МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Воронежский государственный технический университет»

УТВЕРЖДАЮ
Декан факультета _____ С.М. Пасмурнов
«31» августа 2017 г.

РАБОЧАЯ ПРОГРАММА
дисциплины

«Математические основы управления рисками»

Специальность 10.05.03 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Специализация Обеспечение информационной безопасности распределенных информационных систем

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет

Форма обучения очная

Год начала подготовки 2017

Автор программы _____ /Чопоров О.Н./

Заведующий кафедрой Систем информационной безопасности _____ /А.Г. Остапенко/

Руководитель ОПОП _____ /А.Г. Остапенко/

Воронеж 2017

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели дисциплины обеспечить будущими инженерам, базовые знания и умения в области математических основ управления рисками информационной безопасности для изучения последующих дисциплин

1.2. Задачи освоения дисциплины

системное знакомство с основами менеджмента риска информационной безопасности;

знакомство со стандартами в области управления рисками информационной безопасности;

знакомство с инструментальными средствами для управления рисками;

изучение основ принятия решений при управлении рисками информационной безопасности;

изучение методов экспертных оценок и возможностей их использования при управлении рисками информационной безопасности;

знакомство с детерминированными и статистическими моделями и методами принятия решений;

знакомство с основными методами оптимизации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Математические основы управления рисками» относится к дисциплинам вариативной части (дисциплина по выбору) блока Б1.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Математические основы управления рисками» направлен на формирование следующих компетенций:

ПК-2 - способностью создавать и исследовать модели автоматизированных систем;

ПК-5 - способностью проводить анализ рисков информационной безопасности автоматизированной системы;

ПК-6 - способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ПК-2	знать способы формализации задач принятия решений при управлении рисками информационной безопасности
	уметь осуществлять постановку задачи принятия решений при управлении информационными рисками и выбор адекватного математического аппарата для ее решения
	владеть навыками формализации в виде математической модели практических задач принятия решений при

	выборе эффективных защитных мер
ПК-5	знать основы менеджмента риска информационной безопасности технологию оценки и анализ рисков в соответствии с современными стандартами
	уметь проводить оценку, анализ и управление рисками информационной безопасности в соответствии с современными стандартами в области менеджмента рисков
	владеть методикой менеджмента рисков информационной безопасности
ПК-6	знать методы выбора рациональных решений при управлении рисками информационной безопасности
	уметь применять математические методы принятия решений при управлении рисками информационной безопасности
	владеть математическим аппаратом принятия решений при управлении рисками информационной безопасности

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Математические основы управления рисками» составляет 6 з.е.

Распределение трудоемкости дисциплины по видам занятий

очная форма обучения

Виды учебной работы	Всего часов	Семестры	
		5	6
Аудиторные занятия (всего)	134	54	80
В том числе:			
Лекции	76	36	40
Лабораторные работы (ЛР)	58	18	40
Самостоятельная работа	46	18	28
Курсовой проект	+		+
Часы на контроль	36	-	36
Виды промежуточной аттестации - экзамен, зачет	+	+	+
Общая трудоемкость: академические часы зач.ед.	 216 6	 72 2	 144 4

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Содержание разделов дисциплины и распределение трудоемкости по видам занятий

очная форма обучения

№ п/п	Наименование темы	Содержание раздела	Лекц	Лаб. зан.	СРС	Всего, час
1	Основные термины и определения. Система менеджмента информационной безопасности (СМИБ)	Основные термины и определения в области управления рисками информационной безопасности. ГОСТ Р ИСО/МЭК 27000–2012 «Информационная технология «Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология». Система менеджмента информационной безопасности (СМИБ). Процессный подход в СМИБ (модель PDCA). Связи между процессами модели PDCA.	4	2	2	8
2	Менеджмент риска информационной безопасности	Задачи менеджмента риска информационной безопасности. Основные этапы менеджмента риска информационной безопасности. Установление контекста. Идентификация риска. Определение активов. Реестр информационных активов. Определение угроз. Профиль и жизненный цикл угрозы. Определение существующих мер и средств контроля и управления. Выявление уязвимостей. Определение последствий. Количественная оценка риска. Реестр информационных рисков. Обработка риска информационной безопасности. Снижение риска. Сохранение риска. Предотвращение риска. Перенос риска. Мониторинг и переоценка риска информационной безопасности.	16	8	8	32
3	Стандарты в области управления рисками информационной безопасности	ГОСТ Р ИСО/МЭК 17799-2005; ГОСТ Р ИСО/МЭК 27005-2010; NIST 800-30; BS 7799-3: 2006	2	-	2	4
4	Инструментальные средства для управления рисками	Обзор систем OCTAVE; CRAMM; RiskWatch; COBRA; RA2 the art of risk; vsRisk; Callio Secura 17799; Proteus Enterprise.	2	2	2	6
5	Основы принятия решений при управлении рисками информационной безопасности	Основные понятия и обобщенная классификация задач принятия решений. Формальное описание моделей принятия решений.	2	-	2	4
6	Методы экспертных оценок	Основные типы шкал. Методы проведение экспертизы Отбор экспертов и их характеристика. Оценка компетентности экспертов. Оценка согласованности мнений экспертов. Коэффициент ранговой корреляции Спирмена. Коэффициент конкордации Кэндалла. Энтропийный коэффициент конкордации. Обработка экспертной информации на основе метода парных сравнений.	10	6	2	18
7	Детерминированные модели и методы принятия решений	Постановка многокритериальных задач принятия решений. Характеристики приоритета критериев. Нормализация критериев. Принципы оптимальности в задачах принятия решений. Постановка задач оптимизации на основе комбинирования принципов оптимальности. Теория полезности. Аксиоматические методы многокритериальной оценки. Метод аналитической иерархии. Методы порогов несравнимости ЭЛЕКТРА.	20	20	8	48
8	Статистические модели и	Статистическая модель однокритериального	12	12	10	34

