МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

(МГРИ)

Мониторинг информационной безопасности и активный поиск киберугроз

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 48,25
самостоятельная работа 59,75

Виды контроля в семестрах:
зачеты 7

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**7 (4.1)**		Итого	
Недель	16 5/6			
Вид занятий	УП	РП	УП	РП
Лекции	16	16	16	16
Практические	32	32	32	32
Иные виды контактной работы	0,25	0,25	0,25	0,25
В том числе инт.	4	4	4	4
Итого ауд.	48,25	48,25	48,25	48,25
Контактная работа	48,25	48,25	48,25	48,25
Сам. работа	59,75	59,75	59,75	59,75
Итого	108	108	108	108

Москва 2025

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Целью изучения дисциплины «Мониторинг информационной безопасности и активный поиск киберугроз» является теоретическая и практическая подготовка специалистов в области реагирования на инциденты информационной безопасности.
1.2	В рамках освоения дисциплины студенты знакомятся с тактикой, техниками и процедурами атак, а также способами противостояния им.
1.3	На практических занятиях студенты сформируют навыки обнаружения и расследования атак.
1.4	Задачи дисциплины:
1.5	- планирование и организация мониторинга безопасности в компании;
1.6	- использование различных источников аналитических данных об угрозах для обнаружения новых продвинутых угроз;
1.7	- обнаружение и расследование вредоносной активности в инфраструктурах на базе Windows и Linux с учетом использованных злоумышленниками методов;
1.8	- создание инфраструктуры для активного поиска угроз на основе решения с открытым исходным кодом.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	ФТД
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Информационная безопасность открытых систем
2.1.2	Безопасность операционных систем
2.1.3	Безопасность сетей электронных вычислительных машин
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Управление информационной безопасностью
2.2.2	Измерительная аппаратура контроля защищенности объектов информатизации
2.2.3	Контроль безопасности автоматизированных систем
2.2.4	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 администрирования и принципы работы операционных систем семейств UNIX и Windows, устройство и принципы работы операционных систем, структуру и возможности
3.1.2	подсистем защиты операционных систем семейств UNIX и Windows;
3.1.3	методы проектирования вычислительных сетей, методы администрирования вычислительных сетей;
3.1.4	принципы формирования политики информационной безопасности в автоматизированных системах , риски подсистем защиты информации автоматизированных систем и экспериментальные методы их оценки;
3.2	**Уметь:**

3.2.1	настраивать политику безопасности операционных систем семейств UNIX и Windows, использовать средства управления работой операционной системы;
3.2.2	формулировать политику безопасности операционных систем семейств UNIX и Windows;
3.2.3	проектировать вычислительные сети, администрировать вычислительные сети;
3.2.4	реализовывать политику безопасности вычислительной сети;
3.2.5	разрабатывать частные политики информационной безопасности автоматизированных систем , анализировать и оценивать угрозы информационной безопасности автоматизированных; систем
3.3	**Владеть:**
3.3.1	администрирования операционных систем семейств Windows и Unix с учетом требований по обеспечению информационной безопасности, установки операционных систем семейств Windows и Unix";
3.3.2	эксплуатации локальных вычислительных сетей, администрирования локальных вычислительных сетей с учетом требований по обеспечению информационной безопасности;
3.3.3	управления процессами обеспечения безопасности автоматизированных систем, анализа информационной инфраструктуры автоматизированных систем;

