МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Магнитогорский государственный технический университет им. Г.И. Носова»

УТВЕРЖДАЮ
Директор ИЭиАС
_____ В.Р. Храмшин

26.01.2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

БЕЗОПАСНОСТЬ СЕТЕЙ ЭВМ

Направление подготовки (специальность)
10.05.03 Информационная безопасность автоматизированных систем

Направленность (профиль/специализация) программы
10.05.03 специализация N 8 "Разработка автоматизированных систем в защищенном исполнении"

Уровень высшего образования - специалитет

Форма обучения
очная

Институт/ факультет	Институт энергетики и автоматизированных систем
Кафедра	Информатики и информационной безопасности
Курс	3
Семестр	5, 6

Магнитогорск
2022 год

Рабочая программа составлена на основе ФГОС ВО - специалитет по специальности 10.05.03 Информационная безопасность автоматизированных систем (приказ Минобрнауки России от 26.11.2020 г. № 1457)

Рабочая программа рассмотрена и одобрена на заседании кафедры Информатики и информационной безопасности
25.01.2022, протокол № 4

Зав. кафедрой _____ И.И. Баранкова

Рабочая программа одобрена методической комиссией ИЭиАС
26.01.2022 г. протокол № 5

Председатель _____ В.Р. Храмшин

Рабочая программа составлена:
зав. кафедрой ИиИБ, д-р техн. наук _____ И.И. Баранкова

Рецензент:
Начальник отдела информационной безопасности "КУБ" (АО),
_____ М.М. Близнецов

Лист актуализации рабочей программы

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2023 - 2024 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2024 - 2025 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2025 - 2026 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2026 - 2027 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2027 - 2028 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2028 - 2029 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

1 Цели освоения дисциплины (модуля)

Целями освоения дисциплины «Безопасность сетей ЭВМ» являются овладение студентами необходимым и достаточным уровнем общепрофессиональных, профессиональных компетенций в соответствии с требованиями ФГОС ВО по специальности «Информационная безопасность автоматизированных систем».

Целями освоения дисциплины (модуля) «Безопасность сетей ЭВМ» являются:

1. Обучение обучающихся организации защиты сетевых устройств и каналов передачи информации, обнаружения и предотвращения несанкционированного доступа к информации в сетях ЭВМ.

2. Обучение обучающихся принципам построения систем защиты информации в локальных вычислительных сетях (ЛВС) и методам анализа надежности защиты ЛВС

2 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Безопасность сетей ЭВМ входит в обязательную часть учебного плана образовательной программы.

Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:

Информатика

Сети и системы передачи информации

Основы информационной безопасности

Организация ЭВМ и вычислительных систем

Учебная - ознакомительная практика

Теория информации

Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:

Информационная безопасность распределенных информационных систем

Криптографические методы защиты информации

Разработка и эксплуатация защищенных автоматизированных систем

Тестирование систем защиты информации автоматизированных систем

Защита электронного документооборота

Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности

Виртуальные сети

Защита информационно-технологических ресурсов автоматизированных систем

Методы проектирования систем защиты распределенных информационных систем

Научно-исследовательская работа

Производственная-преддипломная практика

Безопасность операционных систем

Разработка и эксплуатация автоматизированных систем в защищенном исполнении

Управление информационной безопасностью

Моделирование угроз информационной безопасности

Методы и стандарты оценки защищенности компьютерных систем

Анализ рисков информационной безопасности

Безопасность Интернета вещей

Аттестация АИС

Анализ уязвимостей программного обеспечения

Анализ безопасности информационных технологий

Разработка систем защиты информации автоматизированных систем

Моделирование систем защиты информации

Разработка эксплуатационной документации на системы защиты информации автоматизированных систем

3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения

В результате освоения дисциплины (модуля) «Безопасность сетей ЭВМ» обучающийся должен обладать следующими компетенциями:

