МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

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

УТВЕРЖДАЮ
Директор ИЭиАС
В.Р. Храмшин

13.02.2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

МЕТОДЫ ПРОЕКТИРОВАНИЯ СИСТЕМ ЗАЩИТЫ РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Направление подготовки (специальность)
10.05.03 Информационная безопасность автоматизированных систем

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

Уровень высшего образования - специалитет

Форма обучения
очная

Институт/ факультет	Институт энергетики и автоматизированных систем
Кафедра	Информатики и информационной безопасности
Курс	5
Семестр	9

Магнитогорск
2024 год

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

Рабочая программа рассмотрена и одобрена на заседании кафедры Информатики и информационной безопасности
09.02.2024, протокол № 4

Зав. кафедрой _____ И.И. Баранкова

Рабочая программа одобрена методической комиссией ИЭиАС
13.02.2024 г. протокол № 4

Председатель _____ В.Р. Храмшин

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

Рецензент:
Начальник отдела информационной безопасности «КУБ» (АО)
_____ М.М. Близнецов

Лист актуализации рабочей программы

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

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

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

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

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

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

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

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

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2029 - 2030 учебном году на заседании кафедры Информатики и информационной безопасности

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

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2030 - 2031 учебном году на заседании кафедры Информатики и информационной безопасности

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

1 Цели освоения дисциплины (модуля)

Целями изучения дисциплины «Методы проектирования защищенных распределенных информационных систем» являются: освоение моделей управления, получение знаний о закономерностях и свойствах процессов управления распределенными объектами, систематическое изучение основ теории и практики математического и имитационного моделирования систем; изучение основных подходов и математических схем к построению имитационных моделей; изучение возможностей применения имитационных моделей; освоение методологий и актуальных CASE-средств для имитационного моделирования систем и процессов в соответствии с требованиями ФГОС ВО по специальности 10.05.03 «Информационная безопасность автоматизированных систем».

2 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Методы проектирования систем защиты распределенных информационных систем входит в часть учебного плана формируемую участниками образовательных отношений образовательной программы.

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

Технология построения защищенных распределенных приложений

Математическое моделирование распределенных систем

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

Обеспечение информационной безопасности критической информационной инфраструктурой

Защита электронного документооборота

Моделирование систем защиты информации

Аттестация АИС

Разработка и эксплуатация автоматизированных систем в защищенном исполнении

Подготовка к процедуре защиты и процедура защиты выпускной квалификационной работы

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

В результате освоения дисциплины (модуля) «Методы проектирования систем защиты распределенных информационных систем» обучающийся должен обладать следующими компетенциями:

Код индикатора	Индикатор достижения компетенции
ПК-7 Способен разрабатывать проектные решения по защите информации в автоматизированных системах	
ПК-7.1	Разрабатывает модели угроз безопасности информации и модели нарушителя в автоматизированных системах
ПК-7.2	Выбирает меры защиты информации, подлежащие реализации в системе защиты информации автоматизированной системы
ПК-7.3	Определяет виды и типы средств защиты информации, обеспечивающих реализацию технических мер защиты информации
ПК-7.4	Определяет структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем

4. Структура, объём и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет 4 зачетных единиц 144 акад. часов, в том числе:

– контактная работа – 57,2 акад. часов:

– аудиторная – 54 акад. часов;

– внеаудиторная – 3,2 акад. часов;

– самостоятельная работа – 51,1 акад. часов;

– в форме практической подготовки – 0 акад. час;

– подготовка к экзамену – 35,7 акад. час

Форма аттестации - экзамен

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа студента	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код компетенции
		Лек.	лаб. зан.	практ. зан.				
1. Введение в распределенные системы								
1.1 Определение распределенной системы. Концепции аппаратных решений. Концепции программных решений. Модель клиент-сервер	9	1	2		4	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями);подготовка к тестированию	тестирование	ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4
Итого по разделу		1	2		4			
2. Связь и процессы в распределенных системах								

2.1 Уровни протоколов. Удаленный вызов процедур. Обращение к удаленным объектам.	9	1,5	3/0,6И		5	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к аудиторной контрольной работе (АКР); подготовка к тестированию	АКР; тестирование	ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4
2.2 Связь по средством сообщений. Связь на основе потоков данных.		0,5	2/1И		5	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к контрольной работе; подготовка к тестированию	АКР; тестирование	ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4
2.3 Потоки выполнения задач. Пользовательские интерфейсы. Серверы объектов		0,5	4/1И		5	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к тестированию	тестирование	ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4
Итого по разделу		2,5	9/2,6И		15			
3. Синхронизация компонент в распределённых системах								

