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)

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
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) «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.

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

Дисциплина «Моделирование угроз информационной безопасности» входит в вариативную часть блока 1 образовательной программы.

Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин: 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 «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 средства моделирования угроз информационной безопасности для решения практических задач обеспечения информационной безопасности;
Владеть	– навыками применения аппарата моделирования для решения прикладных теоретико-информационных задач
ПК-4 способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	
Знать	– Основные источники угроз ИБ и факторы, необходимые для учета при разработке модели ИБ – классификацию угроз информационной безопасности – перечень нормативных документов – Способы реализации угроз безопасности информации и модели нарушителя в автоматизированных системах
Уметь	– анализировать и оценивать угрозы информационной безопасности объекта; – разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем выявлять уязвимости информационно-технологических ресурсов автоматизированных

Структурный элемент компетенции	Планируемые результаты обучения
	систем
Владеть	– Навыками определения информационной инфраструктуры и информационных ресурсов организации, подлежащих защите; – навыками семантического моделирования данных – методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем
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 – Выявление угроз безопасности информации в автоматизированных системах
Уметь	– Оценивать информационные риски в автоматизированных системах – Обнаруживать нарушения правил разграничения доступа – 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 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

- промежуточный контроль - 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	занятиялаборат.	практич. занятия				
Тема 1. Цели и задачи моделирования угроз ИБ Нормативные и правовые акты в области защиты информации.	8	2		2/2	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 з ПК-4 з ПСК-7.1 з**
Тема 2. Этапы моделирования угроз ИБ. 2.1 Выявление объектов информационной системы подлежащих защите. Определение источников угроз.	8	4		4/2	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 зу ПСК-7.1 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	занятиялаборат.	практич. занятия				
2.2 Наиболее часто реализуемые угрозы. Выявление способов реализации угроз.	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 зув ПСК-7.1 зув**
2.3 Архитектура мобильного устройства и экосистемой их взаимодействия с внешним миром. Угрозы мобильным устройствам.	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: – устный опрос (собеседование); – контрольные работы; – семинарские занятия; – проверка индивидуальных заданий	**ПК-4 зу ПСК-7.1 зув**
Тема 3. Описание информационной системы 3.1 Описание используемых технических средств и их назначение. 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 зу ПСК-7.1 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	занятиялаборат.	практич. занятия				
3.2 Методики построение дерева угроз.	8	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 зу ПСК-7.1 зу**
Тема 4. Разработка модели информационной безопасности с учетом реализованных защитных мер. Формирование перечня активов, определение их значимости для компании .	8	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 зу ПК-4 зув ПСК-7.1 зув**
Тема 5. Общая характеристика уязвимостей информационной системы персональных данных. Классификация, Причины возникновения уязвимостей. 5.1 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 зув ПСК-7.1 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	занятиялаборат.	практич. занятия				
5.2 Классификация угроз безопасности персональных данных по способу реализации.	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: – устный опрос (собеседование); – контрольные работы; – семинарские занятия; – проверка индивидуальных заданий	**ПК-4 зув ПСК-7.1 зув**
Тема 6. Основные законы распределения вероятностей для статистического моделирования угроз. 6.1 Ошибки, возникающие при моделировании угроз. 6.2 Определение вероятности возникновения отдельных угроз. 6.3 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 зув ПК-4 зув ПСК-7.1 зув**
Итого по дисциплине	**8**	**51**		**51/22И**	**37,45**		**Промежуточная аттестация (экзамен)**	**ОПК-3 зув ПК-4 зув ПСК-7.1**

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	занятиялаборат.	практич. занятия				
								зув

И – в том числе, часы, отведенные на работу в интерактивной форме.

5 Образовательные и информационные технологии

1. 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.

Формы учебных занятий с использованием традиционных технологий:

Информационная лекция – последовательное изложение материала в дисциплинарной логике, осуществляемое преимущественно вербальными средствами (монолог преподавателя).

Семинар – беседа преподавателя и обучающихся, обсуждение заранее подготовленных сообщений по каждому вопросу плана занятия с единым для всех перечнем рекомендуемой обязательной и дополнительной литературы.

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

Лабораторная работа – организация учебной работы с реальными материальными и информационными объектами, экспериментальная работа с аналоговыми моделями реальных объектов.

2. 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:

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

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.).

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.

3. Игровые технологии – организация образовательного процесса, основанная на реконструкции моделей поведения в рамках предложенных сценарных условий.

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.

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

4. 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 рефлксию.

Основные типы проектов:

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).

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.).

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).

5. 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 специализированных интерактивных технологий:

Лекция «обратной связи» – лекция–провокация (изложение материала с заранее запланированными ошибками), лекция-беседа, лекция-дискуссия, лекция-прессконференция.

