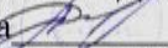


**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ
ФЕДЕРАЦИИ**

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 риск-анализа»

Специальность 10.05.03 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Специализация

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет

Форма обучения очная

Год начала подготовки 2016

Автор программы



/Плотников Д.Г./

Заведующий кафедрой
Систем информационной
безопасности



/ А.Г. Остапенко /

Руководитель ОПОП



/ А.Г. Остапенко /

Воронеж 2017

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели дисциплины: Целью изучения дисциплины является формирование у студентов основных знаний в области риск-анализа и управления рисками, а также умений применения рассматриваемого математического аппарата в профессиональной деятельности.

1.2. Задачи освоения дисциплины:

- знать основные отечественные и зарубежные стандарты в области обеспечения информационной безопасности;
- знать основные концепции управления рисками;
- производить аналитическую оценку рисков при различных плотностях вероятности наступления ущерба;
- оценивать эффективность защиты систем;
- знать способы регулирования рисков.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Математические основы риск-анализа» относится к дисциплинам вариативной части блока Б1.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Математические основы риск-анализа» направлен на формирование следующих компетенций:

ОПК-1 - способность анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач;

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

ПК-24 - способность обеспечить эффективное применение информационных технологий в автоматизированной системе с учетом требований информационной безопасности;

| Компетенция | Результаты обучения, характеризующие сформированность компетенции |
|-------------|--|
| ОПК-1 | знать - сущность и значение информации в развитии современного общества; - основные закономерности функционирования информационных процессов в различных системах; - используемые в современной экономике методы информационно коммуникационных технологий для решения задач информационной безопасности; |

| | |
|------|--|
| | <p>- принципы решений стандартных задач профессиональной деятельности;</p> <p>- основные источники информации для решения задач</p> <p>уметь</p> <p>- на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учетом основных требований информационной безопасности решать стандартные задачи;</p> <p>- использовать базовые знания об информационных системах для решения исследовательских профессиональных задач;</p> <p>- проводить поиск научной и технической информации с использованием общих и специализированных баз данных;</p> <p>владеть</p> <p>- методами решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учетом основных требований информационной безопасности;</p> <p>- навыками разработки специализированных программ для решения задач профессиональной сферы деятельности;</p> |
| ПК-5 | <p>знать</p> <p>- методологию менеджмента рисков информационной безопасности в телекоммуникационных системах;</p> <p>- методики оценки уязвимостей телекоммуникационных систем;</p> <p>- угрозы информационной безопасности телекоммуникационных систем;</p> <p>уметь</p> <p>- применять методологию менеджмента рисков информационной безопасности в телекоммуникационных системах;</p> <p>- выявлять и оценивать угрозы информационной безопасности;</p> <p>владеть</p> <p>- методами расчета и моделирования риска нарушения ИБ;</p> <p>- основными инженерными подходами к оценке надежности ИС и риска нарушения ИБ;</p> <p>- навыками анализа защищенности интегрированных телекоммуникационных и корпоративных сетей от НСД и оценки рисков нарушения их информационной безопасности;</p> |

| | |
|-------|---|
| ПК-24 | <p>знать</p> <ul style="list-style-type: none"> - формальную постановку задачи распределения технологических ресурсов автоматизированной системы с учетом требований информационной безопасности; - основные методы сопоставления результатов экспериментальных данных с реальной системой и полученных решений с моделью; |
| | <p>уметь</p> <ul style="list-style-type: none"> - формировать и обосновывать критерии качества, в том числе и автоматизированной системы с учетом требований информационной безопасности и проводить их оценку; - проводить анализ корректности полученных результатов; - проверять соответствие полученных результатов требованиям теории; - использовать методы оценки правильности выбранной модели; |
| | <p>владеть</p> <ul style="list-style-type: none"> - навыками грамотной обработки результатов опыта и сопоставления их с теоретическими данными; - навыками корректного формулирования результатов исследования и применения математического аппарата для решения физических задач; |

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Математические основы риск-анализа» составляет 53 е.

Распределение трудоемкости дисциплины по видам занятий
очная форма обучения

| Виды учебной работы | Всего часов | Семестры | |
|--|-------------|----------|-----|
| | | 4 | 5 |
| Аудиторные занятия (всего) | 90 | 36 | 54 |
| В том числе: | | | |
| Лекции | 54 | 18 | 36 |
| Практические занятия (ПЗ) | 36 | 18 | 18 |
| Самостоятельная работа | 54 | 36 | 18 |
| Часы на контроль | 36 | - | 36 |
| Виды промежуточной аттестации - экзамен, зачет | + | + | + |
| Общая трудоемкость: | | | |
| академические часы | 180 | 72 | 108 |
| зач.ед. | 5 | 2 | 3 |

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 | Место риск-анализа в системе знаний по обеспечению безопасности систем и процессов. | <p>Понятийный аппарат и терминологическая база дисциплины.</p> <p>Оценка рисков и международных стандартов ISO/IEC 17799:2000(E), ISO/IEC TR 13335-2, NIST800-30, Cobit, SCORE, SYS Trust.</p> <p>Концепции управления рисками OCTAVE, CRAMM, MITRE.</p> <p>Инструментарий управления информационными рисками.</p> <p>Методы анализа рисков на основе экспертных оценок и аппарата теории нечетких множеств.</p> <p>Методы управления информационными рисками в инновационной деятельности.</p> | 10 | 6 | 8 | 24 |
| 2 | Меры риска и защищенности систем. | <p>Меры риска и защищенности систем на основе вероятностных параметров и характеристик ущерба.</p> <p>Функции чувствительности и динамическое моделирование рисков.</p> <p>Оценка рисков сложных систем на основе параметров рисков их компонентов.</p> | 10 | 6 | 8 | 24 |
| 3 | Аналитическая оценка рисков | <p>Аналитическая оценка рисков при нормальном и логнормальном распределениях плотности вероятности наступления ущерба (ПВНУ).</p> <p>Аналитическая оценка рисков при гамма и бета-распределениях ПВНУ.</p> <p>Аналитическая оценка рисков при экспоненциальном, Вейбулла и Эрланга распределениях ПВНУ</p> | 10 | 6 | 8 | 24 |
| 4 | Нерегулярные распределения ущерба и динамика рисков. | <p>Аналитические риск-модели при биномиальном, Паскаля и мультиномальном распределениях вероятности наступления ущерба (ВНУ).</p> <p>Аналитические риск-модели при геометрическом и гипергеометрическом распределениях ВНУ.</p> <p>Аналитические риск-модели при</p> | 8 | 6 | 10 | 24 |

