МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
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
«26» сентября 2018 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

БЕЗОПАСНОСТЬ СЕТЕЙ ЭВМ
наименование дисциплины

Специальность
10.05.03 Информационная безопасность автоматизированных систем
шифр наименование специальности

Специализация программы
Обеспечение информационной безопасности распределенных информационных систем
наименование специализации

Уровень высшего образования
специалитет

Форма обучения
очная

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

Магнитогорск
2018 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)

«07» сентября 2018 г., протокол № 1.

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

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

«26» сентября 2018 г., протокол № 1.

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 07.09.2019	
2.	8	Обновление списка основной и дополнительной литературы	№ 1 от 07.09.2019	
3.	7	Переработка фонда оценочных средств	№ 1 от 04.09.2020	
4.	8	Обновление списка основной и дополнительной литературы	№ 1 от 04.09.2020	

1 Цели освоения дисциплины (модуля)

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

1. Знакомство студентов с назначением, разновидностями и основными принципами организации современных вычислительных сетей в объеме, достаточном для понимания задач обеспечения безопасности операционных систем.
2. Обучение студентов принципам построения защиты информации в локальных вычислительных сетях (ЛВС) и методам анализа надежности защиты ЛВС.

2 Место дисциплины (модуля) в структуре образовательной программы подготовки специалиста

Дисциплина «Безопасность сетей ЭВМ» входит в базовую часть блока 1 образовательной программы.

Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин «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 «Разработка и эксплуатация защищенных автоматизированных систем», «Информационная безопасность распределенных информационных систем», «Управление информационной безопасностью», «Моделирование угроз информационной безопасности» и др.

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
ОПК-8 - способность к освоению новых образцов программных, технических средств и информационных технологий	
Знать	- нормативные и правовые акты в области защиты информации; - тенденции развития современных технологий сетевой безопасности; - основные определения и понятия, используемые в описании и построении современных вычислительных сетей; - классификацию, принципы действия, управления и функциональное назначение современных разновидностей сетевого оборудования; - структуру и принципы работы семиуровневой эталонной модели межсетевого взаимодействия (эталонная модель открытых систем); - существующие стандарты и принципы функционирования современных вычислительных сетей; - основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в сетях ЭВМ;
Уметь	- анализировать основные характеристики и возможности сетей ЭВМ по передаче информации; -самостоятельно разработать топологию вычислительной сети исходя из заданных требований;

Структурный элемент компетенции	Планируемые результаты обучения
	- самостоятельно выполнить настройку управляемого сетевого оборудования (коммутатор, маршрутизатор, межсетевой экран); - разработать политику сетевой безопасности для заданной сети ЭВМ исходя из заданных требований с использованием современных технологий сетевой безопасности;
Владеть	- профессиональным языком и терминологией предметной области (сети ЭВМ) - современным сетевым и диагностическим оборудованием и программным обеспечением, предназначенным для построения вычислительных сетей (сетей ЭВМ) -методикой проектирования защищенных сетей ЭВМ
ПК-23 - способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа	
Знать	- принципы передачи информации по телекоммуникационным каналам; - принципы функционирования и основные рабочие характеристики оборудования сетей ЭВМ; - основные меры и механизмы защиты информации в сетях ЭВМ; - меры предотвращения утечки информации по техническим каналам сетей ЭВМ; - базовую модель угроз и модель нарушителя в сетях ЭВМ; - принципы функционирования средств защиты информации в сетях ЭВМ;
Уметь	- применять действующую нормативную базу при обеспечении безопасности сетей ЭВМ; - Самостоятельно диагностировать неисправности и аномалии сетей ЭВМ; - выявлять 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; - разработать 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 сетевого оборудования; - методиками определения и классификации сетевых атак; - методиками предотвращения сетевых атак; - методиками составления политик сетевой безопасности;

4 Структура 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;

Форма промежуточной аттестации: зачет, экзамен, курсовая работа
- подготовка к экзамену – 35,7 акад. часа