	методы принятия решений в условиях неопределенности	принятия решений в условиях неопределенности. Построение критериев оценки и выбора решений при известном распределении вероятностей состояния внешней среды (критерий Байеса-Лапласа, критерий минимума среднего квадратического отклонения функции полезности или функции потерь, критерий максимизации вероятности распределения функции полезности, модальный критерий, критерий минимума энтропии математического ожидания функции полезности, критерий Гермейера). Построение критериев оценки и выбора решений при активном противодействии среды (максиминный критерий Вальда, критерии минимаксного риска Сэвиджа). Построение критериев оценки и выбора решений при наличии приблизительной априорной информации о состояниях среды (критерий Гурвица, критерий Ходжеса-Лемана).				
9	Методы оптимизации	Классификация задач оптимизации. Постановка задачи линейного программирования. Методы решения. Симплекс-метод. Задача линейного программирования с булевыми переменными. Метод ветвей и границ. Методы решения многокритериальных задач оптимизации.	8	8	10	26
		Итого	**76**	**58**	**46**	**180**

5.2 Перечень лабораторных работ

1. Разработка реестра информационных активов
2. Разработка реестра информационных рисков и плана их обработки
3. Изучение систем OCTAVE; CRAMM.
4. Изучение метода априорного ранжирования
5. Построение множества Парето
6. Использование различных принципов оптимальности в задачах принятия решений
7. Построение функции полезности
8. Метод аналитической иерархии
9. Метод порогов несравнимости ЭЛЕКТРА I
10. Построение критериев оценки и выбора решений при известном распределении вероятностей состояния внешней среды
11. Построение критериев оценки и выбора решений при активном противодействии среды
12. Построение критериев оценки и выбора решений при неопределенной ситуации
13. Формирование оптимизационной модели в зависимости от вида целевой функции и ограничений. Методы решения многокритериальных задач оптимизации.
14. Задача «о ранце» и ее решение методом ветвей и границ

6. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ ПРОЕКТОВ (РАБОТ) И КОНТРОЛЬНЫХ РАБОТ

В соответствии с учебным планом освоение дисциплины предусматривает выполнение курсового проекта в 6 семестре для очной

формы обучения.

Примерная тематика курсового проекта: «Разработка системы управления информационными рисками страхового агентства «Цунами»

Задачи, решаемые при выполнении курсового проекта:

• разработка системы управления информационными рисками организации (в соответствии со стандартом ГОСТ Р ИСО/МЭК 27005-2010);

• реализация одного из методов принятия решений или оптимизационной модели для выбора мер и средств контроля и управления;

• разработка примеров решения задачи выбора.

Курсовой проект включат в себя графическую часть и расчетно-пояснительную записку.

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

7.1.1 Этап текущего контроля

Результаты текущего контроля знаний и межсессионной аттестации оцениваются по следующей системе:

«аттестован»;

«не аттестован».