3.1 Синхронизация часов. Логические часы.	9	1	2/1И		5	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к контрольной работе; подготовка к тестированию	АКР; тестирование	ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4
3.2 Глобальное состояние. Алгоритмы голосования. Взаимное исключение.		2	4/1И		6	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к контрольной работе; подготовка к тестированию	АКР; тестирование	ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4
3.3 Распределенные транзакции		0,5	4/1И		6	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к тестированию	тестирование	ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4
Итого по разделу		3,5	10/3И		17			
4. Непротиворечивость и репликация в распределенных системах								

4.1 Модели непротиворечивости, ориентированные на данные. Модели непротиворечивости, ориентированные на клиента.	9	2	4/2И		2,5	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к контрольной работе; подготовка к тестированию	АКР; тестирование	ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4
4.2 Протоколы распределения. Протоколы реплицируемой записи. Протоколы согласования кэшей.		2	4/2И		3,5	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к контрольной работе; подготовка к тестированию	тестирование	ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4
Итого по разделу		4	8/4И		6			
5. Защищенность распределенных систем								
5.1 Защищенные каналы. Аутентификация. Целостность и конфиденциальность сообщений. Защищенное групповое взаимодействие.	9	2	2/2И		2,1			ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4
5.2 Контроль доступа. Брандмауэры. Защита мобильного кода.		2	2/1И		3			ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4
5.3 Управление защитой. Управление ключами. Управление авторизацией.		3	3		4			ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4
Итого по разделу		7	7/3И		9,1			
6. Экзамен								
6.1 ВНКР	9							ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4

6.2 Экзамен								ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4
Итого по разделу								
Итого за семестр		18	36/12,6И		51,1		экзамен	
Итого по дисциплине		18	36/12,6 И		51,1		экзамен	

5 Образовательные технологии

Для реализации предусмотренных видов учебной работы в качестве образовательных технологий в преподавании дисциплины «Технология построения защищенных распределённых приложений» 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.

Формы учебных занятий с использованием традиционных технологий:

• обзорные лекции – для рассмотрения общих вопросов Информатики и информационных технологий, для систематизации и закрепления знаний;

• информационные – для ознакомления с техническими средствами реализации информационных процессов, со стандартами организации сетей, основными приемами защиты информации, и другой справочной информацией;

• лекции-визуализации – для наглядного представления способов решения алгоритмических и функциональных задач, визуализации результатов решения задач;

• Семинар.

• Практическое занятие, посвященное освоению конкретных умений и навыков по предложенному алгоритму.

Формы учебных занятий с использованием технологий проблемного обучения:

Проблемная лекция – изложение материала, предполагающее постановку проблемных и дискуссионных вопросов, освещение различных научных подходов, авторские комментарии, связанные с различными моделями интерпретации изучаемого материала

проблемная - для развития исследовательских навыков и изучения способов решения задач.

лекции с заранее запланированными ошибками – направленные на поиск обучающимися синтаксических и алгоритмических ошибок при решении алгоритмических и функциональных задач, с последующей диагностикой слушателей и разбором сделанных ошибок.

Практическое занятие в форме практикума – организация учебной работы, направленная на решение комплексной учебно-познавательной задачи, требующей от обучающегося применения как научно-теоретических знаний, так и практических навыков.

Практическое занятие на основе кейс-метода – обучение в контексте моделируемой ситуации, воспроизводящей реальные условия научной, производственной, общественной деятельности. Обучающиеся должны проанализировать ситуацию, разобраться в сути проблем, предложить возможные решения и выбрать лучшее из них. Кейсы базируются на реальном фактическом материале или же приближены к реальной ситуации

Формы учебных занятий с использованием игровых технологий:

Учебная игра – форма воссоздания предметного и социального содержания будущей профессиональной деятельности специалиста, моделирования таких систем отношений, которые характерны для этой деятельности как целого.

Деловая игра – моделирование различных ситуаций, связанных с выработкой и принятием совместных решений, обсуждением вопросов в режиме «мозгового

штурма», реконструкцией функционального взаимодействия в коллективе и т.п.

Технологии проектного обучения

Творческий проект – учебно-познавательная деятельность обучающихся осуществляется в рамках рамочного задания, подчиняясь логике и интересам участников проекта, жанру конечного результата (газета, фильм, праздник, издание, экскурсия, подготовка заданий конкурсов и т.п.).

Информационный проект – учебно-познавательная деятельность с ярко выраженной эвристической направленностью (поиск, отбор и систематизация информации о каком-то объекте, ознакомление участников проекта с этой информацией, ее анализ и обобщение для презентации более широкой аудитории).

