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

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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

МОДЕЛИРОВАНИЕ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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	4
Семестр	8

Магнитогорск
2017 г.

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

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

«03» марта 2017 г., протокол № 10.

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

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

«14» марта 2017 г., протокол № 6.

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

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

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

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

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

Лист регистрации изменений и дополнений

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

1 Цели освоения дисциплины (модуля)

Целями освоения дисциплины (модуля) «Моделирование угроз информационной безопасности» являются: выявление источников и способов реализации угроз информационной безопасности, разработка модели угроз с учетом различных факторов; исследование и оценка существующих моделей согласно требованиям стандартов информационной безопасности и нормативных документов ФСТЭК России.

2 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Моделирование угроз информационной безопасности входит в вариативную часть учебного плана образовательной программы.

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

Разработка и эксплуатация защищенных автоматизированных систем

Организационное и правовое обеспечение информационной безопасности

Методы выявления нарушений информационной безопасности, аттестация АИС

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

Анализ рисков информационной безопасности

Моделирование систем и процессов защиты информации

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

В результате освоения дисциплины (модуля) «Моделирование угроз информационной безопасности» обучающийся должен обладать следующими компетенциями:

Структурный элемент компетенции	Планируемые результаты обучения
ОПК-3 способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности	
Знать	- средства моделирования угроз информационной безопасности.
Уметь	- применять языки, системы и инструментальные средства программирования для моделирования угроз информационной безопасности.
Владеть	- навыками применения инструментальных средств программирования для моделирования угроз.
ПК-4 способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	
Знать	- основные источники угроз ИБ; - классификацию угроз информационной безопасности; - Типовую модель угроз информационной безопасности - Нормативно-методические документы в области моделирования угроз, - способы реализации угроз безопасности информации и модели нарушителя в автоматизированных системах;
Уметь	- Разрабатывать частную модель угроз автоматизированной системы - Определять актуальные угрозы для автоматизированной системы; - разрабатывать модель нарушителя информационной безопасности автоматизированных систем информационно-технологических ресурсов автоматизированных систем.

Владеть	- Навыками определения информационной инфраструктуры и информационных ресурсов организации, подлежащих защите; - Навыками разработки частных моделей угроз
ПСК-7.1 способностью разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах	
Знать	- нормативные правовые акты в области защиты информации; - национальные, межгосударственные и международные стандарты в области защиты информации; - руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации.
Уметь	- оценивать информационные риски в автоматизированных системах; - классифицировать и оценивать угрозы безопасности информации; - определять подлежащие защите информационные ресурсы автоматизированных систем; - анализировать изменения угроз безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации
Владеть	- методами выявления угроз безопасности информации в автоматизированных системах; - методами оценки последствий от реализации угроз безопасности информации в автоматизированной системе.

4. Структура, объём и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет 5 зачетных единиц 180 акад. часов, в том числе:

– контактная работа – 106,85 акад. часов:
– аудиторная – 102 акад. часов;
– внеаудиторная – 4,85 акад. часов
– самостоятельная работа – 37,45 акад. часов;
– подготовка к экзамену – 35,7 акад. часа

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								
1.1 Цели и задачи моделирования угроз ИБ Нормативные и правовые акты в области защиты информации	8	2		2/2И	2	Подготовка к практическому занятию. Самостоятельное изучение учебной и научной литературы. Работа с электронными библиотеками. Поиск дополнительной информации по заданной теме.	Текущий контроль успеваемости: – устный опрос (собеседование); – семинарские занятия;	ОПК-3, ПК-4, ПСК-7.1
Итого по разделу		2		2/2И	2			
2. Этапы моделирования угроз ИБ								
2.1 Выявление объектов информационной системы подлежащих защите. Определение источников угроз	8	4		4/2И	4	Подготовка к практическому занятию. Самостоятельное изучение учебной и научной литературы. Работа с электронными библиотеками. Поиск дополнительной информации по заданной теме	Текущий контроль успеваемости: – контрольные работы; – проверка индивидуальных заданий	ПК-4, ПСК-7.1

