МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

(МГРИ)

Управление информационной безопасностью

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 **4 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>)	**7 (4.1)**		Итого	
Недель	16 1/6			
Вид занятий	УП	РП	УП	РП
Лекции	32	28	32	28
Практические	32	56	32	56
Иные виды контактной работы	2,35	2,35	2,35	2,35
Итого ауд.	66,35	86,35	66,35	86,35
Контактная работа	66,35	86,35	66,35	86,35
Сам. работа	50,65	30,65	50,65	30,65
Часы на контроль	27	27	27	27
Итого	144	144	144	144

Москва 2025

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Дисциплина имеет целью изучение основных понятий, методологии и практических приемов управления технической и организационной инфраструктурой обеспечения информационной безопасности на предприятии.
1.2	Задачами дисциплины являются:
1.3	- приобретение обучаемыми необходимого объема знаний и практических навыков в области стандартизации и нормотворчества в управлении информационной безопасностью, организации работы и разграничения полномочий персонала, ответственного за информационную безопасность;
1.4	- формирование у обучаемых целостного представления об организации и содержании процессов управления информационной безопасностью на предприятии как результата внедрения системного подхода к решению задач обеспечения информационной безопасности.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.В
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Безопасность операционных систем
2.1.2	Безопасность сетей электронных вычислительных машин
2.1.3	Безопасность систем баз данных
2.1.4	Организационное и правовое обеспечение информационной безопасности
2.1.5	Информационная безопасность открытых систем
2.1.6	Мониторинг информационной безопасности и активный поиск киберугроз
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Основы аттестации объектов информатизации
2.2.2	Измерительная аппаратура контроля защищенности объектов информатизации
2.2.3	Технология подготовки выпускной квалификационной работы

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)
ПК-10.3: Способен выявлять требования к типовой ИС в рамках выполнения работ по созданию(модификации) и сопровождению ИС
Знать:
Уметь:
Владеть:

ПК-11.3: Способен осуществлять планирование проектов в соответствии с полученным заданием
Знать:
Уметь:
Владеть:

В результате освоения дисциплины (модуля) обучающийся должен

3.1	**Знать:**
3.1.1	назначение, функции и структуру систем управления базами данных, средства обеспечения безопасности данных;
3.1.2	методы мониторинга информационной безопасности и средства реализации удаленных сетевых атак на автоматизированные системы, организационную структуру и функциональную часть автоматизированных систем;
3.1.3	методы и средства реализации удаленных сетевых атак на автоматизированные системы;
3.1.4	принципы формирования политики информационной безопасности в автоматизированных системах , риски подсистем защиты информации автоматизированных систем и экспериментальные методы их оценки;
3.1.5	содержание основных нормативных правовых актов в сфере противодействия коррупции, 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;
3.1.6	основные понятия и характеристику основных отраслей права, применяемых в профессиональной деятельности организации;
3.1.7	основы российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации;

