МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

(МГРИ)

Основы информационной безопасности

рабочая программа дисциплины (модуля)

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

Учебный план b090302_25_BIS25.plx
09.03.02 Информационные системы и технологии

Квалификация **Бакалавр**

Форма обучения **очная**

Общая трудоемкость **5 ЗЕТ**

Часов по учебному плану 0
в том числе:
аудиторные занятия 0
самостоятельная работа 0

Виды контроля в семестрах:

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**3 (2.1)**		Итого	
Недель	16			
Вид занятий	УП	РП	УП	РП
Лекции	32	32	32	32
Практические	32	48	32	48
Иные виды контактной работы	3,35	3,35	3,35	3,35
Итого ауд.	67,35	83,35	67,35	83,35
Контактная работа	67,35	83,35	67,35	83,35
Сам. работа	85,65	33,65	85,65	33,65
Часы на контроль	27	27	27	27
Итого	180	144	180	144

Москва 2025

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Целью изучения дисциплины является теоретическая и практическая подготовка специалистов к деятельности, связанной с комплексным анализом возможных угроз и созданием адекватной модели нарушителя, постановкой конкретных задач заданной степени сложности в рамках модели для обеспечения информационной безопасности автоматизированных систем, а также содействие фундаментализации образования и развитию системного мышления.
1.2	Задачи дисциплины:
1.3	- изучение основных аспектов обеспечения информационной безопасности государства;
1.4	- изучение методологии создания систем защиты информации;
1.5	- изучение процессов сбора, передачи и накопления информации;
1.6	- изучение основных элементов теории компьютерной безопасности;
1.7	- изучение математических основ моделей безопасности;
1.8	- изучение вопросов оценки защищенности и обеспечения безопасности компьютерных систем.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.В
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)
ПК-6.3: Способен выполнять работы по выявлению и устранению инцидентов в информационно-коммуникационных системах
Знать:
Уметь:
Владеть:

ПК-8.3: Способен проводить администрирование систем защиты информации автоматизированных систем
Знать:
Уметь:
Владеть:

В результате освоения дисциплины (модуля) обучающийся должен

3.1	**Знать:**
3.1.1	сущность и понятие информации, информационной безопасности и характеристику ее составляющих; место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики;
3.1.2	источники и классификацию угроз информационной безопасности; основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации;
3.1.3	основные понятия, связанные с обеспечением информационной безопасности личности, общества и государства, понятия информационного противоборства, информационной войны и формы их проявлений в современном мире
3.2	**Уметь:**
3.2.1	классифицировать и оценивать угрозы информационной безопасности
3.3	**Владеть:**
3.3.1	владения профессиональной терминологией в области информационной безопасности

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. Информационная безопасность в системе национальной безопасности Российской Федерации						
1.1	Понятие национальной безопасности Российской Федерации. Национальные интересы и угрозы национальной безопасности. /Лек/	3	2		Л1.1	0	

1.2	Роль и место информационной безопасности в системе национальной безопасности Российской Федерации. /Лек/	3	2		Л1.1	0	
1.3	Национальные интересы Российской Федерации в информационной сфере. Виды и источники угроз информационной безопасности Российской Федерации. /Лек/	3	2		Л1.1	0	
1.4	Понятие национальной безопасности Российской Федерации. Национальные интересы и угрозы национальной безопасности. /Пр/	3	2		Л1.1	0	
1.5	Роль и место информационной безопасности в системе национальной безопасности Российской Федерации. /Пр/	3	2		Л1.1	0	
1.6	Национальные интересы Российской Федерации в информационной сфере. Виды и источники угроз информационной безопасности Российской Федерации. /Пр/	3	2		Л1.1	0	
1.7	Подготовка докладов на семинарах /Ср/	3	4,4		Л1.1	0	
	Раздел 2. Основы государственной политики Российской Федерации в области информационной безопасности						
2.1	Конституция Российской Федерации о правах и свободах человека и гражданина в информационной сфере. Виды защищаемой информации. /Лек/	3	2		Л1.1	0	
2.2	Организационная система обеспечения информационной безопасности Российской Федерации. /Лек/	3	2		Л1.1	0	
2.3	Структура законодательства Российской Федерации в информационной сфере. Уголовно-процессуальная характеристика компьютерных преступлений. /Лек/	3	2		Л1.1	0	
2.4	Административная ответственность за нарушение требований информационной безопасности. /Лек/	3	2		Л1.1	0	
2.5	Конституция Российской Федерации о правах и свободах человека и гражданина в информационной сфере. Виды защищаемой информации. /Пр/	3	6		Л1.1	0	
2.6	Организационная система обеспечения информационной безопасности Российской Федерации. /Пр/	3	6		Л1.1	0	
2.7	Структура законодательства Российской Федерации в информационной сфере. Уголовно-процессуальная характеристика компьютерных преступлений. /Пр/	3	2		Л1.1	0	
2.8	Административная ответственность за нарушение требований информационной безопасности. /Пр/	3	2		Л1.1	0	
2.9	Подготовка докладов на семинарах /Ср/	3	11,15		Л1.1	0	

