МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Магнитогорский государственный технический университет им. Г.И. Носова»

УТВЕРЖДАЮ:
Директор института
Энергетики и автоматизированных систем
_____ С.И. Лукьянов
«15» марта 2017 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

БЕЗОПАСНОСТЬ СЕТЕЙ ЭВМ
НАИМЕНОВАНИЕ ДИСЦИПЛИНЫ

Направление подготовки (специальность)
10.05.03 Информационная безопасность автоматизированных систем
цифр наименование направления подготовки (специальности)

Направленность (профиль/ специализация) программы
Обеспечение информационной безопасности распределенных информационных систем
наименование направленности (профиля) подготовки (специализации)

Уровень высшего образования
специалитет

Форма обучения
очная

Институт	Энергетики и автоматизированных систем
Кафедра	Информатики и информационной безопасности
Курс	3
Семестр	5,6

Магнитогорск
2017 г.

Рабочая программа составлена на основе ФГОС ВО по специальности 10.05.03 «Информационная безопасность автоматизированных систем», утвержденного приказом МОиН РФ от 01.12.2016 № 1509.

Рабочая программа рассмотрена и одобрена на заседании кафедры
Информатики и информационной безопасности
(наименование кафедры - разработчика)

«03» марта 2017 г., протокол № 10.

Зав. кафедрой _____ /И.И. Баранкова/
(подпись) (И.О. Фамилия)

Рабочая программа одобрена методической комиссией
института Энергетики и автоматизированных систем
(наименование факультета (института) - исполнителя)

«14» марта 2017 г., протокол № 6.

Председатель _____ / С.И. Лукьянов/
(подпись) (И.О. Фамилия)

Рабочая программа составлена: зав.кафедрой ИиИБ, д.т.н., профессор
(должность, ученая степень, ученое звание)

_____ / И.И. Баранкова /
(подпись) (И.О. Фамилия)

Рецензент: зав. кафедрой Бизнес-информатики
и информационных технологий, к.п.н. профессор
(должность, ученая степень, ученое звание)

_____ / Г.Н. Чусавитина/
(подпись) (И.О. Фамилия)

Лист регистрации изменений и дополнений

№ п/п	Раздел программы	Краткое содержание изменения/дополнения	Дата, № протокола заседания кафедры	Подпись зав. кафедрой
1.	7	Переработка фонда оценочных средств	№1 от 20.09.2017	
2.	8	Обновление списка основной и дополнительной литературы	№1 от 20.09.2017	
3.	7	Переработка фонда оценочных средств	№1 от 07.09.2018	
4.	8	Обновление списка основной и дополнительной литературы	№1 от 07.09.2018	
5.	7	Переработка фонда оценочных средств	№ 1 от 07.09.2019	
6.	8	Обновление списка основной и дополнительной литературы	№ 1 от 07.09.2019	
7.	7	Переработка фонда оценочных средств	№1 от 04.09.2020	
8.	8	Обновление списка основной и дополнительной литературы	№1 от 04.09.2020	

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».

Специальными 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 базовую 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

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

Разработка и эксплуатация защищенных автоматизированных систем

Информационная безопасность распределенных информационных систем

Моделирование угроз информационной безопасности

Управление информационной безопасностью

Методы проектирования защищенных распределенных информационных систем

Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности

Производственная-преддипломная практика

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:

Структурный элемент компетенции	Планируемые результаты обучения
ПК-23 способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа	

