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 ОПЕРАЦИОННЫХ СИСТЕМ
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	3,4
Семестр	6,7

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 операционных систем» являются:

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

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

Дисциплина «Безопасность операционных систем» входит в базовую часть блока 1 образовательной программы.

Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин «Информатика», «Безопасность сетей ЭВМ», «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 операционных систем» 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	- основные определения и понятия, используемые в теории операционных систем; - современные подходы к организации и проведению научных исследований с использованием сетевых технологий; - принципы построения и современные технологии, используемые в современных операционных системах, автоматизированных системах и сетях ЭВМ;
Уметь	- разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры; - обосновать выбор решения по обеспечению требуемого уровня защиты ОС (ИС); готовить публикации по результатам выполненных работ;
Владеть	- навыками использования операционных систем, информационных систем и сетевых технологий в системах защиты информации и в учебной деятельности;

Структурный элемент компетенции	Планируемые результаты обучения
	- методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем.
ПК-23 - способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа	
Знать	- правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированной системы - критерии оценки эффективности и надежности средств защиты операционных систем; специализированные средства выявления уязвимостей сетей ЭВМ;
Уметь	- реализовывать политику безопасности операционной системы; - сформировать комплекс мер для обеспечения информационной безопасности автоматизированной системы;
Владеть	- навыками формальной постановки задачи обеспечения информационной безопасности объектов информатизации. - навыками эксплуатации операционных систем и локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности; - навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем;
ПК-25 - способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций	
Знать	- иметь представление об основных средствах защиты информационно-технологических ресурсов автоматизированной системы; - критерии защищенности ОС и сети ЭВМ; - средства защиты сетей ЭВМ; о современных средствах защиты информационно-технологических ресурсов автоматизированной системы; - критерии оценки эффективности и надежности средств защиты операционных систем; - принципы организации и структуру подсистем защиты операционных систем семейств UNIX и Windows;
Уметь	- использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем; - проводить мониторинг угроз безопасности компьютерных сетей, обеспечивать защиту сетевых подключений средствами операционной системы;
Владеть	- профессиональной терминологией в области информационной

Структурный элемент компетенции	Планируемые результаты обучения
	безопасности; - навыками работы с конкретными программными и аппаратными продуктами средств телекоммуникаций, удаленного доступа и сетевыми ОС; - навыками конфигурирования средств защиты информации; - навыками противодействия угрозами типа «недоверенная загрузка (НДЗ) операционной системы» и несанкционированный доступ (НСД) к операционной системе и вычислительной сети;

4 Структура и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет 6 зачетных единиц 216 акад. часов, в том числе:

- контактная работа – 123,95 акад. часов:
  - аудиторная – 119 акад. часов;
  - внеаудиторная – 4,95 акад. часов
- самостоятельная работа – 56,35 акад. часов;
- подготовка к экзамену – 35,7 акад. часа

Форма аттестации: 1 семестр – Зачет, 2 семестр – Экзамен

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. Раздел «Предмет безопасности операционных систем»								
1.1. Тема «Определение предмета безопасности операционных систем (ОС)»	6	1	2/1И		2	Самостоятельная работа с интернет-источниками и учебно-методической литературой	Устный опрос	ОПК-8 з
1.2. Тема Общее понятие безопасности операционных систем, история развития вопроса, характеристика подходов к обеспечению безопасности операционных систем.	6	1	2/1И		2	Самостоятельная работа с интернет-источниками и учебно-методической литературой	Устный опрос	ОПК-8 з
Итого по разделу	**6**	**2**	**4/2И**		**4**			
2. Раздел «Операционная система с точки зрения специалиста по								ОПК-8 зу

