МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

(МГРИ)

Организация и обеспечение защиты персональных данных

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 **3 ЗЕТ**

Часов по учебному плану 108
в том числе:
аудиторные занятия 70,25
самостоятельная работа 37,75

Виды контроля в семестрах:
зачеты 10

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**10 (5.2)**		Итого	
Недель	14 2/6			
Вид занятий	УП	РП	УП	РП
Лекции	42	42	42	42
Практические	28	28	28	28
Иные виды контактной работы	0,25	0,25	0,25	0,25
Итого ауд.	70,25	70,25	70,25	70,25
Контактная работа	70,25	70,25	70,25	70,25
Сам. работа	37,75	37,75	37,75	37,75
Итого	108	108	108	108

Москва 2025

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Цель программы повышения квалификации — совершенствование профессиональных компетенций слушателей в области организации обработки персональных данных и обеспечения их безопасности в информационных системах. Обучающиеся приобретают знания о нормативных правовых актах, принципах и методах защиты персональных данных, угрозах безопасности, организационных и технических мерах защиты, аттестации ИСПДн, контроле защищенности, а также навыки разработки локальных нормативных актов, проектирования и администрирования систем защиты ПДн, реагирования на инциденты и повышения осведомлённости персонала.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	ФТД
2.1	**Требования к предварительной подготовке обучающегося:**
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
УК-3: Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	
Знать:	
Уровень 1	основы стратегии сотрудничества для достижения поставленной цели,
Уровень 2	особенности поведения выделенных групп людей, с которыми работает /взаимодействует, учитывает их в своей деятельности;
Уровень 3	типологию и факторы формирования команд, способы социального взаимодействия
Уметь:	
Уровень 1	эффективно взаимодействовать с другими членами команды, в т.ч. участвовать в обмене информацией, знаниями и опытом;
Уровень 2	планировать последовательность шагов и распределять работу в команде для достижения заданного результата; проводить дифференциацию задач и соответствующих исполнителей, опираясь на их особенности
Уровень 3	представлять публично результаты работы команды;
Владеть:	
Уровень 1	навыками организационной работы для выполнения поставленных задач в научной и общественной деятельности
Уровень 2	методами планирования командной работы, навыками дифференциации задач и исполнителей в научной и общественной деятельности,
Уровень 3	способами оценивания результатов совместной работы, навыками составления отчетов о проделанной работе

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

В результате освоения дисциплины (модуля) обучающийся должен

3.1	**Знать:**
3.1.1	нормативные правовые акты в области обработки и защиты персональных данных, включая Федеральный закон № 152-ФЗ;
3.1.2	основные понятия в сфере ПДн и информационной безопасности;
3.1.3	систему нормативных и локальных актов по защите ПДн;
3.1.4	этапы построения системы защиты ПДн в ИСПДн;
3.1.5	требования к защите ПДн при автоматизированной и неавтоматизированной обработке; методы оценки угроз безопасности и структуру модели угроз;
3.1.6	организационные и технические меры по обеспечению безопасности ПДн;
3.1.7	порядок аттестации ИСПДн, эксплуатации и вывода из эксплуатации систем с ПДн;
3.2	**Уметь:**
3.2.1	разрабатывать локальные нормативные акты по обработке и защите ПДн;
3.2.2	оценивать угрозы безопасности и формировать модель угроз;
3.2.3	выбирать и обосновывать меры защиты ПДн;
3.2.4	подготавливать документацию для аттестации ИСПДн;
3.2.5	настраивать и сопровождать средства защиты информации;
3.2.6	обеспечивать безопасность ПДн в процессе эксплуатации и при её завершении;
3.2.7	реагировать на инциденты, связанные с нарушениями в обработке ПДн;
3.3	**Владеть:**
3.3.1	навыками работы с нормативными и методическими документами;
3.3.2	проектированием и администрированием систем защиты ПДн в ИСПДн;
3.3.3	планированием и внедрением мер защиты на всех этапах жизненного цикла ИСПДн;
3.3.4	использованием баз данных угроз и уязвимостей (например, БДУ, CVE);
3.3.5	организацией обучения сотрудников и контролем за соблюдением требований по защите ПДн;
3.3.6	проведением внутреннего контроля, анализа защищённости и оформлением отчётности.