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа (в акад. часах)	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код и структурный элемент компетенции
		лекции	гиялаборат.	практич. занятия				
1. **Основные понятия сетей ЭВМ**	5							
1.1. Сети ЭВМ – история, функциональное назначение, классификация	5	1	2/1И		1	Самостоятельная работа с интернет-источниками и учебно-методической литературой	Устный опрос	*ОПК-8*
1.2. Принципы передачи информации по сетям ЭВМ	5	1	2/1И		1	Самостоятельная работа с интернет-источниками и учебно-методической литературой	Устный опрос	*ОПК-8*
1.3. Классификация сетевого оборудования: назначение, принципы действия, основные базовые характеристики	5	2	2/1И		2	Самостоятельная работа с интернет-источниками и учебно-методической литературой	Лабораторная работа «Построение одноуровневой ЛВС на лабораторном стенде»	*ОПК-8*
1.4. Сетевые протоколы: назначение, разновидности, характеристики	5	2	2/1И		2	Самостоятельная работа с интернет-источниками и учебно-методической литературой	Лабораторная работа «Знакомство со сканером сетевых протоколов»	*ОПК-8*
Итого по разделу		**6**	**8/4И**		**6**			
2. **Эталонная модель взаимодействия**								*ОПК-8*

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа (в акад. часах)	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код и структурный элемент компетенции
		лекции	тиялаборат.	практич. занятия				
открытых систем								
2.1. Эталонная модель (модель OSI) как фундаментальный принцип построения современных вычислительных сетей	5	1	2		1	Самостоятельная работа с интернет-источниками и учебно-методической литературой	Устный опрос	ОПК-8
2.2. Структурные уровни модели, принципы организации и функциональное назначение каждого из уровней	5	1	2		1	Самостоятельная работа с интернет-источниками и учебно-методической литературой	Лабораторная работа «Использование протокола ARP в ЛВС»	ОПК-8
2.3 Стек протоколов TCP/IP как базовый стек протоколов современных сетей ЭВМ	5	2	4		2	Самостоятельная работа с интернет-источниками и учебно-методической литературой	Лабораторная работа «Получение списка используемых сетевых протоколов стека TCP/IP в ОС Windows»	ОПК-8
Итого по разделу		**4**	**8**		**4**			
3. Раздел «Проблема безопасности вычислительных сетей»								
3.1 Тема «Основные опасности и факторы риска при эксплуатации сетей ЭВМ»	5	1	2/1И		1	Самостоятельная работа с интернет-источниками и учебно-методической литературой	Подготовка самостоятельного сообщения на заданную тему	ПК-23
3.2 Тема «История развития технологий сетевой безопасности»	5	1	2/1И		1	Самостоятельная работа с интернет-источниками и учебно-методической литературой	Подготовка самостоятельного сообщения на заданную тему	ПК-23
3.3 Тема «Классификация сетевых атак»	5	1	2/1И		1	Самостоятельная работа с интернет-источниками и учебно-методической литературой	Подготовка самостоятельного сообщения на заданную тему	ПК-23

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа (в акад. часах)	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код и структурный элемент компетенции
		лекции	гиялаборат.	практич. занятия				
3.4 Тема «Основные меры противодействия сетевым атакам»	5	1	2/1И		1	Самостоятельная работа с интернет-источниками и учебно-методической литературой	Подготовка самостоятельного сообщения на заданную тему	ПК-23
Итого по разделу		**4**	**8/4И**		**4**			
4. Раздел «Технологии безопасности локальных вычислительных сетей»								
4.1. Технология виртуальных ЛВС (VLAN)	5	2	4/2И		1	Самостоятельная работа с интернет-источниками и учебно-методической литературой	Защита лабораторной работы «Организация ЛВС с VLAN»	ПК-23
4.2 Технология Port Security	5	1	4/2И		1	Самостоятельная работа с интернет-источниками и учебно-методической литературой	Защита лабораторной работы «Использование технологии Port Security»	ПК-23
4.3 Технология списков контроля доступа (ACL)	5	1	4/2И		1	Самостоятельная работа с интернет-источниками и учебно-методической литературой	Защита лабораторной работы «Использование технологии ACL»	ПК-23
Итого по разделу		**4**	**12/6И**		**3**			
Итого за семестр		**18**	**36/14 И**		**17**		**Промежуточная аттестация (зачет)**	
5. Раздел «Методы контроля сетей ЭВМ»	6							
5.1. Тема «Анализ сетевого трафика»	6	4		4/2И	4	Самостоятельная работа с интернет-источниками и учебно-методической литературой	Выполнение задания при помощи анализатора сетевых протоколов WireShark или Ethereal	ПК-23
5.2. Тема «Перехват сетевых сообщений»	6	4		4/2И	4	Самостоятельная работа с	Выполнение задания при	ПК-23

