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 10.05.01 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

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:

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

ПСК-3.1 - способностью использовать современные критерии и стандарты для анализа безопасности распределенных компьютерных систем

ПСК-3.2 - способностью анализировать защиту информации в распределенных компьютерных системах, проводить мониторинг, аудит и контрольные проверки работоспособности и защищенности распределенных компьютерных систем

Компетенция	Результаты обучения, характеризующие сформированность компетенции
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.
ПСК-3.1	знать - современные критерии оценки риска и стандарты в области управления рисками для анализа безопасности распределенных компьютерных систем в области риск-анализа и управления рисками, а также умений применения рассматриваемого математического аппарата в профессиональной деятельности.
	уметь - применять на практике подходы к аналитическом оцениванию рисков, в том числе при нерегулярности роапспределениря ущербов и их димнмики
ПСК-3.2	знать - подходы к анализу информации, в то чиле и в реальном времени в РКС в части оценки эффективности системы защиты
	уметь - проводить мониторинг, аудит и контрольные проверки работоспособности и защищенности распределенных компьютерных систем
	владеть -инструментальными средствами проведения мониторинга и аудита РКС на на основе анализа рисков защищенности КС

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Математические основы риск-анализа» составляет 5 з.е.

Распределение трудоемкости дисциплины по видам занятий

очная форма обучения

Виды учебной работы	Всего часов	Семестры	
		4	5
Аудиторные занятия (всего)	90	54	36
В том числе:			
Лекции	36	18	18
Практические занятия (ПЗ)	54	36	18
Самостоятельная работа	54	36	18
Курсовой проект	+		+
Часы на контроль	36	-	36
Виды промежуточной аттестации - экзамен, зачет	+	+	+
Общая трудоемкость: академические часы зач.ед.	 180 5	 90 2.5	 90 2.5

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	Практ зан.	СРС	Всего, час
1	Место риск-анализа в системе знаний по обеспечению безопасности систем и процессов.	Понятийный аппарат и терминологическая база дисциплины. Оценка рисков и международныестрадарты ISO/IEC 17799:2000(E), ISO/IEC TR 13335-2, NIST800-30, Cobit, SCORE, SYS Trust. Концепции управления рисками OCTAVE, CRAMM, MITRE. Инструментарийуправленияинформационнымирисками. Методы анализа рисков на основе экспертных оценок и аппарата теории нечетких множеств. Методы управления информационными рисками в инновационной деятельности.	6	8	8	22
2	Меры риска и защищенности систем.	Меры риска и защищенности систем на основе вероятностных параметров и характеристик ущерба. Функции чувствительности и динамическое моделирование рисков. Оценка рисков сложных систем на основе параметров рисков их компонентов.	6	8	8	22
3	Аналитическая оценка рисков	Аналитическая оценка рисков при нормальном и логнормальном распределениях плотности вероятности наступления ущерба (ПВНУ). Аналитическая оценка рисков при гамма и бета-распределениях ПВНУ. Аналитическая оценка рисков при экспоненциальном, Вейбулла и Эрланга распределениях ПВНУ	6	8	8	22
4	Нерегулярные распределения ущерба и динамика рисков.	Аналитические риск-модели при биномиальном, Паскаля и мультинормальном распределениях вероятности наступления ущерба (ВНУ). Аналитические риск-модели при геометрическом и гипергеометрическом распределениях ВНУ. Аналитические риск-модели при пуассоновском распределении ВНУ и распределениях типа А и В.	6	10	10	26
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.	6	10	10	26
6	Прогнозирование	Понятие эффективности. Понятие шанса. Методы прогнозирования эффективности систем на	6	10	10	26

	эффективности систем на основе анализа рисков ущербности и шансов полезности.	основе анализа рисков ущербности и шансов полезности.				
		Итого	**36**	**54**	**54**	**144**

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 5 семестре для очной формы обучения.

Примерная тематика курсового проекта:

1. Разработка методики информационной безопасности на промышленном предприятии.
2. Функции чувствительности и динамического моделирование рисков.
3. Место риск-анализа в системе знаний по обеспечению безопасности систем и процессов. Понятийный аппарат и терминологическая база дисциплины.
4. Меры риска и защищенности систем на основе вероятностных параметров и характеристик ущерба.
5. Методы анализа рисков на основе экспертных оценок и аппарата теории нечетких множеств.
6. Оценка рисков и международные стандарты ISO/IEC 17799:2000(E), ISO/IECTR 13335-2, NIST 800-30, CobiT, SCORE, SysTrust.
7. Программные средства и методики анализа рисков CORAS, ГРИФ, RiskWatch.
8. Разработка методики информационной безопасности на промышленном предприятии.
9. Аналитический расчет начальных моментов функций риска.

Концепции управления рисками OCTAVE, CRAMM, MITRE. Инструментарий управления информационными рисками.

10. Модели прогнозирования развития компаний с учетом рисков.
11. Методы управления информационными рисками в инновационной деятельности.
12. Методы управления информационными рисками в инновационной деятельности.
13. Аналитический расчет начальных моментов функций риска.
14. Модель поиска рисков в текстовых сообщениях.
15. Методы управления рисками на рынке ценных бумаг.
16. Риск в экономической и предпринимательской деятельности.
17. Инструментарий управления информационными рисками.