Знать	- Характерные уязвимости, присущие каналами связи сетей ЭВМ при передаче информации по ним; - Основные принципы методик противодействия перехвату и несанкционированному съему информации при ее передаче по каналам связи сетей ЭВМ; - Классификацию и основные принципы действия оборудования и ПО, предназначенного для организации защищенных каналов передачи информации.
Уметь	─ Применять действующую нормативную базу при обеспечении безопасности сетей ЭВМ; ─ Определять основные угрозы безопасности в сетях ЭВМ; ─ Контролировать безотказное функционирование средств защиты информации в сетях ЭВМ; ─ Осуществлять подбор инструментальных и программных средств тестирования систем защиты сетей ЭВМ; ─ Разрабатывать комплекс организационных и технических мероприятий для предотвращения несанкционированного доступа к защищаемой информации в сетях ЭВМ.
Владеть	─ Методиками определения и поиска уязвимостей систем защиты информации в сетях ЭВМ; ─ Навыками настройки протоколов безопасности на современном сетевом оборудовании; ─ Приемами определения и классификации сетевых атак; ─ Методологией составления политик сетевой безопасности.
ОПК-8 способностью к освоению новых образцов программных, технических средств и информационных технологий	
Знать	─ Нормативные и правовые акты в области защиты информации передаваемой в сетях ЭВМ; ─ Современные технологии обеспечения информационной безопасности в сетях ЭВМ; ─ Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в сетях ЭВМ.
Уметь	- Производить анализ вычислительной сети и сетевого оборудования на предмет наличия известных уязвимостей; - Выполнять подбор необходимого сетевого оборудования, программных и аппаратных средств обеспечения сетевой безопасности; - Выполнять установку и настройку средств защиты информации при эксплуатации их в современной вычислительной сети; - Разрабатывать и реализовать политику сетевой безопасности при настройке и конфигурировании сетевого оборудования.
Владеть	- Навыками работы с современными программными сканерами сетевых протоколов и сетевых уязвимостей; - Навыками решения задач по поиску неисправностей вычислительных сетей с целью выявления уязвимостей вычислительных сетей и нейтрализации обнаруженных уязвимостей; - Навыками повышения уровня защищенности вычислительных сетей и оптимизации их работы.

4. Структура, объём и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет 7 зачетных единиц 252 акад. часов, в том числе:

– контактная работа – 128 акад. часов:

– аудиторная – 122 акад. часов;

– внеаудиторная – 6 акад. часов

– самостоятельная работа – 88,3 акад. часов;

– подготовка к экзамену – 35,7 акад. часа

Форма аттестации - зачет, курсовая работа, экзамен

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Работа студента Само	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	2/1И		1	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	Устный опрос	ПК-23, ОПК-8
1.2 Основные уязвимости сетей ЭВМ и их использование нарушителем		1	2/1И		1	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	Устный опрос	ПК-23, ОПК-8

1.3 Парольная защита административного и консольного входов на сетевое оборудование		2	2/1И		1	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»	ПК-23, ОПК-8
1.4 Защита удаленного подключения к сетевому оборудованию		2	2/1И		1	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»	ПК-23, ОПК-8
Итого по разделу		6	8/4И		4			
2. Модель безопасности для локальной вычислительной сети								
2.1 Принцип «обороны в глубину» как базовый принцип при организации защиты сети	5	1	2		1	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	Устный опрос	ПК-23, ОПК-8
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»	ПК-23, ОПК-8

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»	ПК-23, ОПК-8
Итого по разделу		4	8		3			
3. Обнаружение и нейтрализация сетевых атак								
3.1 Понятие «сетевой атаки» - история, классификация, современный подход к вопросу	5	1	2/1И		1	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями), подготовка к компьютерному тестированию	Компьютерное тестирование	ПК-23, ОПК-8
3.2 Фазы сетевой атаки		1	2/1И		1	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями), подготовка к компьютерному тестированию	Компьютерное тестирование	ПК-23, ОПК-8

3.3 Методики обнаружения сетевых атак		1	2/1И		1	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями), подготовка к компьютерному тестированию	Компьютерное тестирование	ПК-23, ОПК-8
3.4 Основные меры противодействия сетевым атакам; системы обнаружения и предотвращения вторжений		1	2/1И		1	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями), подготовка к компьютерному тестированию	Компьютерное тестирование	ПК-23, ОПК-8
Итого по разделу		4	8/4И		4			
4. Технологии безопасности локальных вычислительных сетей								
4.1 Технология виртуальных ЛВС (VLAN)	5	2	4/2И		1	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»	ПК-23, ОПК-8

