

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ
Н.Г. ЧЕРНЫШЕВСКОГО»

Механико-математический факультет

УТВЕРЖДАЮ
Декан механико-математического
факультета

 Захаров А.М.

"18" 09 2021г.

Рабочая программа дисциплины

МАТЕМАТИЧЕСКИЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

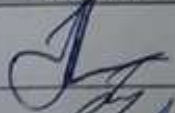
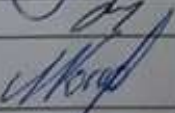
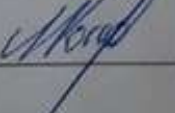
Направление подготовки бакалавриата
09.03.03 – Прикладная информатика

Профиль подготовки бакалавриата
Прикладная информатика в экономике

Квалификация (степень) выпускника
Бакалавр

Форма обучения
очная

Саратов,
2021

Статус	ФИО	Подпись	Дата
Преподаватель-разработчик	Амелин Р.В.		28.09.21
Председатель НМК	Тышкевич С.В.		28.09.21
Заведующий кафедрой	Коссович Л.Ю.		28.09.21
Специалист Учебного управления			

1. Цели освоения дисциплины

Цели освоения дисциплины «Математические основы информационной безопасности» заключаются в получении представления о современной методологии обеспечения информационной безопасности и о роли математических методов и программно-технических средств в обеспечении информационной безопасности, в подготовке к применению методов обеспечения информационной безопасности на этапах проектирования, разработки и эксплуатации сложно организованных программных систем.

2. Место дисциплины в структуре ООП

Дисциплина «Математические основы информационной безопасности» включена в обязательную часть Блока 1 «Дисциплины (модули)» ООП бакалавриата по направлению 09.03.03 «Прикладная информатика». На ее изучение отводится 288 часов (90 часов аудиторной работы, 158 часов СР, 36 часов - контроль). Согласно учебному плану направления и профиля подготовки данный курс в седьмом семестре заканчивается зачетом, в восьмом семестре - экзаменом.

Для этого направления подготовки она является краеугольным камнем общенаучной и специальной подготовки и находится в логической и содержательно-методической взаимосвязи с дисциплинами обязательной части: «Информационные системы и технологии», «Информатика и программирование», «Вычислительные системы, сети и телекоммуникации».

Дисциплина «Математические основы информационной безопасности» изучается на четвертом году обучения и является одной из важнейших терминальных дисциплин, завершающих базовую подготовку бакалавра прикладной информатики.

3. Результаты обучения по дисциплине

Код и наименование компетенции	Код и наименование индикатора (индикаторов) достижения компетенции	Результаты обучения
<p>ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.</p>	<p>1.1_Б.ОПК-3. Применяет принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с использованием информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.</p>	<p>Знать: - основные программно-технические методы и средства обеспечения информационной безопасности подконтрольных объектов, их роль и место в программной архитектуре компьютерных систем;</p> <p>Уметь: - использовать специализированное программное обеспечение для решения задач информационной безопасности.</p> <p>Владеть: - навыками применения положений современных нормативных документов и стандартов в области информационной безопасности.</p>
	<p>2.1_Б.ОПК-3. Решает стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.</p>	<p>Знать: - типовые подходы к программной реализации базовых сервисов безопасности в компьютерных системах; - типовые ошибки программирования, приводящие к уязвимостям компьютерных систем;</p> <p>Уметь: - выявлять угрозы информационной безопасности, обосновывать организационно-технические мероприятия по защите информации в ИС;</p> <p>Владеть: - навыками проведения аудита программного обеспечения на предмет наличия типовых ошибок программирования.</p>
	<p>3.1_Б.ОПК-3. Имеет опыт подготовки обзоров, аннотаций, составления рефератов, научных докладов,</p>	<p>Знать: - математические основы, необходимые для решения задач обеспечения информационной безопасности.</p>

