

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ**
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Воронежский государственный технический университет»

УТВЕРЖДАЮ



Декан факультета ФИТКБ

/Бредихин А.В./

28.08.2025 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«Математические основы риск-анализа»

Специальность 10.05.02 Информационная безопасность телекоммуникационных систем

Специализация специализация № 9 "Управление безопасностью телекоммуникационных систем и сетей"

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет и 6 м.

Форма обучения очная

Год начала подготовки 2025

Автор программы

Л.В. Паринава

Заведующий кафедрой
Техносферной и пожарной
безопасности

А.Г. Остапенко

Руководитель ОПОП

С.С. Куликов

Воронеж 2025

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-9.5 - Способен управлять рисками систем защиты сетей электросвязи от НД, проведении НИОКР в сфере разработки средств и систем защиты СССЭ от НД, создания ЗТКС

ПК-9.7 - Способен выявлять естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности в области моделирования и анализа сложных естественных и искусственных систем

ПК-9.5	<p>Знать: жизненный цикл систем защиты, методы оценки и управления рисками, основы планирования и проведения опытно-конструкторских работ.</p> <p>Уметь: выстраивать баланс между уровнем защиты и производительностью сети, прогнозировать эволюцию угроз и заранее закладывать контрмеры в новые разработки.</p> <p>Владеть: методологией управления рисками на всех этапах жизненного цикла систем защиты СССЭ и ЗТКС, включая прогнозирование эволюции векторов угроз, интеграцию контрмер на стадии НИОКР и обеспечение требуемого уровня остаточного риска при заданных эксплуатационных характеристиках.</p>
--------	--

ПК-9.7	<p>Знать: математические основы теории информации, теории сложности, хаоса и самоорганизации в сложных сетях.</p> <p>Уметь: видеть за внешними проявлениями атак глубинные физические и математические закономерности, переводить реальные угрозы в строгие модели.</p> <p>Владеть: методами физико-математического моделирования сложных информационных систем, выявления фундаментальных закономерностей возникновения уязвимостей и применения естественнонаучного аппарата (теории информации, теории сложности, статистической физики) для анализа и прогнозирования поведения защищаемых систем в условиях дестабилизирующих воздействий.</p>
--------	--

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Математические основы риск-анализа» составляет 3 з.е.

Распределение трудоемкости дисциплины по видам занятий

Очная форма обучения

Виды учебной работы	Всего часов	Семестры
		5
Аудиторные занятия (всего)	72	72
В том числе:		
Лекции	36	36
Практические работы (ПР)		
Самостоятельная работа	36	36
Курсовой проект		
Часы на контроль		
Виды промежуточной аттестации - зачет	+	+
Общая трудоемкость:		
академические часы	108	108
зач.ед.	3	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	Лаб. 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 международные стандарты ISO/IEC 17799:2000(E),				

		<p>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>	6	6	6	18
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>	6	6	6	18
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>	6	6	6	18

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	6	6	18
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	6	6	18
6	Прогнозирование эффективности систем	Понятие эффективности. Понятие шанса. Методы	6	6	6	18
	на основе анализа рисков ущербности и шансов полезности.	прогнозирования эффективности систем на основе анализа рисков ущербности и шансов полезности.				
Итого			36	36	36	108

5.2 Перечень лабораторных работ

Укажите перечень лабораторных работ

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 изащищенности систем на основе вероятностных параметров и характеристик ущерба.

5. Методы анализа рисков на основе экспертных оценок и аппарататеории 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 криптоконтейнеров.

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 включает 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 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
ПК-9.5	знать архитектуру современных систем и средств защиты информации, принципы построения межсетевых экранов, СОВ, обнаружения вторжений и криптографической защиты	знание архитектуры современных систем и средств защиты информации, принципы построения межсетевых экранов, СОВ, обнаружения вторжений и криптографической защиты	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