4.2 Технология Port Security		1	4/2И		1	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»	ПК-23, ОПК-8
4.3 Технология списков контроля доступа (ACL)		1	4/2И		1	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями) , Подготовка к практическому занятию	Защита лабораторной работы «Использование технологии ACL»	ПК-23, ОПК-8
Итого по разделу		4	12/6И		3			
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	ПК-23, ОПК-8
Итого по разделу					3			
Итого за семестр		18	36/14И		17		зачёт	
6. Методы контроля сетей ЭВМ								

6.1 Анализ сетевого трафика	6	4		4/2И	4	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»	ПК-23, ОПК-8
6.2 Перехват сетевых сообщений		4		4/2И	4	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»	ПК-23, ОПК-8
6.3 Использование защищенных протоколов для защиты сетевого трафика		4		4	4	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»	ПК-23, ОПК-8
Итого по разделу		12		12/4И	12			
7. Безопасность беспроводных сетей								
7.1 Устройство и разновидности беспроводных сетей	6	4		4/2И	4	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	Устный опрос	ПК-23, ОПК-8

7.2 Проблема безопасности в беспроводных сетях		4		4/2И	2	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями) , подготовка к практическому занятию	Практическая работа «Организация защиты беспроводных сетей»	ПК-23, ОПК-8
Итого по разделу		8		8/4И	6			
8. Защищенные сети								
8.1 Понятие защищенной сети	6	2		4/2И	4	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	Устный опрос	ПК-23, ОПК-8
8.2 Технология виртуальной частной/защищенной сети (VPN). Классификация сетей VPN		4		4/2И	3	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	Устный опрос	ПК-23, ОПК-8
8.3 Разновидности технологий VPN		4		4/2И	3	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями) , подготовка к практическому занятию	Практическая работа «Организация VPN»	ПК-23, ОПК-8

8.4 Алгоритмы шифрования, применяемые для организации VPN		4		2	3,3	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями) , подготовка к практическому занятию	Практическая работа «Организация VPN»	ПК-23, ОПК-8
Итого по разделу		14		14/6И	13,3			
9. Подготовка к итоговой аттестации и курсовой								
9.1 Подготовка курсовой работы	6				25	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями), выполнение курсовой работы	Защита курсовой работы	ПК-23, ОПК-8
9.2 Подготовка к итоговой аттестации					15	Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	Экзамен	ПК-23, ОПК-8
Итого по разделу					40			
Итого за семестр		34		34/14И	71,3		экзамен,кр	
Итого по дисциплине		52	36/14И	34/14И	88,3		зачет, курсовая работа, экзамен	ПК-23,ОПК-8

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

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.

Лабораторная работа «Парольная защита консольного подключения сетевого оборудования»

Сконфигурируйте пароль, который нужно будет вводить при подключении к устройству через консоль. Провести анализ парольной защиты

Практическая работа «Организация защиты беспроводных сетей»

Изучить специфику задач обеспечения безопасности сети Wi-Fi, стандарты, протоколы и средства аутентификации и шифрации, выполнить настройку сети на разные уровни безопасности.

Изучить средства обеспечения безопасности, поддерживаемые Wi-Fi адаптером**.** Сравнить методы аутентификации и шифрации WEP.

Выполнить настройки в сети Wi-Fi на варианты:

- открытая аутентификация,
- аутентификация с общим ключом,
- аутентификация по MAC-адресу,
- сокрытие SSID.