	публикаций, и библиографии по научно- исследовательской работе с учетом требований информационной безопасности.	Уметь: - готовить обзоры, аннотации по тематике информационной безопасности.
ОПК-4. Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью.	1.1_Б.ОПК-4. Свободно оперирует основными стандартами оформления технической документации на различных стадиях жизненного цикла информационной системы.	Владеть: - понятийным аппаратом информационной безопасности.
		Знать: - математические основы, необходимые для решения задач обеспечения информационной безопасности;
		Уметь: - применять математические методы в обеспечении информационной безопасности
		Владеть: - понятийным аппаратом информационной безопасности;
	2.1_Б.ОПК-4. Использует стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы.	Знать: - основные криптографические методы, алгоритмы и протоколы; - основные положения методологии комплексного подхода к обеспечению информационной безопасности;
	3.1_Б.ОПК-4. Имеет навык	Уметь: - проводить анализ защищенности информационной системы, разрабатывать модели угроз для информационной системы, проектировать и внедрять систему защиты информации в соответствии с разработанной моделью угроз; Владеть: - навыками применения современного математического инструментария для решения задач в сфере информационной безопасности.
	3.1_Б.ОПК-4. Имеет навык	Знать:

	составления технической документации на различных этапах жизненного цикла информационной системы.	- виды угроз ИС и методы обеспечения информационной безопасности; - типовые математические модели информационно безопасных систем.
		Уметь: - проводить анализ защищенности информационной системы.
		Владеть: - методикой построения, анализа и применения математических моделей для оценки степени защищенности информационной системы, качества использованных алгоритмов и технологий.

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 8 зачетных единиц (288 часов).

№ п/п	Раздел дисциплины	С е м е с т р	Недел я семест ра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)						Формы текущего контроля успеваемости (по неделям семестра) Формы промежуточной аттестации (по семестрам)
				Лекции	Лаб.	Прак. занятия	КСР	СРС	Контроль	
1.	Основной понятия информационной безопасности	7	1-2	2	4			10		Устный опрос
2.	Элементы теории информации и кодирования.	7	3-6	4	4			10		Устный опрос
3.	Математические основы криптографии	7	7-10	4	12			12		Устный опрос
4.	Криптографические методы защиты информации.	7	11-16	6	12			10		Устный опрос
5.	Идентификация и аутентификация.	7	17-18	2	4		2	10		Устный опрос
	Промежуточная аттестация									Зачет
	Общая трудоемкость дисциплины за 7 семестр – 108 часов			18	36		2	52		
6.	Протоколирование и аудит.	8	1-2	2	2	2		5		Устный опрос
7.	Компьютерные вирусы.	8	3-4	2	2	2		5		Устный опрос
8.	Средства защиты сети.	8	5-6	2	2	2		5		Устный опрос

9.	Средства и методы противодействия угрозам доступности информации.	8	7-8	2	2	2		5		Устный опрос
10.	Основные принципы построения систем защиты.	8	9-10	2	2	1		4		Устный опрос
11.	Информационная безопасность с точки зрения технологии программирования.	8	11	2	2	2		4		Устный опрос
12.	Техника и методология атаки.	8	12	1	1	1	2	3		Устный опрос
	Промежуточная аттестация								36	Экзамен
	Общая трудоемкость дисциплины за 8 семестр – 108 часов			13	13	13	2	31	36	
	Итого:			31	49	13	4	83	36	

Содержание дисциплины

Раздел 1. Основные понятия информационной безопасности

1.1. Предмет информационной безопасности. Свойства компьютерной информации, важные с точки зрения информационной безопасности: конфиденциальность, целостность и доступность.

1.2. Угрозы информационной безопасности.

1.3. Каналы утечки информации.

1.4. Неформальная модель нарушителя.

1.5. Обзор стандартов и нормативно-правовой базы в сфере информационной безопасности.

Раздел 2. Элементы теории информации и кодирования

2.1. Сигналы, данные и методы получения информации. Свойства информации.