6 Учебно-методическое обеспечение самостоятельной работы обучающихся

По дисциплине «Методы проектирования защищенных распределенных информационных систем» предусмотрена аудиторная и внеаудиторная самостоятельная работа обучающихся.

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

Аудиторная самостоятельная работа обучающихся на практических занятиях осуществляется под контролем преподавателя в виде решения задач и выполнения упражнений, которые определяет преподаватель для обучающихся.

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 индивидуальные домашние задания

Модуль 1. Введение в распределенные приложения.

Файловый сервер ¾ времени работает, а ¼ времени «лежит» по причине ошибок. Сколько реплик этого сервера должно быть сделано, чтобы его доступность составляла не менее 99%?

Модуль 2. Связь и процессы в распределенных системах

Примерный перечень вопросов для подготовки к тестированию обучающегося:

Гомогенные мультикомпьютерные системы.

Гетерогенные мультикомпьютерные системы.

Распределенные операционные системы.

Сетевые операционные системы.

Расширение модели RPC.

Дана корзина элементарных пакетов с максимальным размером элемента данных – 1000 байт, скоростью работы корзины 10 Мбайт/с, емкостью корзины – 1 Мбайт и максимальной скоростью передачи – 50 Мбайт/с. Как долго она сможет работать на максимальной скорости?

Модуль 3. Синхронизация компонент в распределенных системах

Разработать серверную программную компоненту, которая по протоколу HTTP будет передавать сигнал точного времени клиентским программным компонентам.

Разработать серверную программную компоненту осуществляющею контроль за состоянием кэша клиентов.

Модуль 4. Непротиворечивость и репликация в распределенных системах.

Вопросы для подготовки к аудиторной контрольной работе:

Опишите простую реализацию непротиворечивости чтения записей для отображения только что обновленных web-страниц.

Приведите пример, когда непротиворечивость, ориентированная на клиента, может привести к двойной записи данных на сервере.

Файл реплицирован на 10 серверах. Перечислите все комбинации кворумов чтения и записи, которые допускает алгоритм голосования.

Модуль 4. Защищенность распределенных систем

Реализовать простой алгоритм аутентификации с использованием подписей для криптосистемы с открытым кличем.

7 Оценочные средства для проведения промежуточной аттестации

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

Код индикатора	Индикатор достижения компетенции	Оценочные средства
ПК-7 Способен разрабатывать проектные решения по защите информации в автоматизированных системах		
ПК-7.1	Разрабатывает модели угроз безопасности информации и модели нарушителя в автоматизированных системах	1. На примере службы доменных имен укажите функциональные уровни программных компонент. 2. В чем опасность увеличения зоны ответственности программной компоненты распределенной системы? 3. Как применение принципа единой ответственности влияет на структуру программных компонент распределенной системы? 4. Укажите основные типы угроз ИБ в распределенной системе. 5. Укажите основные механизмы защиты распределенной системы от угроз ИБ
ПК-7.2	Выбирает меры защиты информации, подлежащие реализации в системе защиты информации автоматизированной системы	1. Укажите основные способы масштабирования распределенной системы. 2. Какие трудности могут возникнуть при масштабировании распределенной системы по размеру. 3. Укажите функционал пакетных менеджеров различных сред проектирования распределенных систем. 4. Укажите последовательность конфигурирования коммутаторов 2 и 3 уровней. 5. Назовите основные открытые интерфейсы по средствам которых осуществляется конфигурирование аппаратных средств.
ПК-7.3	Определяет виды и типы средств защиты информации, обеспечивающих реализацию технических мер защиты	Перечислить перечень основных структурных элементов применяемых при проектировании

	информации	комплекса средств по обеспечению ИБ распределённой системы Разработать программный документ по ГОСТ 19.101 на систему контроля сессией проекта Django
ПК-7.4	Определяет структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем	1. Разработать программную компоненту с применением библиотеки Django задачей, которой будет получение курса валют ЦБ на указанную дату или период и последующая визуализация полученных данных. 2. Выполнить моделирование аппаратной части распределенной системы торгового предприятия в соответствии с техническим заданием.

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.

Экзамен по данной дисциплине проводится в компьютерном классе по экзаменационным билетам, каждый из которых включает 1 теоретический вопрос и 2 практических задания.

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.

8 Учебно-методическое и информационное обеспечение дисциплины (модуля)

а) Основная литература:

1. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/422772(дата обращения: 01.02.2024).