7 Оценочные средства для проведения промежуточной аттестации

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

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
ОПК-8 - способность к освоению новых образцов программных, технических средств и информационных технологий		
Знать	– Нормативные и правовые акты в области защиты информации передаваемой в сетях ЭВМ; – Современные технологии обеспечения информационной безопасности в сетях ЭВМ; – Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в сетях ЭВМ.	Перечень вопросов: 1. Классифицируйте угрозы безопасности в современных вычислительных сетях. Какие угрозы безопасности в современных вычислительных сетях являются актуальными на сегодняшний день? Какие угрозы безопасности сетей ЭВМ будут, на Ваш взгляд, актуальными завтра? 2. Какие тенденции и подходы к обеспечению безопасности сетей ЭВМ Вы знаете? Охарактеризуйте их. 3. Дайте определение понятий «уязвимость сетевого оборудования» и «уязвимость вычислительной сети». Какие виды уязвимостей Вам известны? Перечислите и охарактеризуйте их. 4. Каким образом осуществляется поиск и устранение уязвимостей сетевого оборудования и вычислительной сети? Какие программные и аппаратные средства используются для поиска уязвимостей? 5. Назовите современные программные и аппаратные средства, позволяющие нейтрализовать угрозы безопасности вычислительной сети. 6. Классифицируйте современные технологии обеспечения безопасности сетей ЭВМ – назначение, область применения, принцип действия, достоинства и недостатки. 7. Дайте определение понятию «сетевая атака». Какие разновидности сетевых атак Вы знаете? Каким образом производится обнаружение и нейтрализация сетевых атак? 8. Назовите известные Вам системы обнаружения сетевых атак? Классифицируйте их (назначение, область применения, принцип действия). 9. Что, на Ваш взгляд, включает в себя понятие «комплексный подход к обеспечению сетевой безопасности»? 10. Дайте определения понятиям «базовая модель

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		угроз» и «модель нарушителя» для сети ЭВМ.
Уметь:	- Производить анализ вычислительной сети и сетевого оборудования на предмет наличия известных уязвимостей; - Выполнять подбор необходимого сетевого оборудования, программных и аппаратных средств обеспечения сетевой безопасности; - Выполнять установку и настройку средств защиты информации при эксплуатации их в современной вычислительной сети; - Разрабатывать и реализовать политику сетевой безопасности при настройке и конфигурировании сетевого оборудования.	1. Произвести анализ вычислительной сети и сетевого оборудования на предмет наличия известных уязвимостей. 2. Разработать план нейтрализации выявленных уязвимостей вычислительной сети и сетевого оборудования. 3. Выполнить подбор необходимого сетевого оборудования, программных и аппаратных средств обеспечения сетевой безопасности. 4. Произвести настройку протоколов обеспечения сетевой безопасности на сетевом оборудовании. 5. Выполнять установку и настройку средств защиты информации при эксплуатации их в современной вычислительной сети. 6. Разработать политику безопасности вычислительной сети как комплексную методику обеспечения безопасности и нейтрализации уязвимостей вычислительной сети. 7. Реализовать разработанную политику сетевой безопасности при настройке и конфигурировании сетевого оборудования.
Владеть	- Навыками работы с современными программными сканерами сетевых протоколов и	При помощи сканеров сетевых протоколов и сетевых уязвимостей произвести обследование вычислительной сети и определить: • Каким образом организован доступ в глобальные сети из данной сети;