| | | | | | | |
|--------------|---|--|-----------|-----------|-----------|------------|
| | | пуассоновском распределении ВНУ и распределениях типа А и В. | | | | |
| 5 | Синтез систем с заданным риском. | Метод синтеза однокомпонентных систем с заданным уровнем риска при реализации атак на систему Метод синтеза многокомпонентных систем с заданным уровнем риска при реализации асинхронных и синхронных атак на компоненты системы. | 8 | 6 | 10 | 24 |
| 6 | Прогнозирование эффективности систем на основе анализа рисков ущерба и шансов полезности. | Понятие эффективности. Понятие шанса. Методы прогнозирования эффективности систем на основе анализа рисков ущерба и шансов полезности. | 8 | 6 | 10 | 24 |
| Итого | | | 54 | 36 | 54 | 144 |

5.2 Перечень лабораторных работ

Непредусмотрено учебным планом

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

В соответствии с учебным планом освоение дисциплины не предусматривает выполнение курсового проекта (работы) или контрольной работы.

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

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

7.1.1 Этап текущего контроля

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

«аттестован»;

«неаттестован».

| Компетенция | Результаты обучения, характеризующие сформированность компетенции | Критерии оценивания | Аттестован | Неаттестован |
|-------------|---|---|---|---|
| ОПК-1 | знать - сущность и значение информации в развитии современного общества; - основные закономерности функционирования информационных процессов в различных системах; - используемые в современной экономике методы информационно | знание сущности и значения информации и информационных технологий по её сбору, хранению и обработке в развитии современного общества знание подходов к решению стандартных задач по оценке рисков | Выполнение работ в срок, предусмотренный в рабочих программах | Невыполнение работ в срок, предусмотренный в рабочих программах |

| | | | | |
|------|--|---|---|---|
| | коммуникационных технологий для решения задач информационной безопасности; - принципы решений стандартных задач профессиональной деятельности; - основные источники информации для решения задач | нарушения безопасности информационных систем | | |
| | уметь - на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учетом основных требований информационной безопасности решать стандартные задачи; - использовать базовые знания об информационных системах для решения исследовательских профессиональных задач; - проводить поиск научной и технической информации с использованием общих и специализированных баз данных; | умение применять инфокоммуникационные технологии для решения задач поиска научной и технической информации с использованием общих и специализированных баз данных | Выполнение работ в срок, предусмотренный в рабочих программах | Невыполнение работ в срок, предусмотренный в рабочих программах |
| | владеть - методами решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учетом основных требований информационной безопасности; - навыками разработки специализированных программ для решения задач профессиональной сферы деятельности; | владение навыками разработки специализированных программ для решения задач профессиональной сферы деятельности с учетом требований информационной безопасности | Выполнение работ в срок, предусмотренный в рабочих программах | Невыполнение работ в срок, предусмотренный в рабочих программах |
| ПК-5 | знать - методологию менеджмента рисков информационной безопасности в телекоммуникационных системах; - методики оценки уязвимостей телекоммуникационных систем; - угрозы информационной | знание основных положений менеджмента рисков, методик оценки уязвимостей и угроз информационной безопасности | Выполнение работ в срок, предусмотренный в рабочих программах | Невыполнение работ в срок, предусмотренный в рабочих программах |

| | | | | |
|-------|--|--|--|--|
| | <p>безопасности телекоммуникационных систем;</p> <p>уметь - применять методологию менеджмента рисков информационной безопасности в телекоммуникационных системах;</p> <p>- выявлять и оценивать угрозы информационной безопасности;</p> | <p>умение оценивания рисков информационной безопасности в информационных системах; умение анализировать угрозы безопасности информации умеет оценивать информационные риски</p> | <p>Выполнение работ в срок, предусмотренный в рабочих программах</p> | <p>Невыполнение работ в срок, предусмотренный в рабочих программах</p> |
| | <p>владеть - методами расчета и моделирования риска нарушения ИБ;</p> <p>- основными инженерными подходами к оценке надежности ИС и риска нарушения ИБ;</p> <p>- навыками анализа защищенности интегрированных телекоммуникационных и корпоративных сетей от НСД и оценки рисков нарушения их информационной безопасности;</p> | <p>владеть навыками расчета рисков и анализа защищенности информационной безопасности, навыками разработки положения о применимости механизмов контроля в контексте управления</p> | <p>Выполнение работ в срок, предусмотренный в рабочих программах</p> | <p>Невыполнение работ в срок, предусмотренный в рабочих программах</p> |
| ПК-24 | <p>знать - формальную постановку задачи распределения ехнологическихресурсовавто матизированнойсистемысуче томтребованийинформацион нойбезопасности;</p> <p>- основные научные методы анализа данных;</p> <p>- методологию разработки и обоснования численных методов решения корректно поставленных математических задач;</p> <p>- основные источники погрешностей измерений и вычислений;</p> <p>- основные методы оценки правильности выбранной модели;</p> <p>- основные методы сопоставления результатов экспериментальных данных с реальной системой и полученных решений с моделью;</p> | <p>Знание формальных постановок задач о распределении ресурсов на основе методов динамического программирования</p> <p>знание методологии разработки и обоснования численных методов решения корректно поставленных математических задач в контексте способности обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы</p> | <p>Выполнение работ в срок, предусмотренный в рабочих программах</p> | <p>Невыполнение работ в срок, предусмотренный в рабочих программах</p> |
| | <p>уметь - формировать и обосновывать критерии качества , в том числе и автоматизированной системы с учетом требований</p> | <p>умение формализовывать критерии качества управления рисками, формулировать обоснованные</p> | <p>Выполнение работ в срок, предусмотренный в рабочих программах</p> | <p>Невыполнение работ в срок, предусмотренный в рабочих программах</p> |