2. Душкин, А. В. Методологические основы построения защищенных автоматизированных систем: Монография / Душкин А.В. - Воронеж:Научная книга, 2016. - 76 с. ISBN 978-5-4446-0902-6. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/923295 (дата обращения: 01.02.2024)

б) Дополнительная литература:

1. Брюхомицкий, Ю. А. Искусственные иммунные системы в информационной безопасности : учебное пособие / Ю. А. Брюхомицкий ; Южный федеральный университет. - Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2019. - 147 с. - ISBN 978-5-9275-3212-4. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/1088177 (дата обращения:01.02.2024)

2. Михайлова У. В. Безопасность корпоративной инфраструктуры : практикум [для вузов] / У. В. Михайлова, М. В. Афанасьева ; Магнитогорский гос. технический ун-т им. Г. И. Носова. - Магнитогорск : МГТУ им. Г. И. Носова, 2021. - 1 CD-ROM. - Загл. с титул. экрана. - URL: https://host.megaprolib.net/MP0109/Download/MObject/3254. - Текст : электронный.* МАКРООБЪЕКТ

*РЕЖИМ ПРОСМОТРА МАКРООБЪЕКТОВ

1. Перейти по адресу электронной библиотеки МГТУ им. Г. И. Носова https://host.megaprolib.net/MP0109/Web.

2. Произвести авторизацию на портале (логин: Фамилия на русском языке, пароль: номер читательского билета)

3. Активизировать гиперссылку макрообъекта.

в) Методические указания:

1. Методические указания по выполнению практических работ (Приложение 1)

2. Методические указания по выполнению внеаудиторных самостоятельных работ (Приложение 2)

г) Программное обеспечение и Интернет-ресурсы:

Программное обеспечение

Наименование ПО	№ договора	Срок действия лицензии
MS Office 2007	№ 135 от 17.09.2007	бессрочно
7Zip	свободно	бессрочно
MathCAD v.15 Education	Д-1662-13 от 22.11.2013	бессрочно
LibreOffice	свободно	бессрочно
Браузер	свободно	бессрочно
Браузер Mozilla	свободно распространя	бессрочно
MS Office 2003	№ 135 от 17.09.2007	бессрочно
NotePad++	свободно	бессрочно
Atom	свободно	бессрочно
FAR	свободно	бессрочно

Профессиональные базы данных и информационные справочные системы

Название курса	Ссылка
Электронные ресурсы библиотеки МГТУ им.	https://host.megaprolib.net/MP0109/Web
Информационная система - Банк данных	https://bdu.fstec.ru/?ysclid=lujkqy7cnw630508962
Информационная система - Нормативные правовые акты, организационно-распоря дительные документы,	https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-tzi?ysclid=lujknksfy724757053
Поисковая система Академия Google (Google	URL: https://scholar.google.ru/
Национальная информационно-аналити ческая система –	URL: https://elibrary.ru/project_risc.asp
Федеральное государственное бюджетное учреждение	URL: http://www1.fips.ru/
Электронная база периодических изданий	https://dlib.eastview.com/

9 Материально-техническое обеспечение дисциплины (модуля)

Материально-техническое обеспечение дисциплины включает:

1) Лаборатория программно-аппаратных средств обеспечения информационной безопасности (2124):

ПЭВМ на базе Windows 10 – 12 шт

2) Лекционная аудитория (ауд. 2124, ауд. 2113, ауд. 365, ауд. 388 и т.д.)- Мультимедийные средства хранения, передачи и представления информации

3) Компьютерный класс (ауд. 372, ауд. 245, ауд. 247, ауд. 144, ауд. 142 и т.д.) - Персональные компьютеры с ПО и выходом в Интернет и доступом в электронную информационно-образовательную среду университета.

4) Аудитория для самостоятельной работы: читальные залы библиотеки, ауд 132а

ПРИЛОЖЕНИЕ 1

Учебно-методическое обеспечение самостоятельной работы обучающихся

Перечень тем для подготовки к практическим занятиям:

Тема 1. Основные понятия информационной безопасности

– Понятие информационной безопасности.

– Основные составляющие информационной безопасности.

– Управление информационной безопасностью.

– Важность и сложность проблемы информационной безопасности.

Тема 2. Оценочные стандарты в информационной безопасности.

– Роль стандартов информационной безопасности.

– «Критерии определения безопасности компьютерных систем» как оценочный стандарт.

– Международный стандарт ISO/IEC 15408. Критерии оценки безопасности информационных систем.

Тема 3. Стандарты управления информационной безопасностью.

–Стандарты управления информационной безопасностью BS 7799 и ISO/IEC 17799.

–Международный стандарт ISO/IEC 27001:2005 "Системы управления информационной безопасности. Требования".

–Сертификация СУИБ на соответствие ISO 27001.