Код индикатора	Индикатор достижения компетенции
ОПК-12 Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем;	
ОПК-12.1	Применяет знания в области безопасности вычислительных сетей при разработке автоматизированных систем
ОПК-12.2	Применяет знания в области безопасности операционных систем при разработке автоматизированных систем
ОПК-12.3	Применяет знания в области безопасности баз данных при разработке автоматизированных систем

4. Структура, объём и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет 7 зачетных единиц 252 акад. часов, в том числе:
– контактная работа – 127 акад. часов:
– аудиторная – 122 акад. часов;
– внеаудиторная – 5 акад. часов;
– самостоятельная работа – 89,3 акад. часов;
– в форме практической подготовки – 0 акад. час;
– подготовка к экзамену – 35,7 акад. час

Форма аттестации - зачет, экзамен

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа студента	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код компетенции
		Лек.	лаб. зан.	практ. зан.				
1. Основные понятия безопасностисетей ЭВМ								
1.1 Безопасность сетей ЭВМ – история вопроса, современное состояние, тенденции	5	1	2/0,6И		4	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	Устный опрос	ОПК-12.1, ОПК-12.2, ОПК-12.3
1.2 Основные уязвимости сетей ЭВМ и их использование нарушителем		1	2		4	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	Устный опрос	ОПК-12.1, ОПК-12.2, ОПК-12.3

1.3 Парольная защита административного и консольного входов на сетевое оборудование		2	2/1И		4	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями), Подготовка к практическому занятию	Лабораторная работа «Парольная защита консольного подключения сетевого оборудования»	ОПК-12.1, ОПК-12.2, ОПК-12.3
1.4 Защита удаленного подключения к сетевому оборудованию		2	2/1И		4	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями), Подготовка к практическому занятию	Лабораторная работа «Защищенные и незащищенные терминальные протоколы – перехват пароля незащищенного протокола при помощи сетевого сканера»	ОПК-12.1, ОПК-12.2, ОПК-12.3
Итого по разделу		6	8/2,6И		16			
2. Модель безопасности для локальной вычислительной сети								
2.1 Принцип «обороны в глубину» как базовый принцип при организации защиты сети	5	1	2		4	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	Устный опрос	ОПК-12.1, ОПК-12.2, ОПК-12.3
2.2 Сегментирование ЛВС как способ повышения безопасности сети		1	2		1	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями), Подготовка к практическому занятию	Лабораторная работа «Использование протокола ARP в сегментированной и несегментированной ЛВС»	

2.3 Мониторинг состояния транспортной подсистемы как средство контроля за состоянием сетевой безопасности		2	4		1	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями) , Подготовка к практическому занятию	Лабораторная работа «Мониторинг открытых TCP-соединений в ОС Windows»	
Итого по разделу		4	8		6			
3. Обнаружение и нейтрализация сетевых атак								
3.1 Понятие «сетевой атаки» - история, классификация, современный подход к вопросу	5	1	2/1И		4	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями), подготовка к компьютерному тестированию	Компьютерное тестирование	ОПК-12.1, ОПК-12.2, ОПК-12.3
3.2 Фазы сетевой атаки		1	2/1И		4	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями), подготовка к компьютерному тестированию	Компьютерное тестирование	ОПК-12.1, ОПК-12.2, ОПК-12.3

3.3 Методики обнаружения сетевых атак		1	2/1И		4	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями), подготовка к компьютерному тестированию	Компьютерное тестирование	ОПК-12.1, ОПК-12.2, ОПК-12.3
3.4 Основные меры противодействия сетевым атакам; системы обнаружения и предотвращения вторжений		1	2/1И		4	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями), подготовка к компьютерному тестированию	Компьютерное тестирование	ОПК-12.1, ОПК-12.2, ОПК-12.3
Итого по разделу		4	8/4И		16			
4. Технологии безопасности локальных вычислительных сетей								
4.1 Технология виртуальных ЛВС (VLAN)	5	2	4/2И		4	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями), Подготовка к практическому занятию	Защита лабораторной работы «Организация ЛВС с VLAN»	ОПК-12.1, ОПК-12.2, ОПК-12.3