	Раздел 3. Информационное противоборство, методы и средства его осуществления						
3.1	Понятие информационного противоборства. Информационные войны, методы и средства их ведения. /Лек/	3	2		Л1.1	0	
3.2	Информационное оружие, его классификация и возможности. /Лек/	3	2		Л1.1	0	
3.3	Понятие информационного противоборства. Информационные войны, методы и средства их ведения. /Пр/	3	6		Л1.1	0	
3.4	Информационное оружие, его классификация и возможности. /Пр/	3	6		Л1.1	0	
3.5	Подготовка докладов на семинарах /Ср/	3	4,5		Л1.1	0	
	Раздел 4. Критическая информационная инфраструктура Российской Федерации.						
4.1	Понятие критической информационной инфраструктуры Российской Федерации. /Лек/	3	2		Л1.1	0	
4.2	Порядок категорирования объектов критической информационной инфраструктуры. /Лек/	3	2		Л1.1	0	
4.3	Контроль и надзор обеспечения безопасности значимых объектов критической инфраструктуры. /Лек/	3	2		Л1.1	0	
4.4	Понятие критической информационной инфраструктуры Российской Федерации. /Пр/	3	2		Л1.1	0	
4.5	Порядок категорирования объектов критической информационной инфраструктуры. /Пр/	3	2		Л1.1	0	
4.6	Контроль и надзор обеспечения безопасности значимых объектов критической инфраструктуры. /Пр/	3	2		Л1.1	0	
4.7	Подготовка докладов на семинарах /Ср/	3	8,9		Л1.1	0	
	Раздел 5. Методы и средства обеспечения информационной безопасности объектов критической информационной инфраструктуры						
5.1	Виды и источники угроз информационной безопасности объекта критической информационной инфраструктуры. /Лек/	3	2		Л1.1	0	
5.2	Моделирование угроз безопасности объекта критической информационной инфраструктуры. /Лек/	3	2		Л1.1	0	
5.3	Методы и средства обеспечения безопасности объектов критической информационной инфраструктуры. /Лек/	3	2		Л1.1	0	
5.4	Задачи и организационная структура подразделения обеспечения информационной безопасности. /Лек/	3	2		Л1.1	0	
5.5	Виды и источники угроз информационной безопасности объекта критической информационной инфраструктуры. /Пр/	3	2		Л1.1	0	
5.6	Моделирование угроз безопасности объекта критической информационной инфраструктуры. /Пр/	3	2		Л1.1	0	

5.7	Методы и средства обеспечения безопасности объектов критической информационной инфраструктуры. /Пр/	3	2		Л1.1	0	
5.8	Задачи и организационная структура подразделения обеспечения информационной безопасности. /Пр/	3	2		Л1.1	0	
5.9	Курсовая работа /КР/	3	27		Л1.1	0	
5.10	Подготовка докладов на семинарах /Ср/	3	4,7		Л1.1	0	
5.11	Экзамен /ИВКР/	3	3,35		Л1.1	0	

