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

«Методы анализа рисков»

Специальность 10.05.01 КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ

Специализация

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет и 6 м.

Форма обучения очная

Год начала подготовки 2016

Автор программы _____/Д.Г. Плотников/

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

Руководитель ОПОП _____/ А.Г. Остапенко /

Воронеж 2017

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1.Цели дисциплины – формирование у обучающихся знаний о рисках и их классификации, методах анализа риска и неопределенности, технологии управления рисками, овладение общетеоретическими знаниями в области риск-менеджмента в контексте обеспечения информационной безопасности распределённых компьютерных систем (РКС).

1.2.Задачи освоения дисциплины

- формирование знаний о методах анализа риска для планирования производства с учётом обеспечения информационной безопасности распределённых компьютерных систем (РКС);
- создание предпосылок для формирования умений и навыков аналитического описания рисковых ситуаций в многокритериальных и конфликтных средах с учётом обеспечения информационной безопасности распределённых компьютерных систем;
- стимулирование студента к владению современным инструментарием оценки риска на основе математических моделях рисковых ситуацийучётом обеспечения информационной безопасности распределённых компьютерных систем.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Методы анализа рисков» относится к дисциплинам базовой части блока Б1.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Методы анализа рисков» направлен на формирование следующих компетенций:

ОПК-3 - способностью понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки информации по профилю деятельности в глобальных компьютерных сетях, библиотечных фондах и иных источниках информации

ОПК-4 - способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами

ПК-2 - способностью участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах, составлять научные отчеты, обзоры по результатам выполнения исследований

ПК-4 - способностью проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем

Компетенция	**Результаты обучения, характеризующие сформированность компетенции**
ОПК-3	знатьзначениеинформациивразвитиисовременногообщества и

	важности ее, сбора, хранения и обработки для обеспечения информационной безопасности распределённых компьютерных систем
	уметьприменятьдостиженияинформационныхтехнологийдля поискаиобработкиинформациипопрофилюдеятельностивглобальныхкомпьютерныхсетях, в том числе и для обеспечения информационной безопасности распределённых компьютерных систем
ОПК-4	знать методологию менеджмента рисков информационной безопасности распределённых КС
	Уметь пользоваться методами расчета и моделирования техногенного и информационного риска, основными инженерными подходами к оценке надежности, техногенного и информационного риска
	владеет навыками анализа защищенности интегрированных распределённых компьютерных систем и корпоративных сетей от НСД и оценки рисков нарушения их информационной безопасности
ПК-2	знать порядок и методику работы пооценкезащищенностиинформациивкомпьютерныхсистемах ,составлятьнаучныеотчеты,обзорыпорезультатамвыполнения исследований, в том числе по обеспечению информационной безопасности распределённых компьютерных систем
	уметь оценивать информационные риски обеспечения безопасности распределённых компьютерных систем
	владеет навыками расчета и управления рисками информационной безопасности, навыками разработки положения о применимости механизмов контроля в контексте управления рисками информационной безопасности
ПК-4	знать - современные угрозы информационной безопасности объектов и принципы обеспечения информационной безопасности объектов защиты; - методики проведения риск-анализа и управления рисками, а также тестирования средств обеспечения информационной безопасности;
	уметь - анализировать угрозы и проводить риск-анализ и реализовывать методики управления рисками с целью обеспечения безопасности объектов информатизации
	владеть - технологиями обеспечения информационной безопасности в части проведения риск-анализа и управления

	риска; - средствами обеспечения информационной безопасности, анализа угроз, риск-анализа и управления рисками.

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Методы анализа рисков» составляет 7 з.е.

Распределение трудоемкости дисциплины по видам занятий

очная форма обучения

Виды учебной работы	Всего часов	Семестры	
		7	8
Аудиторные занятия (всего)	108	54	54
В том числе:			
Лекции	72	36	36
Практические занятия (ПЗ)	36	18	18
Самостоятельная работа	108	72	36
Курсовой проект	+	+	
Часы на контроль	36	-	36
Виды промежуточной аттестации - экзамен, зачет	+	+	+
Общая трудоемкость: академические часы зач.ед.	 252 7	 126 3.5	 126 3.5

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	Прак зан.	СРС	Всего, час
1	Оценка риска информационной безопасности	Общее описание оценки риска информационной безопасности. Анализ риска. Оценивание рисков. Измерение рисков.	12	6	18	36
2	Риски информационных систем: обзор современных стандартов и методов оценки и управления	Анализ современных стандартов в области управления рисками информационных систем. Анализ международного стандарта ISO IEC 17799 (ГОСТ Р ИСО/МЭК 17799-2005) в области управления рисками информационной безопасности. Анализ международного стандарта ISO IEC 27001 (ГОСТ Р ИСО/МЭК 27001-2005) в области мониторинга и управления рисками информационной безопасности.:	12	6	18	36