| | | | | |
|--|--|---|---|---|
| | информационной безопасности и проводить их оценку; - проводить анализ корректности полученных результатов; - проверять соответствие полученных результатов требованиям теории; - оценивать результаты экспериментов с моделью; - использовать методы оценки правильности выбранной модели; | выводы из сопоставления результатов теории и эксперимента и т.д. | | |
| | владеть - навыками грамотной обработки результатов опыта и сопоставления их с теоретическими данными; - навыками корректного формулирования результатов исследования применения математического аппарата для решения физических задач; | владение подходами к обработке результатов эксперимента, навыками планирования и интерпретации результатов эксперимента | 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 4,5 семестре для очной формы обучения по двух/четырёхбалльной системе:

«зачтено»

«незачтено»

| Компетенция | Результаты обучения, характеризующие сформированность компетенции | Критерии оценивания | Зачтено | Незачтено |
|-------------|--|--|--|----------------------|
| ОПК-1 | знать - сущность и значение информации в развитии современного общества; - основные закономерности функционирования информационных процессов в различных системах; - используемые в современной экономике методы информационно-коммуникационных технологий для решения задач информационной безопасности; - принципы решений стандартных задач профессиональной деятельности; - основные источники информации для решения задач | Тест | Выполнение теста на 70-100% | Выполнение менее 70% |
| | уметь - на основе информационной и библиографической культуры с применением | Решение стандартных практических задач | Продемонстрирован верный ход решения в большинстве задач | Задача не решена |

| | | | | |
|------|--|--|--|-------------------------|
| | <p>информационно коммуникационных технологий и с учетом основных требований информационной безопасности решать стандартные задачи;</p> <ul style="list-style-type: none"> - использовать базовые знания об информационных системах для решения исследовательских профессиональных задач; - проводить поиск научной и технической информации с использованием общих и специализированных баз данных; | | | |
| | <p>владеть</p> <ul style="list-style-type: none"> - методами решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учетом основных требований информационной безопасности; - навыками разработки специализированных программ для решения задач профессиональной сферы деятельности; - навыками управления информацией для решения исследовательских профессиональных задач; | Решение прикладных задач в конкретной предметной области | Продемонстрирован верный ход решения в большинстве задач | Задачи решены |
| ПК-5 | <p>знать</p> <ul style="list-style-type: none"> - методологию менеджмента рисков информационной безопасности в телекоммуникационных системах; - методики оценки уязвимостей телекоммуникационных систем; - угрозы информационной безопасности телекоммуникационных систем; | Тест | Выполнение теста на 70-100% | Выполнение не менее 70% |
| | <p>уметь</p> <ul style="list-style-type: none"> - применять методологию менеджмента рисков информационной безопасности в телекоммуникационных системах; - выявлять и оценивать угрозы информационной | Решение стандартных практических задач | Продемонстрирован верный ход решения в большинстве задач | Задачи решены |

| | | | | |
|-------|--|--|--|-------------------------|
| | <p>безопасности;</p> <p>владеть</p> <ul style="list-style-type: none"> - методами расчета и моделирования риска нарушения ИБ; - основными инженерными подходами к оценке надежности ИС и риска нарушения ИБ; - навыками анализа защищенности интегрированных телекоммуникационных и корпоративных сетей от НСД и оценки рисков нарушения их информационной безопасности; | Решение прикладных задач в конкретной предметной области | Продемонстрирован верный ход решения в большинстве задач | Задачи решены |
| ПК-24 | <p>знать</p> <ul style="list-style-type: none"> - формальную постановку задачи распределения технологических ресурсов автоматизированной системы с учетом требований информационной безопасности; - основные научные методы анализа данных; - методологию разработки и обоснования численных методов решения корректно поставленных математических задач; - основные источники погрешностей измерений и вычислений; - основные методы оценки правильности выбранной модели; - основные методы сопоставления результатов экспериментальных данных с реальной системой и полученных решений с моделью; | Тест | Выполнение теста на 70-100% | Выполнение не менее 70% |
| | <p>уметь</p> <ul style="list-style-type: none"> - формировать и обосновывать критерии качества, в том числе и автоматизированной системы с учетом требований информационной безопасности и проводить их оценку; - проводить анализ корректности полученных результатов; - проверять соответствие полученных результатов требованиям теории; - оценивать результаты экспериментов с моделью; - использовать методы оценки правильности выбранной модели; | Решение стандартных практических задач | Продемонстрирован верный ход решения в большинстве задач | Задачи решены |

| | | | | |
|--|--|--|--|---------------|
| | владеть - навыками грамотной обработки результатов опыта и сопоставления их с теоретическими данными; - навыками корректного формулирования результатов исследования и применения математического аппарата для решения физических задач; | Решение прикладных задач в конкретной предметной области | Продемонстрирован верный ход решения в большинстве задач | Задачи решены |
|--|--|--|--|---------------|

или

«отлично»;

«хорошо»;

«удовлетворительно»;

«неудовлетворительно».