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. Основные концепции построения и функционирования SOC						
1.1	Современное положение в области киберугроз. Задачи и подходы операционной безопасности. Архитектура, процессы и инструменты SOC /Лек/	7	2	ОПК-13 ОПК-15	Л1.1 Л1.2	0	
1.2	Аналитика угроз, активный поиск киберугроз /Лек/	7	2	ОПК-13 ОПК-15	Л1.1 Л1.2	0	
1.3	Стек Elasticsearch, Logstash, Kibana (ELK). Настройка среды ELK /Пр/	7	2	ОПК-13 ОПК-15	Л1.1 Л1.2	0	
	Раздел 2. Безопасность сети и периметра, мониторинг безопасности сети						
2.1	Архитектура безопасности сети, программные и аппаратные средства обеспечения безопасности сети /Лек/	7	1	ОПК-13 ОПК-15	Л1.1 Л1.2	0	
2.2	Типовые сетевые атаки /Лек/	7	2	ОПК-13 ОПК-15	Л1.1 Л1.2	0	
2.3	Методы мониторинга сети /Лек/	7	1	ОПК-13 ОПК-15	Л1.1 Л1.2	0	
2.4	Обнаружение атаки ARP-poisoning /Пр/	7	4	ОПК-13 ОПК-15	Л1.1 Л1.2	0	
2.5	Система обнаружения вторжений Bro /Пр/	7	2	ОПК-13 ОПК-15	Л1.1 Л1.2	0	
2.6	Система обнаружения вторжений Suricata IDS /Пр/	7	6	ОПК-13 ОПК-15	Л1.1 Л1.2	2	
2.7	Детектирование атак на сервер /Пр/	7	4	ОПК-13 ОПК-15	Л1.1 Л1.2	0	
2.8	Самостоятельная проработка лекционного и практического материала /Ср/	7	33,75	ОПК-13 ОПК-15	Л1.1 Л1.2	0	
	Раздел 3. Архитектура и средства безопасности Windows						
3.1	Архитектура и средства безопасности Windows /Лек/	7	2	ОПК-13 ОПК-15	Л1.1 Л1.2	0	
3.2	Тактики, инструменты и платформы для постэксплуатации в Windows, методы детектированя и противодействия /Лек/	7	2	ОПК-13 ОПК-15	Л1.1 Л1.2	0	

3.3	Безопасность Windows: права пользователей, незашифрованные пароли и хеши в памяти, привилегии, атаки с кражей токенов, UAC /Пр/	7	6	ОПК-13 ОПК-15	Л1.1 Л1.2	2	
3.4	Аудит безопасности Windows. Конфигурация политики аудита. Переадресация событий в TELK. Аудит доступа к объектам. Обогащение данными с помощью Logstash. Поиск угроз и анализ журналов вручную /Пр/	7	4	ОПК-13 ОПК-15	Л1.1 Л1.2	0	
3.5	Автоматический поиск угроз с использованием X-Pack watcher /Пр/	7	2	ОПК-13 ОПК-15	Л1.1 Л1.2	0	
3.6	Развертывание и использование Sysmon /Пр/	7	1	ОПК-13 ОПК-15	Л1.1 Л1.2	0	
3.7	Autorun, анализ данных Logstash и проверка потоков /Пр/	7	1	ОПК-13 ОПК-15	Л1.1 Л1.2	0	
	Раздел 4. Архитектура и средства безопасности Linux						
4.1	Архитектура и средства безопасности Linux /Лек/	7	2	ОПК-13 ОПК-15	Л1.1 Л1.2	0	
4.2	Журналы Linux, средства мониторинга, Auditd /Лек/	7	2	ОПК-13 ОПК-15	Л1.1 Л1.2	0	
4.3	Самостоятельная работа с предоставленными источниками информации /Ср/	7	26	ОПК-13 ОПК-15	Л1.1 Л1.2	0	
4.4	Зачет /ИВКР/	7	0,25	ОПК-13 ОПК-15	Л1.1 Л1.2	0	

