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)

Информационная безопасность открытых систем 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	4 ЗЕТ		
Часов по учебному плану	144	Виды контроля	в семестрах:
в том числе:		экзамены	б
аудиторные занятия	72,35		
самостоятельная работа	44,65		
часов на контроль	27		

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	6 (3.2)		Итого	
	УП	РП	УП	РП
Неделя	14			
Вид занятий	УП	РП	УП	РП
Лекции	28	28	28	28
Лабораторные	42	42	42	42
Иные виды контактной работы	2,35	2,35	2,35	2,35
В том числе инт.	4	4	4	4
Итого ауд.	72,35	72,35	72,35	72,35
Контактная работа	72,35	72,35	72,35	72,35
Сам. работа	44,65	44,65	44,65	44,65
Часы на контроль	27	27	27	27
Итого	144	144	144	144

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Целью дисциплины является: изучение технологий, методов и средств создания защищенных открытых информационных систем (ИС) .
1.2	Задачами дисциплины являются:
1.3	- привитие обучаемым основ культуры обеспечения информационной безопасности (ИБ) в ОИС;
1.4	- формирование у обучаемых понимания основ построения защищенных ОИС;
1.5	- ознакомление обучаемых с основными уязвимостями, угроза ИБ и сетевыми атаками, характерными для современных ОИС;
1.6	- обучение различным подходам и методам обеспечения ИБ ОИС.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.О
2.1	Требования к предварительной подготовке обучающегося:
2.1.1	Безопасность сетей электронных вычислительных машин
2.1.2	Безопасность операционных систем
2.2	Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:
2.2.1	Измерительная аппаратура контроля защищенности объектов информатизации
2.2.2	Защита информации от утечки по техническим каналам
2.2.3	Безопасность систем баз данных
2.2.4	Мониторинг информационной безопасности и активный поиск киберугроз
2.2.5	Управление информационной безопасностью
2.2.6	Контроль безопасности автоматизированных систем
2.2.7	Эксплуатация автоматизированных систем в защищенном исполнении

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	способы и средства защиты информации от утечки по техническим каналам, контроля их эффективности; организацию защиты информации от утечки по техническим каналам на объектах информатизации; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по обеспечению безопасности информации в автоматизированных системах;
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	навыками анализа информационной инфраструктуры автоматизированных систем; навыками разработки политик информационной безопасности автоматизированных систем;
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-15: Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем	
Знать:	
Уровень 1	методы администрирования вычислительных сетей; методы администрирования и принципы работы операционных систем семейств UNIX и Windows; принципы формирования политики информационной безопасности в автоматизированных системах; методы мониторинга информационной безопасности и средства реализации удаленных сетевых атак на автоматизированные системы;
Уровень 2	средства обеспечения безопасности данных; основные угрозы безопасности информации и модели нарушителя объекта информатизации; цели и задачи управления информационной безопасностью, основные документы по стандартизации в сфере управления информационной безопасностью; принципы формирования политики информационной безопасности объекта информатизации;
Уровень 3	методы и средства контроля защищенности объектов информатизации; узлы автоматизированной системы для измерения параметров информативных сигналов технических средств обработки информации; измерительную аппаратуру, применяемую для контроля защищенности объектов информатизации;
Уметь:	
Уровень 1	администрировать вычислительные сети; реализовывать политику безопасности вычислительной сети; настраивать политику безопасности операционных систем семейств UNIX и Windows; разрабатывать частные политики информационной безопасности автоматизированных систем;
Уровень 2	осуществлять диагностику и мониторинг систем защиты автоматизированных систем; администрировать базы данных; разрабатывать модели угроз и модели нарушителя объекта информатизации;
Уровень 3	оценивать информационные риски объекта информатизации; разрабатывать порядок проведения измерений параметров информативных сигналов технических средств обработки информации; обрабатывать и интерпретировать результаты измерений параметров информативных сигналов технических средств обработки информации;
Владеть:	
Уровень 1	навыками администрирования локальных вычислительных сетей с учетом требований по обеспечению информационной безопасности; навыками администрирования операционных систем семейств Windows и Unix с учетом требований по обеспечению информационной безопасности; навыками управления процессами обеспечения безопасности автоматизированных систем;
Уровень 2	навыками администрирования баз данных с учетом требований по обеспечению информационной безопасности; навыками эксплуатации измерительной аппаратуры контроля защищенности объектов информатизации с учетом требований по обеспечению информационной безопасности;
Уровень 3	навыками применения методов математической обработки результатов измерений параметров информативных сигналов технических средств обработки информации; навыками экспертизы состояния защищенности информации на объектах информатизации