Компе-тенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Аттестован	Не аттестован
ПК-2	знать способы формализации задач принятия решений при управлении рисками информационной безопасности	знает способы формализации задач принятия решений при управлении рисками информационной безопасности	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь осуществлять постановку задачи принятия решений при управлении информационными рисками и выбор адекватного математического аппарата для ее решения	умеет осуществлять постановку задачи принятия решений при управлении информационными рисками и выбор адекватного математического аппарата для ее решения	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть навыками формализации в виде математической модели практических задач принятия решений при выборе эффективных защитных мер	владеет навыками формализации в виде математической модели практических задач принятия решений при выборе эффективных защитных мер	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-5	знать основы менеджмента риска информационной безопасности	знает основы менеджмента риска информационной безопасности технологию оценки и анализ рисков в	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих

	технологию оценки и анализ рисков в соответствии с современными стандартами	соответствии с современными стандартами		программах
	уметь проводить оценку, анализ и управление рисками информационной безопасности в соответствии с современными стандартами в области менеджмента рисков	умеет проводить оценку, анализ и управление рисками информационной безопасности в соответствии с современными стандартами в области менеджмента рисков	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть методикой менеджмента рисков информационной безопасности	владеет методикой менеджмента рисков информационной безопасности	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-6	знать методы выбора рациональных решений при управлении рисками информационной безопасности	знает методы выбора рациональных решений при управлении рисками информационной безопасности	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь применять математические методы принятия решений при управлении рисками информационной безопасности	умеет применять математические методы принятия решений при управлении рисками информационной безопасности	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть математическим аппаратом принятия решений при управлении рисками информационной безопасности	владеет математическим аппаратом принятия решений при управлении рисками информационной безопасности	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 5, 6 семестре для очной формы обучения по двух/четырехбалльной системе:

«зачтено»

«не зачтено»

Компе-тенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Зачтено	Не зачтено
ПК-2	знать способы формализации задач принятия решений при управлении рисками информационной безопасности	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	уметь осуществлять постановку задачи принятия решений при управлении	Решение стандартных практических задач	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены

	информационными рисками и выбор адекватного математического аппарата для ее решения			
	владеть навыками формализации в виде математической модели практических задач принятия решений при выборе эффективных защитных мер	Решение прикладных задач в конкретной предметной области	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены
ПК-5	знать основы менеджмента риска информационной безопасности технологию оценки и анализ рисков в соответствии с современными стандартами	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	уметь проводить оценку, анализ и управление рисками информационной безопасности в соответствии с современными стандартами в области менеджмента рисков	Решение стандартных практических задач	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены
	владеть методикой менеджмента рисков информационной безопасности	Решение прикладных задач в конкретной предметной области	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены
ПК-6	знать методы выбора рациональных решений при управлении рисками информационной безопасности	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	уметь применять математические методы принятия решений при управлении рисками информационной безопасности	Решение стандартных практических задач	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены
	владеть математическим аппаратом принятия решений при управлении рисками информационной безопасности	Решение прикладных задач в конкретной предметной области	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены

или

«отлично»;

«хорошо»;

«удовлетворительно»;

«неудовлетворительно».

Компе-тенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Отлично	Хорошо	Удовл.	Неудовл.
ПК-2	знать способы формализации задач принятия решений при управлении рисками информационной безопасности	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	уметь осуществлять постановку задачи принятия решений при управлении информационными рисками и выбор адекватного математического аппарата для ее решения	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
	владеть навыками формализации в виде математической модели практических задач принятия решений при выборе эффективных защитных мер	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
ПК-5	знать основы менеджмента риска информационной безопасности технологию оценки и анализ рисков в соответствии с современными стандартами	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	уметь проводить оценку, анализ и управление рисками информационной безопасности в соответствии с современными стандартами в области менеджмента рисков	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
	владеть методикой менеджмента рисков информационной безопасности	Решение прикладных задач в конкретной предметной	Задачи решены в полном объеме и получены	Продемонстрирован верный ход решения всех, но не получен	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены

		области	верные ответы	верный ответ во всех задачах		
ПК-6	знать методы выбора рациональных решений при управлении рисками информационной безопасности	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	уметь применять математические методы принятия решений при управлении рисками информационной безопасности	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
	владеть математическим аппаратом принятия решений при управлении рисками информационной безопасности	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены

7.2 Примерный перечень оценочных средств (типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности)

7.2.1 Примерный перечень заданий для подготовки к тестированию

1. Какие имеются типы активов?

- информация, программное обеспечение, материальные активы, услуги, люди, нематериальные активы;

- информация, электронные и бумажные носители, программное и аппаратное обеспечение;

- информация и данные, бизнес-процессы, программное обеспечение, материальные активы.

2. Какие стандарты посвящены вопросам менеджмента рисков информационной безопасности (отметьте все правильные ответы)?