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
	сетевых уязвимостей; - Навыками решения задач по поиску неисправностей вычислительных сетей с целью выявления уязвимостей вычислительных сетей и нейтрализации обнаруженных уязвимостей; - Навыками повышения уровня защищенности вычислительных сетей и оптимизации их работы.	• Системное программное обеспечение, применяемое для обеспечения функционирования сетевых узлов (операционные системы); • Модели и сетевые адреса активного сетевого оборудования в структуре вычислительной сети; • Схемы маршрутизации сетевого трафика; • Используемые сетевые протоколы; • Открытые сетевые порты; • Наличие или отсутствие устройств межсетевого экранирования, систем обнаружения вторжений, сетевых антивирусов и других средств обеспечения сетевой безопасности; • Наличие или отсутствие активных гостевых учетных записей и административных учетных записей с паролем по умолчанию на сетевом оборудовании; • Наличие или отсутствие известных уязвимостей сетевого оборудования и программного обеспечения на узлах сети. По результатам обследования сделать заключение о достаточности или недостаточности мер, принимаемых для обеспечения безопасности вычислительной сети.
ПК-23 - способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа		
Знать	- Характерные уязвимости, присущие каналами связи сетей ЭВМ при передаче информации по ним; - Основные принципы методик противодействия перехвату и несанкционированному съему информации при ее передаче по каналам связи	Перечень вопросов: 1. Характерные уязвимости, присущие каналами связи различной физической природы (проводные электрические, волоконно-оптические, беспроводные) при передаче информации по ним. 2. Методы перехвата информации при передаче ее по различным каналам связи. 3. Основные принципы действия методик по противодействию перехвату и несанкционированному съему информации при ее передаче по каналам связи. 4. Методы защиты информации (криптографические и некриптографические) при ее передаче по незащищенным каналам связи (каналам связи общего пользования). 5. Классификация и основные принципы действия оборудования и программного обеспечения, предназначенного для организации защищенных каналов передачи информации. 6. Принципы применения средств криптографической защиты информации (СКЗИ) при передаче информации по каналам связи.

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
	сетей ЭВМ; - Классификацию и основные принципы действия оборудования и ПО, предназначенного для организации защищенных каналов передачи информации.	
Уметь	─ Применять действующую нормативную базу при обеспечении безопасности сетей ЭВМ; ─ Определять основные угрозы безопасности в сетях ЭВМ; ─ Контролировать безотказное функционирование средств защиты информации в сетях ЭВМ; ─ Осуществлять подбор инструментальных и программных средств тестирования систем защиты сетей ЭВМ; ─ Разрабатывать комплекс организационных и технических мероприятий для предотвращения	1. Самостоятельно диагностировать неисправность или аномалию работы сети ЭВМ или канала связи с целью своевременной диагностики сетевой атаки и оперативного ей противодействия. 2. Сделать самостоятельное заключение о возможности или невозможности несанкционированного доступа к информации при данной неисправности сети из сетей общего пользования. 3. Предложить комплекс мер по устранению неисправности и предотвращению несанкционированного доступа к информации в сети ЭВМ со стороны сетей общего пользования. 4. Разработать комплекс мер для контроля безотказного функционирования сетей ЭВМ

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
	несанкционированного доступа к защищаемой информации в сетях ЭВМ.	
Владеть	– Методиками определения и поиска уязвимостей систем защиты информации в сетях ЭВМ; – Навыками настройки протоколов безопасности на современном сетевом оборудовании; – Приемами определения и классификации сетевых атак; – Методологией составления политик сетевой безопасности.	1. Произвести проверку организации системы защиты информации вычислительной сети на соответствие организационно-техническим требованиям по защите информации. 2. Использовать известные методики для определения наличия уязвимостей вычислительной сети и их характера. 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 курсовой работы:

– на оценку **«отлично»** (5 баллов) – работа выполнена в соответствии с заданием, обучающийся показывает высокий уровень знаний не только на уровне воспроизведения и объяснения информации, но и интеллектуальные навыки решения проблем и задач, нахождения уникальных ответов к проблемам, оценки и вынесения критических суждений;

– на оценку **«хорошо»** (4 балла) – работа выполнена в соответствии с заданием, обучающийся показывает знания не только на уровне воспроизведения и объяснения информации, но и интеллектуальные навыки решения проблем и задач, нахождения уникальных ответов к проблемам;

– на оценку **«удовлетворительно»** (3 балла) – работа выполнена в соответствии с заданием, обучающийся показывает знания на уровне воспроизведения и объяснения информации, интеллектуальные навыки решения простых задач;

– на оценку **«неудовлетворительно»** (2 балла) – задание преподавателя выполнено частично, в процессе защиты работы обучающийся допускает существенные ошибки, не может показать интеллектуальные навыки решения поставленной задачи.