2.2. Количество информации как мера уменьшения неопределенности знаний. Алфавитный подход к вычислению количества информации.

2.3. Определение вероятности и основные правила вычисления количества информации.

2.4. Информационная модель Шеннона.

2.5. Формулы Шеннона и Хартли.

2.6. Понятие кода. Связь между информационной емкостью и средней длиной кода. Избыточность кодирования.

2.7. Метод сжатия по Хаффману. Код Хэмминга

Раздел 3. Математические основы криптографии

3.1. Множества и отношения. Бинарные отображения.

3.2. Основная теорема арифметики. Алгоритм деления в Z .

3.3. Понятие группы. Изоморфизмы групп.

- 3.4. Понятие и свойства колец. Кольцо вычетов.
- 3.5. Понятие поля. Поля Галуа.
- 3.6. Кольца многочленов. Алгоритм деления в $A[X]$. Разложение в кольце многочленов. Неприводимые многочлены.
- 3.7. Китайская теорема об остатках
- 3.8. Эллиптические кривые.

Раздел 4. Криптографические методы защиты информации

- 4.1. Понятие симметричных алгоритмов шифрования.
- 4.2. Обзор классических симметричных алгоритмов. Моноалфавитный шифр. Шифр Гронсфельда. Шифр Плейфейера. Шифр Хилла. Одноразовый блокнот. Перестановочные шифры.
- 4.3. Диффузия и коффузия. Схема Файстеля.
- 4.4. Обзор современных симметричных алгоритмов шифрования. Шифр DES. Шифр AES.
- 4.5. Режимы функционирования блочных шифров.
- 4.6. Скремблеры.
- 4.7. Виды криптоанализа симметричных алгоритмов.
- 4.8. Шифрование с открытым ключом. Алгоритм RSA.
- 4.9. Понятие и свойства хэш-функции. Электронная шифровая подпись.
- 4.10. Обзор современных отечественных и зарубежных стандартов шифрования и ЭЦП.
- 4.11. Понятие криптографического протокола.
- 4.12. Протоколы обмена ключами. Алгоритм Диффи-Хеллмана. Атака «человек посередине».
- 4.13. Алгоритмы генерации псевдослучайных последовательностей.

Раздел 5. Идентификация и аутентификация

- 5.1. Понятия идентификации и аутентификации. Виды аутентификации. Типология протоколов аутентификации.
- 5.2. Строгая односторонняя аутентификация на основе случайных чисел. Строгая двусторонняя аутентификация на основе случайных чисел. Аутентификация на основе асимметричного алгоритма.
- 5.3. Протокол Kerberos.
- 5.4. Механизмы аутентификации при осуществлении подключений. Протокол PPP SHAP. Протокол PPP EAP. Стандарт IEEE 802.1x

5.5. Аутентификация в защищенных соединениях. Протоколы SSL, TLS, SSH, S-HTTP, SOCKS. Семейство протоколов IPSec.

Раздел 6. Протоколирование и аудит

6.1. Понятие и назначение протоколирования и аудита. Подход к протоколированию в «Оранжевой книге».

6.2. Активный аудит. Сигнатура атаки. Функциональные компоненты и архитектура систем активного аудита.

Раздел 7. Компьютерные вирусы

7.1. Общие сведения о компьютерных вирусах. Структура вируса. Классификации вирусов.

7.2. Файловые вирусы и макровирусы. Загрузочные вирусы. Сетевые черви. Другие классы вредоносных программ: троянские кони, логические бомбы.

7.3. Технологии маскировки вирусов. Тенденции современных компьютерных вирусов.

7.4. Понятие антивируса. Методы обнаружения зараженных файлов. Обзор современных антивирусов.

7.5. Развертывание системы антивирусной защиты.

Раздел 8. Средства защиты сети

8.1. Межсетевые экраны.

8.2. Виртуальные частные сети.

8.3. Системы обнаружения вторжений. Анализ защищенности системы.