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа (в акад. часах)	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код и структурный элемент компетенции
		лекции	тиялаборат.	практич. занятия				
						интернет-источниками и учебно-методической литературой	помощи анализатора сетевых протоколов WireShark или Ethereal	
5.3 Тема «Использование защищенных протоколов для защиты сетевого трафика»	6	4		4	4	Самостоятельная работа с интернет-источниками и учебно-методической литературой	Выполнение задания при помощи анализатора сетевых протоколов WireShark или Ethereal	ПК-23
Итого по разделу	**6**	**12**		**12/4И**	**12**			
6. Раздел «Безопасность беспроводных сетей»	**6**							
6.1 Тема «Устройство и разновидности беспроводных сетей»	6	4		4/2И	4	Самостоятельная работа с интернет-источниками и учебно-методической литературой	Устный опрос	ПК-23
6.2 Тема «Проблема безопасности в беспроводных сетях»	6	4		4/2И	4	Самостоятельная работа с интернет-источниками и учебно-методической литературой	Выполнение лабораторной работы «Организация беспроводной сети»	ПК-23
Итого по разделу	**6**	**8**		**8/4И**	**8**			
7. Раздел «Защищенные сети»								
7.1 Тема «Понятие защищенной сети»	6	2		2	3	Самостоятельная работа с интернет-источниками и учебно-методической литературой	Устный опрос	ПК-23
7.2 Тема «Технология виртуальной частной/защищенной сети (VPN). Классификация сетей VPN»	6	4		4/2И	4	Самостоятельная работа с интернет-источниками и учебно-методической литературой	Устный опрос	ПК-23

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа (в акад. часах)	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код и структурный элемент компетенции
		лекции	тиялаборат.	практич. занятия				
7.3 Тема «Разновидности технологий VPN»	6	4		4/2И	4	Самостоятельная работа с интернет-источниками и учебно-методической литературой	Выполнение лабораторной работы «Организация VPN»	ПК-23
7.4 Тема «Алгоритмы шифрования, применяемые для организации VPN»	6	4		4/2И	4,6	Самостоятельная работа с интернет-источниками и учебно-методической литературой	Выполнение лабораторной работы «Организация VPN»	ПК-23
Итого по разделу	**6**	**14**		**14/6И**	**15,6**			
Подготовка к экзамену	**6**				**35,7**		Подготовка к экзамену	
Итого за семестр		**34**		**34/14 И**	**71,3**		**Промежуточная аттестация (экзамен/ курсовая работа)**	
Итого по дисциплине		**54**	**36/14 И**	**34/14 И**	**88,3**			

5 Образовательные и информационные 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.

Для реализации предусмотренных видов учебной работы в качестве образовательных технологий в преподавании дисциплины используются:

а) **Традиционная технология**, включающая в себя объяснение преподавателя на лекциях, самостоятельную работу с учебной и справочной литературой по дисциплине, выполнение заданий по методическим указаниям.

b) ***Вводная лекция*** – для целостного представления об учебном предмете и анализа учебно-методической литературы;

c) ***Обзорные лекции*** – для систематизации научных знаний на высоком уровне с использованием ассоциативных связей в процессе представления и осмысления информации;

d) ***Проблемные лекции*** – для ведения диалога обучающихся с преподавателем по сложным темам, для более полного раскрытия содержания проблемы по некоторым темам, а так же для развития исследовательских навыков и изучения способов решения задач;

2) ***Лекции-визуализации*** – для наглядного представления материалов курса. Лекционные занятия проводятся с использованием презентационного оборудования (проектор, экран, ноутбук), в качестве наглядных материалов используются: Web-ориентированные программные учебные материалы, электронные плакаты, презентации к лекциям.

