МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

(МГРИ)

Безопасность сетей электронных вычислительных машин

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
в том числе:
аудиторные занятия 82,35
самостоятельная работа 34,65
часов на контроль 27

Виды контроля в семестрах:
экзамены 5

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**5 (3.1)**		Итого	
Недель	16 4/6			
Вид занятий	УП	РП	УП	РП
Лекции	32	32	32	32
Лабораторные	16	16	16	16
Практические	32	32	32	32
Иные виды контактной работы	2,35	2,35	2,35	2,35
В том числе инт.	8	8	8	8
Итого ауд.	82,35	82,35	82,35	82,35
Контактная работа	82,35	82,35	82,35	82,35
Сам. работа	34,65	34,65	34,65	34,65
Часы на контроль	27	27	27	27
Итого	144	144	144	144

Москва 2025

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Целью изучения дисциплины «Безопасность сетей ЭВМ» является теоретическая и практическая подготовка специалистов в области построения сетей ЭВМ и
1.2	обеспечения безопасности при эксплуатации сетей ЭВМ.
1.3	Задачи:
1.4	- изучение основных элементов теории построения сетей;
1.5	- изучение основных принципов функционирования сетевых протоколов;
1.6	- привитие навыков комплексного проектирования, построения, обслуживания и анализа защищенных вычислительных сетей;
1.7	- изучение основных угроз в сетях ЭВМ и методов противодействия им;
1.8	- овладение механизмами построения систем безопасности сетей ЭВМ.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.О
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Безопасность операционных систем
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Управление информационной безопасностью
2.2.2	Информационная безопасность открытых систем
2.2.3	Безопасность систем баз данных
2.2.4	Мониторинг информационной безопасности и активный поиск киберугроз

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
ОПК-12: Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем	
Знать:	
Уровень 1	методы проектирования вычислительных сетей;
Уровень 2	устройство и принципы работы операционных систем, структуру и возможности подсистем защиты операционных систем семейств UNIX и Windows;
Уровень 3	назначение, функции и структуру систем управления базами данных;
Уметь:	
Уровень 1	эксплуатировать базы данных; создавать объекты базы данных;
Уровень 2	выполнять запросы к базе данных; разрабатывать прикладные программы, осуществляющие взаимодействие с базами данных;
Уровень 3	навыками эксплуатации локальных вычислительных сетей;
Владеть:	
Уровень 1	навыками эксплуатации локальных вычислительных сетей;
Уровень 2	навыками установки операционных систем семейств Windows и Unix;
Уровень 3	навыком эксплуатации баз данных с учетом требований по обеспечению информационной безопасности;

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
3.2	**Уметь:**
3.2.1	проектировать вычислительные сети; администрировать вычислительные сети; реализовывать политику безопасности вычислительной сети
3.3	**Владеть:**
3.3.1	эксплуатации локальных вычислительных сетей; администрирования локальных вычислительных сетей с учетом требований по обеспечению информационной безопасности

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература	Инте ракт.	Примечание
	Раздел 1. Основы организации и функционирования сетей ЭВМ						
1.1	Цели и задачи курса. Содержание дисциплины. Рекомендуемая литература. Понятие сети ЭВМ. Этапы развития сетей ЭВМ /Лек/	5	2	ОПК-12 ОПК-15	Л1.1	0	
1.2	Критерии классификации сетей ЭВМ. Характеристики сетей ЭВМ /Лек/	5	2	ОПК-12 ОПК-15	Л1.1	0	
1.3	Средства построения сетей ЭВМ. Логическая и физическая структуризация сетей ЭВМ. Модель ISO OSI. Технологии обеспечения безопасности в сетях ЭВМ /Лек/	5	2	ОПК-12 ОПК-15	Л1.1	0	
1.4	Подготовка к лабораторным работам, оформление результатов /Ср/	5	11,55	ОПК-12 ОПК-15	Л1.1	0	
1.5	Подготовка к практическим занятиям, оформление результатов /Ср/	5	11,55	ОПК-12 ОПК-15	Л1.1	0	
	Раздел 2. Сети TCP/IP						