4.2 Технология Port Security		1	4/2И		4	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями) , Подготовка к практическому занятию	Защита лабораторной работы «Использование технологии Port Security»	ОПК-12.1, ОПК-12.2, ОПК-12.3
4.3 Технология списков контроля доступа (ACL)		1	4/2И		4	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями) , Подготовка к практическому занятию	Защита лабораторной работы «Использование технологии ACL»	ОПК-12.1, ОПК-12.2, ОПК-12.3
Итого по разделу		4	12/6И		12			
5. Подготовка к промежуточной аттестации								
5.1 Подготовка к промежуточной аттестации	5				3	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	Зачет	
Итого по разделу					3			
Итого за семестр		18	36/12,6И		53		зачёт	
6. Методы контроля сетей ЭВМ								

6.1 Анализ сетевого трафика	6	4	4/2И		1	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями), подготовка к практическому занятию	Практическая работа «Анализ сетевого трафика защищенных сетей ЭВМ»	ОПК-12.1, ОПК-12.2, ОПК-12.3
6.2 Перехват сетевых сообщений		4	4/2И		1	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями), подготовка к практическому занятию	Практическая работа «Анализ сетевого трафика защищенных сетей ЭВМ»	ОПК-12.1, ОПК-12.2, ОПК-12.3
6.3 Использование защищенных протоколов для защиты сетевого трафика		4	4		2	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями), подготовка к практическому занятию	Практическая работа «Анализ сетевого трафика защищенных сетей ЭВМ»	ОПК-12.1, ОПК-12.2, ОПК-12.3
Итого по разделу		12	12/4И		4			
7. Безопасность беспроводных сетей								
7.1 Устройство и разновидности беспроводных сетей	6	4	4/2И		1	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	Устный опрос	ОПК-12.1, ОПК-12.2, ОПК-12.3

7.2 Проблема безопасности в беспроводных сетях		4	4/2И		1	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями) , подготовка к практическому занятию	Практическая работа «Организация защиты беспроводных сетей»	ОПК-12.1, ОПК-12.2, ОПК-12.3
Итого по разделу		8	8/4И		2			
8. Защищенные сети								
8.1 Понятие защищенной сети	6	2	4/1,9И		1	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	Устный опрос	ОПК-12.1, ОПК-12.2, ОПК-12.3
8.2 Технология виртуальной частной/защищенной сети (VPN). Классификация сетей VPN		4	4/1И		1	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	Устный опрос	ОПК-12.1, ОПК-12.2, ОПК-12.3
8.3 Разновидности технологий VPN		4	4/1И		1	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями) , подготовка к практическому занятию	Практическая работа «Организация VPN»	ОПК-12.1, ОПК-12.2, ОПК-12.3

8.4 Алгоритмы шифрования, применяемые для организации VPN		4	2		1,3	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями) , подготовка к практическому занятию	Практическая работа «Организация VPN»	ОПК-12.1, ОПК-12.2, ОПК-12.3
Итого по разделу		14	14/3,9И		4,3			
9. Подготовка к итоговой аттестации и курсовой работы								
9.1 Подготовка курсовой работы	6				18	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями), выполнение курсовой работы	Защита курсовой работы	
9.2 Подготовка к итоговой аттестации					8	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	Экзамен	
Итого по разделу					26			
Итого за семестр		34	34/11,9И		36,3		экзамен	
Итого по дисциплине		52	70/24,5 И		89,3		зачет, экзамен	

5 Образовательные технологии

Для реализации предусмотренных видов учебной работы в качестве образовательных технологий в преподавании дисциплины «Безопасность сетей ЭВМ» используются традиционная и модульно-компетентностная технологии.

Реализация компетентностного подхода предусматривает использование в учебном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

При проведении учебных занятий преподаватель обеспечивает развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств посредством проведения интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализа ситуаций, учета особенностей профессиональной деятельности выпускников и потребностей работодателей.

6 Учебно-методическое обеспечение самостоятельной работы обучающихся

Представлено в приложении 1.

7 Оценочные средства для проведения промежуточной аттестации

Представлены в приложении 2.