3.1.8	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;
3.1.9	статус и порядок работы основных правовых информационно-справочных систем;
3.1.10	основы организации и деятельности органов государственной власти в Российской Федерации, систему стандартов и нормативных правовых актов уполномоченных федеральных органов исполнительной власти по лицензированию в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации;
3.1.11	систему нормативных правовых актов уполномоченных федеральных органов исполнительной власти по аттестации объектов информатизации и сертификации средств защиты информации;
3.1.12	задачи органов защиты государственной тайны и служб защиты информации на предприятиях;
3.1.13	методы проектирования вычислительных сетей, методы администрирования вычислительных сетей;
3.1.14	методы администрирования и принципы работы операционных систем семейств UNIX и Windows, устройство и принципы работы операционных систем, структуру и возможности
3.1.15	подсистем защиты операционных систем семейств UNIX и Windows;
3.2	**Уметь:**
3.2.1	эксплуатировать базы данных;
3.2.2	создавать объекты базы данных;
3.2.3	выполнять запросы к базе данных;
3.2.4	разрабатывать прикладные программы, осуществляющие взаимодействие с базами
3.2.5	данных, администрировать базы данных;
3.2.6	осуществлять диагностику и мониторинг систем защиты автоматизированных систем, осуществлять управление и администрирование защищенных автоматизированных систем;
3.2.7	разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем;
3.2.8	разрабатывать частные политики информационной безопасности автоматизированных систем , анализировать и оценивать угрозы информационной безопасности автоматизированных систем;
3.2.9	соблюдать требования антикоррупционного законодательства, воздерживаться от поведения, вызывающего сомнение в объективном и беспристрастном исполнении должностных (служебных) обязанностей, применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности;
3.2.10	обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, предпринимать необходимые меры по восстановлению нарушенных
3.2.11	прав;
3.2.12	анализировать и разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации;
3.2.13	формулировать основные требования при лицензировании деятельности в области защиты информации, сертификации и
3.2.14	аттестации по требованиям безопасности информации;
3.2.15	формулировать основные требования информационной безопасности при эксплуатации автоматизированной системы;
3.2.16	формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации,
3.2.17	использовать систему организационных мер, направленных на защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами ФСБ России, ФСТЭК России;
3.2.18	проектировать вычислительные сети, администрировать вычислительные сети;
3.2.19	реализовывать политику безопасности вычислительной сети;
3.2.20	настраивать политику безопасности операционных систем семейств UNIX и Windows, использовать средства управления работой операционной системы;
3.2.21	формулировать политику безопасности операционных систем семейств UNIX и Windows;
3.3	**Владеть:**
3.3.1	эксплуатации баз данных с учетом требований по обеспечению информационной безопасности, администрирования баз данных с учетом требований по обеспечению информационной безопасности;
3.3.2	разработки политик информационной безопасности автоматизированных систем;
3.3.3	управления процессами обеспечения безопасности автоматизированных систем, анализа информационной инфраструктуры автоматизированных систем;

3.3.4	применения основных нормативных правовых актов в сфере противодействия коррупции, работы с нормативными правовыми актами;
3.3.5	эксплуатации локальных вычислительных сетей, администрирования локальных вычислительных сетей с учетом требований по обеспечению информационной безопасности;
3.3.6	администрирования операционных систем семейств Windows и Unix с учетом требований по обеспечению информационной безопасности, установки операционных систем семейств Windows и Unix;

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. Базовые понятия и подходы к управлению информационной безопасностью						
1.1	Базовые понятия и подходы к управлению информационной безопасностью /Лек/	7	2		Л1.1	0	
1.2	Базовые понятия и подходы к управлению информационной безопасностью /Пр/	7	4		Л1.1	0	
	Раздел 2. Международные и российские стандарты по УИБ						
2.1	Отраслевые стандарты по ИБ /Лек/	7	2		Л1.1	0	
2.2	Международные и российские стандарты ИСО по УИБ, отраслевые стандарты /Пр/	7	6		Л1.1	0	
	Раздел 3. Политика ИБ организации						
3.1	Политика ИБ организации /Лек/	7	4		Л1.1	0	
3.2	Политика ИБ /Пр/	7	8		Л1.1	0	
3.3	Политика ИБ в организациях разных типов и видов /Пр/	7	8		Л1.1	0	
	Раздел 4. Система управления информационной безопасностью организации (СУИБ)						
4.1	Управление рисками ИБ /Лек/	7	4		Л1.1	0	
4.2	Управление инцидентами ИБ /Лек/	7	2		Л1.1	0	
4.3	Система управления информационной безопасностью организации (СУИБ): структура и требования /Пр/	7	4		Л1.1	0	
4.4	Подсистемы СУИБ /Пр/	7	8		Л1.1	0	
	Раздел 5. Ресурсное обеспечение СУИБ						
5.1	Техническое обеспечение УИБ /Лек/	7	2		Л1.1	0	
5.2	Организационное и кадровое обеспечение СУИБ /Лек/	7	2		Л1.1	0	
5.3	Организационное и кадровое обеспечение СУИБ /Пр/	7	4		Л1.1	0	
5.4	Техническое обеспечение СУИБ /Пр/	7	2		Л1.1	0	
5.5	Организационное и кадровое обеспечение СУИБ /Ср/	7	30,65		Л1.1	0	
	Раздел 6. Контроль и проверка процессов УИБ						
6.1	Контроль и проверка процессов УИБ /Лек/	7	4		Л1.1	0	
6.2	Инструментальные средства проверки СУИБ /Лек/	7	2		Л1.1	0	
6.3	Контроль процессов УИБ /Пр/	7	2		Л1.1	0	
6.4	Проверка процессов УИБ /Пр/	7	4		Л1.1	0	
	Раздел 7. Документационное обеспечение СУИБ						