2.1	Практические отличия реализации стека TCP/IP от эталонной модели ISO OSI. /Лек/	5	2	ОПК-12 ОПК-15	Л1.1	0	
2.2	Методы коммутации. Методы доступа к разделяемой среде. Угрозы безопасности информации, передаваемой в сетях ЭВМ, на физическом и канальном уровнях. /Лек/	5	2	ОПК-12 ОПК-15	Л1.1	0	
2.3	Сетевой уровень построения сетей ЭВМ. Функции и интерфейсы сетевого уровня. Сетевой уровень Internet. Протоколы IPv4, IPv6, адресация в IP-сетях /Лек/	5	2	ОПК-12 ОПК-15	Л1.1	0	
2.4	Протоколы разрешения адресов ARP, RARP. Алгоритмы маршрутизации, их характеристика. Протоколы и алгоритмы внутренней и междоменной маршрутизации (RIP, OSPF, IGRP, NLSP, EGP, BGP) /Лек/	5	2	ОПК-12 ОПК-15	Л1.1	0	
2.5	Создание элементов структурированной кабельной системы /Пр/	5	4	ОПК-12 ОПК-15	Л1.1	2	
2.6	Построение сетей с помощью коммутаторов, организация подсетей, настройка маршрутизатора /Пр/	5	4	ОПК-12 ОПК-15	Л1.1	0	
2.7	Изучение промышленных коммутаторов и маршрутизаторов. Управление конфигурациями устройств. Построение простейшей сети на базе лаборатории /Лаб/	5	8	ОПК-12 ОПК-15	Л1.1	2	
	Раздел 3. Технологии глобальных сетей						
3.1	Транспортные услуги и технологии глобальных сетей. Технология MPLS /Лек/	5	2	ОПК-12 ОПК-15	Л1.1	0	
3.2	Настройка протоколов внутренней и междоменной маршрутизации /Пр/	5	4	ОПК-12 ОПК-15	Л1.1	2	
	Раздел 4. Сетевые сервисы и службы						
4.1	Сетевые службы и средства управления /Лек/	5	2	ОПК-12 ОПК-15	Л1.1	0	
4.2	Средства контроля внешнего периметра сети. Средства контроля доступа к сетевым службам. Средства активного аудита сетей ЭВМ. Протокол SNMP /Лек/	5	2	ОПК-12 ОПК-15	Л1.1	0	
4.3	Развёртывание доменной структуры (на базе Windows Server), DNS, настройка пользователей, настройка доменных политик /Пр/	5	4	ОПК-12 ОПК-15	Л1.1	0	
4.4	Настройка сервера WEB, VPN, почтовых служб, дополнительных сервисов /Пр/	5	4	ОПК-12 ОПК-15	Л1.1	0	
4.5	Организация доверительных отношений между доменами Active Directory, управление полномочиями пользователей, изучение протокола Kerberos /Лаб/	5	4	ОПК-12 ОПК-15	Л1.1	2	
4.6	Изучение материалов по плану СРС /Ср/	5	11,55	ОПК-12 ОПК-15	Л1.1	0	
	Раздел 5. Средства и способы построения отказоустойчивых сетей						

5.1	Технология VLAN. Угрозы безопасности информации, передаваемой в локальных сетях ЭВМ. Методы их нейтрализации /Лек/	5	2	ОПК-12 ОПК-15	Л1.1	0	
5.2	Протоколы VRRP/HSRP. Основы кластерных решений. DM VPN (Cisco VPN) как пример динамически организующейся сети /Лек/	5	2	ОПК-12 ОПК-15	Л1.1	0	
5.3	Построение сети, сегментированной на VLAN, взаимодействие между различными сегментами, аутентификация в целевой VLAN (протокол 802.1X) /Пр/	5	2	ОПК-12 ОПК-15	Л1.1	0	
5.4	Настройка кластера маршрутизаторов с помощью протокола VRRP или HSRP /Пр/	5	2	ОПК-12 ОПК-15	Л1.1	0	
	Раздел 6. Сетевая безопасность						
6.1	Классификации угроз безопасности телекоммуникационных сетей /Лек/	5	2	ОПК-12 ОПК-15	Л1.1	0	
6.2	Классификация методов защиты. Основные технологии обеспечения безопасности в сети /Лек/	5	2	ОПК-12 ОПК-15	Л1.1	0	
6.3	Межсетевые экраны и средства обнаружения вторжений. Сегментирование. Аутентификация, авторизация, аудит. /Лек/	5	2	ОПК-12 ОПК-15	Л1.1	0	
6.4	Криптографические средства защиты информации в сетях ЭВМ. Виртуальные частные сети. Протокол SSL /Лек/	5	2	ОПК-12 ОПК-15	Л1.1	0	
6.5	Настройка межсетевого экрана, средства обнаружения вторжений (snort или suricata). Аудит журналов /Пр/	5	4	ОПК-12 ОПК-15	Л1.1	0	
6.6	Построение модели сети организации (организация сегментов сети, взаимодействующих через VPN, аутентификация пользователей по протоколу 802.1X) /Пр/	5	4	ОПК-12 ОПК-15	Л1.1	0	
6.7	Организация сегмента сети с применением протоколов группы IEEE 802.11, изучение атак на беспроводные сети /Лаб/	5	4	ОПК-12 ОПК-15	Л1.1	0	
6.8	Экзамен /ИВКР/	5	2,35	ОПК-12 ОПК-15	Л1.1	0	