		Анализ британского стандарта BS 7799-3 «Руководство по управлению информационными рисками». Анализ стандарта США NIST 800-30 «Руководство по управлению информационными рисками IT-систем».				
3	Аналитический подход в методологии оценки и управления рисками: обобщение и пути развития.	Понятие риска системы. Концепции оценки рисков. Обобщенная модель оценки риска. Вероятностная природа риска. Методы оценки риска. Формальное определение меры риска. Основные меры риска, используемые в анализе информационных систем. Методы оптимизации вычислений при расчете риска систем. Объективные и субъективные составляющие риска систем. Аналитические методы управления рисками. Понятие и обобщенная схема управления рисками. Принципы принятия решений по управлению рисками. Основные критерии выбора оптимальных решений по управлению рисками.	12	6	18	36
4	Развитие методического обеспечения оценки риска информационных систем.	Постановка задачи оценки риска информационной системы . Общий вид модели оценки риска информационных систем. Применение кластерного анализа при оценке рисков информационной системы. Формализация оценки риска информационной системы. Критерий принятия решений по управлению рисками на основе функции полезности.	12	6	18	36
5	Алгоритмизация и практическое применение методики управления рисками информационных систем на базе интересо-ориентированного подхода. Коммуникации риска информационной безопасности. Мониторинг и переоценка риска информационной безопасности. Аналитическая формализация ущерба и риска превышения пороговых значений критических переменных состояния.	Алгоритмы управления рисками информационных систем. Коммуникации риска информационной безопасности. Мониторинг и переоценка факторов риска. Пути аналитического развития инструментария оценки рисков. Параметры и характеристика риска для одной переменной состояния.	12	6	18	36
6	Риски и защищенность систем для непрерывных распределений вероятности ущерба.	Оценка рисков и защищенности систем для нормального непрерывного распределения вероятностей ущерба. Оценка рисков и защищенности систем для	12	6	18	36

		непрерывного нормального выборочного U-распределения вероятностей ущерба. Оценка рисков и защищенности систем для непрерывного нормального выборочного t-распределения вероятностей ущерба. Оценка рисков и защищенности систем для χ^2 непрерывного распределения вероятностей ущерба. Оценка рисков и защищенности систем для логарифмически нормального непрерывного распределения вероятностей ущерба. Оценка рисков и защищенности систем для непрерывного Лапласа распределения вероятностей ущерба. Оценка рисков и защищенности систем для непрерывного β -распределения вероятностей ущерба. Оценка рисков и защищенности систем для непрерывного гамма-распределения вероятностей ущерба. Оценка рисков и защищенности систем для непрерывного экспоненциального распределения вероятностей ущерба. Оценка рисков и защищенности систем для равномерного непрерывного распределения вероятностей ущерба. Оценка рисков и защищенности систем для непрерывного Эрланга распределения вероятностей ущерба. Оценка рисков и защищенности систем для степенного непрерывного распределения вероятностей ущерба. Оценка рисков и защищенности систем для непрерывного Парето распределения вероятностей ущерба. Оценка рисков и защищенности систем для непрерывного Вейбулла распределения вероятностей ущерба. Оценка рисков и защищенности систем для непрерывного Релея распределения вероятностей ущерба				
		Итого	**72**	**36**	**108**	**216**

5.2 Перечень лабораторных работ

Не предусмотрено учебным планом

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

В соответствии с учебным планом освоение дисциплины

предусматривает выполнение курсового проекта в 7 семестре для очной формы обучения.

Примерная тематика курсового проекта:

1. Анализ критичных активов предприятия, разработка модели бизнес-процессов предприятия, выявление основных источников угроз на предприятии
2. Оценка информационных рисков на основе анализа по информационным потокам с помощью программного продукта ГРИФ 2006
3. Оценка информационных рисков на основе анализа требований стандарта ГОСТ 27002 с помощью программного продукта Кондор 2006
4. Работа с международной базой уязвимости (NVD), определение уровня уязвимости компонентов локальной вычислительной сети предприятия
5. Расчет рисков ИБ с помощью системы нечеткого логического вывода
6. Расчет рисков нарушения информационной безопасности предприятия с помощью нечетких когнитивных карт
7. Расчет рисков нарушения ИБ с помощью нейронных сетей
8. Расчет рисков ИБ предприятия с помощью Марковских моделей

Задачи, решаемые при выполнении курсового проекта:

• Сформировать знания по теоретическим и методологическим положениям теории информационных рисков.

• Изучить отечественную и зарубежную нормативную правовую базу по оценке рисков нарушения информационной безопасности.

• Приобрести практический опыт использования программ и программных комплексов, реализующих методы анализа информационных рисков.