– на оценку **«неудовлетворительно»** (1 балл) – задание преподавателя выполнено частично, обучающийся не может воспроизвести и объяснить содержание, не может показать интеллектуальные навыки решения поставленной задачи.

Темы курсовых работ

1. Системы обнаружения вторжений
2. Создание собственных сигнатур атаки для СОВ Snort
3. Облачные системы безопасности
4. Методология хакерских атак
5. Разработка комплекса мер по защите сети предприятия
6. Разработка сетевого сниффера
7. Средства мониторинга событий ИБ в сети
8. Беспроводные сети - методики взлома и технологии противодействия
9. Использование СКЗИ для обеспечения ИБ в вычислительной сети
10. Анализ Wi-Fi сети на подключение неизвестных устройств с оповещением при вторжении
11. Распределенные DoS-атаки - методология и методы противодействия
12. Сетевые антивирусные системы
13. Перехват сетевого трафика и методы противодействия перехвату
14. Технологии защиты сетей передачи данных
15. Фишинг: методология атаки и методы противодействия
16. Вопросы социальной инженерии в обеспечении безопасности сетей ЭВМ
17. Атаки типа "человек посредине" (Man in the middle) и принципы

противодействия им
18. Технологии межсетевого экранирования
19. Обеспечение сетевой безопасности при использовании Web-технологий
20. Принцип "оборона в глубину" как концепция построения защищенной сети ЭВМ

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

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

в) Методические указания:

1. Методические указания по выполнению практических работ по дисциплине «Безопасность сетей ЭВМ» (Приложение 1)

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

г) Программное обеспечение и Интернет-ресурсы:

Программное обеспечение

Наименование ПО	№ договора	Срок действия
MS Windows 7 Professional(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
MS Office 2007 Professional	№ 135 от 17.09.2007	бессрочно
7Zip	свободно распространяемое ПО	бессрочно
Kaspersky Endpoint Security для бизнеса-Стандартный	Д-300-18 от 21.03.2018	28.01.2020
LibreOffice	свободно распространяемое ПО	бессрочно
Adobe Reader	свободно распространяемое ПО	бессрочно
MS Windows 10 Professional (для классов)	Д-1227-18 от 08.10.2018	11.10.2021
MS Windows Server(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
VIP Net Client	Д-946-14 от 22.07.2014	бессрочно
VIP Net CryptoService	Д-946-14 от 22.07.2014	бессрочно
Браузер Mozilla Firefox	свободно распространяемое ПО	бессрочно
Браузер Yandex	свободно распространяемое ПО	бессрочно
Wireshark	свободно распространяемое ПО	бессрочно

Профессиональные базы данных и информационные справочные системы

Название курса	Ссылка
Международная справочная система «Полпред» polpred.com отрасль «Образование, наука»	http://education.polpred.com/
Национальная информационно-аналитическая система – Российский индекс научного цитирования (РИНЦ)	URL: https://elibrary.ru/project_risc.asp
Поисковая система Академия Google (Google Scholar)	URL: https://scholar.google.ru/
Информационная система - Единое окно доступа к информационным ресурсам	URL: http://window.edu.ru/
Федеральное государственное бюджетное учреждение «Федеральный институт промышленной собственности»	URL: http://www1.fips.ru/

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

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ПРОВЕДЕНИЮ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

Рекомендации направлены на оказание методической помощи студентам при выполнении практических занятий.

Практическое занятие – это занятие, проводимое под руководством преподавателя в учебной аудитории (компьютерном классе университета), направленное на углубление научно-теоретических знаний и получение практических навыков решения типовых и прикладных задач.

Целью практических занятий является формирование и отработка практических умений и навыков, необходимых в последующей деятельности обучающихся.

Основными задачами практических занятий являются:

- углубление уровня освоения общекультурных и профессиональных компетенций;
- обобщение, систематизация, углубление, закрепление полученных практических знаний по конкретным темам дисциплин различных циклов;
- приобретение студентами умений и навыков использования современных теоретических знаний в решении конкретных практических задач;
- развитие профессионального мышления, профессиональной и познавательной мотивации.

