МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования "Российский государственный геологоразведочный университет имени Серго Орджоникидзе"

(МГРИ)

Организационное и правовое обеспечение информационной безопасности

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Промышленной кибербезопасности и защиты геоданных**

Учебный план s100503_25_BZO25.plx
Специальность 10.05.03 Информационная безопасность автоматизированных систем

Квалификация **Специалист по защите информации**

Форма обучения **очная**

Общая трудоемкость **6 ЗЕТ**

Часов по учебному плану 216
в том числе:
аудиторные занятия 106,6
самостоятельная работа 82,4
часов на контроль 27

Виды контроля в семестрах:
экзамены 7
зачеты 6

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**6 (3.2)**		**7 (4.1)**		Итого	
Недель	14		16 5/6			
Вид занятий	УП	РП	УП	РП	УП	РП
Лекции	28	28	32	32	60	60
Практические	28	28	16	16	44	44
Иные виды контактной работы	0,25	0,25	2,35	2,35	2,6	2,6
В том числе инт.	4	4	4	4	8	8
Итого ауд.	56,25	56,25	50,35	50,35	106,6	106,6
Контактная работа	56,25	56,25	50,35	50,35	106,6	106,6
Сам. работа	51,75	51,75	30,65	30,65	82,4	82,4
Часы на контроль			27	27	27	27
Итого	108	108	108	108	216	216

Москва 2025

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Целью преподавания дисциплины является подготовка специалистов в области управления и организации информационной безопасности, имеющих первичные навыки принятия решения на основе многочисленных нормативно-правовых актов в сфере информационной безопасности, и владеющих общими принципами организации и правового регулирования защиты информации. Задачи дисциплины:
1.2	- изучение основных нормативных правовых актов международного, федерального и ведомственно-отраслевого уровней, определяющих организационные и правовые аспекты в области информационной безопасности;
1.3	- изучение теоретических, методологических и практических проблем формирования, функционирования и развития систем организационного и правового обеспечения информационной безопасности;
1.4	- ознакомление с процессами планирования в организационной
1.5	защиты информации;
1.6	- приобретение навыков работы с нормативной информацией в
1.7	сфере защиты информации;
1.8	- рассмотрение методов и особенностей применяемых в
1.9	организационной защиты информации в зависимости от характера защищаемой
1.10	информации;
1.11	- изучение методов анализа деятельности организаций с целью
1.12	определения информационно-технологических ресурсов, подлежащих защите.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.О
2.1	**Требования к предварительной подготовке обучающегося:**
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Технология подготовки выпускной квалификационной работы
2.2.2	Комплексное обеспечение защиты информации объектов информатизации
2.2.3	Управление информационной безопасностью
2.2.4	Основы аттестации объектов информатизации

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
УК-10: Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	
Знать:	
Уровень 1	природу экстремизма, терроризма, коррупции как социально-правового явления.
Уровень 2	действующие уголовно-правовые нормы, обеспечивающие борьбу и противодействие экстремизму, терроризму и коррупционному поведению в различных областях жизнедеятельности.
Уровень 3	способы профилактики и борьбы с проявлениями экстремизма и терроризма, коррупционного поведения и противодействия им в профессиональной деятельности, а также необходимость формирования нетерпимого отношения к ней
Уметь:	
Уровень 1	проводить мероприятия, обеспечивающие формирование гражданской позиции и предотвращение коррупционного поведения в социуме, предотвращение проявлений экстремизма и терроризма
Уровень 2	планировать и организовывать мероприятия, обеспечивающие формирование гражданской позиции и предотвращение коррупционного поведения в социуме, предотвращение проявлений экстремизма и терроризма
Уровень 3	реализовывать средства обеспечения законности и правопорядка в сфере противодействия коррупционному поведению в социуме и предотвращения проявлений экстремизма и терроризма
Владеть:	
Уровень 1	навыками взаимодействия в обществе на основе нетерпимого отношения к коррупционному поведению в социуме и предотвращения проявлений экстремизма и терроризма
Уровень 2	навыками организации работы в сфере профессиональной деятельности на основе нетерпимого отношения к коррупционному поведению, предотвращения проявлений экстремизма и терроризма
Уровень 3	навыками экспертно-консультативной работы по правовым вопросам противодействия коррупционному поведению, предотвращения проявлений экстремизма и терроризма