2.2 Наиболее часто реализуемые угрозы. Выявление способов реализации угроз		6		6/2И	4	Подготовка к практическому занятию. Самостоятельное изучение учебной и научной литературы. Работа с электронными библиотеками. Поиск дополнительной информации по заданной теме	Текущий контроль успеваемости: – устный опрос (собеседование); – контрольные работы; – проверка индивидуальных заданий	ПК-4, ПСК-7.1
2.3 Угрозы мобильным устройствам.		4		4/2И	4	Подготовка к практическому занятию. Самостоятельное изучение учебной и научной литературы. Работа с электронными библиотеками. Поиск дополнительной информации по заданной теме	Текущий контроль успеваемости: – устный опрос (собеседование); – контрольные работы; – семинарские занятия; – проверка индивидуальных заданий	ПК-4, ПСК-7.1
Итого по разделу		14		14/6И	12			
3. Описание информационной системы								
3.1 Угрозы за счет реализации ТКУИ	8	6		6/2И	4	Подготовка к практическому занятию. Самостоятельное изучение учебной и научной литературы. Работа с электронными библиотеками. Поиск дополнительной информации по заданной теме	Текущий контроль успеваемости: – устный опрос (собеседование); – контрольные работы; – проверка индивидуальных заданий	ПК-4, ПСК-7.1
3.2 Методики построение дерева угроз		4		4/2И	4	Подготовка к практическому занятию. Самостоятельное изучение учебной и научной литературы. Работа с электронными библиотеками.	Текущий контроль успеваемости: – проверка индивидуальных заданий	ПК-4, ПСК-7.1

3.3 Разработка с учетом реализованных защитных мер. Формирование перечня активов, определение их значимости для компании		6		6/4И	4	Подготовка к практическому занятию. Самостоятельное изучение учебной и научной литературы. Работа с электронными библиотеками. Поиск дополнительной информации по заданной теме	Текущий контроль успеваемости: – проверка индивидуальных заданий	ОПК-3, ПК-4, ПСК-7.1
Итого по разделу		16		16/8И	12			
4. Модель угроз ИСПДн информационной системы персональных данных								
4.1 Угрозы безопасности ПДн. Каналы реализации угроз безопасности ПДн.	8	6		6/2И	5,45	Подготовка к практическому занятию. Самостоятельное изучение учебной и научной литературы. Работа с электронными библиотеками. Поиск дополнительной информации по заданной теме	Текущий контроль успеваемости: – устный опрос (собеседование); – контрольные работы; – семинарские занятия; – проверка индивидуальных заданий	ПК-4, ПСК-7.1
4.2 Классификация угроз безопасности персональных данных по способу реализации		4		4/2И	4	Подготовка к практическому занятию. Самостоятельное изучение учебной и научной литературы. Работа с электронными библиотеками. Поиск дополнительной информации по заданной теме	Текущий контроль успеваемости: – устный опрос (собеседование); – контрольные работы; – семинарские занятия; – проверка индивидуальных заданий	ПК-4, ПСК-7.1
Итого по разделу		10		10/4И	9,45			
5. Основные законы распределения вероятностей для статистического моделирования угроз								

5.1 Ошибки, возникающие при моделировании угроз. Определение вероятности возникновения отдельных угроз. Программные средства моделирования угроз	8	9		9/2И	2	Подготовка к практическому занятию. Самостоятельное изучение учебной и научной литературы. Работа с электронными библиотеками. Поиск дополнительной информации по заданной теме	Текущий контроль успеваемости: – устный опрос (собеседование); – контрольные работы; – проверка индивидуальных заданий	ОПК-3, ПК-4, ПСК-7.1
Итого по разделу		9		9/2И	2			
Итого за семестр		51		51/22И	37,45		экзамен	
Итого по дисциплине		51		51/22И	37,45		экзамен	ОПК-3,ПК-4,ПСК-7.1

5 Образовательные технологии

Традиционные образовательные технологии ориентируются на организацию образовательного процесса, предполагающую прямую трансляцию знаний от преподавателя к обучающемуся (преимущественно на основе объяснительно-иллюстративных методов обучения). Учебная деятельность обучающегося носит в таких условиях, как правило, репродуктивный характер.