3) **Модульно-компетентностная технология**, включающая в себя жесткое структурирование содержания учебного материала, сопровождающаяся обязательными блоками домашних заданий, контрольных работ и тестированием по каждой теме содержания курса. Для формирования у обучающихся основных понятий дисциплины используются:

a) ***Кейс-методы*** – для овладения системой знаний и умений и творческого их

использования в профессиональной деятельности и самообразовании; для квалифицированного и независимого решения профессиональных задач; для ориентации в многообразии учебных программ, пособий, литературы и выбора наиболее эффективных в применении к конкретной ситуации; для осуществления саморефлексии для дальнейшего профессионального, творческого роста и социализации личности.

4) **Интерактивное обучение**. Все лабораторные занятия проводятся в интерактивной форме. В рамках интерактивного обучения обучающихся применяются:

   a) *Case-study* – для анализа реальных проблемных ситуаций и поиска лучших вариантов решений, разбор результатов тематических контрольных работ, анализ ошибок, совместный поиск вариантов рационального решения проблемы.
   b) *Методы IT* – для применения компьютеров в процессе освоения дисциплины и доступа к ЭОР кафедры и Интернет-ресурсам.
   c) *Проблемное обучение* – для стимулирования к самостоятельной «добыче» знаний, необходимых для решения конкретной проблемы. Для этого каждому обучающемуся выдаётся индивидуальная тема, по которой он должен выполнить курсовую работу.

5) ***Контекстное обучение*** – для мотивации обучающихся к усвоению знаний путем выявления связей между конкретным знанием и его применение. Овладев в рамках изучения дисциплины навыками обеспечения безопасности информации в сетях ЭВМ, обучающийся приобретет способность участвовать в разработке защищенных сетей ЭВМ и обеспечению безопасности сетей ЭВМ по профилю своей профессиональной деятельности;

   a) ***Междисциплинарное обучение*** – для использования знаний из различных областей, их группировки и концентрации в контексте решаемой задачи. Для реализации данного метола обучения обучающимся выдаются задания по решения задач из другой предметной области.

6) Для приобретения **новых фактических знаний и практических умений** используются лабораторные занятия:
   a) компьютерный практикум;
   b) разбор результатов тематических контрольных работ, анализ ошибок, совместный поиск вариантов рационального решения учебной проблемы.

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.

7 Оценочные средства для проведения промежуточной аттестации

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; - тенденции развития современных технологий сетевой безопасности; - основные определения и понятия, используемые в описании и построении современных вычислительных сетей; - классификацию, принципы действия, управления и функциональное назначение современных разновидностей сетевого оборудования; - структуру и принципы работы семиуровневой эталонной модели межсетевого взаимодействия (эталонная модель открытых систем); - существующие стандарты и принципы функционирования современных вычислительных сетей;	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

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
	- основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в сетях ЭВМ;	
Уметь:	- анализировать основные характеристики и возможности сетей ЭВМ по передаче информации; -самостоятельно разработать топологию вычислительной сети исходя из заданных требований; - самостоятельно выполнить настройку управляемого сетевого оборудования (коммутатор, маршрутизатор, межсетевой экран); - разработать политику сетевой безопасности для заданной сети ЭВМ исходя из заданных требований с использованием современных технологий сетевой безопасности.	Самостоятельно выполнить подбор сетевого оборудования исходя из его рабочих характеристик и наличия средств обеспечения безопасности информации в вычислительных сетях; Уметь разработать топологию вычислительной сети согласно поставленной задаче, определить факторы риска с точки зрения информационной безопасности в разработанной сети; Уметь выполнить настройку сетевого оборудования (коммутатор, маршрутизатор, сежсетевой экран) для построения разработанной топологии сети и соблюдения требований по защите информации; Уметь реализовать разработанную политику сетевой безопасности при настройке и конфигурированию сетевого оборудования.
Владеть	профессиональным языком и терминологией предметной области (сети ЭВМ) - современным сетевым и диагностическим оборудованием и программным обеспечением,	Навыками работы с программными сканерами сетевых протоколов и сетевых уязвимостей (например, свободно распространяемые сканеры WireShark и Ethereal) Навыками диагностики неисправностей и аномальных состояний вычислительных сетей Навыками решения задач по поиску неисправностей вычислительных сетей и оптимизации их работы