- ГОСТ Р ИСО/МЭК 27001-2006;
- ГОСТ Р ИСО/МЭК 27002-2012;
- ГОСТ Р ИСО/МЭК 27003-2012;
- **ГОСТ Р ИСО/МЭК 27005-2010;**
- **NIST-800.**

3. Отметьте синонимы термина «средство управления»?

- регулятор;
- **контрмера;**
- менеджмент;
- **мера безопасности.**

4. Что такое «оценивание риска»?
- правила, по которым оценивают значимость риска;
- процесс сравнения оценочной величины риска с установленным критерием риска с целью определения уровня значимости риска;
- общий процесс анализа риска и оценивания риска.
5. Что включает в себя менеджмент риска?
- политики, процедуры, рекомендации, практики или организационные структуры, которые могут носить административный, технический, управленческий или юридический характер;
- оценку риска, обработку риска, принятие риска, коммуникацию риска, мониторинг и обзор риска;
- анализ контекста, **оценку риска, обработку риска.**
6. Что включает в себя установление контекста системе менеджмента риска ИБ?
- определение основных критериев, области применения и границ, создание организационной структуры, занимающейся менеджментом риска ИБ;
- определение основных критериев, области применения и границ менеджмента риска;
- определение структуры организации, целей организации и происходящих в ней бизнес-процессов.
7. Сколько различных групп требований ИБ выделяется в стандарте ГОСТ Р ИСО/МЭК 27005-2010?
- 3;
- 4;
- 5.
8. Что включает в себя процесс оценки риска?
- анализ контекста, анализ бизнес-процессов, количественную оценку риска;
- **анализ риска и оценивание риска**;
- идентификацию риска и установление значения риска.
9. Какие этапы включает в себя идентификации риска?
- определение ценности активов; определение угроз; определение уязвимостей, оценку риска;
- определение активов; определение угроз; определение существующих мер и средств контроля и управления; выявление уязвимостей; определение последствий;
- сбор статистических данных об угрозах и уязвимостях, выявление рисков.
10. Что относится к основным активам?
- программы и данные;
- информация и бизнес-процессы;
- информация, программное и аппаратное обеспечение.

7.2.2 Примерный перечень заданий для решения стандартных задач

1. Расположите шкалы в порядке возрастания их информативности?

- порядковая шкала, номинальная шкала, шкала интервалов, шкала отношений;

- номинальная шкала, порядковая шкала, шкала интервалов, шкала отношений;

- номинальная шкала, порядковая шкала, шкала отношений, шкала интервалов;

- нет правильного варианта.

2. Какая шкала позволяет только классифицировать объекты?

- порядковая шкала;

- номинальная шкала;

- шкала отношений;

- шкала интервалов.

3. Какая шкала позволяет только классифицировать объекты?

- порядковая шкала;

- номинальная шкала;

- шкала отношений;

- шкала интервалов.

4. Перечислите наиболее распространенные методы измерений при экспертизе.

- ранжирование, непосредственная оценка, парное сравнение;

- анкетирование, интервьюирование, мозговой штурм;

- ранжирование, анкетирование, интервьюирование.

5. Какая шкала используется в процедуре ранжирования?

- номинальная;

- порядковая;

- отношений;

- интервалов.

6. Перечислите методы опроса экспертов.

- ранжирование, непосредственная оценка, парное сравнение;

- анкетирование, интервьюирование, дискуссия, морфологический анализ, мозговой штурм;

- ранжирование, анкетирование, интервьюирование.

7. Для чего используется коэффициент конкордации Кэндалла?

- оценка взаимосвязи альтернатив;

- оценка согласованности экспертов;

- оценка компетентности экспертов.

8. Какие способы нормализации критериев позволяют изменить их направленность?

- нормализация по заданному значению;

- относительная нормализация;

- сравнительная нормализация;

- естественная нормализация;

- нормализация Севиджа;

- полная нормализация.

9. Какие способы нормализации критериев позволяют получать значения в диапазоне от 0 до 1?

- нормализация по заданному значению;
- **относительная нормализация;**
- сравнительная нормализация;
- естественная нормализация;
- нормализация Севиджа;
- **полная нормализация.**

10. К какой группе методов принятия решений относится Метод аналитической иерархии?

- **детерминированный метод принятия решений;**
- стохастический метод принятия решений;
- нечеткий метод принятия решений.

7.2.3 Примерный перечень заданий для решения прикладных задач

1. При оценке 9 альтернатив по двум критериям группа экспертов дала следующие оценки в баллах.

