МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

(МГРИ)

Программно-аппаратные средства защиты информации

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>)	**5 (3.1)**		Итого	
Недель	16			
Вид занятий	УП	РП	УП	РП
Лекции	32	60	32	60
Практические	32	60	32	60
Иные виды контактной работы	2,35	2,6	2,35	2,6
Итого ауд.	66,35	154,6	66,35	154,6
Контактная работа	66,35	154,6	66,35	154,6
Сам. работа	86,65	70,4	86,65	70,4
Часы на контроль	27	27	27	27
Итого	180	252	180	252

Москва 2025

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Целью преподавания дисциплины является подготовка специалистов в области проектирования средств обеспечения информационной безопасности автоматизированных систем и привитие навыков разработки и анализа компонентов автоматизированных систем.
1.2	Задачи дисциплины:
1.3	- изучение моделей угроз и модели нарушителя информационной безопасности автоматизированной системы;
1.4	- изучение методов анализа проектных решений по обеспечению безопасности автоматизированных систем;
1.5	- получение практических навыков проектирования систем защиты информации автоматизированной системы;
1.6	- изучение методов анализа угроз и уязвимостей проектируемых и эксплуатируемых автоматизированных систем;
1.7	- получение навыков использования программно-аппаратных средств обеспечения безопасности сетей автоматизированных систем.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.В
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Инженерная и компьютерная графика
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-2.3: Способен проводить анализ возможностей реализации требований к компьютерному программному обеспечению
Знать:
Уметь:
Владеть:

ПК-6.3: Способен выполнять работы по выявлению и устранению инцидентов в информационно-коммуникационных системах
Знать:
Уметь:
Владеть:

В результате освоения дисциплины (модуля) обучающийся должен

3.1	**Знать:**
3.1.1	основные положения стандартов Единой системы конструкторской документации (ЕСКД) и Единой системы программной документации (ЕСПД), элементы компьютерного дизайна и графического отображения объектов в виде чертежей или рисунков
3.2	**Уметь:**
3.2.1	применять требования стандартов Единой системы конструкторской документации (ЕСКД) и Единой системы программной документации (ЕСПД), применять методы построения компьютерных моделей изделий
3.3	**Владеть:**
3.3.1	разработки технической документации в соответствии с требованиями стандартов Единой системы конструкторской документации (ЕСКД) и Единой системы программной документации (ЕСПД), элементарных геометрических построений при помощи средств компьютерной графики; построения двухмерных и трехмерных (3D) изображений изделий

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. Введение						
1.1	Введение /Лек/	5	2		Л1.1 Л1.2	0	
	Раздел 2. Цели и задачи обеспечения безопасности информационных технологий в различных режимах обработки						

2.1	Цели и задачи обеспечения безопасности информационных технологий в различных режимах обработки /Лек/	5	4		Л1.1 Л1.2	0	
2.2	Подготовка к лабораторным работам, оформление результатов /Ср/	5	4		Л1.1 Л1.2	0	
2.3	Подготовка к лабораторным работам, оформление результатов /Ср/	5	2		Л1.1 Л1.2	0	
	Раздел 3. Правовые, нормативно-технические и организационные требования к средствам защиты информации						
3.1	Требования к защищенности средств вычислительной техники, классы защищенности средств защиты информации от несанкционированного доступа /Лек/	5	4		Л1.1 Л1.2	0	
3.2	Требования к доверию, уровни отсутствия недекларированных возможностей (НДВ) /Лек/	5	4		Л1.1 Л1.2	0	
3.3	Требования к межсетевым экранам (МЭ), типы и классы защищенности МЭ /Лек/	5	2		Л1.1 Л1.2	0	
3.4	Требования к системам обнаружения вторжений (СОВ), типы и классы защищенности СОВ /Лек/	5	2		Л1.1 Л1.2	0	
3.5	Требования к средствам антивирусной защиты (САВЗ), типы и классы защищенности САВЗ /Лек/	5	2		Л1.1 Л1.2	0	
3.6	Требования к средствам доверенной загрузки (СДЗ), типы и классы защищенности СДЗ /Лек/	5	2		Л1.1 Л1.2	0	
3.7	Требования безопасности операционных систем (ОС), типы и классы защищенности ОС /Лек/	5	2		Л1.1 Л1.2	0	
3.8	Система сертификации ФСТЭК РФ /Лек/	5	2		Л1.1 Л1.2	0	
	Раздел 4. Подсистема контроля доступа пользователей к ресурсам						
4.1	Идентификация, аутентификация. Аппаратные и программные средства санкционированной загрузки. Авторизация. Аппаратные ключи пользователей /Лек/	5	2		Л1.1 Л1.2	0	
4.2	Дискреционный доступ. Мандатный доступ, его реализация для файлов, папок и процессов. Управление потоками информации /Лек/	5	2		Л1.1 Л1.2	0	
4.3	Мандатный доступ, его реализация для файлов, папок и процессов. /Пр/	5	16		Л1.1 Л1.2	0	
4.4	Реализация разграничения доступа к внешним устройствам. /Лаб/	5	6		Л1.1 Л1.2	0	
4.5	Управление потоками информации. /Лаб/	5	6		Л1.1 Л1.2	0	