Структурный нт нции	Планируемые результаты обучения	Оценочные средства
	предназначенным для построения вычислительных сетей (сетей ЭВМ) -методикой проектирования защищенных сетей ЭВМ –	
ПК-23 - способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа		
Знать	- принципы передачи информации по телекоммуникационным каналам; - принципы функционирования и основные рабочие характеристики оборудования сетей ЭВМ; - основные меры и механизмы защиты информации в сетях ЭВМ; - меры предотвращения утечки информации по техническим каналам сетей ЭВМ; - базовую модель угроз и модель нарушителя в сетях ЭВМ; - принципы функционирования средств защиты информации в сетях ЭВМ;	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
Уметь	- применять действующую нормативную базу при обеспечении безопасности сетей ЭВМ; - Самостоятельно	Самостоятельно диагностировать неисправность или аномалию работы сети ЭВМ Сделать самостоятельное заключение о возможности или невозможности несанкционированного доступа к информации при данной неисправности сети Предложить комплекс мер по устранению неисправности и предотвращению несанкционированного доступа к

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
	диагностировать неисправности и аномалии сетей ЭВМ; - выявлять 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; – разработать комплекс организационных и технических мероприятий для предотвращения несанкционированного доступа к защищаемой информации в сетях ЭВМ;	информации сети ЭВМ Разработать комплекс мер для контроля безотказного функционирования сетей ЭВМ
Владеть	- методиками определения и поиска уязвимостей систем защиты информации в сетях ЭВМ; - навыками настройки сетевого оборудования; - методиками определения и	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

Структурный компонент компетенции	Планируемые результаты обучения	Оценочные средства
	классификации сетевых атак; - методиками предотвращения сетевых атак; - методиками составления политик сетевой безопасности;	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.

8 Учебно-методическое и информационное обеспечение дисциплины (модуля)

а) Основная литература:

1. Партыка,Т. Л. Операционные системы, среды и оболочки [Электронный ресурс]: Учебное пособие / Т.Л. Партыка, И.И. Попов. - 5-е изд., перераб. и доп. - М.: Форум: НИЦ ИНФРА-М, 2013. - 560 с.: ил.- (Профессиональное образование). Режим доступа: http://znanium.com/bookread.php?book=405821. –Заглавие с экрана.– ISBN 978-5-91134-743-7.

2. Операционная система Linux: Курс лекций [Электронный ресурс]: Учебное пособие/ Г.В. Курячий, К.А.Маслинский. - М.: ДМК Пресс, 2010. – 348 с. - Режим доступа: http://e.lanbook.com/view/book/1202/ –Заглавие с экрана. – ISBN 978-5-94074-591-4.

3. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей [Электронный ресурс]: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: ИНФРА-М, 2012. - 416 с.: ил. - (Профессиональное образование).). - Режим доступа: http://znanium.com/bookread.php?book=335362 –Заглавие с экрана. – ISBN 978-5-8199-0331-5.

4. Жуков, В. Г. Безопасность вычислительных сетей. Ч. I. Базовые протоколы стека TCP/IP [Электронный ресурс] : учеб. пособие / В. Г. Жуков. - Красноярск : Сиб. гос. аэрокосмич. ун-т, 2012. - 124 с. Режим доступа: http://znanium.com/bookread.php?book=463062. -Заглавие с экрана.

5. Громов, Ю.Ю. Информационная безопасность и защита информации [Текст]: учеб. пособие/ Ю.Ю. Громов.– М.: ТНТ, 2010. – 384 с.- ISBN 978-5-94178-216-1

6. Гришина, Н.В. Комплексная система защиты информации на предприятии [Текст]: учеб. пособие/ Н.В Гришина. – М.: ФОРУМ, 2010. – 256 с.

7. Расторгуев, С.П. Основы информационной безопасности [Текст]: учеб. пособие/ С.П.Расторгуев. – М.: Академия, 2009. – 255с. ISBN: 978-5-7695-3098-2.