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	Результатыобучения,характеризующие сформированностькомпетенции	Критерии оценивания	Аттестован	Неаттестован
ОПК-3	знать значение информации в развитии современного общества и важности ее, сбора, хранения и обработки для обеспечения информационной безопасности	Знание общих подходов к анализу и измерению риска, а также процедуры риск-оцениван	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

	распределённых компьютерных систем	ия в контексте значения информации в развитии современного общества для обеспечения информационной безопасности распределённых компьютерных систем		
	уметь применять достижения информационных технологий для поиска в компьютерных сетях, в том числе и для обеспечения информационной безопасности распределённых компьютерных систем	Умение анализировать современные стандарты в области управления рисками с целью применения достижений ИТ для обеспечения информационной безопасности распределённых компьютерных систем	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ОПК-4	знать методологию менеджмента рисков информационной безопасности распределённых КС	Знание методологии оценки и управления рисками в части формальных определений мер риска, объективных и субъективных составляющих риска, принципов принятия решений по управлению рисками.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь пользоваться методами расчета и моделирования информационного риска, основными инженерными подходами к оценке информационного риска	Умение пользоваться алгоритмическими подходами в оценке и управлении рисками, расчёте ущерба и риска превышения пороговых значений	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

		критических переменных состояния защищаемого объекта.		
	владеет навыками анализа защищенности интегрированных распределённых компьютерных систем и корпоративных сетей от НСД и оценки рисков нарушения их информационной безопасности	Владение практическими навыками анализа защищенности систем на основе анализа оценок риска и защищенности в случаях непрерывных распределений вероятности ущерба	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-2	знать порядок и методику работы пооценкезащищенностиинформациивкомпьютерныхсистемах,составлятьнаучныеотчеты,обзорыпорезультатамвыполненияисследований, в том числе по обеспечению информационной безопасности распределённых компьютерных систем	Знание основных этапов и принципы работ по оценке защищенности информации в компьютерных системах, регламентированных в соответствующих стандартах, положениях и уставных документов	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь оценивать информационные риски обеспечения безопасности распределённых компьютерных систем	Умение на основе анализа угроз информационной безопасности оценивать информационные риски обеспечения безопасности распределённых компьютерных систем	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеет навыками расчета и управления рисками информационной безопасности, навыками разработки положения о применимости механизмов	Владение навыками расчёта показателей эффективности защиты, навыками	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программа

	контроля в контексте управления рисками информационной безопасности	разработки положения о применимости механизмов контроля в контексте управления рисками		х
ПК-4	знать - современные угрозы информационной безопасности объектов и принципы обеспечения информационной безопасности объектов защиты; - методики проведенияриск-анализа и управления рисками, а также тестирования средств обеспечения информационной безопасности;	Знает основные угрозы безопасности информации и модели нарушителя объекта информатизации Умеет разрабатывать проекты инструкций, регламентов, положении и приказов и определять политику контроля доступа работников к информации ограниченного доступа	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь - анализировать угрозы и проводить риск-анализ и реализовывать методики управления рисками с целью обеспечения безопасности объектов информатизации	Умеет разрабатывать модели угроз и модели нарушителя объекта информатизации на основе анализа угроз и проведения риск-анализа	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть - технологиями обеспечения информационной безопасности в части проведения риск-анализа и управления риска; - средствами обеспечения информационной безопасности, анализа угроз, риск-анализа и управления рисками.	Владение навыками выработки рекомендаций для приятия решений о совершенствовании системы защиты информации в рамках распределенных КС	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 7, 8 семестре для очной формы обучения по двух/четырехбалльной системе:

«зачтено»

«не зачтено»

Компе-тенция	Результатыобучения,характеризующие сформированностькомпетенции	Критерии оценивания	Зачтено	Незачтено
ОПК-3	знать значение информации в развитии современного общества и важности ее, сбора, хранения и обработки для обеспечения информационной безопасности распределённых компьютерных систем	Тест	Выполнениетестана 70-100%	Выполнениеменее 70%
	уметь применять достижения информационных технологий для поиска в компьютерных сетях, в том числе и для обеспечения информационной безопасности распределённых компьютерных систем	Решениестандартныхпрактическихзадач	Продемонстрирована верный ход решения в большинстве задач	Задачинерешены
ОПК-4	знать методологию менеджмента рисков информационной безопасности распределённых КС	Тест	Выполнениетестана 70-100%	Выполнениеменее 70%
	уметьпользоватьсяметодами расчета и моделирования техногенного и информационного риска, основными инженерными подходами к оценке	Решениестандартныхпрактическихзадач	Продемонстрирована верный ход решения в большинстве задач	Задачинерешены

	надежности, техногенного и информационного риска			
	владеет навыками анализа защищенности интегрированных распределённых компьютерных систем и корпоративных сетей от НСД и оценки рисков нарушения их информационной безопасности	Решение прикладных задач в конкретной предметной области	Продемонстрирова н верный ход решения в большинстве задач	Задачинерешены
ПК-2	знать порядок и методику работы пооценкезащищенно стиинформациивком пьютерныхсистемах, составлятьнаучныеот четы,обзорыпорезуль татамвыполненияисс ледований, в том числе по обеспечению информационной безопасности распределённых компьютерных систем	Тест	Выполнениетестана 70-100%	Выполнениемене е 70%
	уметь оценивать информационные риски обеспечения безопасности распределённых компьютерных систем	Решениестандар тныхпрактическ ихзадач	Продемонстрирова н верный ход решения в большинстве задач	Задачинерешены
	владеет навыками расчета и управления рисками информационной безопасности, навыками разработки положения о применимости механизмов контроля в контексте управления рисками информационной	Решение прикладных задач в конкретной предметной области	Продемонстрирова н верный ход решения в большинстве задач	Задачинерешены