В результате освоения дисциплины (модуля) обучающийся должен

3.1	Знать:
3.1.1	методы проектирования вычислительных сетей, методы администрирования вычислительных сетей;
3.1.2	методы администрирования и принципы работы операционных систем семейств UNIX и Windows, устройство и принципы работы операционных систем, структуру и возможности подсистем защиты операционных систем семейств UNIX и Windows;
3.2	Уметь:
3.2.1	проектировать вычислительные сети, администрировать вычислительные сети; реализовывать политику безопасности вычислительной сети;
3.2.2	семейств UNIX и Windows Умеет: настраивать политику безопасности операционных систем семейств UNIX и Windows, использовать средства управления работой операционной системы;
3.2.3	формулировать политику безопасности операционных систем семейств UNIX Windows
3.3	Владеть:
3.3.1	эксплуатации локальных вычислительных сетей, администрирования локальных вычислительных сетей с учетом требований по обеспечению информационной безопасности;
3.3.2	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	Компетенции	Литература	Инте ракт.	Примечание
	Раздел 1. Нормативные и концептуальные основы ИБОС						

1.1	Нормативные и концептуальные основы ИБОС /Лек/	6	2	ОПК-13 ОПК-15	Л1.1 Л1.2	0	
1.2	Нормативные и концептуальные основы ИБОС в России /Лаб/	6	6	ОПК-13 ОПК-15	Л1.1 Л1.2	1	
1.3	Нормативные и концептуальные основы ИБОС за рубежом /Лаб/	6	4	ОПК-13 ОПК-15	Л1.1 Л1.2	0	
Раздел 2. Атаки по уровням иерархической системы OSI и защита от них							
2.1	Атаки по уровням иерархической системы OSI и защита от них /Лек/	6	4	ОПК-13 ОПК-15	Л1.1 Л1.2	0	
2.2	Атаки на беспроводные устройства /Лек/	6	2	ОПК-13 ОПК-15	Л1.1 Л1.2	0	
2.3	Моделирование угроз ИБОС /Лаб/	6	6	ОПК-13 ОПК-15	Л1.1 Л1.2	0	
2.4	Технологии обеспечения ИБОС с помощью DLP-систем /Лаб/	6	4	ОПК-13 ОПК-15	Л1.1 Л1.2	1	
2.5	Моделирование документационного обеспечения процессов ИБОС /Ср/	6	12	ОПК-13 ОПК-15	Л1.1 Л1.2	0	
Раздел 3. Комплексное обеспечение ИБОС							
3.1	Комплексное обеспечение ИБОС: аутентификация, управление доступом, неотказуемость /Лек/	6	4	ОПК-13 ОПК-15	Л1.1 Л1.2	0	
3.2	Комплексное обеспечение ИБОС: конфиденциальность, целостность /Лек/	6	2	ОПК-13 ОПК-15	Л1.1 Л1.2	0	
3.3	Документационное сопровождение ИБОС: общие подходы /Лек/	6	4	ОПК-13 ОПК-15	Л1.1 Л1.2	0	
3.4	Документационное сопровождение обеспечения отдельных направлений ИБОС /Лек/	6	2	ОПК-13 ОПК-15	Л1.1 Л1.2	0	
3.5	Аутентификация /Лаб/	6	6	ОПК-13 ОПК-15	Л1.1 Л1.2	1	
3.6	Управление доступом к файловым ресурсам /Лаб/	6	4	ОПК-13 ОПК-15	Л1.1 Л1.2	0	
Раздел 4. Средства обеспечения ИБОС							
4.1	Средства обеспечения ИБОС /Лек/	6	2	ОПК-13 ОПК-15	Л1.1 Л1.2	0	
4.2	Обеспечение сетевой безопасности /Лек/	6	2	ОПК-13 ОПК-15	Л1.1 Л1.2	0	
4.3	Инструментальные средства аудита ИБОС /Лек/	6	4	ОПК-13 ОПК-15	Л1.1 Л1.2	0	
4.4	Технологические процессы внедрения средств обеспечения ИБОС /Лаб/	6	6	ОПК-13 ОПК-15	Л1.1 Л1.2	1	
4.5	Разработка политики ИБОС /Лаб/	6	6	ОПК-13 ОПК-15	Л1.1 Л1.2	0	
4.6	Экспертная оценка проблемы ИБОС /Ср/	6	32,65	ОПК-13 ОПК-15	Л1.1 Л1.2	0	
4.7	Экзамен /ИВКР/	6	2,35	ОПК-13 ОПК-15	Л1.1 Л1.2	0	

5. ОЦЕНОЧНЫЕ СРЕДСТВА

5.1. Контрольные вопросы и задания

Тема 1: Нормативные и концептуальные основы ИБОС

1. Какие нормативно-правовые акты регулируют вопросы информационной безопасности в России?
2. Что понимается под информационной безопасностью операционных систем?
3. Какие цели и задачи ставятся при обеспечении ИБОС?
4. Какие угрозы наиболее актуальны для операционных систем?
5. Каково значение международных стандартов (ISO/IEC) в области ИБОС?

