МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

(МГРИ)

Эксплуатация автоматизированных систем в защищенном исполнении

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 50,35
самостоятельная работа 30,65
часов на контроль 27

Виды контроля в семестрах:
экзамены 9

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**9 (5.1)**		Итого	
Недель	16			
Вид занятий	УП	РП	УП	РП
Лекции	16	16	16	16
Практические	32	32	32	32
Иные виды контактной работы	2,35	2,35	2,35	2,35
В том числе инт.	4	4	4	4
Итого ауд.	50,35	50,35	50,35	50,35
Контактная работа	50,35	50,35	50,35	50,35
Сам. работа	30,65	30,65	30,65	30,65
Часы на контроль	27	27	27	27
Итого	108	108	108	108

Москва 2025

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Целью изучения дисциплины является теоретическая и практическая подготовка специалистов к деятельности, связанной с разработкой и эксплуатацией защищенных автоматизированных информационных систем в своей профессиональной деятельности.
1.2	Задачи дисциплины:
1.3	- изучение методов, способов и средств обеспечения отказоустойчивости автоматизированных систем;
1.4	- изучение основных мер по защите информации в автоматизированных системах;
1.5	- овладение навыками эксплуатации автоматизированных информационных систем для решения различных классов задач;
1.6	- формирование у обучаемых научного подхода к осмыслению процессов обработки, хранения и передачи информации;
1.7	- изучение основных мер по защите информации в автоматизированных системах;
1.8	- изучение содержания и порядка деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.О
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Информационная безопасность открытых систем
2.1.2	Контроль безопасности автоматизированных систем
2.1.3	Защита информации от утечки по техническим каналам
2.1.4	Мониторинг информационной безопасности и активный поиск киберугроз
2.1.5	Разработка и эксплуатация автоматизированных систем в защищенном исполнении
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
ОПК-13: Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем	
Знать:	
Уровень 1	риски подсистем защиты информации автоматизированных систем и экспериментальные методы их оценки; организационную структуру и функциональную часть автоматизированных систем; методы и средства реализации удаленных сетевых атак на автоматизированные системы; классификацию и количественные характеристики технических каналов утечки информации;
Уровень 2	риски подсистем защиты информации автоматизированных систем и экспериментальные методы их оценки; организационную структуру и функциональную часть автоматизированных систем; методы и средства реализации удаленных сетевых атак на автоматизированные системы; классификацию и количественные характеристики технических каналов утечки информации;
Уровень 3	способы обеспечения контроля безопасности автоматизированных систем; основные информационные технологии, используемые в автоматизированных системах; методы, способы и средства обеспечения отказоустойчивости автоматизированных систем;
Уметь:	
Уровень 1	анализировать и оценивать угрозы информационной безопасности автоматизированных систем; осуществлять управление и администрирование защищенных автоматизированных систем;
Уровень 2	разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем; использовать средства инструментального контроля показателей эффективности технической защиты информации;
Уровень 3	осуществлять планирование, организацию и контроль над безопасностью автоматизированной системы с учетом требований по защите информации; восстанавливать работоспособность подсистемы информационной безопасности автоматизированных систем в нештатных ситуациях;
Владеть:	
Уровень 1	осуществлять планирование, организацию и контроль над безопасностью автоматизированной системы с учетом требований по защите информации; восстанавливать работоспособность подсистемы информационной безопасности автоматизированных систем в нештатных ситуациях;
Уровень 2	навыками проектирования системы защиты объекта информатизации от утечек по техническим каналам;

	навыками применения способов обеспечения контроля безопасности автоматизированных систем;
Уровень 3	навыками разработки документов для обеспечения контроля безопасности информации в автоматизированной системе при её эксплуатации (включая управление инцидентами информационной безопасности); навыками поддержания работоспособности, обнаружения и устранения неисправностей в работе электронных аппаратных средств автоматизированных систем;

