Документ подписан простой электронной подписью
Информация о владельце:
ФИО: ПАНОВ Юрий Петрович
Должность: Ректор
Дата подписания: 09.06.2025 11:34:26
Уникальный программный ключ:
e30ba4f0895d1683ed43800960e77389e6cbff62

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования "Российский государственный геологоразведочный университет имени Серго Орджоникидзе"

(МГРИ)

Разработка и 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	Виды контроля	в семестрах:
в том числе:		экзамены	8
аудиторные занятия	58,35		
самостоятельная работа	22,65		
часов на контроль	27		

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	8 (4.2)		Итого	
	уп	рп	уп	рп
Неделя	14 5/6			
Вид занятий	уп	рп	уп	рп
Лекции	28	28	28	28
Практические	28	28	28	28
Иные виды контактной работы	2,35	2,35	2,35	2,35
В том числе инт.	4	4	4	4
Итого ауд.	58,35	58,35	58,35	58,35
Контактная работа	58,35	58,35	58,35	58,35
Сам. работа	22,65	22,65	22,65	22,65
Часы на контроль	27	27	27	27
Итого	108	108	108	108

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Целью изучения дисциплины является теоретическая и практическая подготовка специалистов к деятельности, связанной с разработкой защищенных автоматизированных информационных систем в своей профессиональной деятельности.
1.2	Задачи дисциплины:
1.3	- изучение основных угроз безопасности информации в автоматизированных системах и освоение методик оценки данных угроз;
1.4	- изучение методов, способов, средств, последовательности и содержания этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем;
1.5	- изучение основных мер по защите информации в автоматизированных системах;
1.6	- изучение содержания и порядка деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем.
1.7	- изучение методов и средств разработки автоматизированных систем и подсистем безопасности автоматизированных систем;
1.8	- изучение содержания основных этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем;
1.9	- изучение методов, способов и средств обеспечения отказоустойчивости автоматизированных систем;
1.10	- изучение основных мер по защите информации в автоматизированных системах;
1.11	- формирование у обучаемых научного подхода к осмыслению процессов обработки, хранения и передачи информации.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.О
2.1	Требования к предварительной подготовке обучающегося:
2.2	Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:
2.2.1	Эксплуатация автоматизированных систем в защищенном исполнении
2.2.2	Основы аттестации объектов информатизации

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
ОПК-11: Способен разрабатывать компоненты систем защиты информации автоматизированных систем	
Знать:	
Уровень 1	основные понятия теории информации и кодирования; принципы, методы и средства выявления угроз безопасности автоматизированных систем; принципы аутентификации и идентификации пользователей; концепцию построения системы разграничения доступа; основные меры по защите информации в автоматизированных системах
Уровень 2	содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем безопасности автоматизированных систем; особенности межсетевое экранирования
Уровень 3	программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами данных, компьютерных сетях
Уметь:	
Уровень 1	выявлять и уничтожать компьютерные вирусы; работать со специальной технической литературой; использовать электронные цифровые подписи; противодействовать нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты
Уровень 2	проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы
Уровень 3	проектировать информационные системы; обосновывать и планировать состав и архитектуру моделируемых и проектируемых информационных, автоматизированных и автоматических систем; разрабатывать и обосновывать критерии оценки эффективности проектируемой системы обеспечения информационной безопасности; настраивать программное обеспечение системы защиты информации автоматизированной системы
Владеть:	
Уровень 1	навыками эксплуатации и обслуживания аппаратуры, оборудования и программного обеспечения, связанных

	с обеспечением безопасности информации; навыками шифрования и защиты от несанкционированного доступа
Уровень 2	навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем
Уровень 3	навыками участия в разработке системы обеспечения информационной безопасности объекта; навыками проектирования автоматизированных информационных систем и систем обеспечения информационной безопасности