| Компетенция | Результаты обучения, характеризующие сформированность компетенции | Критерии и оценивания | Отлично | Хорошо | Удовл. | Неудовл. |
|-------------|--|--|--|---|--|--------------------------------------|
| ОПК-1 | знать - сущность и значение информации в развитии современного общества; - основные закономерности функционирования информационных процессов в различных системах; - используемые в современной экономике методы информационно-коммуникационных технологий для решения задач информационной безопасности; - принципы решений стандартных задач профессиональной деятельности; - основные источники информации для решения задач | Тест | Выполнено в объеме 90-100% | Выполнено в объеме 80-90% | Выполнено в объеме 70-80% | В тесте менее 70% правильных ответов |
| | уметь - на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности решать стандартные задачи; - использовать базовые знания об информационных системах для 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 решены |

| | | | | | | |
|------|---|--|--|---|--|--------------------------------------|
| | <p>исследовательских профессиональных задач;</p> <ul style="list-style-type: none"> - проводить поиск научной и технической информации с использованием общих и специализированных баз данных; | | | | | |
| | <p>владеть - методами решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры применением информационно коммуникационных технологий и с учетом основных требований информационной безопасности;</p> <ul style="list-style-type: none"> - навыками разработки специализированных программ для решения задач профессиональной сферы деятельности; - навыками управления информацией для решения исследовательских профессиональных задач; | 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 решены |
| ПК-5 | <p>знать методологию менеджмента рисков информационной безопасности в телекоммуникационных системах;</p> <ul style="list-style-type: none"> - методики оценки уязвимостей телекоммуникационных систем; - угрозы информационной безопасности телекоммуникационных систем; | Тест | Выполнено более 90-100% | Выполнено более 80-90% | Выполнено более 70-80% | В тесте менее 70% правильных ответов |
| | <p>уметь - применять методологию менеджмента рисков информационной безопасности в телекоммуникационных системах;</p> <ul style="list-style-type: none"> - выявлять и оценивать угрозы информационной безопасности в телекоммуникационных системах; | 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 решены |

| | | | | | | |
|-------|--|---|---|--|---|---|
| | <p>безопасности;</p> <p>владеть</p> <ul style="list-style-type: none"> - методами расчета и моделирования риска нарушения ИБ; - основными генерными подходами к оценке надежности ИС и риска нарушения ИБ; - навыками анализа защищенности сегрегированных телекоммуникационных и корпоративных сетей от Д и оценки рисков нарушения их информационной безопасности; | <p>Решение прикладных задач в конкретной предметной области</p> | <p>Задачи решены в полном объеме и получены верные ответы</p> | <p>Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах</p> | <p>Продемонстрирован верный ход решения в большинстве задач</p> | <p>Задачи решены</p> |
| ПК-24 | <p>знать</p> <ul style="list-style-type: none"> - формальную постановку задачи распределения технологических ресурсов в автоматизированной системе с учетом требований информационной безопасности; - основные научные методы анализа данных; - методологию разработки и обоснования численных методов решения корректно поставленных математических задач; - основные источники погрешностей измерений и вычислений; - основные методы оценки правильности выбранной модели; - основные методы сопоставления результатов экспериментальных данных с реальной системой и полученных решений с моделью; | <p>Тест</p> | <p>Выполнено не менее 90-100%</p> | <p>Выполнено не менее 80-90%</p> | <p>Выполнено не менее 70-80%</p> | <p>В тесте менее 70% правильных ответов</p> |
| | <p>уметь</p> <ul style="list-style-type: none"> - формировать и обосновывать критерии качества, в том числе и автоматизированной системы с учетом требований информационной безопасности и проводить их оценку; - проводить анализ корректности полученных | <p>Решение стандартных практических задач</p> | <p>Задачи решены в полном объеме и получены верные ответы</p> | <p>Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах</p> | <p>Продемонстрирован верный ход решения в большинстве задач</p> | <p>Задачи решены</p> |

| | | | | | | |
|--|--|--|---|--|---------------|--|
| результатов; - проверять соответствие полученных результатов требованиям теории; - оценивать результаты экспериментов с моделью; - использовать методы оценки правильности выбранной модели; | | | | | | |
| владеть - навыками грамотной обработки результатов опыта и сопоставления их с теоретическими данными; - навыками корректного формулирования результатов исследования и применения математического аппарата для решения физических задач; | 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 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 (минимум 10 вопросов для тестирования с вариантами ответов)

1. Риск - это:

- а) неблагоприятное событие, влекущее за собой убыток;
- б) все предпосылки, имеющие возможность негативно повлиять на достижение стратегических целей в течение строго определенного временного промежутка;
- в) вероятность наступления стихийных бедствий либо технических аварий;
- г) вероятность провала программы;
- д) вероятность успеха.

2. Управление риском - это:

- а) отказ от рискованного проекта;
- б) комплекс мер, направленных на снижение вероятности реализации риска;
- в) комплекс мер, направленных на компенсацию, снижение, перенесение, уход или принятие риска;
- г) комплекс мероприятий, направленных на подготовку к реализации риска.

3. Содержательная сторона управления рисками включает в себя:

- а) планирование деятельности по реализации рискованного проекта;
- б) сравнение вероятностей и характеристик риска, полученных в результате оценки и анализа риска;

4. Что из перечисленного не является элементом системы управления рисками?

- а) выявление расхождений в альтернативах риска;
- б) разработка планов, позволяющих действовать оптимальным образом в ситуации риска;
- в) разработка конкретных мероприятий, направленных на минимизацию или устранение негативных последствий;
- г) учет психологического восприятия рискованных проектов;
- д) ни один из вариантов не являются элементом системы риск-менеджмента;

e) все перечисленные варианты являются элементами системы риск-менеджмента.

5. Как рассчитать остаточный риск?

а) Угрозы x Риски x Ценность актива;

б) $(\text{Угрозы} \times \text{Ценность актива} \times \text{Уязвимости}) \times \text{Риски}$
 $SLE \times \text{Частота} = ALE$;

в) $(\text{Угрозы} \times \text{Уязвимости} \times \text{Ценность актива}) \times \text{Недостаток контроля}$;

6. Что из перечисленного не является целью проведения анализа рисков?