5. ОЦЕНОЧНЫЕ СРЕДСТВА

5.1. Контрольные вопросы и задания

Тема 1: Современное положение в области киберугроз
1. Какие основные тенденции развития киберугроз на современном этапе?
2. Что такое kill chain и как он используется при анализе атак?
3. Как классифицируются угрозы по уровню сложности и масштабу воздействия?
4. Какую роль играют APT (продвинутые целевые угрозы) в современной кибербезопасности?
5. Как влияет цифровизация на увеличение поверхности атак?
Тема 2: Задачи и подходы операционной безопасности. Архитектура SOC
6. Что понимается под операционной кибербезопасностью?
7. Какие задачи решает центр обработки инцидентов (SOC)?
8. Как организуется структура и функционал SOC?
9. Какие процессы реализуются в рамках модели SOC (мониторинг, реагирование, расследование)?
10. Какие ключевые роли существуют в команде SOC?
Тема 3: Аналитика угроз и активный поиск киберугроз
11. Что такое Threat Hunting и зачем он нужен?
12. Какие источники данных используются для поиска скрытых угроз?
13. Как формируются гипотезы и проверяются предположения о наличии угроз?
14. Как работает модель MITRE ATT&CK и как она применяется в аналитике?
15. Какие метрики и показатели эффективности используются в Threat Hunting?
Тема 4: Архитектура безопасности сети. Программные и аппаратные средства
16. Какие компоненты составляют архитектуру защиты корпоративной сети?
17. Какие функции выполняют фаерволы, IDS/IPS, WAF и другие системы?
18. Как происходит взаимодействие между средствами сетевой безопасности?
19. Какие аппаратные решения используются для обеспечения безопасности?
20. Как программные инструменты дополняют аппаратную защиту?
Тема 5: Типовые сетевые атаки
21. Какие виды атак наиболее распространены в корпоративных сетях?
22. Что такое DDoS-атаки и как они реализуются?
23. Как работают атаки типа MITM и способы их обнаружения?
24. Какие методы используются при эксплуатации уязвимостей в ПО?
25. Как проводится атака с использованием фишинга и социальной инженерии?
Тема 6: Методы мониторинга сети
26. Какие данные собираются при мониторинге сетевой активности?
27. Как работает анализ сетевого трафика (NetFlow, PCAP)?

28. Как используются логи маршрутизаторов и коммутаторов?
29. Как строится система сетевого аудита и анализа событий?
30. Какие инструменты используются для мониторинга (Wireshark, Zeek, Suricata)?
Тема 7: Архитектура и средства безопасности Windows
31. Как устроена система безопасности Windows?
32. Какие механизмы контроля доступа реализованы в Windows?
33. Какие компоненты обеспечивают защиту от несанкционированного доступа?
34. Как работают политики безопасности (GPO), шифрование и изоляция процессов?
35. Какие угрозы наиболее актуальны для систем Windows?
Тема 8: Тактики, инструменты и платформы для постэксплуатации в Windows. Детектирование и противодействие
36. Что такое постэксплуатация и какие тактики используют злоумышленники?
37. Какие техники используются для повышения привилегий и перемещения по сети?
38. Как злоумышленники сохраняют доступ к системе (persistence)?
39. Какие методы детектирования постэксплуатационных действий существуют?
40. Какие средства используются для обнаружения и блокирования таких атак?
Тема 9: Архитектура и средства безопасности Linux
41. Как устроена система безопасности в Linux?
42. Какие механизмы разграничения прав используются (SELinux, AppArmor)?
43. Как организованы учетные записи и политики доступа?
44. Как обеспечивается безопасность запускаемых процессов и контейнеров?
45. Какие особенности имеют Unix-подобные системы с точки зрения ИБ?
Тема 10: Журналы Linux, средства мониторинга, Auditd
46. Какие типы журналов существуют в системах Linux?
47. Как используются syslog, journalctl и rsyslog для анализа событий?
48. Как работает утилита auditd и как её настроить?
49. Как формировать правила аудита для отслеживания критических событий?
50. Как использовать ELK Stack, Splunk и другие инструменты для анализа логов Linux?

5.2. Темы письменных работ

не предусмотрены

5.3. Оценочные средства

Рабочая программа "Мониторинг информационной безопасности и активный поиск киберугроз" 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 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	Щеглов А. Ю., Щеглов К. А.	Защита информации: основы теории: учебник для вузов	Москва: Юрайт, 2024
Л1.2	Баланов А. Н.	Комплексная информационная безопасность: учебное пособие для вузов	Санкт-Петербург: Лань, 2025

6.3.1 Перечень программного обеспечения

6.3.1.1	Office Professional Plus 2019	
6.3.1.2	Windows 10	
6.3.1.3	МТС-Линк	Комплексная платформа для коммуникаций, обучения и совместной работы, разработанная с использованием современных технологий. Доступны десктопные и мобильные приложения для удобной работы с системой.

6.3.2 Перечень информационных справочных систем

6.3.2.1	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.	
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 "Мониторинг информационной безопасности и активный поиск киберугроз" 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.