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				
информационной безопасности»								
2.1. Тема Общая концепция построения ОС, виды ОС.	6	1	4/2И		2	Самостоятельная работа с интернет-источниками и учебно-методической литературой		ОПК-8 зу
2.2. Тема «история развития, семейства ОС. Современные ОС и их характеристика»	6	1	4/2И		2	Самостоятельная работа с интернет-источниками и учебно-методической литературой	Устный опрос	ОПК-8 зув
Итого по разделу	**6**	**2**	**8/4И**		**4**		Устный опрос	ОПК-8 зув
3. Раздел «Структурная схема ОС»								
3.1. Тема «Центральные элементы ОС – ядро, пользовательская оболочка, файловая подсистема, сетевая подсистема»	6	2	4/2И		2	Самостоятельная работа с интернет-источниками и учебно-методической литературой	Устный опрос	ОПК-8 зув
3.2. Тема «Периферийные подсистемы ОС. Загрузка ОС и ее этапы»	6	2	4/2И		2	Самостоятельная работа с интернет-источниками и учебно-методической литературой	Устный опрос	ОПК-8 зув
Итого по разделу	**6**	**4**	**8/4И**		**4**			

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	лабораторные	практич. занятия				
4. Раздел «Многозадачные ОС»								
3.1. Тема «Принципы организации многозадачной ОС. Виды многозадачности, технологии обеспечения многозадачности ОС».	6	2	4/1И		2	Самостоятельная работа с интернет-источниками и учебно-методической литературой	Выполнение лабораторной работы «Чтение системной таблицы процессов»	ОПК-8 зув
3.2. Тема «Принципы организации межпрограммного взаимодействия».	6	2	4/1И		2	Самостоятельная работа с интернет-источниками и учебно-методической литературой	Устный опрос	ОПК-8 зув
Итого по разделу	**6**	**4**	**8/2И**		**4**			
4. Раздел «**Сетевая подсистема ОС**»								
4.1. Тема «Сетевые сервисы ОС»	6	2	2/1И		2	Самостоятельная работа с интернет-источниками и учебно-методической литературой	Устный опрос	ПК-23 зув
4.2. Тема «Принципы построения сетевой подсистемы ОС»	6	3	4/1И		2,05	Самостоятельная работа с интернет-источниками и учебно-методической литературой	Устный опрос	ПК-23 зув
Итого по разделу	**6**	**5**	**6/2И**		**4,05**		Устный опрос	
Итого за семестр	**6**	**17**	**34/14 И**		**20,05**		**Промежуточная аттестация (зачет)**	

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	лабораторные	практич. занятия				
5.Раздел «Подсистема безопасности ОС»								
5.1. Тема «Подсистема безопасности ОС. Основные компоненты»	7	4	4/1И		4	Самостоятельная работа с интернет-источниками и учебно-методической литературой	Устный опрос	ПК-23 з
5.2. Тема «Модели безопасности в различных семействах ОС»	7	4	4/1И		4	Самостоятельная работа с интернет-источниками и учебно-методической литературой	Устный опрос	ПК-23 зув
5.3. Тема «Дискреционный и мандатный принципы управления доступом – сравнительный анализ»	7	4	4/1И		4	Самостоятельная работа с интернет-источниками и учебно-методической литературой	Устный опрос	ПК-23 зув
Итого по разделу	7	12	12/3И		12			ПК-23 зув
6. Раздел «Администрирование операционных систем»								
6.1. Тема «Модели пользователей в различных ОС»	7	4	4/2И		4	Самостоятельная работа с интернет-источниками и учебно-методической литературой	Выполнение лабораторной работы «Создание пользователя ОС Linux»	ПК-23 зув
6.2. Профиль пользователя, бюджет, авторизация, аутентификация	7	4	4/2И		4	Самостоятельная работа с интернет-источниками и	Выполнение лабораторной работы «Создание	ПК-23 зув

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	лабораторн.	практич. занятия				
пользователя ОС						учебно-методической литературой	пользователя ОС Windows»	
6.3. Тема «Назначение прав пользователю ОС и аудит его действий»	7	4	4/2И		4	Самостоятельная работа с интернет-источниками и учебно-методической литературой	Выполнение лабораторной работы «Аудит действий пользователя ОС Windows»	ПК-23 зув
6.4. Тема «Аудит системных событий ОС»	7	4	4/2И		4	Самостоятельная работа с интернет-источниками и учебно-методической литературой		ПК-23 зув
Итого по разделу	7	16	16/8И		16			
7. Раздел «Противодействие атакам на информационные системы»							Устный опрос	ПК-25 зув
7.1. Тема «Методология атаки и их разновидности»	7	3	3/1И		4	Самостоятельная работа с интернет-источниками и учебно-методической литературой	Выполнение лабораторной работы «Работа со сканером уязвимостей»	ПК-25 зув
7.2. Тема «Методы обнаружения и предотвращения атак на информационные системы»	7	3	3/2И		4,3	Самостоятельная работа с интернет-источниками и учебно-методической литературой	Текущий контроль успеваемости	ПК-25 зув
Итого по разделу	7	6	6/3И		8,3			