ОПК-5: Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации

Знать:	
Уровень 1	основы правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации; основные понятия и характеристику основных отраслей права, применяемых в профессиональной деятельности организации; основы российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации; правовые основы организации защиты государственной тайны и конфиденциальной информации, правовую характеристику преступлений в сфере компьютерной информации и меры правовой и дисциплинарной ответственности за разглашение защищаемой информации;
Уровень 2	статус и порядок работы основных правовых информационно-справочных систем; основы организации и деятельности органов государственной власти в Российской Федерации; основные документы по стандартизации в сфере управления ИБ; принципы формирования политики информационной безопасности в автоматизированных системах;
Уровень 3	требования информационной безопасности при эксплуатации автоматизированной системы; требования нормативных документов к составу, содержанию и оформлению технической документации объекта информатизации; виды и состав документации современной организации, особенности документирования профессиональной деятельности;
Уметь:	
Уровень 1	применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности; обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, предпринимать необходимые меры по восстановлению нарушенных прав; анализировать и разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно- распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации; формулировать основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации;
Уровень 2	формулировать основные требования информационной безопасности при эксплуатации автоматизированной системы; формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации; формировать политики информационной безопасности организации;
Уровень 3	выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы; разрабатывать техническую документацию объекта информатизации; определять виды документов, необходимых для оформления управленческих действий в профессиональной деятельности, грамотно составлять и оформлять служебные документы;
Владеть:	
Уровень 1	понятийно-категориальным аппаратом юриспруденции; навыками установления фактических обстоятельств, юридической основы и квалификации;
Уровень 2	навыком работы с нормативными правовыми актами различной юридической силы; навыками применения основных законов, связанных с организационно-правовым обеспечением информационной безопасности в профессиональной деятельности;
Уровень 3	навыками организации и обеспечения режима секретности; методами организации и управления служб защиты информации на предприятии; методами формирования требований по защите информации

ОПК-6: Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	
Знать:	
Уровень 1	систему стандартов и нормативных правовых актов уполномоченных федеральных органов исполнительной власти по лицензированию в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации; систему нормативных правовых актов уполномоченных федеральных органов исполнительной власти по аттестации объектов информатизации и сертификации средств защиты информации;
Уровень 2	задачи органов защиты государственной тайны и служб защиты информации на предприятиях;
Уровень 3	принципы формирования комплекса мер по защите информации ограниченного доступа объектов информатизации в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю

Уметь:	
Уровень 1	классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; засекречивать и рассекречивать сведения и их носители;
Уровень 2	использовать систему организационных мер, направленных на защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами ФСБ России, ФСТЭК России; определять комплекс мер для обеспечения защиты информации объектов информатизации;
Уровень 3	применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности; разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации
Владеть:	
Уровень 1	навыком анализа информационной инфраструктуры информационной системы и ее безопасности объектов информатизации; навыками применения основных законов, связанных с организационно-правовым обеспечением информационной безопасности в профессиональной деятельности;
Уровень 2	навыками работы с нормативными правовыми актами; навыками организации и обеспечения режима секретности;
Уровень 3	методами организации и управления деятельностью служб защиты информации на предприятии; методами формирования требований по защите информации;

В результате освоения дисциплины (модуля) обучающийся должен

3.1	**Знать:**
3.1.1	содержание основных нормативных правовых актов в сфере противодействия коррупции;
3.1.2	основы правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации; основные понятия и характеристику основных отраслей права, применяемых в профессиональной деятельности организации; основы российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации; правовые основы организации защиты государственной тайны и конфиденциальной информации, правовую характеристику преступлений в сфере компьютерной информации и меры правовой и дисциплинарной ответственности за разглашение защищаемой информации; статус и порядок работы основных правовых информационно-справочных систем; основы организации и деятельности органов государственной власти в Российской Федерации;
3.1.3	систему стандартов и нормативных правовых актов уполномоченных федеральных органов исполнительной власти по лицензированию в области обеспечения защиты
3.1.4	государственной тайны, технической защиты конфиденциальной информации; систему нормативных правовых актов уполномоченных федеральных органов исполнительной власти по аттестации объектов информатизации и сертификации средств защиты информации; задачи органов защиты государственной тайны и служб защиты информации на предприятиях;
3.2	**Уметь:**
3.2.1	соблюдать требования антикоррупционного законодательства, воздерживаться от поведения, вызывающего сомнение в объективном и беспристрастном исполнении должностных (служебных) обязанностей;
3.2.2	применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности; обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, предпринимать необходимые меры по восстановлению нарушенных прав; анализировать и разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно- распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации; формулировать основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по
3.2.3	требованиям безопасности информации; формулировать основные требования информационной безопасности при эксплуатации автоматизированной системы; формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации;
3.2.4	использовать систему организационных мер, направленных на защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами ФСБ России, ФСТЭК России;
3.3	**Владеть:**
3.3.1	применения основных нормативных правовых актов в сфере противодействия коррупции;
3.3.2	работы с нормативными правовыми актами;