18. Оценка рисков информационной безопасности при использовании крипто контейнеров.
19. Меры риска и защищенности систем на основе вероятностных параметров и характеристик ущерба.
20. Расчет рисков информационной безопасности.
21. Математическая модель рисков, возникающая при выполнении высокотехнологического проекта.
22. Модели управления рисками информационной системы.
23. Разработка модели управления информационными рисками и методов снижения рисков на примере конкретной организации.
24. Нерегулярные распределения ущерба и динамика рисков.
25. Математические модели рисков ИБ в системах персональных данных.
26. Математическая модель рисков информационной безопасности в производственном процессе.

Задачи, решаемые при выполнении курсового проекта:

- Использование математических методов обработки экспериментальных данных.
- Изучение основных стандартов и методов анализа рисков.
- Использование математических методов и моделей для решения прикладных задач.
- Изучение методов количественного риск-анализа процессов обработки, поиска и передачи информации.

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

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

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

7.1.1 Этап текущего контроля

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

«аттестован»;

«не аттестован».

Компе-тенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Аттестован	Не аттестован
ПК-4	знать - современные угрозы информационной безопасности объектов и принципы	знание понятийного аппарата и терминологии дисциплины	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

	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	умение формализовывать аналитическое оценки риска при различных распределениях ущерба	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 инструментарием управления информационными рисками	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

ПСК-3.1	знать - современные критерии оценки риска и стандарты в области управления рисками для анализа безопасности распределенных компьютерных систем в области риск-анализа и управления рисками, а также умений применения рассматриваемого математического аппарата в профессиональной деятельности.	знание системы показателей оценки риска для принятия управленческих решений руководителем при реализации менеджмента безопасности организации	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь - применять на практике подходы к аналитическом оцениванию рисков, в том числе при нерегулярности распределения ущербов и их динамики	умение использовать математические методы и модели для решения прикладных задач оценивания риска с использованием методов теории вероятностей и математической статистики	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПСК-3.2	знать - подходы к анализу информации, в то числе и в реальном времени в РКС в части оценки эффективности системы защиты	знание методик анализа рисков, в том числе на основе экспертных оценок и аппарата теории нечетких множеств	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь - проводить мониторинг, аудит и контрольные проверки работоспособности и защищенности распределенных компьютерных систем	умение на основе мер риска и защищенности проводить мониторинг распределённых КС на основе вероятностных параметров и характеристик ущерба. проекта	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

	владеть -инструментальными средствами проведения мониторинга и аудита РКС на на основе анализа рисков защищенности КС	Владение компьютерными интерактивными средствами мониторирования и аудита РКС по результатам оценки риска защищенности распределённых 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 4, 5 семестре для очной формы обучения по двух/четырех балльной системе:

«зачтено»

«не зачтено»

Компе-тенция	**Результаты обучения, характеризующие сформированность компетенции**	**Критерии оценивания**	**Зачтено**	**Не зачтено**
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;	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	уметь - анализировать угрозы и проводить риск-анализ и реализовывать методики управления рисками с целью обеспечения безопасности объектов информатизации	Решение стандартных практических задач	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены
	владеть	Решение прикладных задач в конкретной предметной	Продемонстрирова н верный ход решения в	Задачи не решены

	- технологиями обеспечения информационной безопасности в части проведения риск-анализа и управления риска; - средствами обеспечения информационной безопасности, анализа угроз, риск-анализа и управления рисками.	области	большинстве задач	
ПСК-3.1	знать - современные критерии оценки риска и стандарты в области управления рисками для анализа безопасности распределенных компьютерных систем в области риск-анализа и управления рисками, а также умений применения рассматриваемого математического аппарата в профессиональной деятельности.	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	уметь - применять на практике подходы к аналитическом оцениванию рисков, в том числе при нерегулярности распределения ущербов и их динамики	Решение стандартных практических задач	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены
ПСК-3.2	знать - подходы к анализу информации, в то числе и в реальном времени в РКС в части оценки эффективности системы защиты	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	уметь	Решение стандартных практических задач	Продемонстрирова н верный ход решения в	Задачи не решены

	- проводить мониторинг, аудит и контрольные проверки работоспособности и защищенности распределенных компьютерных систем		большинстве задач	
	владеть -инструментальными средствами проведения мониторинга и аудита РКС на на основе анализа рисков защищенности КС	Решение прикладных задач в конкретной предметной области	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены

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

Компе-тенция	**Результаты обучения, характеризующие сформированность компетенции**	**Критерии оценивания**	**Отлично**	**Хорошо**	**Удовл.**	**Неудовл.**
ПК-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;	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	уметь - анализировать угрозы и проводить риск-анализ и реализовывать методики управления рисками	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены

	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.	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
ПСК-3.1	знать - современные критерии оценки риска и стандарты в области управления рисками для анализа безопасности распределенных компьютерных систем в области риск-анализа и управления рисками, а также умений применения рассматриваемого математического аппарата в профессиональной деятельности.	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	уметь - применять на практике подходы к аналитическом оцениванию рисков, в том числе при нерегулярности распределения ущербов и их динамики	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
ПСК-3.2	знать - подходы к анализу информации, в то	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов

	числе и в реальном времени в РКС в части оценки эффективности системы защиты					
	уметь - проводить мониторинг, аудит и контрольные проверки работоспособности и защищенности распределенных компьютерных систем	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
	владеть -инструментальными средствами проведения мониторинга и аудита РКС на на основе анализа рисков защищенности КС	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены

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

7.2.1 Примерный перечень заданий для подготовки к тестированию

(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;

е) все перечисленные варианты является элементами системы риск-менеджмента.