а) Делегирование полномочий;

б) Количественная оценка воздействия потенциальных угроз;

в) Выявление рисков;

г) Определение баланса между воздействием риска и стоимостью необходимых контрмер;

7. Что представляет собой стандарт ISO/IEC 27799?

а) Стандарт по защите персональных данных о здоровье;

б) Новая версия BS 17799;

в) Определения для новой серии ISO 27000;

г) Новая версия NIST 800-60

8. OCTAVE, NIST 800-30 и AS/NZS 4360 являются различными подходами к реализации управления рисками в компаниях. В чем заключаются различия между этими методами?

а) NIST и OCTAVE являются корпоративными;

б) NIST и OCTAVE ориентирован на ИТ;

в) AS/NZS ориентирован на ИТ;

г) NIST и AS/NZS являются корпоративными;

9. Какой из следующих методов анализа рисков пытается определить, где вероятнее всего произойдет сбой?

а) Анализ связующего дерева;

б) AS/NZS;

в) NIST;

г) Анализ сбоев и дефектов;

10. Что было разработано, чтобы помочь странам и их правительствам построить законодательство по защите персональных данных похожим образом?

а) Безопасная OECD;

б) ISO\IEC;

в) OECD;

г) CPTED;

7.2.2 Примерный перечень заданий для решения стандартных задач

(минимум 10 вопросов для тестирования с вариантами ответов)

1. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?

1. Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски
2. Когда риски не могут быть приняты во внимание по политическим соображениям
3. Когда необходимые защитные меры слишком сложны
4. Когда стоимость контрмер превышает ценность актива и потенциальные потери

2. Что такое политики безопасности?

1. Пошаговые инструкции по выполнению задач безопасности
2. Общие руководящие требования по достижению определенного уровня безопасности
3. Широкие, высокоуровневые заявления руководства

4. Детализированные документы по обработке инцидентов безопасности
- 3. Какая из приведенных техник является самой важной при выборе конкретных защитных мер?**
 1. Анализ рисков
 2. *Анализ затрат / выгоды*
 3. Результаты ALE
 4. Выявление уязвимостей и угроз, являющихся причиной риска
- 4. Что лучше всего описывает цель расчета ALE?**
 1. Количественно оценить уровень безопасности среды
 2. Оценить возможные потери для каждой контрмеры
 3. Количественно оценить затраты / выгоды
 4. *Оценить потенциальные потери от угрозы в год*
- 5. Что является определением воздействия (exposure) на безопасность?**
 1. *Нечто, приводящее к ущербу от угрозы*
 2. Любая потенциальная опасность для информации или систем
 3. Любой недостаток или отсутствие информационной безопасности
 4. Потенциальные потери от угрозы
- 6. Эффективная программа безопасности требует сбалансированного применения:**
 1. *Технических и нетехнических методов*
 2. Контрмер и защитных механизмов
 3. Физической безопасности и технических средств защиты
 4. Процедур безопасности и шифрования
- 7. Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют:**
 1. Внедрение управления механизмами безопасности
 2. Классификацию данных после внедрения механизмов безопасности
 3. *Уровень доверия, обеспечиваемый механизмом безопасности*
 4. Соотношение затрат / выгод
- 8. Защита информации это:**
 1. процесс сбора, накопления, обработки, хранения, распределения и поиска информации;
 2. преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;
 3. получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
 4. совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;
 5. *деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.*
- 9. Естественные угрозы безопасности информации вызваны:**
 1. деятельностью человека;
 2. ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
 3. *воздействиями объективных физических процессов или стихийных природных явлений, независимых от человека;*
 4. корыстными устремлениями злоумышленников;
 5. ошибками при действиях персонала.
- 10. Искусственные угрозы безопасности информации вызваны:**
 1. *деятельностью человека;*
 2. ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
 3. воздействиями объективных физических процессов или стихийных природных

- явлений, независимых от человека;
4. корыстными устремлениями злоумышленников;
 5. ошибками при действиях персонала.

7.2.3 Примерный перечень заданий для решения прикладных задач (минимум 10 вопросов для тестирования с вариантами ответов)

1. Виды информационной безопасности:

1. Персональная, корпоративная, государственная
2. Клиентская, серверная, сетевая
3. Локальная, глобальная, смешанная

2. Цели информационной безопасности – своевременное обнаружение, предупреждение:

1. несанкционированного доступа, воздействия в сети
2. инсайдерства в организации
3. чрезвычайных ситуаций

3. Основные объекты информационной безопасности:

1. Компьютерные сети, базы данных
2. Информационные системы, психологическое состояние пользователей
3. Бизнес-ориентированные, коммерческие системы

4. Основными рисками информационной безопасности являются:

1. Искажение, уменьшение объема, перекодировка информации
2. Техническое вмешательство, выведение из строя оборудования сети
3. Потеря, искажение, утечка информации

5. К основным принципам обеспечения информационной безопасности относятся:

1. Экономической эффективности системы безопасности
2. Многоплатформенной реализации системы
3. Усиления защищенности всех звеньев системы

6. Почему количественный анализ рисков в чистом виде не достижим?

1. Он достижим и используется
2. Он присваивает уровни критичности. Их сложно перевести в денежный вид.
3. Это связано с точностью количественных элементов
4. Количественные измерения должны применяться к качественным элементам

7. Если используются автоматизированные инструменты для анализа рисков, почему все равно требуется так много времени для проведения анализа?

1. Много информации нужно собрать и ввести в программу
2. Руководство должно одобрить создание группы
3. Анализ рисков не может быть автоматизирован, что связано с самой природой оценки
4. Множество людей должно одобрить данные

8. Что такое CobiT и как он относится к разработке систем информационной безопасности и программ безопасности?