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)							
Код занятия	**Наименование разделов и тем /вид занятия/**	**Семестр / Курс**	**Часов**	**Компетен-ции**	**Литература**	**Инте ракт.**	**Примечание**
	Раздел 1. Информационные отношения как объект правового регулирования. Законодательство Российской Федерации в области информационной безопасности						
1.1	Информационные отношения как объект правового регулирования. Законодательство Российской Федерации в области информационной безопасности /Лек/	6	2	УК-10 ОПК-5 ОПК-6	Л1.1 Л1.2	0	
1.2	Подготовка доклада на семинар /Ср/	6	8	УК-10 ОПК-5 ОПК-6	Л1.1 Л1.2	0	
	Раздел 2. Правовой режим защиты государственной тайны						
2.1	Система защиты государственной тайны /Лек/	6	2	УК-10 ОПК-5 ОПК-6	Л1.1 Л1.2	0	
2.2	Правовой режим защиты государственной тайны /Пр/	6	10	УК-10 ОПК-5 ОПК-6	Л1.1 Л1.2	0	
2.3	Подготовка к практическим занятиям /Ср/	6	23,75	УК-10 ОПК-5 ОПК-6	Л1.1 Л1.2	0	
2.4	Подготовка доклада на семинар /Ср/	6	7	УК-10 ОПК-5 ОПК-6	Л1.1 Л1.2	0	
	Раздел 3. Правовые режимы защиты информации ограниченного доступа						
3.1	Правовые режимы защиты информации ограниченного доступа /Лек/	6	2	УК-10 ОПК-5 ОПК-6	Л1.1 Л1.2	0	
3.2	Правовые режимы защиты информации ограниченного доступа /Пр/	6	2	УК-10 ОПК-5 ОПК-6	Л1.1 Л1.2	2	
3.3	Подготовка доклада на семинар /Ср/	6	4	УК-10 ОПК-5 ОПК-6	Л1.1 Л1.2	0	
	Раздел 4. Правовая охрана результатов интеллектуальной деятельности						
4.1	Правовая охрана результатов интеллектуальной деятельности /Лек/	6	2	УК-10 ОПК-5 ОПК-6	Л1.1 Л1.2	0	
4.2	Правовая охрана результатов интеллектуальной деятельности /Пр/	6	2	УК-10 ОПК-5 ОПК-6	Л1.1 Л1.2	2	
4.3	Подготовка доклада на семинар /Ср/	6	9	УК-10 ОПК-5 ОПК-6	Л1.1 Л1.2	0	
	Раздел 5. Преступления в сфере компьютерной информации						
5.1	Преступления в сфере компьютерной информации /Лек/	6	2	УК-10 ОПК-5 ОПК-6	Л1.1 Л1.2	0	
	Раздел 6. Понятие организационной защиты информации						
6.1	Понятие организационной защиты информации /Лек/	6	2	УК-10 ОПК-5 ОПК-6	Л1.1 Л1.2	0	