	безопасности			
ПК-4	знать - современные угрозы информационной безопасности объектов и принципы обеспечения информационной безопасности объектов защиты; - методики проведенияриск-анализа и управления рисками, а также тестирования средств обеспечения информационной безопасности;	Тест	Выполнениетестана 70-100%	Выполнениеменее 70%
	уметь - анализировать угрозы и проводить риск-анализ и реализовывать методики управления рисками с целью обеспечения безопасности объектов информатизации	Решениестандартныхпрактическихзадач	Продемонстрирована верный ход решения в большинстве задач	Задачинерешены
	владеть - технологиями обеспечения информационной безопасности в части проведения риск-анализа и управления риска; - средствами обеспечения информационной безопасности, анализа угроз, риск-анализа и управления рисками.	Решение прикладных задач в конкретной предметной области	Продемонстрирована верный ход решения в большинстве задач	Задачинерешены

или
«отлично»;
«хорошо»;
«удовлетворительно»;
«неудовлетворительно».

Компе-тенция	Результатыобучения,характеризующие сформированностькомпетенции	Критерии оценивания	Отлично	Хорошо	Удовл.	Неудовл.
ОПК-3	знать значение информации в развитии современного общества и важности ее, сбора, хранения и обработки для обеспечения информационной безопасности распределённых компьютерных систем	Тест	Выполнениетестана 90- 100%	Выполнениетестана 80- 90%	Выполнениетестана 70- 80%	В тесте менее 70% правильных ответов
	уметь применять достижения информационных технологий для поиска в компьютерных сетях, в том числе и для обеспечения информационной безопасности распределённых компьютерных систем	Решениестандартных практическихзадач	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	Задачинерешены
ОПК-4	знать методологию менеджмента рисков информационной безопасности распределённых КС	Тест	Выполнениетестана 90- 100%	Выполнениетестана 80- 90%	Выполнениетестана 70- 80%	В тесте менее 70% правильных ответов
	Уметь пользоваться методами расчета и моделирования техногенного и информационного риска, основными инженерными подходами к оценке надежности,	Решениестандартных практическихзадач	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	Задачинерешены

	техногенного и информационного риска					
	владеет навыками анализа защищенности интегрированных распределённых компьютерных систем и корпоративных сетей от НСД и оценки рисков нарушения их 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	Задачинерешены
ПК-2	знать порядок и методику работы пооценкезащищенностиинформациивкомпьютерныхсистемах,составлятьнаучныеотчеты,обзорырезультатамвыполненияисследований, в том числе по обеспечению информационной безопасности распределённых компьютерных систем	Тест	Выполнениетестана 90- 100%	Выполнениетестана 80- 90%	Выполнениетестана 70- 80%	В тесте менее 70% правильных ответов
	уметь оценивать информационные риски обеспечения безопасности распределённых компьютерных систем	Решениестандартныхпрактическихзадач	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	Задачинерешены
	владеет навыками расчета и управления рисками информационной безопасности, навыками	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	Продемонстрирован верный ход решения в большинстве задач	Задачинерешены

	разработки положения о применимости механизмов контроля в контексте управления рисками информационной безопасности			задачах		
ПК-4	знать - современные угрозы информационной безопасности объектов и принципы обеспечения информационной безопасности объектов защиты; - методики проведенияриск-анализа и управления рисками, а также тестирования средств обеспечения информационной безопасности;	Тест	Выполнениетестана 90- 100%	Выполнениетестана 80- 90%	Выполнениетестана 70- 80%	В тесте менее 70% правильных ответов
	уметь - анализировать угрозы и проводить риск-анализ и реализовывать методики управления рисками с целью обеспечения безопасности объектов информатизации	Решениестандартных практическихзадач	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	Задачинерешены
	владеть - технологиями обеспечения информационной безопасности в части проведения	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	Продемонстрирован верный ход решения в большинстве задач	Задачинерешены

	риск-анализа и управления риска; - средствами обеспечения информационной безопасности, анализа угроз, риск-анализа и управления рисками.			всех задачах		

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

(минимум 10 вопросов для тестирования с вариантами ответов)

1.Какой из перечисленных методов оценки риска основан на расчетах и анализе статистических показателей?

+вероятностный метод

построение дерева решений

метод сценариев

анализ чувствительности

учет рисков при расчете чистой приведенной стоимости

имитационное моделирование

2.Какой из перечисленных методов оценки риска дает представление о наиболее критических факторах инвестиционного проекта?

построение дерева решений

метод сценариев

учет рисков при расчете чистой приведенной стоимости

вероятностный метод

+анализ чувствительности

имитационное моделирование

3.Какой из перечисленных методов оценки риска реализуется путем введения поправки на риск или путем учета вероятности возникновения денежных потоков?