Перечень тем практических занятий определяется рабочей программой дисциплины. План практических занятий отвечает общей направленности лекционного курса и соотнесен с ним в последовательности тем.

Структура практического занятия включает следующие компоненты: вступительная часть; ответы на вопросы обучающихся; практическая часть; заключительное слово преподавателя. Во вступительной части объявляется тема текущего практического занятия, ставится его цели и задачи, проверяется исходный уровень готовности студентов к практическому занятию (выполнение тестов, контрольные вопросы и т.п.)

На практическом занятии преподаватель может использовать разнообразные образовательные технологии (методы IT, работа в команде, case-study, проблемное обучение, учебные дискуссии и т.п.) по своему выбору для достижения качественного уровня обучения.

Правила по технике безопасности для обучающихся при проведении практических работ

Общие правила:

1. Практические работы проводятся под наблюдением преподавателя. К выполнению практических работ студенты допускаются только после прослушивания инструктажа по технике безопасности, правилам поведения в компьютерном классе и противопожарным мерам.

2. Обучаемый должен строго выполнять правила техники безопасности и санитарно-гигиенические нормы при работе в компьютерных классах университета.

Порядок выполнения практических работ

При подготовке к выполнению практических работ студент должен повторить теоретический материал, необходимый для выполнения заданий по текущей теме.

Практическая работа выполняется каждым студентом самостоятельно, согласно индивидуальному заданию.

Студенты, пропустившие занятия, выполняют практические работы во внеурочное время.

После выполнения каждой практической работы студент демонстрирует результат выполнения преподавателю, отвечает на вопросы. Преподаватель оценивает работу в соответствии с заданными критериями оценки практических работ.

Правила оформления результатов и оценивания практической работы

Результаты выполненной практической работы оформляются в соответствии с требованиями к выполнению конкретной работы.

Практическая работа считается выполненной, если студент набрал балл, который составляет половину максимального количества баллов.

Для оценивания работы прилагается следующие критерии.

Оценка «отлично» – работа выполнена в полном объеме и без замечаний.

Оценка «хорошо» – работа выполнена правильно с учетом 2-3 несущественных ошибок исправленных самостоятельно по требованию преподавателя.

Оценка «удовлетворительно» – работа выполнена правильно не менее чем на половину или допущена существенная ошибка.

Оценка «неудовлетворительно» – допущены две (и более) существенные ошибки в ходе работы, которые студент не может исправить даже по требованию преподавателя, или работа не выполнена.

ПРИЛОЖЕНИЕ 2

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ВНЕАУДИТОРНЫХ САМОСТОЯТЕЛЬНЫХ РАБОТ ПО ДИСЦИПЛИНЕ

Общие положения

Настоящие методические указания предназначены для организации внеаудиторной самостоятельной работы студентов по дисциплине «Информатика и информационные технологии» и оказания помощи в самостоятельном изучении теоретического и реализации компетенций обучаемых.

Данные методические указания не являются учебным пособием, поэтому перед началом выполнения самостоятельного задания следует изучить соответствующие разделы лекционных занятий, материалов образовательного портала, разделов основной и дополнительной литературы, представленных в пункте 8. «Учебно-методическое и информационное обеспечение дисциплины (модуля)» данной РПД.

Цели и задачи самостоятельной работы

Цель самостоятельной работы – содействие оптимальному усвоению учебного материала обучающимися, развитие их познавательной активности, готовности и потребности в самообразовании.

Задачи самостоятельной работы:

- повышение исходного уровня владения информационными технологиями;
- углубление и систематизация знаний;
- постановка и решение стандартных задач профессиональной деятельности;
- развитие работы с различной по объему и виду информацией, учебной и научной литературой;
- практическое применение знаний, умений;
- самостоятельно использование стандартных программных средств сбора, обработки, хранения и защиты информации
- развитие навыков организации самостоятельного учебного труда и контроля за его эффективностью.