5. ОЦЕНОЧНЫЕ СРЕДСТВА

5.1. Контрольные вопросы и задания

Тема 1: Цели и задачи курса. Содержание дисциплины. Рекомендуемая литература
1. Какие цели и задачи ставятся при изучении дисциплины «Сети ЭВМ»?
2. Какова структура и содержание курса?
3. Какие учебные пособия рекомендуются для изучения дисциплины?
4. Каково значение курса в подготовке специалистов по информационной безопасности?
5. Какие навыки должен получить студент после освоения дисциплины?
Тема 2: Понятие сети ЭВМ. Этапы развития сетей ЭВМ
6. Что такое сеть ЭВМ? Какие основные компоненты входят в её состав?
7. Охарактеризуйте этапы эволюции компьютерных сетей.
8. Какие ключевые технологии способствовали развитию сетей?
9. Чем отличаются локальные и глобальные сети?
10. Какие современные тенденции наблюдается в развитии сетевых технологий?
Тема 3: Критерии классификации и характеристики сетей ЭВМ
11. По каким критериям классифицируются компьютерные сети?
12. Какие типы сетей выделяют по территориальному признаку?
13. Дайте характеристику одноранговым и клиент-серверным сетям.
14. Что такое масштабируемость сети и почему она важна?

15. Как оценивается производительность и надёжность сетей?
Тема 4: Средства построения сетей ЭВМ. Логическая и физическая структуризация сетей. Модель OSI
16. Какие аппаратные средства используются для построения сетей?
17. В чём разница между логической и физической топологией сети?
18. Как устроена модель взаимодействия открытых систем (ISO/OSI)?
19. Какие функции выполняют уровни модели OSI?
20. Как обеспечивается взаимодействие между уровнями модели OSI?
Тема 5: Технологии обеспечения безопасности в сетях ЭВМ
21. Какие основные угрозы существуют на уровне сетевой инфраструктуры?
22. Какие меры защиты применяются на различных уровнях модели OSI?
23. Что такое политика безопасности сети и как она реализуется?
24. Как обеспечивается конфиденциальность и целостность данных в сетях?
25. Какие стандарты и протоколы обеспечивают безопасность в сетях?
Тема 6: Стек TCP/IP и его отличие от эталонной модели OSI
26. Как устроен стек протоколов TCP/IP?
27. Чем отличается модель TCP/IP от модели OSI?
28. Какие функции выполняют уровни TCP/IP?
29. Как осуществляется маршрутизация пакетов в TCP/IP?
30. Какие преимущества и недостатки имеет стек TCP/IP?
Тема 7: Методы коммутации. Методы доступа к разделяемой среде. Угрозы на физическом и канальном уровнях
31. Какие виды коммутации используются в сетях?
32. В чём различие между коммутацией каналов и пакетов?
33. Какие методы доступа к разделяемой среде существуют?
34. Какие угрозы возникают на физическом уровне сетей?
35. Какие уязвимости присущи канальному уровню и как их предотвратить?
Тема 8: Сетевой уровень. Протоколы IPv4, IPv6, адресация
36. Какие функции выполняет сетевой уровень?
37. Что такое IP-адрес и как он используется?
38. В чём отличие IPv4 от IPv6?
39. Как организована система адресации IPv6?
40. Как происходит маршрутизация IP-пакетов?
Тема 9: ARP, RARP, алгоритмы маршрутизации
41. Для чего используется протокол ARP?
42. Что такое таблица ARP и как она обновляется?
43. Как работает протокол RARP?
44. Какие алгоритмы маршрутизации наиболее распространены?
45. В чём разница между внутридоменной и междоменной маршрутизацией?
Тема 10: Транспортные услуги и технологии глобальных сетей. MPLS
46. Какие функции выполняет транспортный уровень?
47. Чем отличаются протоколы TCP и UDP?
48. Что такое качество обслуживания (QoS) в сетях?
49. Как устроена технология MPLS?
50. Как MPLS влияет на эффективность передачи данных?
Тема 11: Сетевые службы и средства управления