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

6. 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:

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. Выявление способов 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.

Контрольные вопросы по материалу «Методика определения угроз безопасности информации в ИС»

- Сферы определения методики.
- Цель определения угроз безопасности
- Кто организует процесс определения угроз
- Источники угроз ИБ. Классификация источников угроз
- Идентификация угроз
- Оценка вероятности реализации угроз
- Классификация нарушителей
- Оценка возможностей нарушителей
- Потенциал нарушителя ИБ
- Актуальные угрозы безопасности
- Оценки вероятности реализации угрозы
- Показатели проектной защищенности ИС
- Оценка степени ущерба
- 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__АС Защита от НСД Классификация АС и требования
- Определить угрозы безопасности информации на защищаемом объекте (Банк данных угроз безопасности информации)
- Составить согласно ФСТЭК Методика определения актуальных угроз модель нарушителя ИБ

Вопросы по материалу МЕТОДИКА ОПРЕДЕЛЕНИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

- Сферы определения методики.
- 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 опасности 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. Модель угроз персональных данных 2. Методика построения модели безопасности 3. Базовая модель угроз ФСТЭК 4. Модель угроз безопасности организации. Порядок составления, ответственность и полномочия.
Уметь	– применять средства моделирования угроз информационной безопасности для решения практических задач обеспечения информационной безопасности;	Задание «Составление модели угроз для объекта информатизации согласно базовым моделям угроз ФСЭК»
Владеть	– навыками применения аппарата моделирования для решения прикладных теоретико-информационных задач	Задание «Составление модели угроз объекта защиты согласно требованиям методики ФСТЭК и банка данных угроз безопасности информации»
ПК-4 способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы		
Знать	– Основные источники угроз ИБ и факторы, необходимые для учета при разработке модели ИБ – классификацию угроз информационной безопасности – перечень нормативных документов – Способы реализации угроз безопасности информации и модели нарушителя в	Перечень вопросов к экзамену 1. Угрозы мобильным устройствам. 2. Архитектура мобильного устройства и экосистемой их взаимодействия с внешним миром. 3. Угрозы безопасности ПДн. 4. Каналы реализации угроз безопасности ПДн. 5. Угрозы за счет реализации ТКУИ. 6. Классификация угроз безопасности персональных данных по способу реализации.

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
	автоматизированных системах	7. Общая характеристика уязвимостей информационной системы персональных данных. Классификация, Причины возникновения уязвимостей. 8. Наиболее часто реализуемые угрозы. 9. Организационно-распорядительная документация по защите ПДн. 10. Положение по обеспечению безопасности ПДн. 11. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. 12. Средства моделирования угроз. 13. Ошибки, возникающие при моделировании угроз. 14. Определение вероятности возникновения отдельных угроз. 15. Основные законы распределения вероятностей для статистического моделирования угроз.
Уметь	– анализировать и оценивать угрозы информационной безопасности объекта; – разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем выявлять уязвимости информационно-технологических ресурсов автоматизированных систем	Задание 1. Составить модель угроз для объекта информатизации согласно базовым моделям угроз ФСЭК. 2. Построить дерево угроз обьекта КИИ.
Владеть	– Навыками определения информационной инфраструктуры и информационных ресурсов организации, подлежащих защите; – навыками семантического моделирования данных – методами мониторинга и аудита, выявления угроз информационной	Задание 1. Составить модель угроз объекта защиты согласно требованиям методики ФСТЭК и банка данных угроз безопасности информации. 2. Построить дерево угроз АС.

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
	безопасности автоматизированных систем	
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 – Выявление угроз безопасности информации в автоматизированных системах	Перечень вопросов к экзамену 1. Угрозы мобильным устройствам. 2. Архитектура мобильного устройства и экосистемой их взаимодействия с внешним миром. 3. Угрозы безопасности ПДн. 4. Каналы реализации угроз безопасности ПДн. 5. Угрозы за счет реализации ТКУИ. 6. Классификация угроз безопасности персональных данных по способу реализации. 7. Общая характеристика уязвимостей информационной системы персональных данных. Классификация, Причины возникновения уязвимостей. 8. Наиболее часто реализуемые угрозы. 9. Организационно-распорядительная документация по защите ПДн. 10. Положение по обеспечению безопасности ПДн. 11. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. 12. Средства моделирования угроз. 13. Ошибки, возникающие при моделировании угроз. 14. Определение вероятности возникновения отдельных угроз. 15. Основные законы распределения вероятностей для статистического моделирования угроз.
Уметь	– Оценивать информационные риски в автоматизированных системах – Обнаруживать нарушения правил разграничения доступа	Задание: • Построить частную модель угроз ИБ для объекта защиты. • Построить дерево угроз организации, обрабатывающей ПДн.