ОПК-14: Способен осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите информации, проводить подготовку исходных данных для технико-экономического обоснования проектных решений	
Знать:	
Уровень 1	основы построения, расчета и анализа современной системы показателей, характеризующих деятельность хозяйствующих субъектов на микроуровне; критерии оценки защищенности автоматизированной системы; основные угрозы безопасности информации и модели нарушителя в автоматизированных системах;
Уровень 2	регламент проведения аттестационных испытаний; требования защиты информации к аттестованным объектам;
Уровень 3	требования к этапам ввода и вывода из эксплуатации системы защиты информации; организационные, правовые, программно-аппаратные, криптографические, технические меры по защите информации, реализуемые в автоматизированных системах;
Уметь:	
Уровень 1	осуществлять расчет себестоимости продукции; рассчитывать влияние факторов на различные виды расходов; осуществлять расчет потребности в инвестициях;
Уровень 2	контролировать уровень защищенности в автоматизированных системах; разрабатывать программу и методики аттестационных испытаний;
Уровень 3	разрабатывать заключение по результатам аттестационных испытаний; администрировать подсистемы информационной безопасности автоматизированных систем;
Владеть:	
Уровень 1	владения методами распределения накладных затрат и оценки эффективности проектных решений; анализа событий, связанных с защитой информации в автоматизированных системах;
Уровень 2	навыками проведения аттестационных испытаний; мониторинга изменения состояния аттестованного объекта информатизации;
Уровень 3	использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем;

В результате освоения дисциплины (модуля) обучающийся должен

3.1	**Знать:**
3.1.1	методы мониторинга информационной безопасности и средства реализации удаленных сетевых атак на автоматизированные системы, организационную структуру и функциональную часть автоматизированных систем;
3.1.2	методы и средства реализации удаленных сетевых атак на автоматизированные системы;
3.1.3	руководящие и методические документы уполномоченных федеральных органов исполнительной власти по обеспечению
3.1.4	безопасности информации в автоматизированных системах;
3.1.5	способы обеспечения контроля безопасности автоматизированных систем;
3.1.6	критерии оценки защищенности автоматизированной системы;
3.1.7	основные угрозы безопасности информации и модели нарушителя в автоматизированных системах, основные меры по защите информации в автоматизированных системах;
3.1.8	содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем безопасности автоматизированных систем;
3.1.9	принципы формирования политики информационной безопасности в автоматизированных системах , риски подсистем защиты информации автоматизированных систем и экспериментальные методы их оценки;
3.1.10	типовые методики проведения измерений параметров, характеризующих наличие технических каналов утечки информации, классификацию и количественные характеристики технических каналов утечки информации;
3.1.11	способы и средства защиты информации от утечки по техническим каналам, контроля их эффективности;
3.1.12	организацию защиты информации от утечки по техническим каналам на объектах информатизации;
3.1.13	основы построения, расчета и анализа современной системы показателей, характеризующих деятельность хозяйствующих субъектов на микроуровне, подходы к классификации факторов внешней среды организации и их влияние на деятельность организации
3.2	**Уметь:**
3.2.1	осуществлять диагностику и мониторинг систем защиты автоматизированных систем, осуществлять управление и администрирование защищенных автоматизированных систем;

3.2.2	разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем;
3.2.3	осуществлять планирование, организацию и контроль над безопасностью автоматизированной системы с учетом требований по защите информации;
3.2.4	контролировать уровень защищенности в автоматизированных системах, настраивать программное обеспечение системы защиты
3.2.5	информации автоматизированной системы;
3.2.6	разрабатывать частные политики информационной безопасности автоматизированных систем , анализировать и оценивать угрозы информационной безопасности автоматизированных систем;
3.2.7	проводить контрольно-измерительные работы в целях оценки количественных характеристик технических каналов утечки информации, использовать средства инструментального контроля показателей эффективности технической защиты информации;
3.2.8	осуществлять расчет себестоимости продукции;
3.2.9	рассчитывать влияние факторов на различные виды расходов;
3.2.10	осуществлять расчет потребности в инвестициях, формулировать управленческие решения по результатам анализа внешней и внутренней среды организации
3.3	**Владеть:**
3.3.1	разработки политик информационной безопасности автоматизированных систем;
3.3.2	применения способов обеспечения контроля безопасности автоматизированных систем;
3.3.3	разработки документов для обеспечения контроля безопасности информации в автоматизированной системе при её эксплуатации (включая управление инцидентами информационной безопасности);
3.3.4	анализа событий, связанных с защитой информации в автоматизированных системах, выявления и анализа уязвимостей автоматизированной системы, приводящих к возникновению угроз безопасности информации;
3.3.5	управления процессами обеспечения безопасности автоматизированных систем, анализа информационной инфраструктуры автоматизированных систем;
3.3.6	проектирования системы защиты объекта информатизации от утечек по техническим каналам;
3.3.7	владения методами распределения накладных затрат и оценки эффективности проектных решений, методами оценки экономической эффективности результатов хозяйственной деятельности различных субъектов экономической системы