5. ОЦЕНОЧНЫЕ СРЕДСТВА

5.1. Контрольные вопросы и задания

Тема: 1. Национальная безопасность РФ
1. Что такое национальная безопасность Российской Федерации? Какие ключевые принципы определены в Стратегии национальной безопасности (2021)?
2. Какие национальные интересы России включены в Стратегию национальной безопасности? Приведите примеры.
3. Какие угрозы национальной безопасности наиболее актуальны в современных условиях (например, гибридные войны, кибератаки)?
4. Как связаны государственная политика в сфере ИБ и обеспечение суверенитета цифрового пространства?
5. Какие цели и задачи определены в Стратегии национальной безопасности РФ в контексте информационной безопасности?
Тема: 2. Информационная безопасность в системе национальной безопасности
6. Каково место информационной безопасности в системе национальной безопасности РФ?
7. Какие национальные интересы России в информационной сфере указаны в Указе Президента РФ № 2019-631?
8. Какие угрозы информационной безопасности затрагивают интересы государства, общества и личности?
9. Какие ключевые документы регулируют информационную безопасность в РФ (например, ФЗ-187, ФЗ-149, ФЗ-139)?
10. Как связаны государственная политика в сфере ИБ и обеспечение суверенитета цифрового пространства?
Тема: 3. Правовые основы информационной безопасности
11. Какие положения Конституции РФ регулируют права и свободы в информационной сфере (например, статьи 23, 29, 75)?
12. Что такое защищаемая информация? Какие виды информации требуют особой охраны (персональные данные, государственная тайна, данные КИИ)?
13. Какие нормы УК РФ регулируют компьютерные преступления (например, статьи 272, 272.1, 272.2, 273)?
14. Какие меры административной ответственности предусмотрены за нарушение требований ИБ (например, ст. 13.11 КоАП РФ)?
15. Какие международные обязательства России влияют на подходы к ИБ (например, Конвенция Совета Европы о киберпреступности)?
Тема: 4. Угрозы информационной безопасности
16. Какие виды угроз информационной безопасности наиболее критичны для РФ (например, кибершпионаж, дезинформация, DDoS-атаки)?
17. Какие источники угроз в информационной сфере выделены в Стратегии национальной безопасности РФ (государственные, корпоративные, международные)?
18. Что такое информационное противоборство? Какие методы и средства используются в его ведении?
19. Какие примеры информационных войн известны (например, атаки на выборы, энергетические системы)?
20. Какие риски связаны с зависимостью от иностранных ИТ-технологий (например, микропрограммы, уязвимости в ПО)?
Тема: 5. Критическая информационная инфраструктура (КИИ)
21. Что такое критическая информационная инфраструктура РФ? Какие объекты в неё входят (например, энергетика, финансы, связи)?
22. Какие критерии значимости объектов КИИ установлены ФЗ-187?
23. Как проводится категорирование объектов КИИ? Какие уровни защищенности определены?
24. Какие меры контроля и надзора реализуются для объектов КИИ (например, проверки, сертификация СЗИ)?
25. Какие угрозы наиболее критичны для КИИ (например, ransomware, APT, физические атаки на ЦОД)?
Тема: 6. Моделирование угроз и реагирование
26. Какие методологии используются для моделирования угроз безопасности объектов КИИ (например, MITRE ATT&CK, STRIDE)?
27. Как строится модель угроз для объекта КИИ с учетом специфики (например, АСУ ТП, банки, транспорт)?
28. Какие параметры учитываются при оценке вероятности реализации угроз и их последствий?
29. Какие этапы включает процесс реагирования на инциденты в КИИ (обнаружение, локализация, восстановление)?
30. Какие метрики позволяют оценить эффективность мер против угроз (например, MTTD, MTTR, уровень утечки данных)?
Тема: 7. Методы и средства обеспечения безопасности КИИ
31. Какие технические средства защиты применяются для объектов КИИ (например, межсетевые экраны, СОВ, антивирусы)?
32. Какие классы защищенности установлены для СЗИ на объектах КИИ (например, по ГОСТ Р 57580)?
33. Какие меры физической и логической защиты реализуются для систем КИИ (например, контроль доступа,