Раздел 9. Средства и методы противодействия угрозам доступности информации

9.1. Понятие и основные угрозы доступности информации. Показатели эффективности системы. Коэффициент готовности.

9.2. Методы обеспечения отказоустойчивости. Нейтрализация отказов. Живучесть. Резервирование. Программное обеспечение промежуточного слоя.

9.3. Архитектурные принципы обеспечения обслуживаемости. Восстановление после отказов.

Раздел 10. Основные принципы построения систем защиты

- 10.1. Меры противодействия угрозам безопасности.
- 10.2. Принципы построения систем защиты.
- 10.3. Понятие и назначение модели безопасности.
- 10.4. Модель дискреционного доступа. Модель Белла-ЛаПадулы. Ролевая модель контроля доступа.
- 10.5. Системы разграничения доступа

Раздел 11. Информационная безопасность с точки зрения технологии программирования

- 11.1. Основные принципы разработки безопасных систем.
- 11.2. Основные ошибки программирования. Причины и последствия переполнения буфера.
- 11.3. Анализ некоторых программных реализаций сервисов безопасности.

Раздел 12. Техника и методология атаки

- 12.1. Стратегия злоумышленника. Внешний анализ системы. Сканирование портов. Методы определения программно-аппаратной конфигурации системы и способы противодействия. Системы автоматического сканирования.
- 12.2. Использование уязвимостей в программном обеспечении. Эксплойты. Примеры наиболее известных уязвимостей в современных компьютерных системах.
- 12.3. Виды популярных атак и средства противодействия. SQL-инъекции. Межсайтовый скриптинг.

5. Образовательные технологии, применяемые при освоении дисциплины

Для реализации компетентностного подхода в учебном процессе применяются следующие образовательные технологии:

- 1) при проведении лекционных занятий: информационные лекции, проблемные лекции, лекции беседы, лекции дискуссии, лекции с заранее запланированными ошибками;
- 2) при проведении практических занятий: традиционные занятия, занятия исследования, проблемные ситуации, ситуации с ошибкой;
- 3) при организации самостоятельной работы студентов: поиск и обработка информации, в том числе с использованием информационно-

телекоммуникационных технологий; исследование проблемной ситуации; постановка и решение задач из предметной области; отработка навыков применения стандартных методов к решению задач предметной области.

Успешное освоение материала курса предполагает большую самостоятельную работу студентов и руководство этой работой со стороны преподавателей. Применяются следующие формы контроля: устный опрос, проверка решения практических задач, контрольная работа.

При обучении лиц с ограниченными возможностями здоровья и инвалидов используются подходы, способствующие созданию безбарьерной образовательной среды: технологии дифференциации и индивидуального обучения, применение соответствующих методик по работе с инвалидами, использование средств дистанционного общения, проведение дополнительных индивидуальных консультаций по изучаемым теоретическим вопросам и практическим занятиям, оказание помощи при подготовке к промежуточной аттестации. Подготовка, при необходимости, учебных и контрольно-измерительных материалов в формах, доступных для изучения студентами с особыми образовательными потребностями (для студентов с нарушениями зрения учебные материалы подготавливаются с применением укрупненного шрифта, используются аудиозаписи занятий; для студентов с нарушением слуха предоставляются электронные лекции, печатные раздаточные материалы с заданиями для самостоятельной работы).

При необходимости, для подготовки к ответу на практическом занятии, студентам с инвалидностью и студентам с ограниченными возможностями здоровья среднее время увеличивается в 1,5–2 раза по сравнению со средним временем подготовки обычного студента.

Для студентов с инвалидностью или с ограниченными возможностями здоровья форма промежуточной аттестации устанавливается с учетом индивидуальных психофизических особенностей (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п.). Промежуточная аттестация по дисциплине может проводиться в несколько этапов в форме рубежного контроля по завершению изучения отдельных тем дисциплины.