Тема 4. Создание СУИБ на предприятии.

–Этапы разработки и внедрения системы управления ИБ.

–Содержание этапов разработки и внедрения системы управления ИБ.

Тема 5. Методика оценки рисков информационной безопасности предприятия.

–Управление рисками. Основные понятия.

–Метод оценки рисков на основе модели угроз и уязвимостей.

Тема 6. Методика оценки рисков информационной организации.

– Метод оценки рисков на основе модели информационных потоков.

– Расчет рисков по угрозе конфиденциальность.

Тема 7. Методики и технологии управления рисками.

– Качественные методики управления рисками.

– Количественные методики управления рисками. Метод CRAMM.

Тема 8. Разработка корпоративной методики анализа рисков.

– Методы оценивания информационных рисков.

– Табличные методы оценки рисков.

– Оценка рисков по двум факторам.

– Разделение рисков на приемлемые и неприемлемые.

– Оценка рисков по трем факторам.

– Методика анализа рисков Microsoft.

Тема 9 Современные методы и средства анализа и управление рисками информационных систем.

– Методика FRAP.

– Методика OCTAVE.

– Методика RiskWatch.

Перечень контрольных вопросов по терминологии:

Угроза (Threat)

Уязвимость (Vulnerability)

• *Анализ рисков.*

Базовый уровень безопасности .

Базовый (Baseline) анализ рисков .

Полный (Full) анализ рисков.
Риск нарушения ИБ (Security Risk).
Оценка рисков (Risk Assessment).
Управление рисками (Risk Management).
Система управления ИБ (Information Security Management System).
Класс рисков.
Терминология COBIT
• *Риски*
Типы рисков.
Приемлемый уровень риска
Стандарт управления рисками.
Матрица ИТ рисков.
• *Руководство рисками*
Владелец процессов оценки рисков.
План работ по снижению рисков.
Политики и процедуры.
Обновление величин рисков.
Глобальный и системный уровни оценки ИТ- рисков.
Резюме для руководителя.
Стратегия управления ИТ
• *Идентификация*
Определение компонентов риска.
Области рисков.
Обновление матрицы рисков.
Меры оценки
Количественная оценка.
Качественная оценка.
• *Способы управления*
Независимое мнение.
Возврат инвестиций.
Баланс способов управления
Управление конфликтами.
• *Мониторинг*
Мониторинг используемых способов управления.
Процедура реагирования на инциденты.
Согласование плана работ по снижению рисков.

ПРИЛОЖЕНИЕ 2

Оценочные средства для проведения промежуточной аттестации

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

Код индикатора	Индикатор достижения компетенции	Оценочные средства
ПК-2 Способен разрабатывать требования по защите, формировать политики безопасности компьютерных систем и сетей		
ПК-2.1	Разрабатывает профили защиты компьютерных систем	1. Методика оценки рисков информационной безопасности компании. 2. Управление рисками. Перечислить основные понятия. 3. Метод оценки рисков на основе модели угроз и уязвимостей. 4. Расчет рисков по угрозе информационной безопасности. 5. Метод оценки рисков на основе модели информационных потоков. Задание: Провести расчеты оценки рисков информационной безопасности компании по методу оценки рисков на основе частной модели угроз.
ПК-2.2	Формирует политики безопасности компьютерных систем и сетей	***Задание*** Для заданного предприятия разработать: – карту информационных активов фирмы; – карты уязвимостей и угроз; – отчет о результатах оценки рисков; – план по обработке рисков; – частные политики безопасности.

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

– на оценку «**зачтено**» – обучающийся должен показать пороговый уровень знаний на уровне воспроизведения и объяснения информации;

– на оценку «**не зачтено**» – обучающийся не может показать знания на уровне воспроизведения и объяснения информации.

ПРИЛОЖЕНИЕ 3

Методические указания по выполнению практических работ

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, противопожарным мерам в компьютерном классе и специализированных лабораториях.

2. Обучаемый должен строго выполнять правила техники безопасности и санитарно-гигиенические нормы при работе в компьютерных классах и специализированных лабораториях 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 4

Методические указания по выполнению внеаудиторных самостоятельных работ

Общие положения

Настоящие методические указания предназначены для организации внеаудиторной самостоятельной работы студентов 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.

Виды внеаудиторной самостоятельной работы и формы контроля и время на выполнение каждого вида самостоятельной работы указаны в пункте 4. «Структура и содержание дисциплины» 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.
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: индивидуальные задания, аудиторные контрольные работы, компьютерное тестирование.

Максимальное количество баллов обучающийся получает, если:

– выполняет индивидуальные задания 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.