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	основные меры по защите информации в автоматизированных системах;
3.1.2	содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем безопасности автоматизированных систем
3.1.3	критерии оценки защищенности автоматизированной системы;
3.1.4	основные угрозы безопасности информации и модели нарушителя в автоматизированных системах
3.2	Уметь:
3.2.1	настраивать программное обеспечение системы защиты информации автоматизированной системы
3.2.2	контролировать уровень защищенности в автоматизированных системах
3.3	Владеть:
3.3.1	выявления и анализа уязвимостей автоматизированной системы, приводящих к возникновению угроз безопасности информации
3.3.2	анализа событий, связанных с защитой информации в автоматизированных системах

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетенции	Литература	Инте ракт.	Примечание
	Раздел 1. Требования защищенности автоматизированных систем в условиях ак-туальных угроз безопасности информации						

1.1	Критерии оценки защищенности автоматизированных систем. ГОСТ 15408 часть 1 общие положения /Лек/	8	4	ОПК-11 ОПК-14	Л1.1	0	
1.2	Оценка угроз безопасности автоматизированных систем. Методика оценки угроз безопасности информации /Лек/	8	4	ОПК-11 ОПК-14	Л1.1	0	
1.3	Критерии оценки защищенности автоматизированных систем. ГОСТ 15408 часть 2 Функции безопасности /Лек/	8	4	ОПК-11 ОПК-14	Л1.1	0	
1.4	Модели данных, систем и процессов защиты информации в автоматизированных системах /Пр/	8	2	ОПК-11 ОПК-14	Л1.1	0	
1.5	Критерии оценки защищенности автоматизированных систем /Пр/	8	2	ОПК-11 ОПК-14	Л1.1	0	
1.6	Определение и содержание понятия угрозы безопасности автоматизированных систем /Пр/	8	2	ОПК-11 ОПК-14	Л1.1	0	
1.7	Требования защищенности автоматизированных систем в условиях актуальных угроз безопасности информации /Пр/	8	2	ОПК-11 ОПК-14	Л1.1	0	
1.8	Порядок разработки модели угроз и нарушителей информационной безопасности автоматизированных систем /Пр/	8	2	ОПК-11 ОПК-14	Л1.1	0	
1.9	Оценка угроз безопасности информационных систем персональных данных /Пр/	8	2	ОПК-11 ОПК-14	Л1.1	0	
	Раздел 2. Разработка защищенных автоматизированных систем						
2.1	Стадии и этапы разработки автоматизированных систем /Лек/	8	4	ОПК-11 ОПК-14	Л1.1	0	
2.2	Техническое задание на создание автоматизированных систем /Лек/	8	4	ОПК-11 ОПК-14	Л1.1	0	
2.3	Разработка автоматизированных систем в защищенном исполнении /Лек/	8	2	ОПК-11 ОПК-14	Л1.1	0	
2.4	Реализация моделей безопасности автоматизированных систем /Лек/	8	2	ОПК-11 ОПК-14	Л1.1	0	
2.5	Автоматизированные системы в защищенном исполнении для объектов КИИ /Лек/	8	4	ОПК-11 ОПК-14	Л1.1	0	
2.6	Стадии и этапы разработки автоматизированных систем /Пр/	8	4	ОПК-11 ОПК-14	Л1.1	0	
2.7	Техническое задание на создание системы защиты информации /Пр/	8	2	ОПК-11 ОПК-14	Л1.1	2	
2.8	Работы на стадиях и этапах создания автоматизированных систем в защищенном исполнении /Пр/	8	4	ОПК-11 ОПК-14	Л1.1	0	
2.9	Ввод в эксплуатацию защищенных автоматизированных систем /Пр/	8	2	ОПК-11 ОПК-14	Л1.1	2	
2.10	Автоматизированные системы в защищенном исполнении для объектов КИИ /Пр/	8	4	ОПК-11 ОПК-14	Л1.1	0	
2.11	Выполнение индивидуальных заданий по модулю /Ср/	8	11	ОПК-11 ОПК-14	Л1.1	0	
2.12	Самостоятельное изучение теоретического материала /Ср/	8	11,65	ОПК-11 ОПК-14	Л1.1	0	
2.13	Экзамен /ИВКР/	8	2,35	ОПК-11 ОПК-14	Л1.1	0	