8 Учебно-методическое и информационное обеспечение дисциплины (модуля)

а) Основная литература:

1. Сети и телекоммуникации : учебник и практикум для вузов / К. Е. Самуйлов [и др.] ; под редакцией К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. — Москва : Издательство Юрайт, 2020. — 363 с. — (Высшее образование). — ISBN 978-5-534-00949-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/450234 (дата обращения: 12.03.2020).

2. Дибров, М. В. Сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 1 : учебник и практикум для вузов / М. В. Дибров. — Москва : Издательство Юрайт, 2020. — 333 с. — (Высшее образование). — ISBN 978-5-9916-9956-3. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/452430 (дата обращения: 12.03.2020).

3. Дибров, М. В. Сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 2 : учебник и практикум для вузов / М. В. Дибров. — Москва : Издательство Юрайт, 2020. — 351 с. — (Высшее образование). — ISBN 978-5-9916-9958-7. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/453063 (дата обращения: 12.03.2020).

б) Дополнительная литература:

1. Замятина, О. М. Вычислительные системы, сети и телекоммуникации. Моделирование сетей : учебное пособие для магистратуры / О. М. Замятина. — Москва : Издательство Юрайт, 2019. — 159 с. — (Университеты России). — ISBN 978-5-534-00335-2. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/433938 (дата обращения: 12.03.2020).

2. Котенко, В. В. Технологии информационного анализа пользовательского уровня телекоммуникационных систем : учебное пособие / В. В. Котенко ; Южный федеральный университет. - Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2019. - 194 с. - ISBN 978-5-9275-3176-9. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/1088143 (дата обращения: 26.02.2020)

МАКРООБЪЕКТЫ:

3. Развертывание и настройка виртуальных сетей : учебное пособие [для вузов] /

[сост.: В. В. Баранков, И. И. Баранкова, У. В. Михайлова, О. Б. Калугина] ; МГТУ. - Магнитогорск : МГТУ, 2019. - 1 электрон. опт. диск (CD-ROM). - Загл. с титул. экрана. - URL: https://magtu.informsystema.ru/uploader/fileUpload?name=3813.pdf&show=dcatalogues/1/1529986/3813.pdf&view=true (дата обращения: 15.10.2019). - Макрообъект. - ISBN 978-5-9967-1305-9. - Текст : электронный. - Сведения доступны также на CD-ROM.

4. Сетевая защита информации. Лабораторный практикум : учебное пособие [для вузов] / Д. Н. Мазнин [и др.] ; Магнитогорский гос. технический ун-т им. Г. И. Носова. - Магнитогорск : МГТУ им. Г. И. Носова, 2019. - 1 CD-ROM. - Загл. с титул. экрана. - URL: https://magtu.informsystema.ru/uploader/fileUpload?name=3824.pdf&show=dcatalogues/1/1530260/3824.pdf&view=true (дата обращения: 22.10.2019). - Макрообъект. - ISBN 978-5-9967-1605-0. - Текст : электронный. - Сведения доступны также на CD-ROM.

*РЕЖИМ ПРОСМОТРА МАКРООБЪЕКТОВ

1. Перейти по адресу электронного каталога https://magtu.informsystema.ru
2. Произвести авторизацию (Логин: Читатель1 Пароль: 111111)
3. Активизировать гиперссылку макрообъекта

в) Методические указания:

1. Методические указания по выполнению практических работ по дисциплине «Безопасность сетей ЭВМ» (Приложение 1)
2. Методические указания по выполнению лабораторных работ по дисциплине «Безопасность сетей ЭВМ» (Приложение 2)
3. Методические указания по выполнению внеаудиторных самостоятельных работ по дисциплине «Безопасность сетей ЭВМ» (Приложение 3)

г) Программное обеспечение и Интернет-ресурсы:

Программное обеспечение

Наименование ПО	№ договора	Срок действия лицензии
MS Office 2007 Professional	№ 135 от 17.09.2007	бессрочно
7Zip	свободно	бессрочно
LibreOffice	свободно	бессрочно
Adobe Reader	свободно	бессрочно
Браузер Mozilla Firefox	свободно распространяемое ПО	бессрочно
Браузер Yandex	свободно	бессрочно
Linux Calculate	свободно	бессрочно
FAR Manager	свободно	бессрочно

Профессиональные базы данных и информационные справочные системы

Название курса	Ссылка
Российская Государственная библиотека. Каталоги	https://www.rsl.ru/ru/4readers/catalogues/
Электронные ресурсы библиотеки МГТУ им. Г.И. Носова	https://magtu.informsystema.ru/Marc.html?locale=ru
Федеральный образовательный портал – Экономика. Социология. Менеджмент	http://ecsocman.hse.ru/

Университетская информационная система	https://uisrussia.msu.ru
Международная реферативная и полнотекстовая справочная база	http://scopus.com
Международная база полнотекстовых журналов	http://link.springer.com/
Международная коллекция научных протоколов по	http://www.springerprotocols.com/
Международная база научных материалов в области	http://materials.springer.com/
Международная база справочных изданий по всем	http://www.springer.com/references
Международная реферативная база данных по чистой и	http://zbmath.org/
Международная реферативная и полнотекстовая справочная база данных научных изданий	https://www.nature.com/siteindex
Архив научных журналов «Национальный электронно-информационный	https://archive.neicon.ru/xmlui/
Информационная система - Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и	https://fstec.ru/normotvorcheskaya/tekhnicheskaya-zashchita-informatsii
Информационная система - Банк данных угроз безопасности	https://bdu.fstec.ru/
Федеральное государственное бюджетное учреждение «Федеральный институт	URL: http://www1.fips.ru/
Информационная система - Единое окно доступа к	URL: http://window.edu.ru/
Поисковая система Академия Google (Google Scholar)	URL: https://scholar.google.ru/
Национальная информационно-аналитическая система – Российский индекс	URL: https://elibrary.ru/project_risc.asp
Электронная база периодических изданий East	https://dlib.eastview.com/

9 Материально-техническое обеспечение дисциплины (модуля)

Материально-техническое обеспечение дисциплины включает:

Лекционная аудитория Мультимедийные средства хранения, передачи и представления информации

Лаборатория сетей и систем передачи данных. Лаборатория безопасности сетей ЭВМ:

1. Учебно-лабораторный стенд "Кодирование и модуляция информации в системах связи", комплектация полная

2. Учебно-лабораторный стенд "Системы спутниковой навигации" GPS.(2 шт)

3. Комплект типового учебного оборудования "Сети сотовой связи GSM"

4. Комплект типового учебного оборудования "Телекоммуникационные линии связи" ТЛС-01

5. Комплект типового учебного оборудования "Сетевая безопасность типа SECURITY-3M"

6. Комплект учебного оборудования "Беспроводные компьютерные сети ЭВМ"

7. Модуль учебно-лабораторный для изучения низкоуровнего контроллера Ethernet

8. Стенд коммуникационного оборудования сервером для моделирования облачного сервиса

9. Комплекс программно-аппаратный ViPNet

Компьютерный класс - Персональные компьютеры с ПО и выходом в Интернет и доступом в электронную информационно-образовательную среду университета.

Аудитория для самостоятельной работы читальные залы библиотеки - Персональные компьютеры с ПО и выходом в Интернет и доступом в электронную информационно-образовательную среду университета.

Приложение 1

Учебно-методическое обеспечение самостоятельной работы обучающихся

По дисциплине «Безопасность сетей ЭВМ» предусмотрена аудиторная и внеаудиторная самостоятельная работа обучающихся.

Аудиторная самостоятельная работа обучающихся предполагает выполнение контрольных задач на практических занятиях.

Аудиторная самостоятельная работа обучающихся на практических занятиях осуществляется под контролем преподавателя в виде выполнения лабораторных работ, которые определяет преподаватель для обучающегося.

Внеаудиторная самостоятельная работа обучающихся осуществляется в виде изучения литературы по соответствующему разделу с проработкой материала; выполнения домашних заданий, подготовки к аудиторным контрольным работам и выполнения домашних заданий с консультациями преподавателя.