7.1	Документационное обеспечение СУИБ /Лек/	7	4		Л1.1	0	
7.2	Документационное обеспечение СУИБ: определение состава /Пр/	7	2		Л1.1	0	
7.3	Документационное обеспечение СУИБ: разработка /Пр/	7	4		Л1.1	0	
7.4	Экзамен /ИВКР/	7	2,35		Л1.1	0	

5. ОЦЕНОЧНЫЕ СРЕДСТВА

5.1. Контрольные вопросы и задания

Тема: 1. Базовые понятия и подходы к управлению информационной безопасностью
1. Какие ключевые понятия определяют информационную безопасность (конфиденциальность, целостность, доступность)?
2. Какие основные угрозы информационной безопасности актуальны в современных организациях?
3. Какие модели управления ИБ существуют (например, PDCA, COBIT, NIST)? В чем их отличие?
4. Что такое «защита в глубину» (defense-in-depth) и как она применяется на практике?
5. Как связаны корпоративная стратегия и стратегия управления информационной безопасностью?
Тема: 2. Стандарты ISO серии 27000
6. Какова структура и назначение стандартов ISO/IEC 27000-серии?
7. Какие основные требования предъявляет ISO 27001 к системе управления информационной безопасностью (СУИБ)?
8. Как проводится оценка соответствия требованиям ISO 27001? Какие этапы сертификации?
9. Как стандарт ISO 27005 регулирует управление рисками информационной безопасности?
10. Какие документы обязательны для внедрения ISO 27001 (например, реестр активов, матрица рисков)?
Тема: 3. Отраслевые стандарты по ИБ
11. Какие отраслевые стандарты ИБ применяются в финансовой сфере (например, PCI DSS)? Какие требования они включают?
12. Как регулируется защита данных в здравоохранении (HIPAA)? Какие особенности реализации?
13. Какие нормы и стандарты ИБ актуальны в государственных организациях (например, ФСТЭК России, ГОСТ Р)?
14. Как стандарты GDPR влияют на управление данными в международных компаниях?
15. Какие отраслевые угрозы требуют специфических мер защиты (например, ICS/SCADA в промышленности)?
Тема: 4. Политика ИБ организации
16. Какие элементы включает политика информационной безопасности организации?
17. Как политика ИБ согласуется с законодательством и внутренними регламентами?
18. Как обеспечивается коммуникация политики ИБ среди сотрудников и сторонних лиц?
19. Как часто обновляется политика ИБ? Какие критерии актуализации?
20. Какие последствия наступают при нарушении положений политики ИБ?
Тема: 5. Организационные основы политики ИБ
21. Какие роли и ответственности определяются в рамках СУИБ (например, CISO, менеджеры по ИБ)?
22. Как организуется взаимодействие между службой ИБ и другими отделами (IT, HR, юридический)?
23. Какие процессы управления доступом реализуются в соответствии с принципами минимальных привилегий?
24. Как управляются внешние поставщики и подрядчики в контексте ИБ?
25. Какие меры предпринимаются для обеспечения бизнес-континуитета (BCM)?
Тема: 6. Управление рисками ИБ
26. Какие этапы включает процесс управления рисками ИБ (идентификация, оценка, лечение, мониторинг)?
27. Какие методологии оценки рисков используются (например, OCTAVE, FAIR, MEHARI)?
28. Что такое «приемлемый уровень риска»? Как он определяется?
29. Какие методы снижения рисков применяются (избегание, передача, снижение, принятие)?
30. Как документируется реестр рисков и план мероприятий по их минимизации?
Тема: 7. Управление инцидентами ИБ
31. Какие этапы включает жизненный цикл инцидента информационной безопасности?
32. Как организуется система обнаружения и реагирования на инциденты (SIEM, SOC)?
33. Что такое план реагирования на инциденты (IRP)? Какие ключевые элементы он содержит?
34. Как проводится анализ инцидентов (post-incident review) и извлечение уроков?
35. Какие требования предъявляются к уведомлению о нарушении конфиденциальности (например, GDPR)?
Тема: 8. Техническое обеспечение УИБ
36. Какие технические средства используются для обеспечения конфиденциальности (шифрование, DLP)?
37. Какие решения применяются для обеспечения целостности данных (хэширование, контроль изменений)?
38. Как обеспечивается доступность информации (резервное копирование, отказоустойчивые системы)?
39. Какие технологии используются для защиты периметра сети (межсетевые экраны, IDS/IPS)?
40. Как реализуется защита endpoint-устройств (антивирусы, EDR, шифрование дисков)?
Тема: 9. Организационное и кадровое обеспечение СУИБ
41. Какие процессы управления персоналом связаны с ИБ (проверка при приеме, обучение, увольнение)?
42. Как организуется обучение сотрудников по вопросам ИБ? Какие формы используются?
43. Какие меры применяются для предотвращения социальной инженерии?
44. Как оценивается эффективность кадрового обеспечения СУИБ?
45. Какие роли и полномочия определяются в рамках модели RBAC (Role-Based Access Control)?