4.6	Изучение материалов по плану СРС /Ср/	5	3,75		Л1.1 Л1.2	0	
	Раздел 5. Подсистема регистрации и учета						
5.1	Регистрация событий в ОС и СЗИ. Реализация маркировки и учета документов. Гарантированное удаление информации /Лек/	5	2		Л1.1 Л1.2	0	
5.2	Регистрация событий входа-выхода, запуска задач. /Пр/	5	16		Л1.1 Л1.2	0	
5.3	Гарантированное удаление информации. /Лаб/	5	6		Л1.1 Л1.2	0	
5.4	Зачет /ИВКР/	5	0,25		Л1.1 Л1.2	0	
	Раздел 6. Подсистема контроля целостности						
6.1	Контроль целостности файлов и папок. Контроль нарушения аппаратной конфигурации. Санкционированное использование внешних носителей /Лек/	5	4		Л1.1 Л1.2	0	
6.2	Замкнутая программная среда. Особенности реализации в различных СЗИ /Лек/	5	4		Л1.1 Л1.2	0	
6.3	Подсистема контроля целостности /Пр/	5	6		Л1.1 Л1.2	0	
6.4	Контроль целостности файлов и папок. /Лаб/	5	6		Л1.1 Л1.2	0	
6.5	Контроль нарушения аппаратной конфигурации. Санкционированное использование внешних носителей. /Лаб/	5	6		Л1.1 Л1.2	0	
	Раздел 7. Подсистема криптографической защиты						
7.1	Хранение информации в шифрованном виде. Монопольный и коллективный доступ к контейнерам. Особенности реализации в различных СЗИ /Лек/	5	4		Л1.1 Л1.2	0	
7.2	Протокол Kerberos 5 в доменных сетях /Лек/	5	4		Л1.1 Л1.2	0	
7.3	Подсистема криптографической защиты /Пр/	5	8		Л1.1 Л1.2	0	
	Раздел 8. Межсетевое экранирование						
8.1	Фильтрация пакетов. Трансляция сетевых адресов. Администрирование МЭ, схемы применения. Особенности реализации в различных СЗИ /Лек/	5	4		Л1.1 Л1.2	0	
8.2	Межсетевое экранирование /Пр/	5	6		Л1.1 Л1.2	0	
8.3	Фильтрация пакетов. /Лаб/	5	2		Л1.1 Л1.2	0	
8.4	Изучение материалов по плану СРС /Ср/	5	2		Л1.1 Л1.2	0	
	Раздел 9. Правовые, нормативно-технические и организационные требования к криптографическим средствам защиты информации						
9.1	Симметричное шифрование, ГОСТ Р 34.12-2018 /Лек/	5	4		Л1.1 Л1.2	0	
9.2	ЭЦП, и ассиметричное шифрование, хеширование. ГОСТ Р 34.10-2018, ГОСТ 34.11-2018 /Лек/	5	2		Л1.1 Л1.2	0	

9.3	Проблемы распределения и управления ключевой информацией. Система сертификация средств криптографической защиты информации /Лек/	5	2		Л1.1 Л1.2	0	
9.4	Правовые, нормативно-технические и организационные требования к криптографическим средствам защиты информации /Пр/	5	8		Л1.1 Л1.2	0	
9.5	Курсовая работа /Ср/	5	58,65		Л1.1 Л1.2	0	
9.6	Зачет /ИВКР/	5	2,35		Л1.1 Л1.2	0	