	Раздел 7. Подбор сотрудников на должности, связанные с работой с конфиденциальной информацией, и текущая работа с ним.						
7.1	Подбор сотрудников на должности, связанные с работой с конфиденциальнойинформацией, и текущая работа с ним. /Лек/	6	2	УК-10 ОПК-5 ОПК-6	Л1.1 Л1.2	0	
7.2	Подбор сотрудников на должности, связанные с работой с конфиденциальной информацией, и текущая работа с ним. /Пр/	6	2	УК-10 ОПК-5 ОПК-6	Л1.1 Л1.2	0	
	Раздел 8. Допуск и доступ к государственной, служебной тайнам и персональным данным сотрудников.						
8.1	Допуск и доступ к государственной, служебной тайнам и персональным данным сотрудников. /Лек/	6	2	УК-10 ОПК-5 ОПК-6	Л1.1 Л1.2	0	
8.2	Допуск и доступ к государственной, служебной тайнам и персональным данным сотрудников. /Пр/	6	2	УК-10 ОПК-5 ОПК-6	Л1.1 Л1.2	0	
	Раздел 9. Организация служебного расследования по фактам разглашения и утечки конфиденциальной информации.						
9.1	Организация служебного расследования по фактам разглашения и утечки конфиденциальной информации. /Лек/	6	2	УК-10 ОПК-5 ОПК-6	Л1.1 Л1.2	0	
9.2	Организация служебного расследования по фактам разглашения и утечки конфиденциальной информации. /Пр/	6	2	УК-10 ОПК-5 ОПК-6	Л1.1 Л1.2	0	
	Раздел 10. Требования к помещениям и хранилищам, в которых ведутся закрытые работы и хранятся конфиденциальные документы и изделия.						
10.1	Требования к помещениям и хранилищам, в которых ведутся закрытые работы и хранятся конфиденциальные документы и изделия. /Лек/	6	2	УК-10 ОПК-5 ОПК-6	Л1.1 Л1.2	0	
10.2	Требования к помещениям и хранилищам, в которых ведутся закрытые работы и хранятся конфиденциальные документы и изделия. /Пр/	6	2	УК-10 ОПК-5 ОПК-6	Л1.1 Л1.2	0	
	Раздел 11. Организация охраны территории, зданий, помещений и сотрудников. Организация пропускного и внутриобъектового режимов						
11.1	Организация охраны территории, зданий, помещений и сотрудников. Организация пропускного и внутриобъектового режимов /Лек/	6	2	УК-10 ОПК-5 ОПК-6	Л1.1 Л1.2	0	
11.2	Организация охраны территории, зданий, помещений и сотрудников. Организация пропускного и внутриобъектового режимов /Пр/	6	2	УК-10 ОПК-5 ОПК-6	Л1.1 Л1.2	0	
	Раздел 12. Информационная безопасность в системе информационного права						

12.1	Информационное право как отрасль права /Лек/	6	2	УК-10 ОПК-5 ОПК-6	Л1.1 Л1.2	0	
12.2	Информационные правоотношения. Объекты и субъекты информационных правоотношений /Лек/	6	4	УК-10 ОПК-5 ОПК-6	Л1.1 Л1.2	0	
12.3	Понятие об информационном объекте и его элементах /Пр/	6	2	УК-10 ОПК-5 ОПК-6	Л1.1 Л1.2	0	
12.4	Информационные правоотношения /Пр/	6	2	УК-10 ОПК-5 ОПК-6	Л1.1 Л1.2	0	
12.5	Зачет /ИВКР/	6	0,25	УК-10 ОПК-5 ОПК-6	Л1.1 Л1.2	0	
	Раздел 13. Информационная безопасность						
13.1	Основные задачи и методы обеспечения информационной безопасности /Лек/	7	4	УК-10 ОПК-5 ОПК-6	Л1.1 Л1.2	0	
13.2	Правовое регулирование отношений в сфере информации, информационных систем, информационных технологий и защиты информации /Лек/	7	2	УК-10 ОПК-5 ОПК-6	Л1.1 Л1.2	0	
13.3	Правовые режимы защиты конфиденциальной информации /Лек/	7	4	УК-10 ОПК-5 ОПК-6	Л1.1 Л1.2	0	
13.4	Коммерческая тайна /Лек/	7	2	УК-10 ОПК-5 ОПК-6	Л1.1 Л1.2	0	
13.5	Лицензирование в области защиты информации /Лек/	7	2	УК-10 ОПК-5 ОПК-6	Л1.1 Л1.2	0	
13.6	Сертификация средств защиты информации /Лек/	7	6	УК-10 ОПК-5 ОПК-6	Л1.1 Л1.2	0	
13.7	Лицензирование программного обеспечивания /Лек/	7	6	УК-10 ОПК-5 ОПК-6	Л1.1 Л1.2	0	
13.8	Защита интеллектуальной собственности /Лек/	7	2	УК-10 ОПК-5 ОПК-6	Л1.1 Л1.2	0	
13.9	Информационная безопасность личности /Пр/	7	4	УК-10 ОПК-5 ОПК-6	Л1.1 Л1.2	4	
13.10	Сертификационная деятельность в области защиты информации. /Пр/	7	4	УК-10 ОПК-5 ОПК-6	Л1.1 Л1.2	0	
13.11	Интеллектуальная собственность /Пр/	7	4	УК-10 ОПК-5 ОПК-6	Л1.1 Л1.2	0	
	Раздел 14. Ответственность за нарушение информационного законодательства						
14.1	Ответственность за правонарушения в информационной сфере /Лек/	7	4	УК-10 ОПК-5 ОПК-6	Л1.1 Л1.2	0	
14.2	Юридическая ответственность за нарушения правового режима конфиденциальной информации /Пр/	7	2	УК-10 ОПК-5 ОПК-6	Л1.1 Л1.2	0	
14.3	Преступления в сфере компьютерной информации /Пр/	7	2	УК-10 ОПК-5 ОПК-6	Л1.1 Л1.2	0	