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. Правовые и организационные основы обработки персональных данных						
1.1	Нормативные правовые акты в сфере ПДн /Лек/	10	4	УК-3 ОПК-5	Л1.1	0	
1.2	Права субъектов ПДн и обязанности операторов /Лек/	10	4	УК-3 ОПК-5	Л1.1	0	
1.3	Политика и регламент обработки ПДн /Лек/	10	4	УК-3 ОПК-5	Л1.1	0	
1.4	Разработка политики в отношении обработки ПДн /Пр/	10	4	УК-3 ОПК-5	Л1.1	0	
1.5	азработка регламента обработки ПДн /Пр/	10	4	УК-3 ОПК-5	Л1.1	0	
1.6	Изучение Федерального закона №152-ФЗ /Ср/	10	4	УК-3 ОПК-5	Л1.1	0	
1.7	Сравнение форм обработки ПДн (вручную / автоматизированно) /Ср/	10	4,75	УК-3 ОПК-5	Л1.1	0	
	Раздел 2. Обеспечение безопасности персональных данных в ИСПДн						
2.1	Требования к защите ПДн в ИСПДн /Лек/	10	4	УК-3 ОПК-5	Л1.1	0	
2.2	Основные угрозы безопасности и модель угроз /Лек/	10	4	УК-3 ОПК-5	Л1.1	0	
2.3	Меры по обеспечению безопасности ПДн /Лек/	10	4	УК-3 ОПК-5	Л1.1	0	
2.4	Разработка модели угроз /Пр/	10	2	УК-3 ОПК-5	Л1.1	0	
2.5	Выбор и описание мер защиты /Пр/	10	2	УК-3 ОПК-5	Л1.1	0	
2.6	Разработка технического задания на создание СЗИ /Пр/	10	2	УК-3 ОПК-5	Л1.1	0	
2.7	Изучение уровней защищённости ПДн /Ср/	10	4	УК-3 ОПК-5	Л1.1	0	
2.8	Составление карты угроз и мер защиты /Пр/	10	4	УК-3 ОПК-5	Л1.1	0	
	Раздел 3. Внедрение и контроль системы защиты ПДн						
3.1	Этапы создания системы защиты ПДн /Лек/	10	6	УК-3 ОПК-5	Л1.1	0	
3.2	Контроль и аудит защищённости /Лек/	10	4	УК-3 ОПК-5	Л1.1	0	
3.3	Проведение оценки защищённости /Пр/	10	4	УК-3 ОПК-5	Л1.1	0	
3.4	Подготовка отчёта по результатам контроля /Пр/	10	2	УК-3 ОПК-5	Л1.1	0	
3.5	Анализ методик контроля и аудита /Ср/	10	7	УК-3 ОПК-5	Л1.1	0	
3.6	Разработка внутреннего регламента контроля /Ср/	10	6	УК-3 ОПК-5	Л1.1	0	
	Раздел 4. Работа с персоналом и реагирование на инциденты						
4.1	Обучение сотрудников и повышение осведомлённости /Лек/	10	4	УК-3 ОПК-5	Л1.1	0	
4.2	Действия при нарушении законодательства в сфере ПДн /Лек/	10	4	УК-3 ОПК-5	Л1.1	0	
4.3	Разработка инструктажа по работе с ПДн /Пр/	10	2	УК-3 ОПК-5	Л1.1	0	
4.4	Разработка регламента реагирования на инциденты /Пр/	10	2	УК-3 ОПК-5	Л1.1	0	

4.5	Изучение типичных нарушений и примеров судебной практики /Ср/	10	6	УК-3 ОПК-5	Л1.1	0	
4.6	Подготовка памятки для сотрудников по защите ПДн /Ср/	10	6	УК-3 ОПК-5	Л1.1	0	
4.7	Экзамен /ИВКР/	10	0,25	УК-3 ОПК-5	Л1.1	0	