Примерные задания и вопросы по темам:

1. Цели и задачи защиты информации в вычислительных сетях.
2. Развитие технологий обеспечения безопасности сетей ЭВМ, эволюция подходов к обеспечению безопасности.
3. Угрозы информационной безопасности в современных вычислительных сетях.
4. Виды вычислительных сетей с характеристикой основных принципов построения.
5. Понятие целостности информации в вычислительных сетях. Причины нарушения целостности информации, их последствия и методы предотвращения.
6. Сетевая уязвимость – понятие, виды уязвимостей, их классификация, методы устранения.
7. Семиуровневая эталонная модель межсетевого взаимодействия (модель OSI). Дайте краткую характеристику задач каждого уровня модели.
8. Классификация современного сетевого оборудования с характеристикой каждого из классов.
9. Сетевой протокол – понятие, назначение, классификация с привязкой к уровням модели OSI. Перечислите известные Вам уязвимости современных сетевых протоколов.
10. Протокол TCP/IP как базовый протокол современных вычислительных сетей. Протоколы стека протоколов TCP/IP с краткой характеристикой основных.
11. Принципы работы IP-сетей. Маршрутизация, организация межсетевого взаимодействия, - основные принципы и технологии.

12. Глобальные вычислительные сети – история, технологии, базовые принципы построения, основные сервисы. Использование глобальных вычислительных сетей в контексте сетевой безопасности.
13. Технологии построения защищенной локальной вычислительной сети – структурирование сети, использование технологии VLAN, списков контроля доступа и т.д.
14. Сетевая атака. Классификация, методы проведения, фазы сетевой атаки.
15. Перечислите известные Вам методы сетевых атак. Оцените возможный ущерб для каждой из них и предложите известные методы противодействия.
16. Маршрутизация трафика в IP-сетях. Назначение, основные алгоритмы и принципы. Использование принципов маршрутизации злоумышленником (подмена субъекта или объекта маршрутизации, навязывание ложного маршрута) и методы предотвращения таких действий.
17. Межсетевые экраны – назначение, принцип действия, классификация, характеристики.
18. Построение защищенной вычислительной сети по принципу «оборона в глубину» - базовые понятия, основные структурные зоны и элементы сети.
19. Системы обнаружения вторжений. Системы предотвращения вторжений. Базовые принципы работы и основные характеристики.
20. Антивирусная защита в вычислительной сети.
21. Программное обеспечение, предназначенное для поиска и анализа уязвимостей в сетях ЭВМ.
22. Виртуальные частные сети (VPN). Виртуальные защищенные сети. Принципы построения, использование технологии VPN в контексте построения безопасной вычислительной сети.
23. Беспроводные сети. Основные принципы работы, основные уязвимости и методы их устранения.
24. Использование технологий шифрования и криптографической защиты информации в обеспечении безопасности сетей ЭВМ.

Приложение 2

Оценочные средства для проведения промежуточной аттестации

7. Оценочные средства для проведения промежуточной аттестации

а) Планируемые результаты обучения и оценочные средства для проведения промежуточной аттестации:

Оценочные средства
ОПК-12 Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем;
ОПК-12.1 Применяет знания в области безопасности вычислительных сетей при разработке автоматизированных систем
1. Способность к самостоятельному анализу тенденций развития технологий современных глобальных и локальных вычислительных сетей с точки зрения специалиста по информационной безопасности; 2. Способность прогнозировать потребности организации в технологиях защиты информации в сетях ЭВМ исходя из характера хозяйственной деятельности организации и обрабатываемой ею информации; 3. Знание основных рабочих характеристик современного сетевого оборудования, способность к самостоятельному выбору необходимого сетевого оборудования при разработке проекта защищенной вычислительной сети; 4. Понимание принципов функционирования средств защиты информации (СЗИ) и средств криптографической защиты информации (СКЗИ) 5. Знание номенклатуры сетевого оборудования и средств защиты информации в вычислительных сетях отечественного и мирового производства 6. Самостоятельно выполнить подбор сетевого оборудования исходя из его рабочих характеристик и наличия средств обеспечения безопасности информации в вычислительных сетях; 7. Разработать топологию вычислительной сети согласно поставленной задаче, определить факторы риска с точки зрения информационной безопасности в разработанной сети; 8. Выполнить настройку сетевого оборудования (коммутатор, маршрутизатор, сежсетевой экран) для построения разработанной топологии сети и соблюдения требований по защите информации; 9. Реализовать разработанную политику сетевой безопасности при настройке и конфигурированию сетевого оборудования. 10. Продемонстрировать работу с программными сканерами сетевых протоколов и сетевых уязвимостей (например, свободно распространяемые сканеры WireShark и Ethereal) 11. Диагностировать неисправности и аномальные состояний вычислительных сетей 12. Решить задачу по поиску неисправностей вычислительных сетей и оптимизации их работы
ОПК-12.2 Применяет знания в области безопасности операционных систем при разработке автоматизированных систем
1. знать физические принципы передачи информации по различным каналам связи 2. знать и понимать характерные уязвимости, присущие каналами связи при передаче информации по ним 3. Четко представлять методы перехвата информации при передаче ее по различным каналам связи

Оценочные средства
4. Самостоятельно диагностировать неисправность или аномалию работы сети ЭВМ 5. Сделать самостоятельное заключение о возможности или невозможности несанкционированного доступа к информации при данной неисправности сети 6. Предложить комплекс мер по устранению неисправности и предотвращению несанкционированного доступа к информации сети ЭВМ 7. Разработать комплекс мер для контроля безотказного функционирования сетей ЭВМ
ОПК-12.3 Применяет знания в области безопасности баз данных при разработке автоматизированных систем
1. Произвести проверку организации системы защиты информации вычислительной сети на соответствие организационно-техническим требованиям по защите информации. 2. Определить состав методов и объем испытаний для определения наличия уязвимостей вычислительной сети и их характер. 3. Произвести фильтрацию трафика вычислительной сети с помощью свободно распространяемых программ-анализаторов WireShark или Ethereal 4. Определить характерные признаки сетевой атаки на основе анализа сетевого трафика

б) Порядок проведения промежуточной аттестации, показатели и критерии оценивания:

Промежуточная аттестация по дисциплине включает теоретические вопросы, позволяющие оценить уровень усвоения обучающимися знаний, и практические задания, выявляющие степень сформированности умений и владений, проводится в форме экзамена.

Показатели и критерии оценивания экзамена:

– на оценку **«отлично»** (5 баллов) – обучающийся демонстрирует высокий уровень сформированности компетенций, всестороннее, систематическое и глубокое знание учебного материала, свободно выполняет практические задания, свободно оперирует знаниями, умениями, применяет их в ситуациях повышенной сложности.

– на оценку **«хорошо»** (4 балла) – обучающийся демонстрирует средний уровень сформированности компетенций: основные знания, умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.

– на оценку **«удовлетворительно»** (3 балла) – обучающийся демонстрирует пороговый уровень сформированности компетенций: в ходе контрольных мероприятий допускаются ошибки, проявляется отсутствие отдельных знаний, умений, навыков, обучающийся испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

– на оценку **«неудовлетворительно»** (2 балла) – обучающийся демонстрирует знания не более 20% теоретического материала, допускает существенные ошибки, не может показать интеллектуальные навыки решения простых задач.

– на оценку **«неудовлетворительно»** (1 балл) – обучающийся не может показать знания на уровне воспроизведения и объяснения информации, не может показать интеллектуальные навыки решения простых задач.

Показатели и критерии оценивания зачета:

– на оценку **«зачтено»** – обучающийся показывает знания на уровне воспроизведения и объяснения информации, интеллектуальные навыки решения простых задач;

– на оценку **«не зачтено»** – обучающийся не может показать знания на уровне воспроизведения и объяснения информации, не может показать интеллектуальные навыки решения простых задач.