51. Какие основные сетевые службы используются в корпоративных сетях?
52. Что такое DNS и как он работает?
53. Как организовано управление сетью через SNMP?
54. Какие функции выполняет протокол DHCP?
55. Как обеспечивается централизованное управление сетью?
Тема 12: Средства контроля внешнего периметра и доступа. Активный аудит
56. Что такое брандмауэр и как он защищает сеть?
57. Как работают системы обнаружения и предотвращения вторжений (IDS/IPS)?
58. Что такое активный сетевой аудит и зачем он нужен?
59. Какие протоколы используются для мониторинга и управления сетью?
60. Как обеспечивается контроль доступа к сетевым ресурсам?
Тема 13: VLAN. Угрозы в локальных сетях и методы их нейтрализации
61. Что такое VLAN и как он реализуется?
62. Какие преимущества даёт использование VLAN?
63. Какие угрозы характерны для локальных сетей?
64. Как предотвращаются атаки типа ARP spoofing?
65. Как обеспечивается безопасность внутри VLAN?
Тема 14: VRRP/HSRP. Кластеризация. DMVPN
66. Что такое протоколы VRRP и HSRP?
67. Как они обеспечивают отказоустойчивость шлюзов?
68. Что такое кластерные решения и где они применяются?
69. Как устроена технология DMVPN?
70. Какие преимущества даёт организация динамически изменяющихся сетей?
Тема 15: Классификация угроз безопасности телекоммуникационных сетей

71. Как классифицируются угрозы в телекоммуникационных сетях?
72. Какие угрозы являются наиболее опасными?
73. Как угрозы связаны с архитектурой сетей и протоколами?
74. Какие последствия могут быть при реализации сетевых угроз?
75. Как строится система анализа угроз?
Тема 16: Методы и технологии обеспечения безопасности в сетях
76. Какие основные методы защиты информации в сетях используются?
77. Что такое многоуровневая защита и зачем она нужна?
78. Какие технологии обеспечивают безопасную передачу данных?
79. Как использовать принцип минимальных привилегий в сетях?
80. Какие современные технологии обеспечивают комплексную защиту сетей?
Тема 17: Межсетевые экраны, IDS, аутентификация, авторизация, аудит
81. Как работают межсетевые экраны разных поколений?
82. Какие функции выполняют системы обнаружения вторжений (IDS)?
83. Какие виды аутентификации поддерживаются в сетях?
84. Что такое AAA-системы и как они работают?
85. Как организуется аудит действий пользователей в сетях?
Тема 18: Криптографические средства защиты. Виртуальные частные сети. SSL/TLS
86. Какие криптографические протоколы используются в сетях?
87. Что такое виртуальная частная сеть (VPN) и как она реализуется?
88. Как работает протокол SSL/TLS?
89. Какие режимы работы IPSec вы знаете?
90. Как обеспечивается безопасность соединения через интернет?

5.2. Темы письменных работ

Не предусмотрены

5.3. Оценочные средства

Рабочая программа "Безопасность сетей электронных вычислительных машин" 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 5 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	Рабчевский А. Н.	Компьютерные сети и системы связи. Вводный курс: учебное пособие 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

3	Специализированная многофункциональная учебная аудитория № 3 для проведения учебных занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной/ итоговой аттестации	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	
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 безопасности вычислительных сетей № 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.	

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 "Безопасность сетей электронных вычислительных машин" 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.