1) **Традиционная технология**, включающая в себя объяснение преподавателя на лекциях, самостоятельную работу с учебной и справочной литературой по дисциплине, выполнение заданий по методическим указаниям. Формы учебных занятий с использованием традиционных технологий:
   a) ***Вводная лекция*** – для целостного представления об учебном предмете и анализа учебно-методической литературы;
   b) ***Обзорные лекции*** – для систематизации научных знаний на высоком уровне с использованием ассоциативных связей в процессе представления и осмысления информации;
   c) ***Информационная лекция*** – последовательное изложение материала в дисциплинарной логике, осуществляемое преимущественно вербальными средствами (монолог преподавателя);
   d) ***Семинар*** – беседа преподавателя и обучающихся, обсуждение заранее подготовленных сообщений по каждому вопросу плана занятия с единым для всех перечнем рекомендуемой обязательной и дополнительной литературы;
   e) ***Практическое занятие***, посвященное освоению конкретных умений и навыков по предложенному алгоритму;
   f) ***Лабораторная работа*** – организация учебной работы с реальными материальными и информационными объектами, экспериментальная работа с аналоговыми моделями реальных объектов.

2) **Разделно-компетентностная технология**, включающая в себя жесткое структурирование содержания учебного материала, сопровождающаяся обязательными блоками домашних заданий, контрольных работ и тестированием по каждой теме содержания курса. Формы учебных занятий с использованием Разделно-компетентностной технологии:
   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.

3) **Интерактивные технологии –** организация образовательного процесса, которая предполагает активное и нелинейное взаимодействие всех участников, достижение на этой основе личностно значимого для них образовательного результата. Наряду со специализированными технологиями такого рода принцип интерактивности прослеживается в большинстве современных образовательных технологий. Интерактивность подразумевает субъект-субъектные отношения в ходе образовательного процесса и, как следствие, формирование саморазвивающейся информационно-ресурсной среды. Формы учебных занятий с использованием интерактивных технологий:
   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) ***Лекция «обратной связи»*** – лекция–провокация (изложение материала с заранее

запланированными ошибками), лекция-беседа, лекция-дискуссия, лекция-прессконференция.

d) ***Семинар-дискуссия*** – коллективное обсуждение какого-либо спорного вопроса, проблемы, выявление мнений в группе (межгрупповой диалог, дискуссия как спор-диалог).

e) ***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 с помощью типовых программных средств, обучающийся приобретет способность участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности;

f) ***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.

4) **Технологии проблемного обучения** – организация образовательного процесса, которая предполагает постановку проблемных вопросов, создание учебных проблемных ситуаций для стимулирования активной познавательной деятельности обучающихся. Формы учебных занятий с использованием технологий проблемного обучения:

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

b) ***Лекция «вдвоем» (бинарная лекция)*** – изложение материала в форме диалогического общения двух преподавателей (например, реконструкция диалога представителей различных научных школ, «ученого» и «практика» и т.п.).

c) ***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.

d) ***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. разбор результатов тематических контрольных работ, анализ ошибок, совместный поиск вариантов рационального решения учебной проблемы.

5) **Игровые технологии** – организация образовательного процесса, основанная на реконструкции моделей поведения Формы учебных занятий с использованием предложенных сценарных условий. Формы учебных занятий с использованием игровых технологий:

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

b) ***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.

c) ***Ролевая игра*** – имитация или реконструкция моделей ролевого поведения в предложенных сценарных условиях.

6) **Технологии проектного обучения** – организация образовательного процесса в соответствии с алгоритмом поэтапного решения проблемной задачи или выполнения

учебного задания. Проект предполагает совместную учебно-познавательную деятельность группы обучающихся, направленную на выработку концепции, установление целей и задач, формулировку ожидаемых результатов, определение принципов и методик решения поставленных задач, планирование хода работы, поиск доступных и оптимальных ресурсов, поэтапную реализацию плана работы, презентацию результатов работы, их осмысление и рефлексию. Основные типы проектов:

a) ***Исследовательский проект*** – структура приближена к формату научного исследования (доказательство актуальности темы, определение научной проблемы, предмета и объекта исследования, целей и задач, методов, источников, выдвижение гипотезы, обобщение результатов, выводы, обозначение новых проблем).
b) ***Творческий проект***, как правило, не имеет детально проработанной структуры; учебно-познавательная деятельность обучающихся осуществляется в рамках рамочного задания, подчиняясь логике и интересам участников проекта, жанру конечного результата (газета, фильм, праздник, издание, экскурсия и т.п.).
c) ***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).

7) **Информационно-коммуникационные образовательные технологии** – организация образовательного процесса, основанная на применении специализированных программных сред и технических средств работы с информацией. Формы учебных занятий с использованием информационно-коммуникационных технологий:

a) ***Лекция-визуализация*** – изложение содержания сопровождается презентацией (демонстрацией учебных материалов, представленных в различных знаковых системах, в т.ч. иллюстративных, графических, аудио- и видеоматериалов).