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
	– 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	Задание: • Построить дерево угроз ОИ имеющего выход в глобальную сеть; • Составить перечень актуальных угроз согласно БДУ ФСТЭК.

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. Девянин, П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками : учеб. пособие для вузов / П.Н. Девянин .— 2-е изд., испр. и доп. — М. : Горячая линия – Телеком, 2013 .— 339 с. — ISBN 978-5-9912-0328-9 . — Режим доступа: http://ibooks.ru/reading.php?productid=344413

б) Дополнительная литература:

1. УнижаевН.В. Информационно-аналитическое обеспечение безопасности организации: учебное пособие/Унижаев Н.В.–СПб.: Издательскийцентр «Интермедия», 2018.–408с. https://ibooks.ru/reading.php?productid=356934
2. Царегородцев А. В., Тараскин М. М. Методы и средства защиты информации в государственном управлении : учебное пособие. — Москва : Проспект, 2017. — 208 с. https://ibooks.ru/reading.php?productid=356008
3. 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.
4. Грибанова-Подкина М.Ю. Построение модели угроз информационной безопасности информационной системы с использованием методологии объектно-ориентированного проектирования // Вопросы безопасности. — 2017. - № 2. - С.25-34. DOI: 10.7256/2409-7543.2017.2.22065. URL: http://e-notabene.ru/nb/article_22065.html
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. 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.
8. Федеральный закон «Об информации, информационных технологиях и защите информации» от 27 июля 2006 г. № 149-ФЗ.
9. Причинно-следственные связи. Определение и алгоритм построения.- 2010 г. http://artofbusiness.ru/2010/04/prichinno-sledstvennye-svyazi-opredelenie-i-algoritm-postroeniya/

в) Программное обеспечение и Интернет-ресурсы:

1. ЭБС "КОНСУЛЬТАНТ СТУДЕНТА" http://www.studentlibrary.ru/catalogue/switch_kit/x2016-034.html
2. Банк данных угроз безопасности информации [Электронный ресурс] – Режим доступа: https://bdu.fstec.ru .– Загл. с экрана. Яз. рус.
3. 1. Журнал Information Security. Информационная безопасность: периодич. интернет-

изд. URL: http://www.itsec.ru/articles2/allpubliks – Загл. с экрана. Яз. рус.
4. 2. Журнал «Безопасность информационных технологий» : периодич. интернет-изд. URL: http://www.pvti.ru/articles_18.htm – Загл. с экрана. Яз. рус.
5. 3. Журнал «Вопросы кибербезопасности»: периодич. интернет-изд. URL: http://cyberrus.com/ – Загл. с экрана. Яз. рус.
6. 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.
7. 5. Государственная публичная научно-техническая библиотека России [Электронный ресурс] / – Режим доступа: http://www.gpntb.ru , свободный.– Загл. с экрана. Яз. рус.
8. 6. Российская национальная библиотека. [Электронный ресурс] / –URL: http://www.nlr.ru . Яз. рус.
9. 7. Безопасник [Электронный ресурс] – Режим доступа: http://www.безопасник.рф .– Загл. с экрана. Яз. рус.
10. 8. Компьтерра: все новости про компьютеры, железо, новые технологии, информационные технологии [Электронный ресурс]. – Периодическое электронное Интернет-издание – Режим доступа: http://www.computerra.ru/ – Загл. с экрана. Яз. рус.
11. 9. ФСТЭК России [Электронный ресурс] – Режим доступа: http://fstec.ru/ .– Загл. с экрана. Яз. рус.

9 Материально-техническое обеспечение дисциплины

Тип и название аудитории	Оснащение аудитории
Лекционная аудитория (ауд. 2124, ауд. 226, 309а, ауд. 365, ауд. 388 и т.д.)	Мультимедийные средства хранения, передачи и представления информации
Компьютерный класс (ауд. 372, ауд. 245, ауд. 247, ауд. 144, ауд. 142 и т.д.)	Персональные компьютеры с ПО: Операционная система MS Windows 7 (Microsoft Imagine Premium D-1227-18 от 08.10.2018 до 08.10.2021); Пакет MS Office 2007 (Microsoft Open License 42649837, бессрочная); Выход в Интернет и доступ в электронную информационно-образовательную среду университета.
Аудитория для самостоятельной работы читальные залы библиотеки, ауд 132а	Персональные компьютеры с ПО: Операционная система MS Windows 7 (Microsoft Imagine Premium D-1227-18 от 08.10.2018 до 08.10.2021); Пакет MS Office 2007 (Microsoft Open License 42649837, бессрочная); Выход в Интернет и доступ в электронную информационно-образовательную среду университета.