	каналов.	каналов.		
	<p>уметь - проектировать и реализовывать защитные механизмы, способные отражать целенаправленные компьютерные атаки и блокировать несанкционированный доступ.</p>	<p>умение проектировать и реализовывать защитные механизмы, способные отражать целенаправленные компьютерные атаки и блокировать несанкционированный доступ.</p>		
	<p>владеть - навыками создания «живучих» систем защиты, которые сохраняют работоспособность даже под интенсивным воздействием противника.</p>	<p>владеет навыками работы с различными источниками современной информации в профессиональной сфере</p>		
ПК-9.7	<p>Знать: математические основы теории информации, теории сложности, хаоса и самоорганизации в сложных сетях. Уметь: видеть за внешними проявлениями атак глубинные физические и математические закономерности, переводить реальные угрозы в строгие модели. Владеть: методами физико-математического моделирования сложных информационных систем, выявления фундаментальных закономерностей возникновения уязвимостей и применения естественнонаучного аппарата (теории информации, теории сложности, статистической физики) для анализа и прогнозирования поведения защищаемых систем в условиях дестабилизирующих воздействий.</p>	<p>Знание математических основ теории информации, теории сложности, хаоса и самоорганизации в сложных сетях. Умение видеть за внешними проявлениями атак глубинные физические и математические закономерности, переводить реальные угрозы в строгие модели. Владение методами физико-математического моделирования сложных информационных систем, выявления фундаментальных закономерностей возникновения уязвимостей и применения естественнонаучного аппарата (теории информации, теории сложности, статистической физики) для анализа и прогнозирования поведения защищаемых систем в условиях дестабилизирующих воздействий.</p>	<p>Выполнение работ в срок, предусмотренный в рабочих программах</p>	<p>Невыполнение работ в срок, предусмотренный в рабочих программах</p>

7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 4,5 семестре в очной форме обучения по двух/четырёхбалльной системе:

«зачтено»

«незачтено»

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Зачтено	Незачтено
ПК-9.5	знать - жизненный цикл систем защиты, методы оценки и управления рисками, основы планирования и проведения опытно-конструкторских работ.	Тест	Выполнение теста на 70-100%	Выполнение не менее 70%
	уметь - выстраивать баланс между уровнем защиты и производительностью сети, прогнозировать эволюцию угроз и заранее закладывать контрмеры в новые разработки.	Решение стандартных практических задач	Продемонстрирован верный ход решения в большинстве задач	Задачи решены
	владеть - методологией управления рисками на всех этапах жизненного цикла систем защиты СССЭ и ЗТКС, включая прогнозирование эволюции векторов угроз, интеграцию контрмер на стадии НИОКР и обеспечение требуемого уровня остаточного риска при заданных эксплуатационных характеристиках.	Решение прикладных задач в конкретной предметной области	Продемонстрирован верный ход решения в большинстве задач	Задачи решены
ПК-9.7	знать - математические основы теории информации, теории сложности, хаоса и самоорганизации в сложных сетях.	Тест	Выполнение теста на 70-100%	Выполнение не менее 70%
	уметь - видеть за внешними проявлениями атак глубинные физические и математические закономерности, переводить реальные угрозы в строгие модели.	Решение стандартных практических задач	Продемонстрирован	Задачи решены

			верный ход решения в большинстве задач	
владеть	методами физико-математического моделирования сложных информационных систем, выявления фундаментальных закономерностей возникновения уязвимостей и применения естественнонаучного аппарата (теории информации, теории сложности, статистической физики) для анализа и прогнозирования поведения защищаемых систем в условиях дестабилизирующих воздействий.	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 оценивания	Отлично	Хорошо	Удовл.	Неудовл.
ПК-9.5	знать - жизненный цикл систем защиты, методы оценки и управления рисками, основы планирования и проведения опытно-конструкторских работ.	Тест	Выполнено не менее 90-100%	Выполнено не менее 80-90%	Выполнено не менее 70-80%	В тесте менее 70% правильных ответов
	уметь - выстраивать баланс между уровнем защиты и производительностью сети, прогнозировать эволюцию угроз и заранее закладывать контрмеры в новые разработки.	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не полученных верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи решены