шифрование)?
34. Как искусственный интеллект и машинное обучение используются для обнаружения аномалий в КИИ?
35. Какие технологии обеспечивают целостность и доступность данных в системах КИИ (например, резервное копирование, blockchain)?
Тема: 8. Организационные основы ИБ в РФ
36. Какова организационная структура обеспечения ИБ в России (например, ФСТЭК, ФСБ, Минцифры)?
37. Какие функции выполняет Центр реагирования на компьютерные инциденты (ЦРКИ) при работе с КИИ?
38. Как взаимодействуют субъекты КИИ с государственными органами (например, ФСТЭК, ФСБ, Роскомнадзор)?
39. Какие требования предъявляются к обучению персонала и тестированию готовности к инцидентам?
40. Какие документы обязательны для разработки и реализации политики безопасности объектов КИИ?
Тема: 9. Политики безопасности и управление рисками
41. Какие элементы включает политика ИБ на объекте КИИ (цели, ограничения, ответственность)?
42. Как политики ИБ согласуются с требованиями ФЗ-187 и стандартами ФСТЭК?
43. Какие этапы включает процесс управления рисками (идентификация, анализ, лечение)?
44. Какие методологии управления рисками применяются в КИИ (например, OCTAVE, FAIR, MEHARI)?
45. Какие меры минимизации рисков реализуются (например, сегментация, Zero Trust, резервирование)?
Тема: 10. Информационное противоборство и кибервойны
46. Что такое информационное противоборство? Какие методы и средства используются в его ведении?
47. Какие виды информационных войн существуют (например, кибератаки, психологическое воздействие через СМИ)?
48. Какие примеры информационных атак на РФ известны (например, атаки на выборы, энергетические системы)?
49. Какие меры противостояния информационным угрозам реализуются в России (например, система мониторинга угроз, обучение персонала)?
50. Как международное сотрудничество (например, INTERPOL, ENISA) помогает в борьбе с киберугрозами?
Тема: 11. Современные вызовы и уязвимости
51. Какие риски связаны с внедрением 5G и IoT в системы КИИ?
52. Как квантовые вычисления могут повлиять на криптографические средства защиты в КИИ?
53. Какие угрозы возникают из-за устаревших протоколов в промышленных системах (например, Modbus, DNP3)?
54. Как искусственный интеллект используется для автоматизации атак на информационные системы?
55. Какие меры защиты разрабатываются для гибридных систем (локальные + облачные) на объектах КИИ?
Тема: 12. Практические аспекты и кейсы
56. Какие этапы включает подготовка к атаке на объект КИИ (например, разработка сценариев, пентестинг)?
57. Как организовать симуляцию атаки (red team/blue team) на объекте КИИ?
58. Какие ошибки чаще всего приводят к утечкам данных на объектах КИИ?
59. Какие меры реагирования на атаку Ransomware в энергетических системах?
60. Как подготовить отчет по результатам инцидента (структура, содержание, передача в ФСТЭК)?
Тема: 13. Сравнение с международным опытом
61. Какие отличия в подходах к защите КИИ в ЕС (NIS, NIS2), США (CISA) и России (ФЗ-187)?
62. Какие стандарты и фреймворки используются за рубежом для управления рисками (например, NIST Cybersecurity Framework, ISO/IEC 27001)?
63. Какие уроки из зарубежных инцидентов (например, Colonial Pipeline, SolarWinds) применимы к российским объектам КИИ?
64. Как международное сотрудничество (INTERPOL, ENISA) помогает в борьбе с киберугрозами?
65. Какие ограничения у российских подходов к защите КИИ по сравнению с зарубежными?
Тема: 14. Перспективные технологии и стратегии
66. Как технологии Zero Trust применяются для защиты объектов КИИ?
67. Как цифровые двойники используются для тестирования устойчивости КИИ к атакам?
68. Как блокчейн может быть применен для обеспечения целостности данных на объектах КИИ?
69. Какие меры защиты разрабатываются для гибридных систем (локальные + облачные)?
70. Какие тренды будут определять развитие ИБ в КИИ в ближайшие 5 лет (например, защита IIoT, AI-мониторинг)?
Тема: 15. Защита от дезинформации и кибервойн
71. Какие методы борьбы с дезинфекцией используются в государственных и корпоративных системах?
72. Как deepfake-технологии используются в информационных войнах? Как их обнаруживать и блокировать?
73. Какие меры защиты от фишинга и социальной инженерии реализуются в системах КИИ?
74. Как системы мониторинга социальных сетей и СМИ помогают выявлять дезинформационные кампании?
75. Какие этические и правовые аспекты возникают при борьбе с кибервойнами?
Тема: 16. Организация подразделений по ИБ
76. Какие функции выполняет служба информационной безопасности на предприятии?
77. Как строится взаимодействие между службой ИБ, ИТ-подразделением и юридическим отделом?
78. Какие этапы включает разработка политики безопасности организации?
79. Как организовать защиту от внутренних угроз (инсайдеры, ошибки персонала)?
80. Какие метрики используются для оценки эффективности работы подразделения ИБ?
Тема: 17. Законодательные и нормативные аспекты
81. Какие документы обязательны для субъектов КИИ (например, план реагирования, реестр активов)?
82. Как ФЗ-187 регулирует защиту объектов КИИ? Какие требования к сертификации СЗИ?
83. Какие изменения в законодательстве РФ связаны с развитием цифровых технологий и киберугрозами?
84. Какие обязанности у операторов КИИ по передаче данных в государственные органы (например, ЦРКИ)?
85. Какие проблемы возникают при внедрении требований ФЗ-187 в малом и среднем бизнесе?
Тема: 18. Управление киберугрозами и инцидентами