14.4	Подготовка к экзамену /Ср/	7	30,65	УК-10 ОПК-5 ОПК-6	Л1.1 Л1.2	0	
14.5	Экзамен /ИВКР/	7	2,35	УК-10 ОПК-5 ОПК-6	Л1.1 Л1.2	0	

5. ОЦЕНОЧНЫЕ СРЕДСТВА

5.1. Контрольные вопросы и задания

1. Что понимается под информационными отношениями в правовом контексте?
2. Почему информационные отношения требуют правового регулирования?
3. Какие категории субъектов участвуют в информационных отношениях?
4. Что является объектом правовых норм в сфере информационных отношений?
5. Какие основные цели правового регулирования информационных отношений?
6. Какие законы РФ составляют законодательную базу по информационной безопасности?
7. Что регулирует Федеральный закон «О информации, информационных технологиях и о защите информации»?
8. Какие положения содержит закон «О персональных данных»?
9. Что включает в себя законодательство о государственной тайне?
10. Какие виды информации подлежат охране на государственном уровне?
11. Что такое информационная безопасность с правовой точки зрения?
12. Какие органы уполномочены обеспечивать информационную безопасность в РФ?
13. Что такое система защиты государственной тайны?
14. Какие уровни секретности существуют в России?
15. Какие сведения подлежат отнесению к государственной тайне?
16. Кто имеет право устанавливать грифы секретности?
17. Как осуществляется допуск к государственной тайне?
18. Какие формы ответственности предусмотрены за разглашение государственной тайны?
19. Что такое режим ограниченного доступа к информации?
20. Чем отличается служебная тайна от государственной?
21. Какие сведения составляют служебную тайну?
22. Какие условия должны соблюдаться для установления режима коммерческой тайны?
23. Что такое персональные данные и как они защищаются?
24. В каких случаях обработка персональных данных разрешена без согласия субъекта?
25. Какие меры безопасности должны обеспечивать операторы персональных данных?
26. Что такое конфиденциальная информация?
27. Что представляет собой правовая охрана интеллектуальной собственности?
28. Какие результаты интеллектуальной деятельности подлежат охране?
29. Какие законы регулируют защиту авторских прав в РФ?
30. Что такое патентное право?
31. Как осуществляется защита программ для ЭВМ?
32. Что такое база данных с точки зрения права?
33. Какие правонарушения относятся к преступлениям в сфере компьютерной информации?
34. Какие статьи УК РФ регулируют преступления в сфере ИТ?
35. Что такое неправомерный доступ к компьютерной информации?
36. Что считается созданием, использованием или распространением вредоносных программ?
37. Какие санкции предусмотрены за вмешательство в работу ЭВМ?
38. Что такое организационная защита информации?
39. Какие меры входят в состав организационной защиты информации?
40. Какова роль локальных нормативных актов в защите информации?
41. Что включает в себя политика информационной безопасности организации?
42. Как осуществляется подбор сотрудников на должности, связанные с конфиденциальной информацией?
43. Какие требования предъявляются к кандидатам на такие должности?
44. Какие этапы включает в себя проверка при приеме на работу?
45. Что такое служебная проверка?
46. Какие документы подписывает сотрудник при трудоустройстве на "секретную" должность?
47. Что такое неразглашение конфиденциальной информации?
48. Как осуществляется текущий контроль за действиями сотрудников?
49. Какие меры применяются при нарушении режима конфиденциальности?
50. Что такое допуск к государственной тайне?
51. Чем допуск отличается от доступа?
52. Какие категории допуска к гостайне существуют?
53. Какие документы оформляются при получении допуска?
54. Что такое служебная тайна в трудовых отношениях?
55. Как регулируется доступ к персональным данным сотрудников?
56. Как организуется защита персональных данных в организации?
57. Кто несет ответственность за утечку персональных данных?