Особенностью изучения дисциплины «Информатика» является освоение теоретического материала и получение практических умений, направленных на использование современных информационных технологий.

Виды внеаудиторной самостоятельной работы и формы контроля и время на выполнение каждого вида самостоятельной работы указаны в пункте 4. «Структура и содержание дисциплины (модуля)» данной РПД.

Порядок выполнения

При выполнении текущей внеаудиторной самостоятельной работы обучающемуся следует придерживаться следующего порядка действий:

1) внимательно изучить соответствующие теоретические разделы дисциплины, пользуясь материалами (лекционными, презентационными, аудио-визуальными):
   a) предоставляемыми преподавателем на лекционных занятиях;
   b) предоставляемыми преподавателем в рамках электронных образовательных курсов;
   c) содержащимися в учебниках и учебных пособиях ЭБС (электронно-библиотечных систем), электронных каталогов университета и интернет-ресурсов.
2) Подробно разобрать типовые примеры решения задач, рассмотренные в рамках аудиторной контактной работы с преподавателем.

3) Применить полученные теоретические знания и практические навыки к решению индивидуальных заданий, к прохождению компьютерных тестирований и к решению олимпиадных заданий.
4) При необходимости, сформировать перечень вопросов, вызвавших затруднения в процессе самостоятельной работы. Обсудить возникшие вопросы со студентами группы, в рамках командно-проектной работы, и с преподавателем, в рамках консультационной помощи, реализованной либо в контактной форме, либо средствами информационно-образовательной среды ВУЗа.

Критерии оценки внеаудиторных самостоятельных работ

Качество выполнения внеаудиторной самостоятельной работы обучающихся оценивается посредством текущего контроля самостоятельной работы обучающихся с использованием балльно-рейтинговой системы.

В качестве форм текущего контроля по дисциплине используются: защита реферата, индивидуальные домашние задания, аудиторные контрольные работы, компьютерное тестирование, участие в конкурсах и олимпиадах.

Максимальное количество баллов обучающийся получает, если:

- выполняет ИДЗ в соответствии со всеми заявленными требованиями;
- дает правильные формулировки, точные определения, понятия терминов;
- может обосновать рациональность решения текущей задачи.;
- обстоятельно с достаточной полнотой излагает соответствующую теоретический раздел;
- правильно отвечает на дополнительные вопросы преподавателя, имеющие целью выяснить степень понимания им данного материала.

50~85% от максимального количества баллов обучающийся получает, если:

- неполно (не менее 70% от полного), но правильно выполнено задание;
- при изложении были допущены 1-2 несущественные ошибки, которые он исправляет после замечания преподавателя;
- дает правильные формулировки, точные определения, понятия терминов;
- может обосновать свой ответ, привести необходимые примеры;
- правильно отвечает на дополнительные вопросы преподавателя, имеющие целью выяснить степень понимания им данного материала.

36~50% от максимального количества баллов обучающийся получает, если:

- неполно (не менее 50% от полного), но правильно изложено задание;
- при изложении была допущена 1 существенная ошибка;
- знает и понимает основные положения данной темы, но допускает неточности в формулировке понятий;
- излагает выполнение задания недостаточно логично и последовательно;
- затрудняется при ответах на вопросы преподавателя.

35% и менее от максимального количества баллов обучающийся получает, если:

- неполно (менее 50% от полного) изложено задание;
- при изложении были допущены существенные ошибки. В "0" баллов преподаватель вправе оценить выполненное обучающимся задание, если оно не удовлетворяет требованиям, установленным преподавателем к данному виду работы или не было представлено для проверки.

Сумма полученных баллов по всем видам заданий внеаудиторной самостоятельной работы составляет рейтинговый показатель обучающегося. Рейтинговый показатель обучающегося влияет на выставление итоговой оценки по результатам изучения дисциплины.

Показатели и критерии оценивания полученных знаний представлены в пункте 7.б) «Оценочные средства для проведения промежуточной аттестации» данной РПД.