Тема: 10. Контроль и проверка процессов УИБ
46. Какие виды аудита применяются в СУИБ (внутренний, независимый, сертификационный)?
47. Какие метрики используются для оценки эффективности СУИБ?
48. Как проводится пентестинг и как он помогает выявлять уязвимости?
49. Какие инструменты автоматизации используются для мониторинга состояния ИБ?
50. Как анализируется соответствие требованиям регуляторов и стандартов?
Тема: 11. Инструментальные средства проверки СУИБ
51. Какие системы управления уязвимостями (VMS) применяются на практике?
52. Как используются инструменты сканирования уязвимостей (Nessus, OpenVAS)?
53. Какие средства анализа логов и событий безопасности (SIEM, Splunk, QRadar)?
54. Как проводится автоматизированная проверка соответствия стандартам (например, Tenable.sc)?
55. Какие инструменты применяются для тестирования на проникновение (Kali Linux, Metasploit)?
Тема: 12. Документационное обеспечение СУИБ
56. Какие документы обязательны для СУИБ согласно ISO 27001?
57. Как организуется ведение реестра активов информации?
58. Как оформляются процедуры управления инцидентами и аварийным восстановлением?
59. Какие требования предъявляются к документации по политикам и стандартам ИБ?
60. Как обеспечивается актуальность и контроль версий документов СУИБ?

5.2. Темы письменных работ

не предусмотрены

5.3. Оценочные средства

Рабочая программа "Управление информационной безопасностью" 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 8 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	Краковский Ю. М.	Методы и средства защиты информации: 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	Электронно-библиотечная система «Книжный Дом Университета» ("БиблиоТех")
6.3.2.2	Электронно-библиотечная система "Лань" Доступ к коллекциям электронных изданий ЭБС "Издательство "Лань"
6.3.2.3	База данных научных электронных журналов "eLibrary"

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 "Управление информационной безопасностью" 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.