86. Какие этапы включает жизненный цикл реагирования на инциденты ИБ на объектах КИИ?
87. Как организован обмен данными о киберугрозах между субъектами КИИ (например, через платформы CSIRT)?
88. Какие формы отчетности используются для передачи информации о киберинцидентах в ЦРКИ?
89. Какие метрики позволяют оценить эффективность реагирования (например, MTTD, MTTR)?
90. Какие проблемы возникают при синхронизации действий между различными организациями КИИ?
Тема: 19. Практические задачи и кейсы
91. Разработка модели угроз для системы управления водоснабжением города.
92. Анализ уязвимостей в реализации СОВ на объекте КИИ.
93. Сравнение эффективности мер защиты от APT на энергетических объектах.
94. Проектирование политики безопасности для банка с учетом требований ФЗ-187.
95. Реализация системы мониторинга угроз на основе TAXII/STIX.
Тема: 20. Современные тенденции и вызовы
96. Какие риски связаны с использованием искусственного интеллекта в кибератаках?
97. Как квантовые технологии меняют подходы к криптографии?
98. Какие угрозы возникают из-за утечки данных через побочные каналы (TEMPEST, акустический шум)?
99. Как облачные технологии изменяют подходы к обеспечению безопасности (например, Zero Trust, шифрование на стороне клиента)?
100. Какие угрозы связаны с программно-определяемыми радиоустройствами в атаках на ИБ?

5.2. Темы письменных работ

Тема: 1. Теоретические и правовые аспекты
1. Анализ Стратегии национальной безопасности РФ 2021: место информационной безопасности в системе угроз государству.
2. Сравнительный анализ национальных интересов России и стран Запада в информационной сфере.
3. Правовая основа обеспечения информационной безопасности в Конституции РФ: анализ статей 23, 29, 75.
4. Соотношение государственной тайны и персональных данных в законодательстве РФ.
5. Уголовно-процессуальные особенности расследования компьютерных преступлений по статьям УК РФ (272, 272.1, 273).
Тема: 2. Угрозы и моделирование угроз
6. Моделирование угроз безопасности объектов КИИ в энергетике: примеры атак и методы защиты.
7. Анализ источников угроз информационной безопасности в транспортных системах РФ.
8. Кибератаки как инструмент гибридных угроз: кейс атаки на выборы в России.
9. Исследование уязвимостей в системах управления технологическими процессами (АСУ ТП) на объектах КИИ.
10. Классификация информационного оружия и его применения в современных войнах.
Тема: 3. Критическая информационная инфраструктура (КИИ)
11. Категорирование объектов КИИ: сравнение методологий ФСТЭК и международных стандартов.
12. Оценка рисков информационной безопасности на примере объекта КИИ в финансовой сфере.
13. Анализ эффективности мер контроля и надзора за объектами КИИ по ФЗ-187.
14. Проблемы сертификации средств защиты информации на объектах КИИ.
15. Роль криптошлюзов в обеспечении безопасности межсетевого взаимодействия на объектах КИИ.
Тема: 4. Информационное противоборство и кибервойны
16. Информационное противоборство: методы, средства и современные примеры из практики.
17. Использование deepfake-технологий в информационных войнах: угрозы и методы противодействия.
18. Сравнение стратегий противостояния дезинформации в России и ЕС.
19. Анализ кибератак на критические системы: кейс Colonial Pipeline и его аналоги в РФ.
20. Этические и правовые аспекты использования информационного оружия в международных конфликтах.
Тема: 5. Организационные и технологические меры
21. Разработка политики информационной безопасности для банка с учетом требований ФЗ-187.
22. Применение методологии Zero Trust для защиты объектов КИИ.
23. Сравнительный анализ эффективности межсетевых экранов и систем обнаружения вторжений (СОВ) на объектах КИИ.
24. Организация службы информационной безопасности на предприятии: задачи, структура, метрики эффективности.
25. Интеграция систем мониторинга угроз (например, TAXII/STIX) в инфраструктуру КИИ.
Тема: 6. Современные технологии и вызовы
26. Влияние квантовых вычислений на криптографические средства защиты информации в КИИ.
27. Применение искусственного интеллекта для обнаружения аномалий в системах КИИ.
28. Риски внедрения 5G-технологий в объекты критической инфраструктуры РФ.
29. Использование blockchain для обеспечения целостности данных на объектах КИИ.
30. Угрозы утечки информации через побочные каналы (TEMPEST) и методы их минимизации.

5.3. Оценочные средства

Рабочая программа "Основы 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 5 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	Нестеров С. А.	Основы информационной безопасности	Санкт-Петербург: Лань, 2022

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

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.	
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 "Основы 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.