6. Учебно-методическое обеспечение самостоятельной работы студентов. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

Самостоятельная внеаудиторная работа студентов проводится в форме изучения и анализа лекционного материала, изучения отдельных теоретических вопросов по предлагаемой литературе, подбора дополнительных источников для извлечения научно-технической

информации, связанной с проблемами, изучаемыми в рамках данной дисциплины и решения задач с дальнейшим их разбором или обсуждением на аудиторных занятиях, подготовки к промежуточной аттестации.

Самостоятельная аудиторная работа студентов проводится в форме самостоятельного решения задач на практических занятиях с дальнейшим их разбором и обсуждением; проведения контрольной работы; поиска решений проблемных ситуаций, предложенных на лекциях и практических занятиях; поиска и устранения ошибок, заложенных в представлении материала преподавателем и допущенных другими студентами.

Текущий контроль усвоения дисциплины «Математические основы информационной безопасности» проводится в форме устных опросов на лекционных и практических занятиях, практических задач, связанных с программированием, на практических занятиях, контрольных работ по темам «Комплексный анализ защищенности информационной системы организации», «Разработка политики безопасности и модели угроз для заданной организации», промежуточного тестирования. Примерные варианты контрольных работ, задач и тестов содержатся в фонде оценочных средств текущего контроля и промежуточной аттестации по дисциплине.

Промежуточная аттестация по дисциплине «Математические основы информационной безопасности» проводится в форме зачета в 7 семестре и в форме экзамена в 8 семестре.

Список вопросов к устному зачету

- Свойства компьютерной информации, важные с точки зрения информационной безопасности: конфиденциальность, целостность и доступность.
- Угрозы информационной безопасности.
- Каналы утечки информации.
- Неформальная модель нарушителя.
- Обзор стандартов и нормативно-правовой базы в сфере информационной безопасности.
- Сигналы, данные и методы получения информации. Свойства информации.
- Количество информации как мера уменьшения неопределенности знаний. Алфавитный подход к вычислению количества информации.
- Определение вероятности и основные правила вычисления количества информации.
- Информационная модель Шеннона.

- Формулы Шеннона и Хартли.
- Понятие кода. Связь между информационной емкостью и средней длиной кода. Избыточность кодирования.
- Метод сжатия по Хаффману.
- Код Хэмминга
- Множества и отношения. Бинарные отображения.
- Основная теорема арифметики. Алгоритм деления в Z .
- Понятие группы. Изоморфизмы групп.
- Понятие и свойства колец. Кольцо вычетов.
- Понятие поля. Поля Галуа.
- Кольца многочленов. Алгоритм деления в $A[X]$. Разложение в кольце многочленов. Неприводимые многочлены.
- Китайская теорема об остатках
- Эллиптические кривые.
- Понятие симметричных алгоритмов шифрования.

Список вопросов к устному экзамену

- Обзор классических симметричных алгоритмов. Моноалфавитный шифр. Шифр Гронсфельда. Шифр Плейфейера. Шифр Хилла. Одноразовый блокнот. Перестановочные шифры.
- Диффузия и коффузия. Схема Файстеля.
- Обзор современных симметричных алгоритмов шифрования. Шифр DES. Шифр AES.
- Режимы функционирования блочных шифров.
- Скремблеры.
- Виды криптоанализа симметричных алгоритмов.
- Шифрование с открытым ключом. Алгоритм RSA.
- Понятие и свойства хэш-функции.
- Электронная шифровая подпись.
- Обзор современных отечественных и зарубежных стандартов шифрования и ЭЦП.
- Понятие криптографического протокола.
- Протоколы обмена ключами. Алгоритм Диффи-Хеллмана. Атака «человек посередине».
- Алгоритмы генерации псевдослучайных последовательностей.

- Понятия идентификации и аутентификации. Виды аутентификации. Типология протоколов аутентификации.

- Строгая односторонняя аутентификация на основе случайных чисел. Строгая двусторонняя аутентификация на основе случайных чисел. Аутентификация на основе асимметричного алгоритма.

- Протокол Kerberos.