построение дерева решений

метод сценариев

+учет рисков при расчете чистой приведенной стоимости

анализ чувствительности

вероятностный метод

имитационное моделирование

4.Какой из перечисленных методов оценки риска используется в ситуациях, когда принимаемые решения сильно зависят от принятых ранее и определяют сценарии дальнейшего развития событий?

имитационное моделирование

вероятностный метод

учет рисков при расчете чистой приведенной стоимости

+построение дерева решений

анализ чувствительности

метод сценариев

5.Какой из перечисленных методов оценки риска представляет собой серию численных экспериментов, призванных получить эмпирические оценки степени влияния различных факторов на некоторые зависящие от них результаты?

учет рисков при расчете чистой приведенной стоимости

анализ чувствительности

построение дерева решений

вероятностный метод

метод сценариев

+имитационное моделирование

6.Каким образом при расчете чистой приведенной стоимости можно учитывать риск?

в знаменателе формулы NPV посредством корректировки ставки дисконта

комбинация формул NPV посредством корректировки чистых денежных потоков

+все варианты верны

в числителе формулы NPV посредством корректировки чистых денежных потоков

7.Что является субъектом управления в риск-менеджменте?

+специальная группа людей, которая посредством различных приемов и способов управленческого воздействия осуществляет управление рисками

все варианты верны

риск, рисковые вложения капитала и экономические отношения между хозяйствующими субъектами

8.Что является объектом управления в риск-менеджменте?

+риск, рисковые вложения капитала и экономические отношения между хозяйствующими субъектами

все варианты верны

специальная группа людей, которая посредством различных приемов и способов управленческого воздействия осуществляет управление рисками

9.Утверждение о том, что «деятельность любой организации всегда сопровождается рисками, присутствующими в ее внешней или внутренней

среде» отражает смысл…

+закона неизбежности риска

закона сочетания потенциальных потерь и выгод

закона прямой зависимости между степенью риска и уровнем планируемых доходов

10.Утверждение о том, что «практически в любых ситуациях риска потенциальная возможность потерь или убытков сочетается с потенциальной возможностью получения дополнительных доходов» отражает смысл…

закона прямой зависимости между степенью риска и уровнем планируемых доходов

закона неизбежности риска

+закона сочетания потенциальных потерь и выгод

7.2.2 Примерный перечень заданий для решения стандартных задач

(минимум 10 вопросов для тестирования с вариантами ответов)

1.Утверждение о том, что «чем выше степень риска приосуществлении хозяйственной операции, тем выше уровень планируемых от этой операции доходов» отражает смысл…

+закона прямой зависимости между степенью риска и уровнем планируемых доходов

закона неизбежности риска

закона сочетания потенциальных потерь и выгод

2.К какой группе методов управления рисками относится прогнозирование внешней обстановки?

+методы компенсации рисков

методы уклонения от рисков

методы локализации рисков

методы диверсификации рисков

3.К какой группе методов управления рисками относится страхование?

+методы уклонения от рисков

методы диверсификации рисков

методы локализации рисков

методы компенсации рисков

4.К какой группе методов управления рисками относится распределение риска по этапам работы?

методы локализации рисков

методы компенсации рисков

методы уклонения от рисков

+методы диверсификации рисков

5.К какой группе методов управления рисками относится заключение договоров о совместной деятельности для реализации рискованных проектов?

методы диверсификации рисков

методы уклонения от рисков

методы компенсации рисков

+методы локализации рисков

6.К какой группе методов управления рисками относится обучение и инструктирование персонала?

методы уклонения от рисков

+методы компенсации рисков

методы диверсификации рисков

методы локализации рисков

7.К какой группе методов управления рисками относится распределение ответственности между участниками проекта?

+методы диверсификации рисков

методы компенсации рисков

методы локализации рисков

методы уклонения от рисков

8.К какой группе методов управления рисками относится увольнение некомпетентных сотрудников?

методы локализации рисков

методы диверсификации рисков

+методы уклонения от рисков

методы компенсации рисков

9.К какой группе методов управления рисками относится создание системы резервов?

методы уклонения от рисков

методы диверсификации рисков

+методы компенсации рисков

методы локализации рисков

10.К какой группе методов управления рисками относится создание специальных инновационных подразделений?

+методы локализации рисков

методы диверсификации рисков

методы компенсации рисков

методы уклонения от рисков

7.2.3 Примерный перечень заданий для решения прикладных задач

(минимум 10 вопросов для тестирования с вариантами ответов)

1.К какой группе методов управления рисками относится распределение инвестиций в разных отраслях и сферах деятельности?