5. ОЦЕНОЧНЫЕ СРЕДСТВА**5.1. Контрольные вопросы и задания**

Тема: 1. Критерии оценки защищенности АС по ГОСТ Р 15408-1 (Общие положения)

1. Какие цели и задачи регламентируются ГОСТ Р 15408-1 при оценке защищенности АС?
2. Какие основные понятия и термины определяются в части 1 стандарта (например, уровень защищенности, критерии оценки)?
3. Как классифицируются уровни защищенности АС по ГОСТ Р 15408-1? Какие параметры учитываются?
4. Какие виды угроз рассматриваются при оценке защищенности АС согласно ГОСТ Р 15408-1?
5. Какие этапы включает процесс сертификации АС по требованиям ГОСТ Р 15408-1?

Тема: 2. Оценка угроз безопасности АС

6. Какие источники угроз информационной безопасности наиболее актуальны для автоматизированных систем?
7. Какие методики используются для оценки угроз безопасности информации в АС (например, STRIDE, DREAD, OSTATE)?
8. Как строится модель угроз для АС с учетом специфики объекта КИИ?
9. Какие параметры учитываются при анализе вероятности реализации угроз и их последствий?
10. Как классифицируются угрозы по степени воздействия на конфиденциальность, целостность и доступность информации?

Тема: 3. Функции безопасности по ГОСТ Р 15408-2

11. Какие функции безопасности регламентируются ГОСТ Р 15408-2? Приведите примеры.
12. Какие требования предъявляются к механизмам контроля доступа в АС по ГОСТ Р 15408-2?
13. Какие методы защиты от несанкционированного доступа (НСД) реализуются в соответствии с ГОСТ Р 15408-2?
14. Какие функции безопасности обеспечивают целостность данных и предотвращение их модификации?
15. Как в стандарте описываются средства обеспечения доступности информации в условиях отказов или атак?

Тема: 4. Стадии и этапы разработки АС

16. Какие стадии жизненного цикла АС выделяются по ГОСТ? Какие требования к безопасности на каждом этапе?
17. Какие особенности проектирования АС для объектов КИИ по сравнению с обычными системами?
18. Как учитывается угрозный профиль системы при разработке технического задания?
19. Какие этапы включает внедрение и тестирование АС на соответствие требованиям безопасности?
20. Как организуется поддержка и обновление АС в рамках жизненного цикла?

Тема: 5. Техническое задание на создание АС

21. Какие разделы обязательны в ТЗ на разработку АС с учетом требований ИБ?
22. Как формулируются требования к защите информации в ТЗ (например, уровень защищенности, функции безопасности)?
23. Какие нормативные ссылки должны быть указаны в ТЗ (например, ГОСТ Р 15408, ФЗ-187)?
24. Как учитывается необходимость соответствия требованиям регуляторов (ФСТЭК, ФСБ) при разработке ТЗ?
25. Какие критерии приемки системы определяются в ТЗ при сертификации по ГОСТ Р 15408?

Тема: 6. Разработка АС в защищенном исполнении

26. Какие меры безопасности необходимо реализовать на этапе проектирования АС для объектов КИИ?
27. Как проводится анализ уязвимостей на этапе разработки АС? Какие инструменты используются?
28. Какие архитектурные решения применяются для повышения защищенности АС (например, разделение зон, многоуровневая защита)?
29. Как обеспечивается соответствие требованиям ГОСТ Р 15408 при выборе программного и аппаратного обеспечения?
30. Какие тесты проводятся для верификации функций безопасности (например, пентестинг, тестирование на проникновение)?

Тема: 7. Реализация моделей безопасности АС

31. Какие модели безопасности применяются для АС (например, Белл-Лападула, Биба, RBAC)?
32. Как строится модель угроз для АС в соответствии с ГОСТ Р 15408?
33. Какие компоненты включает модель безопасности объекта КИИ (политики, механизмы, мониторинг)?
34. Как обеспечивается соответствие модели безопасности требованиям ГОСТ Р 15408-2?
35. Какие метрики используются для оценки эффективности реализованной модели безопасности?