58. В каких случаях проводится служебное расследование?
59. Какие основания для начала служебного расследования по утечке информации?
60. Кто уполномочен проводить служебные расследования?
61. Какие этапы включает служебное расследование?
62. Как оформляются результаты служебного расследования?
63. Что такое акт служебного расследования?
64. Какие меры могут быть применены по итогам расследования?
65. Какие права имеет работник в ходе служебного расследования?
66. Какие существуют формы дисциплинарной ответственности за разглашение?
67. Какие требования к хранению конфиденциальной информации?
68. Какие документы регламентируют защиту информации на предприятии?
69. Какие обязанности у работника по защите информации?
70. Какова роль внутреннего аудита в защите информации?

5.2. Темы письменных работ

не предусмотрены

5.3. Оценочные средства

Рабочая программа "Организационное и правовое обеспечение информационной безопасности" обеспечена оценочными средствами для проведения текущего контроля и промежуточной аттестации, включающими контрольные вопросы для проведения промежуточной аттестации, критерии оценивания учебной деятельности обучающихся по балльно-рейтинговой системе, примеры заданий для практических и лабораторных занятий, билеты для проведения промежуточной аттестации.
Все оценочные средства представлены в Приложении 1.

5.4. Перечень видов оценочных средств

Оценочные средства разработаны для всех видов учебной деятельности студента - лекций, практических занятий, самостоятельной работы и промежуточной аттестации. Оценочные средства представлены в виде:
- средства текущего контроля: проверочных работ по решению задач, дискуссии по теме;
- средств итогового контроля - промежуточной аттестации: экзамена в 6,7 семестре.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год
Л1.1	Полякова Т. А., Чубукова С. Г., Ниесов В. А., Стрельцов А. А.	Организационное и правовое обеспечение информационной безопасности: учебник и практикум для вузов	Москва: Юрайт, 2024
Л1.2	Тумбинская М. В., Петровский М. В.	Комплексное обеспечение информационной безопасности на предприятии: учебник для вузов	Санкт-Петербург: Лань, 2025

6.3.1 Перечень программного обеспечения

6.3.1.1	Office Professional Plus 2019	
6.3.1.2	Windows 10	
6.3.1.3	МТС-Линк	Комплексная платформа для коммуникаций, обучения и совместной работы, разработанная с использованием современных технологий. Доступны десктопные и мобильные приложения для удобной работы с системой.

6.3.2 Перечень информационных справочных систем

6.3.2.1	База данных научных электронных журналов "eLibrary"
6.3.2.2	Электронно-библиотечная система "Лань" Доступ к коллекциям электронных изданий ЭБС "Издательство "Лань"
6.3.2.3	Электронно-библиотечная система «Книжный Дом Университета» ("БиблиоТех")

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Аудитория	Назначение	Оснащение	Вид
6-25	Специализированная многофункциональная лаборатория № 6-25 для проведения практических и лабораторных занятий, текущего контроля и промежуточной/ итоговой аттестации, в том числе для	Компьютерные столы; Стулья; Письменный стол педагогического работника; Стул педагогического работника; Магнитно-маркерная доска; Мультимедийный проектор;	

	организации практической подготовки обучающихся	Экран; ПК с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде лицензиата; Телекоммуникационные шкафы; Средства отображения информации. Стенды сетей передачи информации с коммутацией пакетов и коммутацией каналов в составе: Учебный стенд "Основы IP-сетей" (маршрутизаторы, коммутаторы L2/L3); Учебный стенд "Виртуальные сети (VLAN, VPN)"; Учебный стенд "Беспроводные сети (Wi-Fi, IoT)"; Учебный стенд "Телефония (ISDN, VoIP)"; Учебный стенд "Оптические сети (PON, DWDM)"; Стенд "Цифровые системы передачи (E1, SDH)". Стенды для изучения проводных и беспроводных компьютерных сетей в составе: абонентские устройства; коммутаторы; маршрутизаторы; точкидоступа, межсетевые экраны; средства обнаружения компьютерных атак; системы углубленной проверки сетевых пакетов; системы защиты от утечки данных; анализаторы кабельных сетей. Учебно-лабораторные комплексы в составе: Учебный лабораторный комплекс контроля сетевой безопасности (системы обнаружения вторжений и анализа защищенности, сетевые сканеры). Учебный лабораторный комплекс проведения анализа защищенности значимого объекта КИИ на соответствие требованиям по обеспечению безопасности. Учебный лабораторный комплекс для обеспечения исследований специального программного обеспечения и аппаратного СЗИ в составе: средства защиты	