+методы диверсификации рисков

методы локализации рисков

методы компенсации рисков

методы уклонения от рисков

2. Какой подход к обеспечению безопасности имеет место:

теоретический

+комплексный

логический

3. Таргетированная атака – это:

атака на сетевое оборудование

+атака на компьютерную систему крупного предприятия

атака на конкретный компьютер пользователя

4. Под информационной безопасностью понимается:

+защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре

программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия

нет верного ответа

5. Защита информации:

небольшая программа для выполнения определенной задачи

+комплекс мероприятий, направленных на обеспечение информационной безопасности

процесс разработки структуры базы данных в соответствии с требованиями пользователей

6. Информационная безопасность зависит от:

+компьютеров, поддерживающей инфраструктуры

пользователей

информации

7. Процедурой называется:

+пошаговая инструкция по выполнению задачи

обязательные действия

руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах

8. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков:

когда риски не могут быть приняты во внимание по политическим соображениям

для обеспечения хорошей безопасности нужно учитывать и снижать все риски

+когда стоимость контрмер превышает ценность актива и потенциальные потери

9. Что такое политика безопасности:
детализированные документы по обработке инцидентов безопасности
+широкие, высокоуровневые заявления руководства
общие руководящие требования по достижению определенного уровня безопасности

10. Что из перечисленного не является целью проведения анализа рисков:
выявление рисков
+делегирование полномочий
количественная оценка воздействия потенциальных угроз

7.2.4 Примерный перечень вопросов для подготовки к зачету

Укажите вопросы для зачета

1. Общее описание оценки риска информационной безопасности.
2. Анализ риска.
3. Оценивание рисков.
4. Измерение рисков.
5. Оценка последствий.
6. Установление значений уровня рисков информационной безопасности.
7. Анализ международного стандарта ISO IEC 27001 (ГОСТ Р ИСО/МЭК 27001-2005) в области мониторинга и управления рисками информационной безопасности.
8. Анализ британского стандарта BS 7799-3 «Руководство по управлению информационными рисками».
9. Анализ стандарта США NIST 800-30 «Руководство по управлению информационными рисками IT-систем».
10. Анализ существующих экспертных методов оценки рисков информационных систем
11. Анализ современных стандартов в области управления рисками информационных систем.
12. Анализ международного стандарта ISO IEC 17799 (ГОСТ Р ИСО/МЭК 17799-2005) в области управления рисками
13. Понятие риска системы.
14. Концепции оценки рисков.
15. Обобщенная модель оценки риска.
16. Вероятностная природа риска.
17. Методы оценки риска.
18. Формальное определение меры риска.
19. Основные меры риска, используемые в анализе информационных систем.
20. Методы оптимизации вычислений при расчете риска систем.
21. Объективные и субъективные составляющие риска систем.
22. Аналитические методы управления рисками.
23. Понятие и обобщенная схема управления рисками.
24. Принципы принятия решений по управлению рисками.
25. Основные критерии выбора оптимальных решений по управлению рисками
26. Применение методов теории чувствительности в управлении рисками информационных систем.
27. Динамические характеристики риска систем.
28. Наиболее распространенные на практике виды рисков информационных систем и их анализ.
29. Пути аналитического развития инструментария оценки рисков.

30. Алгоритмы управления рисками информационных систем.
31. Практическое применение алгоритма управления рисками.
32. Коммуникации риска информационной безопасности
33. Мониторинг и переоценка факторов риска.
34. Мониторинг, анализ и улучшение менеджмента риска
35. Параметры и характеристика риска для одной переменной состояния.
36. Оценка риска для множества переменных состояния.
37. Постановка задачи оценки риска информационной системы .
38. Общий вид модели оценки риска информационных систем.
39. Применение кластерного анализа при оценке рисков информационной системы.
40. Формализация оценки риска информационной системы.
41. Критерий принятия решений по управлению рисками на основе функции полезности.
42. Развитие интересо-ориентированного подхода к оценке и управлению рисками информационных систем.
43. Учет динамики развития информационных систем в управлении рисками.
44. Оценка рисков и защищенности систем для нормального непрерывного распределения вероятностей ущерба.
45. Оценка рисков и защищенности систем для непрерывного нормального выборочного U-распределения вероятностей ущерба.
46. Оценка рисков и защищенности систем для непрерывного нормального выборочного t-распределения вероятностей ущерба.
47. Оценка рисков и защищенности систем для χ^2 непрерывного распределения вероятностей ущерба.
48. Оценка рисков и защищенности систем для логарифмически нормального непрерывного распределения вероятностей ущерба.
49. Оценка рисков и защищенности систем для непрерывного Лапласа распределения вероятностей ущерба.
50. Оценка рисков и защищенности систем для непрерывного β -распределения вероятностей ущерба.
51. Оценка рисков и защищенности систем для непрерывного гамма-распределения вероятностей ущерба.
52. Оценка рисков и защищенности систем для непрерывного экспоненциального распределения вероятностей ущерба.
53. Оценка рисков и защищенности систем для равномерного непрерывного распределения вероятностей ущерба.
54. Оценка рисков и защищенности систем для непрерывного Эрланга распределения вероятностей ущерба.
55. Оценка рисков и защищенности систем для степенного непрерывного распределения вероятностей ущерба.
56. Оценка рисков и защищенности систем для непрерывного Парето распределения вероятностей ущерба.
57. Оценка рисков и защищенности систем для непрерывного Вейбулла распределения вероятностей ущерба.
58. Оценка рисков и защищенности систем для непрерывного Релея распределения вероятностей ущерба

7.2.5 Примерный перечень заданий для решения прикладных задач

Примерный перечь вопросов для экзамена:

Задание 1.