Критерии	Альтернативы								
	x1	x2	x3	x4	x5	x6	x7	x8	x9
z1	9	7	2	4	3	2	1	4	8
z2	4	3	6	4	5	4	5	2	5

Считая, что наилучшими оценками по критериям являются те, которые имеют наибольшее число баллов, определить альтернативы, входящие в множество Парето

- x3, x4, x5, x9,
- **x1, x3, x9,**
- x1, x3, x5, x9,
- ни один вариант не является верным.

2. При оценке 9 альтернатив по двум критериям группа экспертов дала следующие оценки в баллах.

Критерии	Альтернативы								
	x1	x2	x3	x4	x5	x6	x7	x8	x9
z1	9	7	2	4	3	2	1	4	8
z2	4	3	6	4	5	4	5	2	5

Считая, что наилучшими оценками по критериям являются те, которые имеют наибольшее число баллов, определить наилучшую альтернативу с использованием принципа идеальной точки.

- x1,
- x3,
- x4,
- **x9,**
- ни один вариант не является верным.

3. При оценке 9 альтернатив по двум критериям группа экспертов дала следующие оценки в баллах.

Критерии	Альтернативы								
	x1	x2	x3	x4	x5	x6	x7	x8	x9
z1	9	7	2	4	3	2	1	4	8
z2	4	3	6	4	5	4	5	2	5

Считая, что наилучшими оценками по критериям являются те, которые имеют наибольшее число баллов, определить наилучшую альтернативу с использованием принципа антиидеальной точки.

- x1,

- x3,
- x4,
- x9,
- ни один вариант не является верным.

4. При оценке 9 альтернатив по двум критериям группа экспертов дала следующие оценки в баллах.

Критерии	Альтернативы								
	x1	x2	x3	x4	x5	x6	x7	x8	x9
z1	9	7	2	4	3	2	1	4	8
z2	4	3	6	4	5	4	5	2	5

Считая, что наилучшими оценками по критериям являются те, которые имеют наибольшее число баллов, определить наилучшую альтернативу с использованием принципа равенства.

- x1,

- x4,

- x9,
- ни один вариант не является верным.

5. При оценке 9 альтернатив по двум критериям группа экспертов дала следующие оценки в баллах.

Критерии	Альтернативы								
	x1	x2	x3	x4	x5	x6	x7	x8	x9
z1	9	7	2	4	3	2	1	4	8
z2	4	3	6	4	5	4	5	2	5

Считая, что наилучшими оценками по критериям являются те, которые имеют наибольшее число баллов, определить наилучшую альтернативу с использованием принципа максимина.

- x6,
- x7,

- x8,

- ни один вариант не является верным.

6. При оценке 9 альтернатив по двум критериям группа экспертов дала следующие оценки в баллах.

Критерии	Альтернативы								
	x1	x2	x3	x4	x5	x6	x7	x8	x9
z1	9	7	2	4	3	2	1	4	8
z2	4	3	6	4	5	4	5	2	5

Считая, что наилучшими оценками по критериям являются те, которые имеют наибольшее число баллов, определить наилучшую альтернативу с использованием принципа абсолютной уступки.

- x1,
- **x1 и x9;**
- x3,
- x9,
- ни один вариант не является верным.

7. При оценке 9 альтернатив по двум критериям группа экспертов дала следующие оценки в баллах.

Критерии	Альтернативы								
	x1	x2	x3	x4	x5	x6	x7	x8	x9
z1	9	7	2	4	3	2	1	4	8
z2	4	3	6	4	5	4	5	2	5

Считая, что наилучшими оценками по критериям являются те, которые имеют наибольшее число баллов, определить наилучшую альтернативу с использованием принципа относительной уступки.

- x1,
- x3,
- **x9,**
- ни один вариант не является верным.

8. При оценке 9 альтернатив по двум критериям группа экспертов дала следующие оценки в баллах.

Критерии	Альтернативы								
	x1	x2	x3	x4	x5	x6	x7	x8	x9
z1	9	7	2	4	3	2	1	4	8
z2	4	3	6	4	5	4	5	2	5

Считая, что наилучшими оценками по критериям являются те, которые имеют наибольшее число баллов, а первый критерий в 1,5 важнее второго, определить наилучшую альтернативу с использованием принципа главного критерия.

- **x1,**
- x3,
- x9,
- ни один вариант не является верным.

9. При оценке 9 альтернатив по двум критериям группа экспертов дала следующие оценки в баллах.

Критерии	Альтернативы								
	x1	x2	x3	x4	x5	x6	x7	x8	x9
z1	9	7	2	4	3	2	1	4	8
z2	4	3	6	4	5	4	5	2	5

Считая, что наилучшими оценками по критериям являются те, которые имеют наибольшее число баллов, а первый критерий в 1,5 важнее второго, определить наилучшую альтернативу с использованием лексикографического

принципа.

