендаций по данным вопросам с преподавателями кафедры на их еженедельных консультациях.
- проведение самоконтроля путем ответов на вопросы текущего контроля знаний, решения представленных вопросов и задач, тестов.

Перед выполнением внеаудиторной самостоятельной работы преподаватель проводит инструктаж (консультацию) с определением цели задания, его содержания, сроков

выполнения, основных требований к результатам работы, критериев оценки, форм контроля и перечня источников и литературы.

Обычно постановку задачи обучаемым на проведение самостоятельной работы преподаватель осуществляет на одном из занятий, предшествующему данному.

Методику самостоятельной работы все обучаемые выбирают индивидуально.

Контроль самостоятельной работы обучающихся осуществляется на групповых и индивидуальных консультациях, на практических занятиях, при проверке и защите отчетов о выполнении практических заданий в рамках текущего контроля.

Обучающимся очной формы обучения при освоении вопросов для самостоятельного изучения, рекомендуется соблюдать последовательность их изучения, представленную в таблице.

Таблица – Учебный материал, выносимый на самостоятельное изучение обучающимся очной формы обучения

№	Темы, разделы, вынесенные на самостоятельную подготовку, вопросы для подготовки к практическим и лабораторным занятиям; курсовые работы, содержание контрольных работ и др.	Часов всего: 44
Модуль 1		22
1	Законодательство РФ в области информационной безопасности.	2
2	Изучение положений о государственном лицензировании деятельности в области защиты информации.	4
3	Защита компьютерной информации.	4
4	Технические каналы утечки компьютерной информации	4
5	Защита информации от утечки по техническим каналам.	2
6	Государственное регулирование деятельности в области защиты информации.	2
7	Организация режима секретности.	2
8	Допуск к государственной тайне.	2
Модуль 2		22
1	Изучение положений о сертификации средств защиты информации по требованиям безопасности информации	4
2	Система сертификации средств криптографической защиты информации.	4
3	Классификация компьютерных преступлений.	4
4	Криминалистические особенности расследования компьютерных преступлений.	4
5	Международные стандарты и соглашения в области безопасности информационных технологий.	4
6	Преступления в сфере компьютерной информации.	2

Самостоятельная работа обучающихся над усвоением материала по дисциплине может выполняться в помещении для самостоятельной работы СКФ МТУСИ, посредством использования электронной библиотеки и ЭИОС.