1. Методы оптимизации вычислений при расчете риска систем.
2. Применение методов теории чувствительности в управлении рисками

информационных систем.

Задание 2.

1. Формальное описание моделей принятия решений.

2. Теория полезности.

Задание 3.

2. Методы экспертных оценок. Основные типы шкал.

3. Принципы принятия решений по управлению рисками.

Задание 4.

1. Методы экспертных оценок. Методы проведение экспертизы.

2. Детерминированные модели и методы принятия решений. Нормализация критериев.

Задание 5.

1. Методы оптимизации вычислений при расчете риска систем.

2. Методы экспертных оценок. Отбор экспертов и их характеристика. Оценка компетентности экспертов.

Задание 6.

1. Менеджмент риска информационной безопасности. Идентификация риска. Определение угроз. Профиль и жизненный цикл угрозы.

2. Методы экспертных оценок. Методы опроса экспертов.

Задание 7.

1. Общая модель процесса нарушения физической целостности информации.

2. Основные меры риска, используемые в анализе информационных систем.

Задание 8.

1. Идентификация риска. Выявление уязвимостей. Определение последствий.

2. Метод аналитической иерархии.

Задание 9.

1. Количественная оценка риска. Реестр информационных рисков.

2. Методы оценки риска.

Задание 10.

1. Обработка риска информационной безопасности.

2. Методологические подходы к оценке уязвимости информации.

Примерный вариант прикладной задачи для экзамена:

«Построение концепции информационной безопасности предприятия»

Задание: Используя предложенные образцы, разработать концепцию информационной безопасности компании, содержащую следующие основные пункты (приведен примерный план, в который в случае необходимости могут быть внесены изменения):

Общие положения

Назначение Концепции по обеспечению информационной безопасности.

Цели системы информационной безопасности

Задачи системы информационной безопасности.
Проблемная ситуация в сфере информационной безопасности.
Объекты информационной безопасности.
Определение вероятного нарушителя.
Описание особенностей (профиля) каждой из групп вероятных нарушителей.
Основные виды угроз информационной безопасности Предприятия.
(Классификации угроз. Основные непреднамеренные искусственные угрозы. Основные преднамеренные искусственные угрозы.)
Общестатистическая информация по искусственным нарушениям информационной безопасности.
Оценка потенциального ущерба от реализации угрозы.
Механизмы обеспечения информационной безопасности Предприятия.
Принципы, условия и требования к организации и функционированию системы информационной безопасности.
Основные направления политики в сфере информационной безопасности.
Планирование мероприятий по обеспечению информационной безопасности Предприятия.
Критерии и показатели информационной безопасности Предприятия.
Мероприятия по реализации мер информационной безопасности Предприятия
Организационное обеспечение информационной безопасности. (Задачи организационного обеспечения информационной безопасности. Подразделения, занятые в обеспечении информационной безопасности. Взаимодействие подразделений, занятых в обеспечении информационной безопасности.)
Техническое обеспечение информационной безопасности Предприятия.
(Общие положения. Защита информационных ресурсов от несанкционированного доступа. Средства комплексной защиты от потенциальных угроз. Обеспечение качества в системе безопасности. Принципы организации работ обслуживающего персонала.)
Правовое обеспечение информационной безопасности Предприятия.
(Правовое обеспечение юридических отношений с работниками Предприятия. Правовое обеспечение юридических отношений с партнерами Предприятия. Правовое обеспечение применения электронной цифровой подписи.)
Оценивание эффективности системы информационной безопасности Предприятия.
Программа создания системы информационной безопасности Предприятия.

7.2.6. Методика выставления оценки при проведении промежуточной аттестации

Зачет/экзамен с оценкой проводится по тест-билетам, каждый из которых содержит 10 вопросов и задачу. Каждый правильный ответ на вопрос в тесте оценивается 1 баллом, задача оценивается в 10 баллов (5 баллов верное решение и 5 баллов за верный ответ). Максимальное количество набранных баллов – 20.

1. Оценка «Неудовлетворительно» ставится в случае, если студент набрал менее 6 баллов.

2. Оценка «Удовлетворительно» ставится в случае, если студент набрал от 6 до 10 баллов

3. Оценка «Хорошо» ставится в случае, если студент набрал от 11 до 15 баллов.

4. Оценка «Отлично» ставится, если студент набрал от 16 до 20 баллов.)