- x1,

- x3,

- x9,

- ни один вариант не является верным.

10. При оценке 9 альтернатив по двум критериям группа экспертов дала следующие оценки в баллах.

Критерии	Альтернативы								
	x1	x2	x3	x4	x5	x6	x7	x8	x9
z1	9	7	2	4	3	2	1	4	8
z2	4	3	6	4	5	4	5	2	5

Считая, что наилучшими оценками по критериям являются те, которые имеют наибольшее число баллов, а первый критерий в 3 раза важнее второго, определить наилучшую альтернативу с использованием принципа абсолютной уступки.

- x1,

- x3,

- x9,

- ни один вариант не является верным.

7.2.4 Примерный перечень вопросов для подготовки к зачету

1. Что представляет собой менеджмент риска информационной безопасности? Перечислите задачи менеджмента риска информационной безопасности.

2. Перечислите основные этапы менеджмента риска информационной безопасности и их взаимосвязи.

3. Что включает в себя этап установление контента? Перечислите основные критерии, необходимые для менеджмента риска ИБ.

4. В чем заключается и какие этапы включает в себя оценка риска ИБ?

5. В чем заключается и какие этапы включает в себя анализ риска ИБ?

6. В чем заключается идентификация риска ИБ? Перечислите этапы идентификации риска ИБ.

7. Что включает в себя идентификация активов? Перечислите основные виды активов.

8. Что представляют собой требования безопасности для активов?

9. Что включает в себя реестр информационных активов?

10. Каким образом может быть определена ценность активов? Приведите пример критериев и соответствующих шкал для оценки возможного ущерба.

11. Что такое профиль и жизненный цикл угрозы?

12. По каким признакам классифицируются угрозы информационной безопасности?

13. Какими способами может быть выполнена оценка вероятности угроз информационной безопасности?

14. Какими способами может быть выполнена оценка уязвимостей?

15. Каким образом может быть получена количественная оценка риска информационной безопасности?

16. Что включает в себя реестр рисков информационной безопасности?

17. В чем заключается оценивание рисков информационной безопасности?

18. Какие существуют варианты обработки риской информационной безопасности?

19. В чем заключается снижение риска информационной безопасности? Перечислите способы снижения рисков. Какие типичные ограничения должны быть учтены?

20. В чем заключается сохранение риска информационной безопасности? Перечислите факторы, влияющие не решение о принятии рисков.

21. В чем заключается предотвращение риска информационной безопасности? Перечислите основные способы предотвращения риска.

22. Что такое перенос риска информационной безопасности?

23. Какие задачи решаются в процессе коммуникации риска информационной безопасности?

24. Какие факторы подлежат мониторингу в процессе переоценки риска информационной безопасности?

7.2.5 Примерный перечень заданий для решения прикладных задач

1. Что представляет собой менеджмент риска информационной безопасности? Перечислите задачи менеджмента риска информационной безопасности.

2. Перечислите основные этапы менеджмента риска информационной безопасности и их взаимосвязи.

3. Что включает в себя этап установление контента? Перечислите основные критерии, необходимые для менеджмента риска ИБ.

4. В чем заключается и какие этапы включает в себя оценка риска ИБ?

5. В чем заключается и какие этапы включает в себя анализ риска ИБ?

6. В чем заключается идентификация риска ИБ? Перечислите этапы идентификации риска ИБ.

7. Что включает в себя идентификация активов? Перечислите основные виды активов.

8. Что представляют собой требования безопасности для активов?

9. Что включает в себя реестр информационных активов?

10. Каким образом может быть определена ценность активов? Приведите пример критериев и соответствующих шкал для оценки возможного ущерба.

11. Что такое профиль и жизненный цикл угрозы?

12. По каким признакам классифицируются угрозы информационной безопасности?

13. Какими способами может быть выполнена оценка вероятности угроз информационной безопасности?

14. Какими способами может быть выполнена оценка уязвимостей?

15. Каким образом может быть получена количественная оценка риска информационной безопасности?

16. Что включает в себя реестр рисков информационной безопасности?

17. В чем заключается оценивание рисков информационной безопасности?

18. Какие существуют варианты обработки риской информационной безопасности?

19. В чем заключается снижение риска информационной безопасности? Перечислите способы снижения рисков. Какие типичные ограничения должны быть учтены?

20. В чем заключается сохранение риска информационной безопасности? Перечислите факторы, влияющие не решение о принятии рисков.

21. В чем заключается предотвращение риска информационной безопасности? Перечислите основные способы предотвращения риска.