1. Список стандартов, процедур и политик для разработки программы безопасности
2. Текущая версия ISO 17799
3. Структура, которая была разработана для снижения внутреннего мошенничества в компаниях
4. Открытый стандарт, определяющий цели контроля

9. Из каких четырех доменов состоит CobiT?

1. Планирование и Организация, Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка
2. Планирование и Организация, Поддержка и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка

3. Планирование и Организация, Приобретение и Внедрение, Сопровождение и Покупка, Мониторинг и Оценка
4. Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка

10. CobiT был разработан на основе структуры COSO. Что является основными целями и задачами COSO?

1. COSO – это подход к управлению рисками, который относится к контрольным объектам и бизнес-процессам
2. *COSO относится к стратегическому уровню, тогда как CobiT больше направлен на операционный уровень*
3. COSO учитывает корпоративную культуру и разработку политик
4. COSO – это система отказоустойчивости

7.2.4 Примерный перечень вопросов для подготовки к зачету

Укажите вопросы для зачета

1. Сформулируйте понятие атаки.
2. Сформулируйте понятие угрозы.
3. Сформулируйте понятие риска.
4. Сформулируйте понятие защищенности.
5. Сформулируйте понятие ущерба.
6. Сформулируйте понятие уязвимости.
7. Сформулируйте понятие риска-анализа.
8. Что представляет собой процесс оценки рисков?
9. Какими понятиями оперируют при анализе рисков в отношении конкретной системы?
10. По каким критериям можно оценивать риски?
11. Что представляет собой объективная вероятность?
12. Что представляет собой субъективная вероятность?
13. Перечислите основные отечественные стандарты по оценке и управлению рисками.
14. Перечислите основные зарубежные стандарты по оценке и управлению рисками.
15. Перечислите основные отечественные концепции по оценке и управлению рисками.
16. Перечислите основные зарубежные концепции по оценке и управлению рисками.
17. Что понимается под предупреждением риска?
18. Что понимается под компенсацией ущерба?
19. Что понимается под поглощением риска?
20. Какой стандарт лег в основу многих современных концепций по управлению рисками?
21. Что представляет собой процесс управления риском?
22. Какие принципы лежат в основе процесса управления риском?
23. Какие управляющие воздействия возможны по отношению к риску?
24. Опишите структуру стандарта ISO 17799.
25. Что содержится в первой части стандарта ISO 17799?
26. Что содержится во второй части стандарта ISO 17799?
27. Какие методики управления рисками относятся к качественным методикам на основе требований ISO 17799?
28. На базе каких стандартов и руководств построена методика управления рисками RASoftwareTool?
29. Чем обусловлена актуальность количественных методик управления рисками?
30. Перечислите известные Вам качественные методики управления рисками.
31. Перечислите известные Вам количественные методики управления рисками.

32. Какие задачи возможно решать посредством использования методики управления рисками CRAMM?
33. Что лежит в основе метода управления рисками CRAMM?
34. Опишите основные этапы управления риском посредством методики CRAMM.
35. Перечислите недостатки методики CRAMM.
36. Какие программные продукты входят в семейство RiskWatch?
37. Опишите фазы реализации методики управления рисками RiskWatch.
38. Перечислите недостатки методики RiskWatch.
39. Опишите отличительные черты метода управления рисками ГРИФ.
40. Опишите основные этапы методики управления рисками ГРИФ.
41. Перечислите недостатки методики управления рисками ГРИФ.
42. Опишите сущность и этапы реализации методики управления рисками OCTAVE.
43. Опишите особенности методики управления рисками MITRE.
44. Какие стандарты являются в общепризнанными в области информационной безопасности?
45. Что легло в основу стандарта ИСО/МЭК 17799?
46. Что представляет собой оценка риска согласно стандарту ИСО/МЭК 17799?
47. На каких подходах основывается стратегия анализа рисков согласно стандарту ИСО/МЭК 17799?
48. Опишите преимущества базового подхода анализа рисков стандарта ИСО/МЭК 17799.
49. Опишите преимущества неформального подхода анализа рисков стандарта ИСО/МЭК 17799.
50. Опишите преимущества смешанного подхода анализа рисков стандарта ИСО/МЭК 17799.
51. Какие составные части включает в себя стандарт CobiT?
52. Каким образом группируются требования к информационной технологии согласно стандарту CobiT?
53. Опишите отличительные особенности стандарта SCORE.
54. Какая идея лежит в основе стандарта SysTrust?
55. Составьте таблицу методологии оценки рисков согласно стандарту NIST.
56. Опишите основные особенности стандарта NIST.
57. В каких случаях приходится использовать экспертные методы оценки риска?
58. Основные этапы определения субъективной вероятности.
59. По каким критериям можно классифицировать методы получения субъективной вероятности?
60. Перечислите основные группы методов нахождения субъективных вероятностей и сами методы, входящие в них.
61. Опишите особенности методов оценки непрерывных распределений.
62. Перечислите особенности, которые необходимо учитывать при использовании методов определения субъективной вероятности.
63. Дайте определение непрерывной случайной величины.
64. Дайте определение закона распределения вероятности случайной величины.
65. Что является основными характеристиками ущерба как случайной величины.
66. Математическое ожидание случайной величины.
67. Дисперсия случайной величины.
68. Среднеквадратическое отклонение случайной величины.
69. Начальные моменты случайной величины.
70. Центральные моменты случайной величины.
71. Коэффициент асимметрии случайной величины.
72. Коэффициент эксцесса случайной величины.
73. Алгоритм расчета общего риска системы на основе пиковых оценок риска в ее

компонентах.

74. Алгоритм расчета общего риска системы на основе усредненных оценок риска в ее компонентах.

75. С помощью какой теории производится анализ информационного риска в динамике?