Тема: 8. АС в защищенном исполнении для объектов КИИ

36. Какие дополнительные требования предъявляются к АС, эксплуатируемым на объектах КИИ (например, ФСТЭК России)?
37. Какие меры физической и логической защиты реализуются для АС на КИИ?
38. Как организуется резервирование и восстановление АС после инцидентов на объектах КИИ?
39. Какие особенности управления доступом в АС КИИ (например, двухфакторная аутентификация, разделение ролей)?
40. Какие инструменты мониторинга безопасности используются в АС КИИ (например, SIEM, EDR)?

Тема: 9. Практические аспекты и современные вызовы

41. Какие ошибки наиболее часто допускаются при сертификации АС по ГОСТ Р 15408?
42. Как интеграция ОТ и ИТ влияет на требования к защите АС на объектах КИИ?
43. Какие методы используются для минимизации рисков утечки данных через побочные каналы (например, TEMPEST)?
44. Как искусственный интеллект применяется для обнаружения атак на АС КИИ?
45. Какие угрозы связаны с устаревшими протоколами в промышленных системах (например, Modbus, DNP3)?

Тема: 10. Сравнение с международными стандартами

46. Как ГОСТ Р 15408 соотносится с ISO/IEC 15408 (Common Criteria)?
47. Чем отличаются подходы к оценке защищенности АС в NIST SP 800-53 и ГОСТ Р 15408?

48. Как требования ГОСТ Р 15408-2 пересекаются с ISO/IEC 27001 при управлении рисками?
 49. Какие стандарты и практики могут использоваться для сертификации АС КИИ за рубежом (например, NISTIR 8183A, ENISA)?
 50. Как влияет цифровизация и внедрение IoT на необходимость адаптации ГОСТ Р 15408?

5.2. Темы письменных работ

не предусмотрены

5.3. Оценочные средства

Рабочая программа "Разработка и 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 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	Козырь Н. С., Оганесян Л. Л.	Экономические аспекты информационной безопасности: учебник и практикум для вузов	Москва: Юрайт, 2024

6.3.1 Перечень программного обеспечения

6.3.1.1	Office Professional Plus 2019	
6.3.1.2	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.
6.3.1.3	Windows 10	

6.3.2 Перечень информационных справочных систем

6.3.2.1	Электронно-библиотечная система "Лань" Доступ к коллекциям электронных изданий ЭБС "Издательство "Лань"	
6.3.2.2	База данных научных электронных журналов "eLibrary"	
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	<p>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</p>	<p>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; точки доступа, 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</p>	
------	--	--	--

		<p>требованиям по обеспечению безопасности.</p> <p>Учебный лабораторный комплекс для обеспечения исследований специального программного обеспечения и аппаратного СЗИ в составе:</p> <ul style="list-style-type: none">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. <p>Учебный лабораторный комплекс для обеспечения исследований типовых сертифицированных программных и программно-технических средств защиты информации от НСД.</p> <p>Учебный лабораторный комплекс для обеспечения исследований сертифицированных средств в которых реализованы средства защиты информации от НСД.</p> <p>УЛК для проведения аттестационных испытаний автоматизированных систем от НСД по требованиям безопасности информации.</p> <p>Аппаратно-программные комплексы в составе:</p> <ul style="list-style-type: none">аппаратно-программные средства управления	
--	--	--	--

		<p>доступом к данным; средства криптографической защиты информации; средства дублирования и восстановления данных; средства мониторинга состояния автоматизированных систем; средства контроля и управления доступом в помещения.</p>	
3-79	<p>Аудитория (защищаемое помещение) для проведения учебных занятий, в ходе которых до обучающихся доводится информация ограниченного доступа, не содержащая сведений, составляющих государственную тайну № 3-79</p>	<p>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 батарее.</p>	
3-79 А	<p>Специальная библиотека (библиотека литературы ограниченного доступа), предназначенная для хранения и обеспечения использования в образовательном процессе нормативных и методических документов ограниченного доступа № 3-79 А</p>	<p>рулонная штора; стол письменный; стул; шкаф металлический (двдверный) для хранения ДСП материалов; шкаф металлический для хранения мобильных телефонов типа ШСТ-26; экраны на батарее.</p>	

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 "Разработка и 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.