22. Что такое перенос риска информационной безопасности?

23. Какие задачи решаются в процессе коммуникации риска информационной безопасности?

24. Какие факторы подлежат мониторингу в процессе переоценки риска информационной безопасности?

25.Охарактеризовать роль лица, принимающего решения, экспертов, консультантов в задачах принятия решений.

26. Привести общую схему алгоритма экспертизы.

27. Описать основные этапы экспертизы.

28. Описать основные формы опроса экспертов, взаимодействия экспертов при опросе.

29. Составить алгоритм оценивания согласованности мнений экспертов.

30. Описать методы формирования исходного множества альтернатив.

31. Что такое область компромиссов, область согласия, множество Парето, множество эффективных решений? Как выделяют область компромиссов?

32. Описать признаки и свойства методов решения многокритериальных задач принятия решений. Провести классификацию методов многокритериальной оценки альтернатив и методов решения многокритериальных задач принятия решений.

33. Охарактеризовать аксиоматические методы многокритериальной оценки альтернатив.

34. Какие принципы оптимальности используются в прямых методах многокритериальной оценки альтернатив?

35. Каковы основные приемы нормализации критериев?

36. Как определяется важность критериев?

37. Построить структурные схемы методов порогов несравнимости. К каким решениям могут приводить данные методы?

38. Построить структурную схему метода аналитической иерархии.

38. Чем различаются задачи принятия решений при риске и при определенности? В чем состоит неопределенность задачи принятия решений при риске?

39. Описать основные особенности однокритериальной модели принятия решений при риске.

40. Описать основные особенности многокритериальной модели принятия решений при риске.

41. В чем заключается неопределенность задачи принятия решений при риске? Как преодолевается эта неопределенность?

42. С помощью каких критериев преодолевается неопределенность задач принятия решений при риске? Каковы преимущества и недостатки этих критериев?

7.2.6. Методика выставления оценки при проведении промежуточной аттестации

Экзамен проводится по билетам, каждый из которых содержит 3 вопроса. Первый вопрос оценивается на 3 балла, второй – на 4 балла, третий – на 5 баллов. Максимальное количество набранных баллов – 12.

1. Оценка «Неудовлетворительно» ставится в случае, если студент набрал менее 5 баллов.

2. Оценка «Удовлетворительно» ставится в случае, если студент набрал от 5 до 7 баллов

3. Оценка «Хорошо» ставится в случае, если студент набрал от 8 до 9 баллов.

4. Оценка «Отлично» ставится, если студент набрал от 10 до 12 баллов.

7.2.7 Паспорт оценочных материалов

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1	Основные термины и определения. Система менеджмента информационной безопасности (СМИБ)	ПК-2, ПК-5, ПК-6	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
2	Менеджмент риска информационной безопасности	ПК-2, ПК-5, ПК-6	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
3	Стандарты в области управления рисками информационной безопасности	ПК-2, ПК-5, ПК-6	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
4	Инструментальные средства для	ПК-2, ПК-5, ПК-6	Тест, контрольная работа,

	управления рисками		защита лабораторных работ, защита реферата, требования к курсовому проекту….
5	Основы принятия решений при управлении рисками информационной безопасности	ПК-2, ПК-5, ПК-6	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
6	Методы экспертных оценок	ПК-2, ПК-5, ПК-6	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
7	Детерминированные модели и методы принятия решений	ПК-2, ПК-5, ПК-6	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
8	Статистические модели и методы принятия решений в условиях неопределенности	ПК-2, ПК-5, ПК-6	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
9	Методы оптимизации	ПК-2, ПК-5, ПК-6	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….

7.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Тестирование осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных тест-заданий на бумажном носителе. Время тестирования 30 мин. Затем осуществляется проверка теста экзаменатором и выставляется оценка согласно методики выставления оценки при проведении промежуточной аттестации.

Решение стандартных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

Решение прикладных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

Защита курсовой работы, курсового проекта или отчета по всем видам практик осуществляется согласно требованиям, предъявляемым к работе,

описанным в методических материалах. Примерное время защиты на одного студента составляет 20 мин.

8 УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ)

8.1 Перечень учебной литературы, необходимой для освоения дисциплины

Основная литература

1. Остапенко А.Г., Математические основы управления рисками нарушения информационной безопасности [Электронный ресурс] : Учеб. пособие. - Электрон. текстовые, граф. дан. (4,12 Мб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2014. - 1 файл. - 30-00.

2. Методическое обеспечение оценки и регулирования рисков распределенных информационных систем : Учеб. пособие. - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2011. - 178 с. - 182-77.