76. Коэффициенты относительной чувствительности риска.

77. Коэффициенты дифференциальной чувствительности риска.

78. Формула дополнительного движения риска.

79. Матрица дифференциальной чувствительности риска.

80. Матрица относительной чувствительности риска.

81. Методы оценки защищенности атакуемых систем.

7.2.5 Примерный перечень заданий для решения прикладных задач

Примерный перечень заданий для подготовки к экзамену

Задание 1

1. Методика управления рисками RA Software Tool.

2. Стандарт ИСО/МЭК 17799.

Задание 2

1. Методы прямой оценки вероятностей событий.

2. Методика управления рисками CRAMM.

Задание 3

1. Метод изменяющегося интервала.

2. Графический метод.

Задание 4

1. Мода функции риска.

2. Стандарт BS 7799.

Задание 5

1. Начальные моменты функции риска.

2. Методика управления рисками OCTAVE.

Задание 6

1. Центральные моменты функции риска.

2. Пик функции риска.

Задание 7

1. Стандарт CobIT.

2. Методика управления рисками RiskWatch.

Задание 8

1. Метод отношений.

2. Риск-анализ в диапазоне ущербов.

Задание 9

1. Метод собственного значения.
2. Оценка риска сложных систем на основании риска их компонентов при реализации асинхронных атак.

Задание 10

1. Стандарт SCORE.
2. Методика управления рисками MITRE.

Задание 11

1. Метод равноценной корзины.
2. Оценка риска сложных систем на основании риска их компонентов при реализации синхронных атак.

Задание 12

1. Методика управления рисками ГРИФ.
2. Стандарт SysTrust.

Задание 13

1. Метод фиксированного интервала.
2. Графический метод.

Задание 14

1. Стандарт CobIT.
2. Метод собственного значения.

Задание 15

1. Метод изменяющегося интервала.
2. Методика управления рисками OCTAVE.

Задание 16

1. Стандарт SCORE.
2. Стандарт ИСО/МЭК 17799.

Задание 17

1. Начальные моменты функции риска.
2. Методы прямой оценки вероятностей событий.

Задание 18

1. Стандарт CobiT.
2. Метод отношений.

Задание 19

1. Оценка риска сложных систем на основании риска их компонентов при реализации асинхронных атак.
2. Методика управления рисками MITRE.

Задание 20

1. Риск-анализ в диапазоне ущербов.
2. Оценка риска сложных систем на основании риска их компонентов при реализации асинхронных атак.

7.2.6. Методика выставления оценки при проведении промежуточной аттестации

Экзамен проводится по тест-билетам, каждый из которых содержит вопрос и задачу. Каждый правильный ответ на вопрос оценивается 1 баллом, за задачу оценивается в 10 баллов (5 баллов за верно решенную 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 | Место риск-анализа в системе знаний по обеспечению безопасности систем и процессов. | ОПК-1, ПК-5, ПК-24 | Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту.... |
| 2 | Меры риска и защищенности систем. | ПК-5, ПК- 24 | Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту.... |
| 3 | Аналитическая оценка рисков | ПК-5, ПК- 24 | Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту.... |
| 4 | Нерегулярные распределения ущерба и динамика рисков. | ПК-5, ПК- 24 | Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту.... |
| 5 | Синтез систем с заданным | ПК-5, ПК- 24 | Тест, контрольная работа, |

| | | | |
|---|---|--------------|--|
| | риском. | | защита лабораторных работ, защита реферата, требования к курсовому проекту.... |
| 6 | Прогнозирование эффективности систем на основе анализа рисков ущербности и шансов полезности. | ПК-5, ПК- 24 | Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту.... |

7.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков (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 методике 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 методике 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 методике выставления оценки при проведении промежуточной аттестации.

8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

8.1. Перечень учебной литературы, необходимой для освоения дисциплины

Основная литература:

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

2. Методическое обеспечение оценки и регулирования рисков распределенных информационных систем : Учеб. пособие / Г. А. Остапенко [и др.]. - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2011. - 178 с. - 182-77; 250 экз.

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

Дополнительная литература:

1. Эпидемии в телекоммуникационных сетях [Текст] / Остапенко Александр Григорьевич [и др.] ; под ред. Д. А. Новикова. - Москва : Горячая линия - Телеком, 2018. - 282 с. : ил. - (Теория сетевых войн. № 1). - Библиогр.: с. 231-245 (244 назв.). - ISBN 978-5-9912-0682-2 : 736-00.

2. 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.

3. Моделирование риск-анализа социотехнических систем [Электронный ресурс] : учеб. пособие / В. П. Дуров [и др.]. - Электрон. текстовые дан. (3087 Кб). - Воронеж : ГОУВПО "Воронежский государственный технический университет", 2007. - 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/> (ЭБС IPRbooks)

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 «Математические основы риск-анализа» 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. **Примерный перечень заданий:**

Задание 1

1. Нормальное распределение ПВНУ. Аналитический расчет начальных моментов функции риска. Аналитический расчет моды ущерба и пика функции риска.

2. Нерегулярное экспоненциальное распределение ПВНУ. Аналитический расчет центральных моментов функции риска. Аналитический расчет коэффициента асимметрии и коэффициента эксцесса.

Задание 2

1. Распределение Фреше ПВНУ. Аналитический расчет центральных моментов функции риска. Аналитический расчет коэффициента асимметрии и коэффициента эксцесса.

2. Гамма-распределение ПВНУ. Аналитический расчет центральных моментов функции риска. Аналитический расчет коэффициента асимметрии и коэффициента эксцесса.

Задание 3

1. Распределение Парето ПВНУ. Аналитический расчет начальных моментов функции риска. Аналитический расчет моды ущерба и пика функции риска.

2. Бета-распределение ПВНУ. Аналитический расчет центральных моментов функции риска. Аналитический расчет коэффициента асимметрии и коэффициента эксцесса.