Практическое занятие в форме презентации – представление результатов проектной или исследовательской деятельности с использованием специализированных программных сред.

6 Учебно-методическое обеспечение самостоятельной работы обучающихся

Темы практических работ

1. Цели и задачи моделирования угроз ИБ
2. Нормативная база предметной области
3. Этапы моделирования угроз ИБ.
4. Описание структуры ИС,состав ИС, взаимосвязи между сегментами ИС, взаимосвязи с другими ИС и ИТКС, и условия функционирования ИС
5. Определение источников угроз. Выявление критических объектов информационной системы
6. Определение перечня угроз для каждого критического объекта
7. Способы реализации угроз
8. Разработка мер по защите ИС. Базовый набор мер;-адаптированный базовый набор мер; -уточненный адаптированный базовый набор мер
9. Оценка материального ущерба и других последствий возможной реализации угроз, ранжирование угроз по потенциальному ущербу
10. . Формирование перечня активов, определение их значимости для компании.
11. Составление модели нарушителя, типы нарушителей, категории нарушителей
12. Разработка модели информационной безопасности с учетом реализованных защитных мер.
13. Построение дерева угроз.
14. Источники угроз ИБ. Классификация источников угроз
15. Оценка вероятности реализации угроз
16. Классификация нарушителей

17. Оценка возможностей нарушителей
18. Потенциал нарушителя ИБ
19. Актуальные угрозы безопасности
20. Оценка степени ущерба
21. Структура модели угроз

Индивидуальное задание «Составление модели угроз для объекта информатизации»

- Определить перечень защищаемых ресурсов, состав персонала и категории доступа
- Определить класс (уровень защищенности от НСД) согласно РД ФСТЭК
- Определить угрозы безопасности информации на защищаемом объекте (Использовать Банк данных угроз безопасности информации)
- Определение «Угроза безопасности Пдн»
- Реализация угроз безопасности Пдн
- Источники угроз
- Определение «Нарушитель»
- Классификация нарушителей
- Порядок определения исходной степени защищенности
- Понятие «Частота (вероятность) реализации угрозы»
- Оценка ущерба от реализации угрозы

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-3 способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности		
Знать	- средства моделирования угроз информационной безопасности	Перечень вопросов к экзамену 1. Средства моделирования угроз 2. Средства для вычисления вероятности возникновения отдельных угроз. 3. Назовите основные законы распределения вероятностей для статистического моделирования угроз.
Уметь	- применять языки, системы и инструментальные средства программирования для моделирования угроз информационной безопасности.	Определить вероятность возникновения угрозы по полученным данным
Владеть	- навыками применения инструментальных средств программирования для моделирования угроз.	Провести прогнозирование атак на сервер объекта информатизации
ПК-4 способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы		
Знать	- основные источники угроз ИБ; - классификацию угроз информационной безопасности;	Перечень вопросов к экзамену 1. Угрозы мобильным устройствам. 2. Угрозы безопасности ПДн.

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
	- Типовую модель угроз информационной безопасности - Нормативно-методические документы в области моделирования угроз, - способы реализации угроз безопасности информации и модели нарушителя в автоматизированных системах;	3. Каналы реализации угроз безопасности ПДн. 4. Угрозы за счет реализации ТКУИ. 5. Классификация угроз безопасности персональных данных по способу реализации. 6. Общая характеристика уязвимостей информационной системы персональных данных. Классификация, Причины возникновения уязвимостей. 7. Наиболее часто реализуемые угрозы. 8. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. 9. Ошибки, возникающие при моделировании угроз.
Уметь	- Разрабатывать частную модель угроз автоматизированной системы - Определять актуальные угрозы для автоматизированной системы; - разрабатывать модель нарушителя информационной безопасности автоматизированных систем информационно-технологических ресурсов автоматизированных систем.	Задание 1.Определить источники угроз для объекта информатизации. 2. Сформировать список уязвимостей объекта защиты, которые могут быть использованы для реализации угроз. 3. Определить перечень угроз безопасности на основе имеющихся отечественных каталогов угроз. 4. Определить Типы и возможности нарушителей
Владеть	- Навыками определения информационной инфраструктуры и информационных ресурсов организации, подлежащих защите; - Навыками разработки частных моделей угроз	Задание 1. Составить частную модель угроз ПДн объекта информатизации 2. Построить дерево угроз АС. 3. Составить модель нарушителя
ПСК-7.1 способностью разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах		
Знать	- Нормативные правовые акты в области защиты информации - Национальные,	Перечень вопросов к экзамену 1. Назовите логические уровни АСУТП, предложенные в 31-ом