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				
Подготовка к экзамену	**7**				**35,7**	**Подготовка к экзамену**		
Итого за семестр	**7**	**34**	**34/14 И**		**72**		**Итоговая аттестация (экзамен)**	
Итого по дисциплине		**51**	**68/28 И**		**92,05**		**Итоговая аттестация (зачет/экзамен)**	

5 Образовательные и информационные технологии

Для реализации предусмотренных видов учебной работы в качестве образовательных технологий в преподавании дисциплины «Безопасность операционных систем» 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 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 а так же с применением кейс-технологий.

Перечень лабораторных работ по курсу «Безопасность операционных систем»

Лабораторная работа №1.

Основные структурные элементы операционной системы. Отличительные свойства операционных систем на примере сравнения ОС семейства Microsoft Windows и Linux.

Лабораторная работа №2.

Загрузка ОС. Порядок загрузки ОС. Известные способы перехвата загрузки ОС. Понятие доверенной загрузки.

Лабораторная работа №3.

Файловые подсистемы ОС. Характеристики, разновидности, принципы организации. Известные уязвимости наиболее распространенных файловых систем.

Лабораторная работа №4.

Сетевая подсистема ОС. Принципы организации, основные структурные элементы.

Лабораторная работа №5.

Подсистема безопасности ОС. Сравнительный анализ подсистем безопасности ОС семейства Microsoft Windows и Linux.

Лабораторная работа №6.

Известные уязвимости наиболее популярных ОС. Принципы обнаружения уязвимостей, приемы использования, методы обнаружения и устранения уязвимостей ОС. Специализированное ПО для поиска и анализа уязвимостей ОС.

Лабораторная работа №7.

Использование встроенных межсетевых экранов на примере настройки межсетевого экрана Iptables ОС Linux.

Лабораторная работа №8.

Средства шифрования и их роль в современных ОС. Сравнительный анализ использования средств шифрования в различных ОС.

Примерный перечень индивидуальных домашних заданий

1. Исследование методов идентификации и аутентификации в ОС Windows.
2. Исследование методов идентификации и аутентификации в ОС Unix.
3. Исследование методов разграничение доступа к ресурсам в ОС Windows, Unix.
4. Настройка системы аудита в Windows.
5. Настройка системы аудита в Unix.

6. Изучение средств защиты сетевого взаимодействия Windows. Конфигурирование средств защиты каналов средствами Windows XP/2003/Vista, Windows Firewall. Виртуальные частные сети, протоколы L2TP и PPTP.

7 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	- основные определения и понятия, используемые в теории операционных систем; - современные подходы к организации и проведению научных исследований с использованием сетевых технологий; принципы построения и современные технологии, используемые в современных операционных системах, автоматизированных системах и сетях ЭВМ;	1. Принципы классификации операционных систем, их основные характеристики и функциональное назначение; 2. Основные структурные элементы и подсистемы операционной системы, их характеристики и функциональное назначение; 3. Принципы функционирования ядра, дисковой, файловой, сетевой подсистем операционной системы 4. Основные принципы построения подсистем безопасности операционных систем
Уметь	разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры; обосновать выбор решения по обеспечению требуемого уровня защиты ОС (ИС); готовить публикации по результатам выполненных работ;	1. Провести сравнительный анализ различных операционных систем с точки зрения защищенности информации; 2. Обосновать выбор операционной системы при построении информационной системы на ее базе;
	навыками использования операционных систем, информационных систем и сетевых технологий в	1. Навыками администрирования дисковой, файловой, сетевой подсистемами, подсистемой

Перечень теоретических вопросов к зачету:

1. Общее понятие безопасности операционных систем, история развития вопроса, характеристика подходов к обеспечению безопасности операционных систем.