5. ОЦЕНОЧНЫЕ СРЕДСТВА

5.1. Контрольные вопросы и задания

Тема: 1. Информационное право как отрасль
1. Что такое информационное право? Какие его цели, задачи и место в системе российского права?
2. Какие субъекты и объекты информационных правоотношений? Приведите примеры.
3. Какие принципы регулирования информационных отношений установлены в Конституции РФ (ст. 23, 29, 75)?
4. Как информационное право связано с другими отраслями права (например, административное, уголовное, трудовое)?
5. Какие ключевые законы и указы регулируют ИБ в РФ (ФЗ-187, ФЗ-149, Указ Президента № 313)?
Тема: 2. Законодательство в сфере информационной безопасности
6. Какие положения ФЗ «О безопасности» (2012) регулируют защиту информационных систем?
7. Какие требования к защите информации установлены в ФЗ-149 «Об информации, ИТ и о защите информации»?
8. Как связаны ФЗ-187 «О критической информационной инфраструктуре» и ФЗ-149?
9. Какие нормы регулируют защиту персональных данных (ФЗ-152)? Как они пересекаются с ИБ?
10. Какие международные обязательства России влияют на законодательство в сфере ИБ (например, Конвенция о киберпреступности)?
Тема: 3. Правовые режимы защиты информации
11. Что такое информация ограниченного доступа? Какие виды режимов защиты установлены (гостайна, коммерческая тайна, служебная тайна)?
12. Какие особенности правового режима государственной тайны (ФЗ-5 «О государственной тайне»)?
13. Какие процедуры установления, распространения и прекращения режима государственной тайны?
14. Как регулируется защита коммерческой тайны (ФЗ-9 «О коммерческой тайне»)?
15. Какие угрозы возникают при несоблюдении режима ограниченного доступа к информации?
Тема: 4. Организационные меры защиты
16. Какие этапы включает подбор сотрудников на должности, связанные с конфиденциальной информацией?
17. Как организуется допуск к государственной тайне (процедура оформления, проверка, контроль)?
18. Какие требования предъявляются к помещениям и хранилищам для работы с конфиденциальной информацией?
19. Как организуется пропускной и внутриобъектовый режимы? Какие технические средства используются?
20. Как проводится служебное расследование при утечке информации? Какие этапы и документы оформляются?
Тема: 5. Преступления и ответственность
21. Какие виды преступлений в сфере компьютерной информации регулируются статьями УК РФ (272, 272.1, 272.2, 273)?
22. Какие меры административной ответственности за нарушение ИБ (например, ст. 13.11 КоАП РФ)?
23. Какие квалификационные признаки составов преступлений в сфере ИБ?
24. Какие последствия наступают за неправомерный доступ к информации ограниченного доступа?
25. Какие проблемы возникают при расследовании компьютерных преступлений (например, доказательственная база, цифровые следы)?
Тема: 6. Система защиты государственной тайны
26. Какова структура системы защиты государственной тайны в РФ (ФСБ, уполномоченные органы)?
27. Какие этапы включает процесс передачи информации в государственную тайну?
28. Как организовано хранение и использование государственной тайны (например, классификация, маркировка)?
29. Какие меры применяются для предотвращения утечки государственной тайны (например, контроль доступа, аудит)?
30. Какие последствия разглашения государственной тайны (уголовная ответственность, гражданская ответственность)?
Тема: 7. Лицензирование и сертификация
31. Какие требования к лицензированию деятельности в сфере защиты информации (например, ФСТЭК, ФСБ)?
32. Как проводится сертификация средств защиты информации (СЗИ)? Какие классы защищенности установлены?
33. Какие особенности лицензирования программного обеспечения, предназначенного для защиты информации?
34. Как связаны сертификация СЗИ и требования ФЗ-187?
35. Какие проблемы возникают при сертификации отечественного ПО в условиях санкций?
Тема: 8. Защита интеллектуальной собственности
36. Какие правовые меры обеспечивают защиту результатов интеллектуальной деятельности (патенты, авторские права)?
37. Как регулируется защита программного обеспечения (ПО) как объекта интеллектуальной собственности?
38. Какие угрозы связаны с кибершпионажем и утечкой коммерческой тайны?
39. Какие меры защиты интеллектуальной собственности в цифровой среде (например, DRM, блокчейн)?
40. Какие последствия нарушения прав на программное обеспечение (например, использование нелицензированного ПО)?
Тема: 9. Современные вызовы и технологии
41. Как искусственный интеллект влияет на защиту информации (например, автоматизация атак, обнаружение угроз)?
42. Как квантовые вычисления могут повлиять на криптографические средства защиты в РФ?
43. Какие угрозы связаны с утечкой данных через побочные каналы (TEMPEST, акустический шум)?