Дополнительная литература

1. Методические указания к практическим занятиям по дисциплине «Математические основы управления рисками» для студентов специальностей 090301 «Компьютерная безопасность», 090302 «Информационная безопасность телекоммуникационных систем», 090303 «Информационная безопасность автоматизированных систем» очной формы обучения [Электронный ресурс] / Каф. систем информационной безопасности; Сост. О. Н. Чопоров. - Электрон. текстовые, граф. дан. (1,20 Мб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2015. - 1 файл. - 00-00.

2. Методические указания к курсовой работе по дисциплине «Математические основы управления рисками» для студентов специальности 090303 «Информационная безопасность автоматизированных систем» очной формы обучения [Электронный ресурс] / Каф. систем информационной безопасности; Сост. О. Н. Чопоров. - Электрон. текстовые, граф. дан. (1,10 Мб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2015. - 1 файл. - 00-00.

3. Методические указания к самостоятельным работам по дисциплине «Математические основы управления рисками» для студентов специальностей 090301 «Компьютерная безопасность», 090302 «Информационная безопасность телекоммуникационных систем», 090303 «Информационная безопасность автоматизированных систем» очной формы обучения Воронеж [Электронный ресурс] / Каф. систем информационной безопасности; Сост. О. Н. Чопоров. - Электрон. текстовые, граф. дан. (432 Кб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2015. - 1 файл. - 00-00.

4. Остапенко О.А. Риски систем: Оценка и управление [Электронный ресурс] : учеб. пособие. - Электрон. дан. (1 файл :5250 Кбайта). - Воронеж :

ГОУВПО "Воронежский государственный технический университет", 2006. - 1 файл. - 30-00.

5. Остапенко, А.Г. Теория управления рисками информационных систем [Электронный ресурс] : Учеб. пособия. - Электрон. текстовые, граф. дан. (190 Кб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2013. - 1 файл. - 30-00.

6. Остапенко, А.Г. Математические основы риск-анализа [Электронный ресурс] : Учеб. пособие. - Электрон. текстовые, граф. дан. (446 Кб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2013. - 1 файл. - 30-00.

8.2 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения, ресурсов информационно-телекоммуникационной сети «Интернет», современных профессиональных баз данных и информационных справочных систем:

Операционная система, не ниже Windows 7.

Пакет офисных программ, не ниже MS Office 2007.

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Для проведения лекций – аудитория с проектором и проекционной доской.

Для проведения лабораторных работ – десять рабочих мест, оборудованных ПЭВМ, с установленным программным обеспечением: Windows 7, MS Office 2007.

10. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

По дисциплине «Математические основы управления рисками» читаются лекции, проводятся лабораторные работы, выполняется курсовой проект.

Основой изучения дисциплины являются лекции, на которых излагаются наиболее существенные и трудные вопросы, а также вопросы, не нашедшие отражения в учебной литературе.

Лабораторные работы выполняются на лабораторном оборудовании в соответствии с методиками, приведенными в указаниях к выполнению работ.

Методика выполнения курсового проекта изложена в учебно-методическом пособии. Выполнять этапы курсового проекта должны своевременно и в установленные сроки.

Контроль усвоения материала дисциплины производится проверкой курсового проекта, защитой курсового проекта.

Вид учебных занятий	Деятельность студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначение вопросов, терминов, материала, которые вызывают трудности, поиск ответов в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на лекции или на практическом занятии.
Лабораторная работа	Лабораторные работы позволяют научиться применять теоретические знания, полученные на лекции при решении конкретных задач. Чтобы наиболее рационально и полно использовать все возможности лабораторных для подготовки к ним необходимо: следует разобрать лекцию по соответствующей теме, ознакомится с соответствующим разделом учебника, проработать дополнительную литературу и источники, решить задачи и выполнить другие письменные задания.
Самостоятельная работа	Самостоятельная работа студентов способствует глубокому усвоения учебного материала и развитию навыков самообразования. Самостоятельная работа предполагает следующие составляющие: - работа с текстами: учебниками, справочниками, дополнительной литературой, а также проработка конспектов лекций; - выполнение домашних заданий и расчетов; - работа над темами для самостоятельного изучения; - участие в работе студенческих научных конференций, олимпиад; - подготовка к промежуточной аттестации.
Подготовка к промежуточной аттестации	Готовиться к промежуточной аттестации следует систематически, в течение всего семестра. Интенсивная подготовка должна начаться не позднее, чем за месяц-полтора до промежуточной аттестации. Данные перед зачетом, экзаменом три дня эффективнее всего использовать для повторения и систематизации материала.