5. ОЦЕНОЧНЫЕ СРЕДСТВА

5.1. Контрольные вопросы и задания

Тема: 1. Введение и основы безопасности ИТ
1. Каковы цели и задачи обеспечения безопасности информационных технологий в различных режимах обработки данных (локальный, сетевой, облачный)?
2. Какие ключевые угрозы информационной безопасности актуальны для современных ИТ-систем?
3. Как связаны требования к конфиденциальности, целостности и доступности информации (CIA-триада) с задачами защиты ИТ?
4. Какие нормативные документы регулируют безопасность ИТ в России (например, ФЗ-187, ГОСТ Р 57580, требования ФСТЭК РФ)?
5. Какие международные стандарты и практики (например, ISO/IEC 27001, NIST Cybersecurity Framework) влияют на российские подходы к ИБ?
Тема: 2. Требования к защищенности средств вычислительной техники
6. Что такое классы защищенности средств вычислительной техники (СВТ) по ГОСТ Р 57580? Какие параметры определяют класс?
7. Какие основные функции безопасности должны реализовывать СВТ для соответствия требованиям ФСТЭК РФ?
8. Какие уязвимости СВТ наиболее распространены (например, утечки данных через побочные каналы, аппаратные бэкдоры)?
9. Как проводится сертификация СВТ на соответствие требованиям безопасности?
10. Какие меры применяются для минимизации рисков использования СВТ с недекларированными возможностями (НДВ)?
Тема: 3. Средства защиты информации (СЗИ) и их классификация
11. Какие типы и классы защищенности межсетевых экранов (МЭ) регламентированы в России?
12. Какие требования предъявляются к системам обнаружения вторжений (СОВ) по ФСТЭК РФ?
13. Как классифицируются средства антивирусной защиты (САВЗ) и какие классы защищенности для них установлены?
14. Что такое средства доверенной загрузки (СДЗ) и как они обеспечивают целостность ОС?
15. Какие функции безопасности обязательны для операционных систем (ОС) в контексте классов защищенности?
Тема: 4. Сертификация и регуляторные аспекты
16. Какова процедура сертификации СЗИ в системе ФСТЭК РФ? Какие этапы включает?
17. Какие документы обязательны для подтверждения соответствия СЗИ требованиям безопасности?
18. Как сертификация СЗИ связана с требованиями ФЗ-187 к объектам КИИ?
19. Какие особенности сертификации средств криптографической защиты информации (СКЗИ)?
20. Какие последствия несоответствия СЗИ установленным классам защищенности?
Тема: 5. Контроль доступа и идентификация
21. Как реализуются дискреционный и мандатный доступ в операционных системах? Приведите примеры (SELinux, Windows DACL/RBAC).
22. Что такое протокол Kerberos 5? Как он используется для аутентификации в доменных сетях?
23. Какие методы идентификации и аутентификации применяются в СЗИ (например, двухфакторная, биометрия, аппаратные ключи)?
24. Как организуется санкционированная загрузка и контроль целостности систем?
25. Какие требования предъявляются к управлению учетными записями пользователей и правами доступа?
Тема: 6. Регистрация событий и защита данных
26. Какие требования к регистрации и анализу событий безопасности в ОС и СЗИ (логирование, корреляция, аудит)?
27. Как реализуется маркировка и учет документов в защищенных системах?
28. Какие методы гарантированного удаления информации используются (например, шрединг, перезапись, криптографическое уничтожение)?
29. Как контролируется целостность файлов и папок (например, хэш-суммы, контрольные списки)?
30. Как ограничивается использование внешних носителей (например, через политики контроля устройств, шифрование)?
Тема: 7. Шифрование и криптографические стандарты
31. Какие алгоритмы симметричного шифрования регламентированы ГОСТ Р 34.12-2018 («Магма», «Кузнечик»)?
32. Как работает электронная цифровая подпись (ЭЦП) по ГОСТ Р 34.10-2018? Какие этапы генерации и проверки?
33. Какие хэш-функции используются в ГОСТ 34.11-2018? Какие у них преимущества и ограничения?
34. Какие проблемы возникают при распределении и управлении ключевой информацией в криптографических системах?
35. Как строится система сертификации открытых ключей (PKI) в соответствии с требованиями ФСТЭК РФ?