Тема 2: Атаки по уровням модели OSI и защита от них

6. Как классифицируются атаки на основе уровней модели OSI?
 7. Какие угрозы существуют на физическом уровне и как их предотвратить?
 8. Как осуществляются атаки на канальном уровне и способы защиты?
 9. Какие типичные уязвимости сетевого уровня и методы их нейтрализации?
 10. Как защищать транспортный уровень от сетевых атак?
- Тема 3: Атаки на беспроводные устройства
11. Какие виды беспроводных технологий наиболее уязвимы с точки зрения ИБ?
 12. В чём суть атак типа Man-in-the-Middle в беспроводных сетях?
 13. Какие уязвимости имеют протоколы Wi-Fi (WEP, WPA, WPA2, WPA3)?
 14. Как организуется безопасное подключение через Bluetooth?
 15. Как предотвращать прослушивание и перехват данных в беспроводных сетях?
- Тема 4: Комплексное обеспечение ИБОС: аутентификация, управление доступом, неотказуемость
16. Что такое аутентификация и какие её виды используются в ОС?
 17. Как реализуется многофакторная аутентификация в современных ОС?
 18. Чем отличаются дискреционный и мандатный принципы управления доступом?
 19. Как обеспечивается контроль за действиями пользователей (неотказуемость)?
 20. Какие механизмы учёта и регистрации событий используются в ОС?
- Тема 5: Комплексное обеспечение ИБОС: конфиденциальность, целостность
21. Как обеспечивается конфиденциальность информации в ОС?
 22. Какие алгоритмы шифрования применяются в современных ОС?
 23. Что такое целостность данных и как она контролируется?
 24. Как используется хэширование для проверки целостности информации?
 25. Как реализуется политика безопасности в контексте конфиденциальности и целостности?
- Тема 6: Документационное сопровождение ИБОС: общие подходы
26. Каково назначение документации в системе обеспечения ИБОС?
 27. Какие документы формируются в рамках политики информационной безопасности?
 28. Какова роль процедур и инструкций в обеспечении ИБОС?
 29. Как проводится документирование инцидентов информационной безопасности?
 30. Какие требования предъявляются к политикам безопасности ОС?
- Тема 7: Документационное сопровождение отдельных направлений ИБОС
31. Как оформляется политика парольной защиты в организации?
 32. Как составляются процедуры разграничения прав доступа?
 33. Как документируется процесс обновления программного обеспечения и патч-менеджмент?
 34. Как оформляется политика использования административных привилегий?
 35. Как создаются и поддерживаются журналы аудита безопасности?
- Тема 8: Средства обеспечения ИБОС
36. Какие средства обеспечения безопасности предоставляют современные ОС?
 37. Как работают встроенные фаерволы Windows/Linux/macOS?
 38. Какие антивирусные средства используются в ОС?
 39. Какие функции выполняет система контроля целостности (например, Tripwire)?
 40. Как используются технологии виртуализации для изоляции угроз?
- Тема 9: Обеспечение сетевой безопасности
41. Как организуется защита ОС при подключении к корпоративной сети?
 42. Как работает защита через виртуальные частные сети (VPN)?
 43. Как ограничивается доступ к внешним ресурсам через брандмауэр?
 44. Какие протоколы обеспечивают безопасную передачу данных?
 45. Как организуется защита от DDoS-атак на уровне ОС?
- Тема 10: Инструментальные средства аудита ИБОС
46. Какие средства используются для проведения аудита безопасности ОС?
 47. Как работает система логирования (syslog, Event Viewer)?
 48. Как анализируются журналы безопасности с помощью SIEM-систем?
 49. Какие инструменты используются для сканирования уязвимостей (Nessus, OpenVAS)?
 50. Как осуществляется автоматизация процесса аудита безопасности?

5.2. Темы письменных работ

не предусмотрены

5.3. Оценочные средства

Рабочая программа "Информационная безопасность открытых систем" 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 6 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	Богатырев В. А.	Информационные системы и технологии. Теория надежности: учебное пособие для вузов	Москва: Юрайт, 2024
Л1.2	Зараменских Е. П.	Управление жизненным циклом информационных систем: 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	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
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>	Лаб
------	--	--	-----

		<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	<p>Специализированная многофункциональная учебная аудитория № 3 для проведения учебных занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной/итоговой аттестации</p>	<p>Компьютерные столы обучающихся; Стулья обучающихся; Письменный стол педагогического работника; Стул педагогического работника; Стеллаж для учебно-методических материалов, в том числе учебно-наглядных пособий; Многофункциональное устройство (принтер, сканер, ксерокс); Интерактивная доска; Мультимедийный проектор; Ноутбуки с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде</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 "Информационная безопасность открытых систем" 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.