44. Как облачные технологии изменяют подходы к защите информации ограниченного доступа?
45. Какие риски внедрения 5G и IoT в системы с ограниченным доступом к информации?
Тема: 10. Международный опыт и сравнение
46. Как отличаются подходы к защите информации в РФ и ЕС (например, GDPR vs ФЗ-152)?
47. Какие стандарты и фреймворки используются за рубежом для управления рисками ИБ (NIST, ISO/IEC 27001)?
48. Какие уроки из зарубежных инцидентов (например, утечки в Equifax, атаки на выборы) применимы к РФ?
49. Как международное сотрудничество (INTERPOL, ENISA) помогает в борьбе с киберпреступностью?
50. Какие ограничения у российских подходов к защите информации по сравнению с зарубежными?
Тема: 11. Практические аспекты и кейсы
51. Какие этапы включает подготовка к аттестации системы управления нефтепроводом?
52. Как организовать служебное расследование при утечке коммерческой тайны в корпорации?
53. Какие ошибки чаще всего приводят к разглашению государственной тайны (например, нарушение хранения, несанкционированный доступ)?
54. Какие меры защиты применяются для предотвращения утечки данных через мобильные устройства сотрудников?
55. Как подготовить отчет по результатам служебного расследования (структура, содержание, передача в ФСБ)?
Тема: 12. Этика и правовые дилеммы
56. Какие этические аспекты возникают при использовании ИИ для анализа конфиденциальной информации?
57. Как балансировать между защитой информации и правом на доступ к данным (например, открытые данные vs ИБ)?
58. Какие правовые дилеммы связаны с применением deepfake-технологий в утечках информации?
59. Как использовать блокчейн для обеспечения целостности данных в системах с ограниченным доступом?
60. Какие ограничения у российских подходов к защите информации по сравнению с зарубежными?
Тема: 13. Перспективные технологии и стратегии
61. Как технологии Zero Trust применяются для защиты информации ограниченного доступа?
62. Как цифровые двойники используются для тестирования устойчивости систем к утечкам данных?
63. Какие меры защиты разрабатываются для гибридных систем (локальные + облачные) с ограниченным доступом?
64. Как искусственный интеллект используется для автоматизации обнаружения угроз в системах с гостайной?
65. Какие тренды будут определять развитие ИБ в ближайшие 5 лет (например, защита IIoT, квантовое шифрование)?

5.2. Темы письменных работ

не предусмотрены

5.3. Оценочные средства

Рабочая программа "Организация и обеспечение защиты персональных данных" 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 10 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	Петренко В. И., Мандрица И. В.	Защита персональных данных в информационных системах. Практикум: учебное пособие 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
1	Специализированная многофункциональная учебная аудитория № 1 для проведения учебных занятий лекционного и семинарского типов, групповых и индивидуальных консультаций, текущего контроля и промежуточной/ итоговой аттестации	Столы обучающихся; Стулья обучающихся; Письменный стол педагогического работника; Стул педагогического работника; Кафедра; Магнитно-маркерная доска; Мультимедийный проектор; Экран; Ноутбук 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	

6-25	Специализированная многофункциональная лаборатория № 6-25 для проведения практических и лабораторных занятий, текущего контроля и промежуточной/ итоговой аттестации, в том числе для организации практической подготовки обучающихся	Компьютерные столы; Стулья; Письменный стол педагогического работника; Стул педагогического работника; Магнитно-маркерная доска; Мультимедийный проектор; 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.	
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 "Организация и обеспечение защиты персональных данных" 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.