Тема: 8. Сетевая безопасность и мониторинг
36. Как реализуется фильтрация пакетов и трансляция сетевых адресов (NAT) в межсетевых экранах?
37. Какие схемы применения МЭ используются в корпоративных и промышленных сетях?
38. Как работают криптошлюзы для обеспечения защищенного обмена данными?
39. Какие особенности реализации туннелирования в СЗИ (например, IPsec, TLS, OpenVPN)?
40. Какие методы мониторинга сетевого трафика используются для обнаружения аномалий?
Тема: 9. Замкнутые программные среды и контроль конфигурации
41. Что такое замкнутая программная среда? Какие требования к ней предъявляются в контексте СЗИ?
42. Как контролируется нарушение аппаратной конфигурации (например, через хардверные мониторы, интеграционные проверки)?
43. Какие механизмы применяются для предотвращения запуска несанкционированного ПО (например, AppLocker, контроль целостности)?
44. Как реализуется шифрование информации при хранении и передаче (например, шифрованные контейнеры, EFS, BitLocker)?
45. Какие ограничения существуют для коллективного доступа к защищенным контейнерам?
Тема: 10. Современные технологии и вызовы
46. Как искусственный интеллект и машинное обучение используются для анализа угроз в ИТ-системах?
47. Как квантовые вычисления влияют на устойчивость криптографических алгоритмов?
48. Какие риски связаны с утечкой данных через побочные каналы (например, акустический, электромагнитный)?
49. Как облачные технологии изменяют подходы к обеспечению безопасности (например, Zero Trust, шифрование на стороне клиента)?
50. Какие угрозы возникают при использовании IoT-устройств в защищенных системах?
Тема: 11. Практические аспекты и кейсы
51. Какие этапы включает внедрение замкнутой программной среды в корпоративной инфраструктуре?
52. Как организовать гарантированное удаление данных на SSD-накопителях с учетом особенностей их архитектуры?
53. Какие ошибки чаще всего приводят к компрометации систем при использовании СДЗ?
54. Как реализовать многофакторную аутентификацию в среде с поддержкой Kerberos и LDAP?
55. Как протестировать эффективность СОВ в обнаружении APT-атак на тестовой инфраструктуре?
Тема: 12. Управление ключами и криптография
56. Какие этапы включает жизненный цикл криптографических ключей (генерация, хранение, отзыв, уничтожение)?
57. Как связаны длина ключа и стойкость алгоритмов шифрования (например, AES-256 vs ГОСТ «Кузнечник»)?
58. Как удостоверяющие центры (ЦУК) обеспечивают доверие к сертификатам и ключам?
59. Какие методы управления ключами применяются в гибридных (локальные + облачные) системах?
60. Как использовать Hardware Security Module (HSM) для повышения безопасности криптографических операций?
Тема: 13. Методы и средства контроля защищенности
61. Какие метрики используются для оценки эффективности СЗИ (например, MTTD, MTTR, покрытие угроз)?
62. Как проводится тестирование на проникновение (пентестинг) в системах с высокими требованиями к защите?
63. Какие инструменты применяются для автоматизации контроля защищенности (например, Nessus, OpenVAS, SIEM-системы)?
64. Как анализ логов и событий помогает выявлять атаки (например, через корреляцию, детектирование аномалий)?
65. Какие методы идентификации уязвимостей используются в автоматизированных системах (например, CVSS, CVE)?
Тема: 14. Объекты КИИ и специфика защиты
66. Какие дополнительные требования предъявляются к АС на объектах КИИ (например, изоляция, резервирование)?
67. Как обеспечить безопасность ОТ-сетей (например, АСУ ТП) при интеграции с IT-инфраструктурой?
68. Какие сценарии атак наиболее критичны для объектов КИИ (например, ransomware, DDoS, физический доступ)?
69. Какие меры защиты применяются для систем реального времени (например, минимальные задержки, отказоустойчивость)?
70. Как организовать мониторинг и реагирование на инциденты в условиях ограниченного доступа к системам КИИ?
Тема: 15. Практические задачи и кейсы
71. Разработка политики шифрования данных на предприятии с учетом требований ФЗ-152.
72. Анализ уязвимостей в реализации протокола Kerberos 5 в доменных сетях.
73. Проектирование замкнутой программной среды для работы с конфиденциальной информацией.
74. Сравнение эффективности СОВ от разных производителей в обнаружении APT.
75. Реализация системы гарантированного удаления данных в соответствии с ГОСТ Р 57580.

5.2. Темы письменных работ

не предусмотрены

5.3. Оценочные средства

Рабочая программа "Программно-аппаратные средства защиты информации" 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 7,8 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	Уймин А. Г.	Практикум. Демонстрационный экзамен базового уровня. Сетевое и системное администрирование: учебное пособие для вузов	Санкт-Петербург: Лань, 2024
Л1.2	Прохорова О. В.	Информационная безопасность и защита информации: учебник 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	Лаборатория программно-аппаратных средств защиты информации № 6-25	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	Лаб

		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 "Программно-аппаратные средства защиты информации" 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.