7.2.7 Паспорт оценочных материалов

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1	Оценка риска информационной безопасности	ОПК-3, ОПК-4, ПК -2, ПК-4	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
2	Риски информационных систем: обзор современных стандартов и методов оценки и управления	ОПК-4, ПК -2, ПК-4	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
3	Аналитический подход в методологии оценки и управления рисками: обобщение и пути развития.	ПК -2, ПК-4	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
4	Развитие методического обеспечения оценки риска информационных систем.	ПК -2, ПК-4	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
5	Алгоритмизация и практическое применение методики управления рисками информационных систем на базе интересо-ориентированного подхода. Коммуникации риска информационной безопасности. Мониторинг и переоценка риска информационной безопасности. Аналитическая формализация ущерба и риска превышения пороговых значений критических переменных состояния.	ПК -2, ПК-4	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
6	Риски и защищенность систем для непрерывных распределений вероятности ущерба.	ПК -2, ПК-4	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. Методология риск-анализа и моделирования кибернетических систем, атакуемых вредоносным программным обеспечением [Электронный ресурс]: Учеб. пособие / А. Г. Остапенко, Д. Г. Плотников, С. В. Машин. - Электрон. текстовые, граф. дан. (112 Кб). - Воронеж: ФГБОУ ВПО "Воронежский государственный технический университет", 2012. - 1 файл. - 30-00.
2. Скобелев, И.О. Методы анализа информационных рисков и управления защищенностью информационно-телекоммуникационных систем [Электронный ресурс]: Учеб. пособие / И. О. Скобелев, Н. М. Радько; под ред. А. Г. Остапенко. - Электрон. текстовые, граф. дан. (3938457 байт). - Воронеж: ГОУВПО "Воронежский государственный технический университет", 2008. - 1 файл. - 30-00.
3. Остапенко О. А. Риски систем: Оценка и управление [Электронный ресурс]: учеб. пособие / О. А. Остапенко, Д. О. Карпеев, В. Н. Асеев. - Электрон. дан. (1 файл :5250 Кбайта). - Воронеж: ГОУВПО "Воронежский государственный технический университет", 2006. - 1 файл. - 30-00.

Дополнительная литература:

1. Методические указания к самостоятельным работам по дисциплине «Методы анализа рисков» для студентов специальности 090301 «Компьютерная безопасность» очной формы обучения

[Электронный ресурс] / Каф. систем информационной безопасности; Сост.: Е. С. Соколова, О. А. Остапенко. - Электрон. текстовые, граф. дан. (274 Кб). - Воронеж: ФГБОУ ВПО "Воронежский государственный технический университет", 2015. - 1 файл. - 00-00.

2. Методические указания к практическим занятиям по дисциплине «Методы анализа рисков» для студентов специальности 090301 «Компьютерная безопасность» очной формы обучения [Электронный ресурс] / Каф. систем информационной безопасности; Сост.: А. Е. Дешина. - Электрон. текстовые, граф. дан. (773 Кб). - Воронеж: ФГБОУ ВПО "Воронежский государственный технический университет", 2015. - 1 файл. - 00-00.
3. Скобелев, И.О. Методы анализа информационных рисков и управления защищенностью информационно - телекоммуникационных систем [Электронный ресурс]: Учеб. пособие / И. О. Скобелев, Н. М. Радько; под ред. А. Г. Остапенко. - Электрон. текстовые, граф. дан. (3938457 байт). - Воронеж: ГОУВПО "Воронежский государственный технический университет", 2008. - 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:

http://att.nica.ru
http://www.edu.ru/
http://window.edu.ru/window/library
http://www.intuit.ru/catalog/
http://bibl.cchgeu.ru/MarcWeb2/ExtSearch.asp
https://cchgeu.ru/education/cafedras/kafsib/?docs
http://www.eios.vorstu.ru
http://e.lanbook.com/ (ЭБС Лань)
http://IPRbookshop.ru/ (ЭБСIPRbooks)

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Специализированная лекционная аудитория, оснащенная оборудованием для лекционных демонстраций и проекционной аппаратурой.

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

По дисциплине «Методы анализа рисков» читаются лекции, проводятся практические занятия, 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.

Практические занятия направлены на приобретение практических навыков расчета. Занятия проводятся путем решения конкретных задач в аудитории.

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.

Типовой вариант задания на контрольную работу:

Контрольная работа выполняется в форме реферата по заданной теме, оформляется на сброшюрованных листах формата А4 и представляется преподавателю в установленный срок. Студент выбирает номер темы по сумме последней и предпоследней цифр шифра. Если сумма цифр равна нулю, то выбирается тема № 10. Перечень тем рефератов:

1. Угрозы информационной безопасности предприятия (организации) и способы борьбы с ними
2. Современные средства защиты информации
3. Современные системы компьютерной безопасности
4. Современные средства противодействия экономическому шпионажу
5. Современные криптографические системы
6. Криптоанализ, современное состояние
7. Правовые основы защиты информации
8. Технические аспекты обеспечения защиты информации. Современное состояние
9. Атаки на систему безопасности и современные методы защиты
10. Современные пути решения проблемы информационной безопасности РФ

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.
Практическое занятие	Конспектирование рекомендуемых источников. Работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы. Прослушивание аудио- и видеозаписей по заданной теме, выполнение расчетно-графических заданий, решение задач по алгоритму.

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.