Задание 4

1. Логнормальное распределение ПВНУ. Аналитический расчет начальных моментов функции риска. Аналитический расчет моды ущерба и пика функции риска.

2. Нерегулярное показательное распределение ПВНУ. Аналитический расчет центральных моментов функции риска. Аналитический расчет коэффициента асимметрии и коэффициента эксцесса.

Задание 5

1. Нормальное распределение ПВНУ. Аналитический расчет центральных моментов функции риска. Аналитический расчет коэффициента асимметрии и коэффициента эксцесса.

2. Аналитическая оценка эффективности защиты системы.

Задание 6

1. Логнормальное распределение ПВНУ. Аналитический расчет центральных моментов функции риска. Аналитический расчет коэффициента асимметрии и коэффициента эксцесса.

2. Нерегулярное показательное распределение ПВНУ. Аналитический расчет начальных моментов функции риска. Аналитический расчет моды ущерба и пика функции риска

Задание 7

1. Нерегулярное экспоненциальное распределение ПВНУ. Аналитический расчет начальных моментов функции риска. Аналитический расчет моды ущерба и пика функции риска.

2. Распределение Эрланга ПВНУ. Аналитический расчет центральных моментов функции риска. Аналитический расчет коэффициента асимметрии и коэффициента эксцесса.

Задание 8

1. Распределение Вейбулла ПВНУ. Аналитический расчет начальных моментов функции риска. Аналитический расчет моды ущерба и пика функции риска.

2. Распределение Парето ПВНУ. Аналитический расчет центральных моментов функции риска. Аналитический расчет коэффициента асимметрии и коэффициента эксцесса.

Задание 9

1. Бета-распределение ПВНУ. Аналитический расчет начальных моментов функции риска. Аналитический расчет моды ущерба и пика функции риска.

2. Распределение Вейбулла ПВНУ. Аналитический расчет центральных моментов функции риска. Аналитический расчет коэффициента асимметрии и коэффициента эксцесса.

Задание 10

1. Распределение Фреше ПВНУ. Аналитический расчет начальных моментов функции риска. Аналитический расчет моды ущерба и пика функции риска.
2. Гамма-распределение ПВНУ. Аналитический расчет начальных моментов функции риска. Аналитический расчет моды ущерба и пика функции риска.

Задание 11

1. Распределение Эрланга ПВНУ. Аналитический расчет начальных моментов функции риска. Аналитический расчет моды ущерба и пика функции риска.
2. Аналитическая оценка эффективности защиты системы.

Задание 12

1. Нерегулярное экспоненциальное распределение ПВНУ. Аналитический расчет начальных моментов функции риска. Аналитический расчет моды ущерба и пика функции риска.
2. Логнормальное распределение ПВНУ. Аналитический расчет центральных моментов функции риска. Аналитический расчет коэффициента асимметрии и коэффициента эксцесса.

Задание 13

1. Нормальное распределение ПВНУ. Аналитический расчет начальных моментов функции риска. Аналитический расчет моды ущерба и пика функции риска.
2. Распределение Вейбулла ПВНУ. Аналитический расчет центральных моментов функции риска. Аналитический расчет коэффициента асимметрии и коэффициента эксцесса.

Задание 14

1. Распределение Эрланга ПВНУ. Аналитический расчет начальных моментов функции риска. Аналитический расчет моды ущерба и пика функции риска.
2. Гамма-распределение ПВНУ. Аналитический расчет центральных моментов функции риска. Аналитический расчет коэффициента асимметрии и коэффициента эксцесса.

Задание 15

1. Нерегулярное показательное распределение ПВНУ. Аналитический расчет начальных моментов функции риска. Аналитический расчет моды ущерба и пика функции риска.
2. Бета-распределение ПВНУ. Аналитический расчет центральных моментов функции риска. Аналитический расчет коэффициента асимметрии и коэффициента эксцесса.

Задание 16

1. Гамма-распределение ПВНУ. Аналитический расчет начальных моментов функции риска. Аналитический расчет моды ущерба и пика функции риска.
2. Нормальное распределение ПВНУ. Аналитический расчет центральных моментов функции риска. Аналитический расчет коэффициента асимметрии и коэффициента эксцесса.

Задание 17

1. Распределение Парето ПВНУ. Аналитический расчет начальных моментов функции риска. Аналитический расчет моды ущерба и пика функции риска.
2. Распределение Фреше ПВНУ. Аналитический расчет центральных моментов функции риска. Аналитический расчет коэффициента асимметрии и коэффициента эксцесса.

Задание 18

1. Аналитическая оценка эффективности защиты системы.
2. Нерегулярное экспоненциальное распределение ПВНУ. Аналитический расчет начальных моментов функции риска. Аналитический расчет моды ущерба и пика функции риска.

Задание 19

1. Распределение Вейбулла ПВНУ. Аналитический расчет центральных моментов функции риска. Аналитический расчет коэффициента асимметрии и коэффициента эксцесса.
2. Распределение Фреше ПВНУ. Аналитический расчет центральных моментов функции риска. Аналитический расчет коэффициента асимметрии и коэффициента эксцесса.

Задание 20

1. Распределение Эрланга ПВНУ. Аналитический расчет начальных моментов функции риска. Аналитический расчет модуля ущерба и пика функции риска.
2. Нерегулярное экспоненциальное распределение ПВНУ. Аналитический расчет начальных моментов функции риска. Аналитический расчет модуля ущерба и пика функции риска.

Занятия проводятся путем решения конкретных задач в аудитории.

Методика выполнения курсового проекта изложена в учебно-методическом пособии. Выполнять этапы курсового проекта должны своевременно 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; пометать 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 удастся 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 усвоению учебного материала и развитию навыков самообразования. Самостоятельная работа предполагает следующие составляющие: <ul style="list-style-type: none"> - 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. |