		информации от НСД; программно-аппаратный комплекс доверенной нагрузки; антивирусные программные комплексы; межсетевые экраны; средства создания модели разграничения доступа; программа контроля полномочий доступа к информационным ресурсам; программа фиксации и контроля исходного состояния программного комплекса; программа поиска и гарантированного уничтожения информации на дисках; аппаратные средства аутентификации пользователя; системы обнаружения вторжений и анализа защищенности; средства анализа защищенности компьютерных сетей; сканеры безопасности; устройства чтения смарт-карт и радиометок; программно-аппаратные комплексы защиты информации; средства криптографической защиты информации. Учебный лабораторный комплекс для обеспечения исследований типовых сертифицированных программных и программно-технических средств защиты информации от НСД. Учебный лабораторный комплекс для обеспечения исследований сертифицированных средств в которых реализованы средства защиты информации от НСД. УЛК для проведения аттестационных испытаний автоматизированных систем от НСД по требованиям безопасности информации. Аппаратно-программные комплексы в составе: аппаратно-программные средства управления доступом к данным; средства криптографической защиты информации; средства дублирования и восстановления данных; средства мониторинга состояния автоматизированных систем;	

		средства контроля и управления доступом в помещения.	
3	Специализированная многофункциональная учебная аудитория № 3 для проведения учебных занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной/ итоговой аттестации	Компьютерные столы обучающихся; Стулья обучающихся; Письменный стол педагогического работника; Стул педагогического работника; Стеллаж для учебно-методических материалов, в том числе учебно-наглядных пособий; Многофункциональное устройство (принтер, сканер, ксерокс); Интерактивная доска; Мультимедийный проектор; Ноутбуки с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде	
5	Помещение № 5 для самостоятельной работы обучающихся	Письменный стол обучающегося; Стул обучающегося; Письменный стол обучающегося с ограниченными возможностями здоровья; Стул обучающегося с ограниченными возможностями здоровья; Ноутбук с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде лицензиата; Моноблок (в том числе, клавиатура, мышь, наушники) с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде	
3-79	Аудитория (защищаемое помещение) для проведения учебных занятий, в ходе которых до обучающихся доводится информация ограниченного доступа, не содержащая сведений, составляющих государственную тайну № 3-79	рулонные шторы; система виброакустической защиты информации; столы аудиторные для обучающихся, стол преподавателя и стол для размещения компьютера; стулья, доска маркерная; экран; компьютер (в исполнении - моноблок со встроенным или подключаемым DVD/CD-дисководом); проектор; кондиционер; экраны на батареи.	

3-79 А	Специальная библиотека (библиотека литературы ограниченного доступа), предназначенная для хранения и обеспечения использования в образовательном процессе нормативных и методических документов ограниченного доступа № 3-79 А	рулонная штора; стол письменный; стул; шкаф металлический (двудверный) для хранения ДСП материалов; шкаф металлический для хранения мобильных телефонов типа ШСТ-26; экраны на батареи.	
Ауд. 8	Аудитория для научно-исследовательской работы обучающихся, курсового и дипломного проектирования № 8	Рабочие места на базе вычислительной техники с набором необходимых для проведения и оформления результатов исследований дополнительных аппаратных и/или программных средств; Письменный стол обучающегося; Стул обучающегося; Письменный стол обучающегося с ограниченными возможностями здоровья; Стул обучающегося с ограниченными возможностями здоровья; Ноутбук с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде лицензиата; Моноблок (в том числе, клавиатура, мышь, наушники) с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде; Многофункциональное устройство (принтер, сканер, ксерокс).	

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Методические указания по изучению дисциплины "Организационное и правовое обеспечение информационной безопасности" представлены в Приложении 2 и включают в себя:
1. Методические указания для обучающихся по организации учебной деятельности.
2. Методические указания по организации самостоятельной работы обучающихся.
3. Методические указания по организации процедуры оценивания знания, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.