б) Дополнительная литература:

1. Шаньгин, В.Ф. Комплексная защита информации в корпоративных системах [Электронный ресурс]: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2013. - 592 с.: ил. - (Высшее образование). Режим доступа: http://znanium.com/bookread.php?book=402686 –Заглавие с экрана.– ISBN 978-5-8199-0411-4

2. Компьютерные сети [Электронный ресурс]: Учебное пособие для студ. учреждений СПО/ Н.В. Максимов, И.И. Попов. - 6-е изд., перераб. и доп. - М.: Форум: НИЦ ИНФРА-М, 2013. - 464 с.: ил.- (Профессиональное образование). Режим доступа:

http://znanium.com/bookread.php?book=163728. -Заглавие с экрана.– ISBN 978-5-91134-764-2.

3. Исаченко, О.В Программное обеспечение компьютерных сетей сценариев [Электронный ресурс]: Учебное пособие / Исаченко О.В.. - М.: ИНФРА-М, 2012. - 117 с- (Среднее профессиональное образование). Режим доступа: http://znanium.com/bookread.php?book=232661. - Заглавие с экрана.- ISBN 978-5-16-004858-1.

4. Васильков, А.В. Безопасность и управление доступом в информационных системах [Электронный ресурс]: Учебное пособие / А.В. Васильков, И.А. Васильков. - М.: Форум: НИЦ ИНФРА-М, 2013. - 368 с.: ил.(Профессиональное образование). - Режим доступа: http://znanium.com/bookread.php?book=405313.- Заглавие с экрана. ISBN 978-5-91134-360-6.

5. Хорев, П.Б. Программно-аппаратная защита информации [Электронный ресурс]: Учебное пособие / П.Б. Хорев. - 2-е изд., испр. и доп. - М.: Форум: НИЦ ИНФРА-М, 2015. - 352 с.: ил. Режим доступа: http://znanium.com/bookread.php?book=489084 – Заглавие с экрана. - ISBN 978-5-00091-004-7.

6. Грибунин, В.Г. Комплексная система защиты информации на предприятии [Текст]: учеб. пособие/ В.Г. Грибунин. – М.: Академия, 2009. –416 с. - ISBN 978-5-7695-5448-3.

в) Программное обеспечение и Интернет-ресурсы:

1. Журнал Information Security. Информационная безопасность: периодич. интернет-изд. URL: http://www.itsec.ru/articles2/allpubliks – Загл. с экрана. Яз. рус.

2. Журнал «Безопасность информационных технологий» : периодич. интернет-изд. URL: http://www.pvti.ru/articles_14.htm – Загл. с экрана. Яз. рус.

3. Журнал «Вопросы кибербезопасности»: периодич. интернет-изд. URL: http://cyberrus.com/ – Загл. с экрана. Яз. рус.

4. «Журнал сетевых решений LAN»: периодич. интернет-изд. URL: http://www.osp.ru/lan/ Издательство "Открытые системы. СУБД".http://www.osp.ru/os/– Загл. с экрана. Яз. рус.

5. Государственная публичная научно-техническая библиотека России [Электронный ресурс] / – Режим доступа: http://www.gpntb.ru, свободный.– Загл. с экрана. Яз. рус.

6. Российская национальная библиотека. [Электронный ресурс] / –URL: http://www.nlr.ru. Яз. рус.

7. Компьтерра: все новости про компьютеры, железо, новые технологии, информационные : периодич. интернет-изд. URL: http://www.computerra.ru/ – Загл. с экрана. Яз. рус.

8. http://www.безопасник.рф

9 Материально-техническое обеспечение дисциплины (модуля)

Материально-техническое обеспечение дисциплины включает:

Тип и название аудитории	Оснащение аудитории
Лекционная аудитория	Мультимедийные средства хранения, передачи и представления информации

Тип и название аудитории	Оснащение аудитории
Лаборатория радиомониторинга и контроля утечек информации, ауд. 226	K Комплект учебного оборудования «Криптографические системы» K Комплект учебного оборудования «Сетевая безопасность» SECURITY-CISCO-3M K Комплект учебного оборудования «Беспроводные компьютерные сети ЭВМ» K Модуль «Низкоуровневый контроллер Ethernet» K Комплекс средств защиты информации ViPNet: криптошлюз и межсетевой экран (3шт)
Компьютерный класс 372-2,3	Персональные компьютеры с пакетом MS Office и выходом в Интернет