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
	межгосударственные и международные стандарты в области защиты информации - Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации - Выявление угроз безопасности информации в автоматизированных системах; - Порядок разработки модели угроз	приказе ФСТЭК России 2. Назовите группы технических средств, присущие каждому уровню 3. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных.
Уметь	- Оценивать информационные риски в автоматизированных системах - Классифицировать и оценивать угрозы безопасности информации - Определять подлежащие защите информационные ресурсы автоматизированных систем - Анализировать изменения угроз безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации	Задание: • Построить частную модель угроз ИБ для объекта защиты. • Составьте типизированный состав компонентов распределенной информационной системы • Определите источники угроз для АС • Сформировать список уязвимостей объекта защиты, которые могут быть использованы для реализации угроз. • Определить типы и возможности нарушителей в распределенной информационной системе
Владеть	- методами выявления угроз безопасности информации в автоматизированных системах - методами оценки последствий от реализации угроз безопасности информации в автоматизированной системе	Задание: • Построить дерево угроз ОИ имеющего выход в глобальную сеть; • Составить перечень актуальных угроз распределенной информационной системы. • Составить частную модель угроз для выбранного объекта информатизации

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

Примерная структура и содержание пункта:

Промежуточная аттестация по дисциплине «Моделирование угроз информационной безопасности» 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, 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. Баранкова И. И. Определение критически значимых ресурсов объекта защиты при составлении модели угроз информационной безопасности [Электронный ресурс] : учебное пособие / И. И. Баранкова, О. В. Пермякова ; МГТУ. - Магнитогорск : МГТУ, 2017. - 1 электрон. опт. диск (CD-ROM). - Режим доступа: https://magtu.informsystema.ru/uploader/fileUpload?name=3323.pdf&show=dcatalogues/1/1138331/3323.pdf&view=true . - Макрообъект*. - ISBN 978-5-9967-1031-7

2. Защита информации : учеб. пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 3-е изд. - Москва : РИОР: ИНФРА-М, 2019. - 400 с. - (Высшее образование). - DOI: https://doi.org/10.12737/1759-3. - ISBN 978-5-16-106478-8. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/1018901 (дата обращения: 26.02.2020)

*РЕЖИМ ПРОСМОТРА МАКРООБЪЕКТОВ

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

Примечание: при открытии макрообъектов учитывать особенности настройки антивирусной защиты

б) Дополнительная литература:

1. Модель угроз ПД. : Организационно-распорядительная документация по защите ПД [Электронный ресурс]. Национальный открытый университет «Интуит»/.- Режим доступа: http://www.intuit.ru/studies/courses/697/553/lecture2447 .- Заглавие с экрана.

2. Веселов, Г. Е. Менеджмент риска информационной безопасности: Учебное пособие / Веселов Г.Е., Абрамов Е.С., Шилов А.К. - Таганрог:Южный федеральный университет, 2016. - 107 с.: ISBN 978-5-9275-2327-5. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/997108 (дата обращения: 26.02.2020)

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 Windows 7 Professional(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
MS Office 2007 Professional	№ 135 от 17.09.2007	бессрочно
7Zip	свободно	бессрочно
FAR Manager	свободно распространяемое ПО	бессрочно
LibreOffice	свободно	бессрочно
Браузер Mozilla Firefox	свободно распространяемое ПО	бессрочно
Браузер Yandex	свободно	бессрочно
MS Office 2003 Professional	№ 135 от 17.09.2007	бессрочно
MS Windows XP Professional(для классов)	Д-1227-18 от 08.10.2018	11.10.2021

Профессиональные базы данных и информационные справочные системы

Название курса	Ссылка
Федеральная служба по техническому и экспортному контролю России (ФСТЭК России)	URL: www.fstec.ru
Федеральное государственное бюджетное учреждение «Федеральный институт промышленной собственности»	URL: http://www1.fips.ru/
Информационная система - Единое окно доступа к информационным ресурсам	URL: http://window.edu.ru/
Национальная информационно-аналитическая система – Российский индекс научного цитирования (РИНЦ)	URL: https://elibrary.ru/project_risc.asp

ПРИЛОЖЕНИЕ 1

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 2

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.