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. Основы эксплуатации защищенных АИС						
1.1	Аттестация АИС по требованиям безопасности. Содержание основных документов, определяющих цели, задачи, порядок проведения аттестации. Требования и рекомендации по защите служебной тайны и персональных данных при работе АИС. Порядок обеспечения защиты информации при эксплуатации АИС /Лек/	9	2	ОПК-13 ОПК-14	Л1.1 Л1.2Л2.1	0	
1.2	Особенности эксплуатации АИС на объекте защиты. Технические и программные средства защиты АИС от несанкционированного доступа. Организация технического обслуживания защищенных АИС. Содержание и порядок ведения эксплуатационной документации /Лек/	9	4	ОПК-13 ОПК-14	Л1.1 Л1.2Л2.1	0	
1.3	Методы проверки защищенных АИС. Содержание и порядок ведения эксплуатационной документации /Лек/	9	2	ОПК-13 ОПК-14	Л1.1 Л1.2Л2.1	0	
1.4	Анализ основных документов, определяющих цели, задачи, порядок проведения аттестации /Пр/	9	4	ОПК-13 ОПК-14	Л1.1 Л1.2Л2.1	4	
1.5	Анализ требований к эксплуатации АИС на объекте защиты /Пр/	9	4	ОПК-13 ОПК-14	Л1.1 Л1.2Л2.1	0	

1.6	Анализ этапов обеспечения защиты информации при эксплуатации АИС /Пр/	9	4	ОПК-13 ОПК-14	Л1.1 Л1.2Л2.1	0	
1.7	Содержание и порядок ведения эксплуатационной документации, при организации технического обслуживания защищенных АИС /Пр/	9	4	ОПК-13 ОПК-14	Л1.1 Л1.2Л2.1	0	
1.8	Анализ содержания и порядка ведения эксплуатационной документации /Пр/	9	2	ОПК-13 ОПК-14	Л1.1 Л1.2Л2.1	0	
1.9	Подготовка к практическим занятиям /Ср/	9	30,65	ОПК-13 ОПК-14	Л1.1 Л1.2Л2.1	0	
	Раздел 2. Диагностика программных и аппаратных средств АИС						
2.1	Средства диагностирования защищенных АИС. Контрольно-измерительное оборудование, используемое при поиске неисправностей аппаратных средств /Лек/	9	2	ОПК-13 ОПК-14	Л1.1 Л1.2Л2.1	0	
2.2	Технологическое оборудование для ремонта аппаратных средств АИС. Диагностические программы и пакеты диагностических программ, их назначение, возможности и порядок использования /Лек/	9	2	ОПК-13 ОПК-14	Л1.1 Л1.2Л2.1	0	
2.3	Аппаратно-программные средства диагностики АИС /Лек/	9	2	ОПК-13 ОПК-14	Л1.1 Л1.2Л2.1	0	
2.4	Аппаратно-программные средства контроля функционирования отдельных элементов, узлов, блоков. /Лек/	9	2	ОПК-13 ОПК-14	Л1.1 Л1.2Л2.1	0	
2.5	Контрольно-измерительное оборудование, используемое при поиске неисправностей аппаратных средств /Пр/	9	4	ОПК-13 ОПК-14	Л1.1 Л1.2Л2.1	0	
2.6	Диагностические программы и пакеты диагностических про-грамм, их назначение, возможности и порядок использования /Пр/	9	4	ОПК-13 ОПК-14	Л1.1 Л1.2Л2.1	0	
2.7	Аппаратно-программные средства диагностики АИС /Пр/	9	4	ОПК-13 ОПК-14	Л1.1 Л1.2Л2.1	0	
2.8	Аппаратно-программные средства контроля функционирования отдельных элементов, узлов, блоков /Пр/	9	2	ОПК-13 ОПК-14	Л1.1 Л1.2Л2.1	0	
2.9	Экзамен /ИВКР/	9	2,35	ОПК-13 ОПК-14	Л1.1 Л1.2Л2.1	0	