5. Как рассчитать остаточный риск?

а)Угрозы х Риски х Ценность актива;

б) (Угрозы х Ценность актива х Уязвимости) х Риски

SLE х Частоту = ALE;

в) (Угрозы х Уязвимости х Ценность актива) х 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, независящих 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, независящих 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 относится:

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 риск-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. Опишитеструктурустандарта 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. Перечислитенедостаткиметодики CRAMM.

36. Какие программные продукты входит в семейство RiskWatch?

37. Опишите фазы реализации методики управления рисками RiskWatch.

38. ПеречислитенедостаткиметодикиRiskWatch.

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 стандартны 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. Математическоеожиданиеслучайнойвеличины.
67. Дисперсияслучайнойвеличины.
68. Среднеквадратическоеотклонениеслучайнойвеличины.
69. Начальныемоментыслучайнойвеличины.
70. Центральныемоментыслучайнойвеличины.
71. Коэффициентассиметриислучайнойвеличины.
72. Коэффициентэксцессаслучайнойвеличины.
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 дифференциальнойчувствительности 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 (Зачет) *проводится по тест-билетам, каждый из которых содержит вопрос 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	Место риск-анализа в системе знаний по обеспечению безопасности систем и процессов.	ПК-4	Тест, контрольная работа, защита лабораторных работ, защита реферата,

			требования к курсовому проекту….
2	Меры риска и защищенности систем.	ПК-4	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
3	Аналитическая оценка рисков	ПК-4	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
4	Нерегулярные распределения ущерба и динамика рисков.	ПК-4	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
5	Синтез систем с заданным риском.	ПК-4	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
6	Прогнозирование эффективности систем на основе анализа рисков ущербности и шансов полезности.	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. 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. Эпидемии в телекоммуникационных сетях [Текст] / Остапенко Александр Григорьевич [и др.]; под ред. Д. А. Новикова. - Москва: Горячая линия - Телеком, 2014. - 282 с.: ил. - (Теория сетевых войн. № 1). - Библиогр.: с. 231-245 (244 назв.). - ISBN 978-5-9912-0682-2: 736-00.
3. Атакуемые взвешенные сети [Текст] / Остапенко Александр Григорьевич [и др.]; под ред. Д. А. Новикова. - Москва: Горячая линия - Телеком, 2014. - 247 с.: ил. - (Теория сетевых войн. № 2). - Библиогр.: с. 201-213 (214 назв.). - ISBN 978-5-9912-0684-6: 708-00.

Дополнительная литература:

1. Методические указания к практическим занятиям по дисциплине "Математические основы риск-анализа" для студентов специальностей 090301 "Компьютерная безопасность", 090302 "Информационная безопасность телекоммуникационных систем",

090303 "Информационная безопасность автоматизированных систем" очной формы обучения [Электронный ресурс]. - Электрон. текстовые, граф. дан. (705 Кб). - Воронеж: ФГБОУ ВПО "Воронежский государственный технический университет", 2014. - 1 файл. - 00-00.

2. Методические указания к курсовому проектированию по дисциплине "Математические основы риск-анализа" для студентов специальностей 090301 "Компьютерная безопасность", 090302 "Информационная безопасность телекоммуникационных систем", 090303 "Информационная безопасность автоматизированных систем" очной формы обучения [Электронный ресурс] / Каф. систем информационной безопасности; Сост.: А. Г. Остапенко, М.В. Бурса. - Электрон. текстовые, граф. дан. (551 Кбайт). - Воронеж: ФГБОУ ВПО "Воронежский государственный технический университет", 2014. - 1 файл. - 00-00.
3. Методические указания к самостоятельным работам по дисциплине «Математические основы риск-анализа» для студентов специальностей 090301 «Компьютерная безопасность», 090302 «Информационная безопасность телекоммуникационных систем», 090303 «Информационная безопасность автоматизированных систем» очной формы обучения [Электронный ресурс] / Каф. систем информационной безопасности; Сост.М. В. Бурса. - Электрон. текстовые, граф. дан. (423 Кб). - Воронеж: ФГБОУ ВПО "Воронежский государственный технический университет", 2014. - 1 файл. - 00-00.

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 «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 моды ущерба и пика функции риска.
2. Нерегулярное экспоненциальное распределение ПВНУ. Аналитический расчет начальных моментов функции риска. Аналитический расчет моды 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 и в установленные сроки.

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

По дисциплине «Математические основы риск-анализа» читаются лекции, проводятся практические занятия, выполняется курсовой проект.

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.