	<p>знать</p> <p>- жизненный цикл систем защиты, методы оценки и управления рисками, основы планирования и проведения опытно-конструкторских работ.</p>	<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 полученных верный ответ во всех задачах</p>	<p>Продемонстрирован верный ход решения в большинстве задач</p>	<p>Задачи решены</p>
ПК - 9.7	<p>знать</p> <p>- математические основы теории информации, теории сложности, хаоса и самоорганизации в сложных сетях.</p>	<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> <p>- видеть за внешними проявлениями атак глубинные физические и математические закономерности, переводить реальные угрозы в строгие модели.</p>	<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 полученных верный ответ во всех задачах</p>	<p>Продемонстрирован верный ход решения в большинстве задач</p>	<p>Задачи решены</p>
	<p>владеть</p> <p>- методами физико-математического моделирования сложных информационных систем, выявления фундаментальных закономерностей возникновения уязвимостей и применения естественнонаучного аппарата (теории информации, теории сложности, статистической физики) для анализа и прогнозирования поведения защищаемых систем в условиях дестабилизирующих воздействий.</p>	<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 полученных верный ответ во всех задачах</p>	<p>Продемонстрирован верный ход решения в большинстве задач</p>	<p>Задачи решены</p>

7.2 Примерный перечень оценочных средств (типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков (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 является элементом системы риск-менеджмента;
- е) *все перечисленные варианты являются элементами системы риск-менеджмента.*

5. Как рассчитать остаточный риск?

- а) Угрозы x Риски x Ценность актива;
- б) *(Угрозы x Ценность актива x Уязвимости) x Риски*
 $SLE \times Частота = ALE$;
- в) *(Угрозы x Уязвимости x Ценность актива) x 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 пытаются 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 свариваемых вариантов 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 нее.*

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 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. 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 OSTA VE.
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

Укажите вопросы для экзамена

Примерный перечень заданий для подготовки к экзамену

Задание 1

1. Методика управления рисками RASoftwareTool.

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 оценивается 1 баллом, задача оценивается в 10 баллов (5 баллов за 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

тбдо10баллов

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-9.5, ПК-9.7	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту....
2	Меры риска и защищенности систем.	ПК-9.5, ПК-9.7	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту....
3	Аналитическая оценка рисков	ПК-9.5, ПК-9.7	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту....
4	Нерегулярные распределения ущерба и динамика рисков.	ПК-9.5, ПК-9.7	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту....
5	Синтез систем с заданным риском.	ПК-9.5, ПК-9.7	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-9.5, ПК-9.7	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 экзаменатор

омивыставляетсяоценкасогласнометодикивыставленияоценкиприпроведении промежуточнойаттестации.

Решениестандартныхзадачосуществляется,либоприпомощикомпьютернойсистемьтестирования,либоиспользованиемвыданныхзадачнабумажномносителе.Времярешениязадач30мин.Затемосуществляетсяпроверкарешениязадачэкзаменаторомивыставляетсяоценка,согласнометодикивыставленияоценкиприпроведениипромежуточнойаттестации.

Решениеприкладныхзадачосуществляется,либоприпомощикомпьютернойсистемьтестирования,либоиспользованиемвыданныхзадачнабумажномносителе.Времярешениязадач30мин.Затемосуществляетсяпроверкарешениязадачэкзаменаторомивыставляетсяоценка,согласнометодикивыставленияоценкиприпроведениипромежуточнойаттестации.

Защитакурсовойработы,курсовогопроектаилиотчетаповсемвидампрактикосуществляетсясогласнотребованиям,предъявляемымкработе,описаннымв методическихматериалах.Примерноевремязащитынаодногостудентасоставляет20мин.

8 УЧЕБНОМЕТОДИЧЕСКОЕИИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕДИСЦИПЛИНЫ)

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.
681.3
Э 71
Эпидемии в телекоммуникационных сетях [Текст] / 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.
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.

681.3

А 92

Атакуемые взвешенные сети [Текст] / под ред. Д. А. Новикова. - Москва : Горячая линия - Телеком, 2018. - 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/> (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.

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 установленные сроки.

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

Под 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; 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.
Лабораторная работа	Лабораторные работы позволяют научиться применять теоретические знания, полученные на лекции при решении конкретных задач. Чтобы наиболее рационально и полно использовать все возможности лабораторных для подготовки к ним необходимо: следует разобрать лекцию по соответствующей теме, ознакомиться с соответствующим разделом учебника, проработать дополнительную литературу и источники, решить задачи и выполнить другие письменные задания.
Самостоятельная работа	Самостоятельная работа студентов способствует глубокому усвоению 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.