5. ОЦЕНОЧНЫЕ СРЕДСТВА

5.1. Контрольные вопросы и задания

Тема: 1. Аттестация АИС по требованиям безопасности
1. Какие цели и задачи определяются при проведении аттестации АИС на соответствие требованиям безопасности?
2. Какие основные документы регламентируют порядок проведения аттестации АИС? Приведите примеры.
3. Какие критерии и параметры оценки безопасности используются при аттестации АИС?
4. Что включает подготовительный этап аттестации АИС? Какие документы готовятся?
Тема: 2. Защита служебной тайны и персональных данных в АИС
5. Какие требования предъявляются к обеспечению конфиденциальности служебной информации в АИС?
6. Какие меры защиты персональных данных реализуются при эксплуатации АИС?
7. Какие нормативные и правовые акты регулируют защиту служебной тайны и персональных данных?
8. Как организуется контроль за соблюдением требований по защите конфиденциальной информации?
Тема: 3. Обеспечение защиты информации в АИС
9. Какие технические средства защиты используются для предотвращения несанкционированного доступа (НСД) к АИС?
10. Какие программные средства обеспечивают защиту информации в АИС? Приведите примеры.
11. Что включает политика безопасности информации в АИС? Как она реализуется?

12. Какие методы шифрования и аутентификации применяются в защищенных АИС?
Тема: 4. Эксплуатация АИС на объекте защиты
13. Какие особенности эксплуатации АИС учитываются на объекте защиты с высокими требованиями к безопасности?
14. Как организуется физическая защита аппаратных средств АИС на объекте?
15. Какие процедуры ввода/вывода из эксплуатации применяются для защищенных АИС?
16. Какие меры предпринимаются для минимизации рисков аварийного выхода из строя компонентов АИС?
Тема: 5. Техническое обслуживание и документация
17. Как организуется техническое обслуживание защищенных АИС? Какие этапы включает?
18. Какие требования предъявляются к ведению эксплуатационной документации АИС?
19. Что включает регламент технического обслуживания АИС? Как он согласуется с нормативами?
20. Какие документы обязательны для ведения при эксплуатации защищенных АИС?
Тема: 6. Методы проверки и диагностики АИС
21. Какие методы используются для проверки соответствия АИС требованиям защищенности?
22. Что такое плановая и внеплановая диагностика АИС? В чем их отличие?
23. Какие критерии оценки работоспособности системы применяются при диагностике?
24. Как организуется взаимодействие между службами безопасности и техническим персоналом при проверке АИС?
Тема: 7. Средства диагностирования и контрольно-измерительное оборудование
25. Какие контрольно-измерительные приборы используются для диагностики аппаратных средств АИС?
26. Какие диагностические программы применяются для выявления неисправностей в АИС?
27. Что включают пакеты диагностических программ? Каковы их возможности и ограничения?
28. Какие средства аппаратной диагностики используются для тестирования процессоров, памяти и интерфейсов?
Тема: 8. Технологическое оборудование для ремонта АИС
29. Какое оборудование используется для ремонта аппаратных средств АИС?
30. Какие требования предъявляются к сервисным центрам, занимающимся ремонтом защищенных АИС?
31. Как обеспечивается конфиденциальность данных при ремонте оборудования АИС?
32. Какие меры предосторожности применяются при замене критически важных компонентов?
Тема: 9. Аппаратно-программные средства диагностики и контроля
33. Что такое аппаратно-программные средства диагностики АИС? Приведите примеры.
34. Какие функции выполняют средства контроля функционирования отдельных элементов, узлов и блоков АИС?
35. Как осуществляется мониторинг состояния системы в реальном времени?
36. Какие алгоритмы используются для прогнозирования отказов и планирования профилактического обслуживания?
Тема: 10. Интеграция и оптимизация диагностики
37. Как интегрируются аппаратно-программные средства диагностики в общую архитектуру АИС?
38. Какие методы оптимизации времени диагностики применяются в защищенных системах?
39. Как оценивается эффективность диагностических процедур в АИС?
40. Какие современные технологии (например, ИИ, машинное обучение) используются для анализа состояния АИС?

5.2. Темы письменных работ

Не предусмотрены

5.3. Оценочные средства

Рабочая программа "Эксплуатация автоматизированных систем в защищенном исполнении" 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 9 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	Казарин О. В., Шубинский И. Б.	Надежность и безопасность программного обеспечения: учебное пособие для вузов	Москва: Юрайт, 2024
Л1.2	Богатырев В. А.	Информационные системы и технологии. Теория надежности: учебное пособие для вузов	Москва: Юрайт, 2024

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год
Л2.1	Запечников С. В., Казарин О. В., Тарасов А. А.	Криптографические методы защиты информации: учебник для вузов	Москва: Юрайт, 2024

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.	
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 "Эксплуатация автоматизированных систем в защищенном исполнении" 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.