2. Анализ угроз информационной безопасности. Методы обеспечения информационной безопасности. Классификация злоумышленников. Основные направления и методы реализации угроз информационной безопасности.

3. Операционная система с точки зрения специалиста по информационной безопасности

4. Общая концепция построения ОС, виды ОС, история развития, семейства ОС. Разграничение доступа в ОС. Идентификация и аутентификация пользователей ОС.

5. Разграничение доступа в ОС.

6. Субъекты, объекты, методы и права доступа. Привилегии субъектов доступа. Избирательное и полномочное разграничение доступа, изолированная программная среда. Примеры реализации разграничения доступа в современных ОС.

7. Формальная процедура установки прав доступа к системным сервисам и ресурсам.

8. Идентификация и аутентификация пользователей ОС.

9. Понятия идентификации и аутентификации пользователей. Аутентификация на основе паролей, методы подбора паролей, средства и методы повышения защищенности ОС от подбора паролей.

10. Аутентификация на основе внешних носителей ключа, биометрических характеристик пользователя. Примеры реализации идентификации и аутентификации в современных ОС.

11. Необходимость аудита. Требования к подсистеме аудита. Примеры реализации аудита в современных ОС.

12. Состав операционной системы. Группы компонентов ОС: ядро, пользовательская оболочка, файловая подсистема, сетевая подсистема.

13. Принципы организации многозадачной ОС. Виды многозадачности, технологии обеспечения многозадачности ОС.

14. Принципы организации межпрограммного взаимодействия.

Критерии оценки для получения зачета

«зачтено» – обучающийся показывает средний уровень сформированности компетенций.

«не зачтено» – результат обучения не достигнут, студент не может показать знания на уровне воспроизведения и объяснения информации, не может показать интеллектуальные навыки решения простых задач, не может показать знания на уровне воспроизведения и объяснения информации.

Перечень теоретических вопросов к экзамену:

1. Подсистема безопасности ОС. Модели безопасности в различных семействах ОС.
2. Анализ защищенности современных операционных систем. Встроенные средства защиты Windows, Unix.
3. Многопользовательские ОС. Методы авторизации и аутентификации пользователей. Известные уязвимости.
4. Обеспечение безопасности ОС – журналирование системных событий, системный аудит и анализ инцидентов. Угрозы безопасности информации в информационно-вычислительных системах.
5. Угрозы безопасности ОС.
6. Инциденты информационной безопасности.
7. Организация режима информационной безопасности.
8. Мониторинг информационной безопасности.
9. Понятие защищенной ОС. Подходы к организации защиты ОС и их недостатки. Этапы построения защиты. Административные меры защиты. Стандарты безопасности ОС.
10. Классификация требований к системам защиты. Формализованные требования к защите информации от НСД.
11. Общие подходы к построению систем защиты компьютерной информации.
12. Требования к защите ОС. Использование средств шифрования в современных ОС. Понятие криптоядра.
13. Сравнительный анализ использования средств шифрования в ОС семейства Microsoft Windows и Linux.
14. Анализ защищенности операционных систем семейства Windows.
15. Анализ защищенности операционных систем семейства Unix.

Критерии оценки (в соответствии с формируемыми компетенциями и планируемыми результатами обучения):

– на оценку «отлично» – студент должен показать высокий уровень знаний, умений и навыков в соответствии с формируемыми компетенциями; т.е. всесторонние,

систематизированные, глубокие знания учебной программы дисциплины и умение уверенно применять их на практике при решении конкретных задач, свободно и правильно обосновывать принятые решения;

– на оценку «хорошо» – студент должен показать средний уровень знаний, умений и навыков в соответствии с формируемыми компетенциями; т.е. твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике;

– на оценку «удовлетворительно» – студент должен показать пороговый уровень знаний, умений и навыков в соответствии с формируемыми компетенциями; т.е. владеет основными разделами учебной программы, необходимыми для дальнейшего обучения и может применять полученные знания по образцу в стандартной ситуации;

– на оценку «неудовлетворительно» – студент не может показать знания на уровне воспроизведения и объяснения информации, не умеет использовать полученные знания при решении типовых практических задач.

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