- Механизмы аутентификации при осуществлении подключений. Протокол PPP CHAP. Протокол PPP EAP. Стандарт IEEE 802.1x

- Аутентификация в защищенных соединениях. Протоколы SSL, TLS, SSH, S-HTTP, SOCKS. Семейство протоколов IPSec.

- Понятие и назначение протоколирования и аудита. Подход к протоколированию в «Оранжевой книге».

- Активный аудит. Сигнатура атаки. Функциональные компоненты и архитектура систем активного аудита.

- Общие сведения о компьютерных вирусах. Структура вируса. Классификации вирусов.

- Файловые вирусы и макровирусы. Загрузочные вирусы. Сетевые черви. Другие классы вредоносных программ: троянские кони, логические бомбы.

- Технологии маскировки вирусов. Тенденции современных компьютерных вирусов.

- Понятие антивируса. Методы обнаружения зараженных файлов. Обзор современных антивирусов.

- Развертывание системы антивирусной защиты.

- Межсетевые экраны.

- Виртуальные частные сети.

- Системы обнаружения вторжений. Анализ защищенности системы.

- Понятие и основные угрозы доступности информации. Показатели эффективности системы. Коэффициент готовности.

- Методы обеспечения отказоустойчивости. Нейтрализация отказов. Живучесть. Резервирование. Программное обеспечение промежуточного слоя.

- Архитектурные принципы обеспечения обслуживаемости. Восстановление после отказов.

- Меры противодействия угрозам безопасности.

- Принципы построения систем защиты.

- Понятие и назначение модели безопасности.
- Модель дискреционного доступа. Модель Белла-ЛаПадулы. Ролевая модель контроля доступа.
- Системы разграничения доступа
- Основные принципы разработки безопасных систем.
- Основные ошибки программирования. Причины и последствия переполнения буфера.
- Анализ некоторых программных реализаций сервисов безопасности.
- Стратегия злоумышленника.
- Использование уязвимостей в программном обеспечении.
- SQL-инъекции.
- Межсайтовый скриптинг.

7. Данные для учета успеваемости студентов в БАРС

Таблица максимальных баллов по видам учебной деятельности.

1	2	3	4	5	6	7	8	9
Семестр	Лекции	Лабораторные занятия	Практические занятия	Самостоятельная работа	Автоматизированное тестирование	Другие виды учебной деятельности	Промежуточная аттестация	Итого
7	20	40	0	0	0	0	40	100
8	20	20	20	0	0	0	40	100

Программа оценивания учебной деятельности студента

7 семестр

Лекции

Оценивается посещаемость, активность, умение выделить главную мысль и др. Преподаватель выдает красивые именные карточки с изображением болот и равнин (а также островов) за попытки студентов сказать что-то умное и поучаствовать в дискуссии. В конце семестра карточки подсчитываются и пропорционально начисляются баллы. Максимальный балл (20) получает обладатель наибольшего числа карточек.

Лабораторные работы

Оценивается самостоятельность при выполнении работы, грамотность в оформлении, правильность выполнения и т.д. Заработать можно максимум 40

баллов, которые начисляются преподавателем за решение поставленных задач (программирование, работа в программах и т.д.)

Промежуточная аттестация

Проходит в виде устного ответа по билетам. Максимально возможный балл 40.

При проведении промежуточной аттестации

ответ на «отлично» оценивается от 31 до 40 баллов;

ответ на «хорошо» оценивается от 21 до 30 баллов;

ответ на «удовлетворительно» оценивается от 11 до 20 баллов;

ответ на «неудовлетворительно» оценивается от 0 до 10 баллов.

Таким образом, максимально возможная сумма баллов за все виды учебной деятельности студента за 7 семестр по дисциплине «Математические основы информационной безопасности» составляет 100 баллов.

Таблица пересчета полученной студентом суммы баллов по дисциплине «Математические основы информационной безопасности» за 7 семестр в оценку (зачет):

50 баллов и более	«зачтено»
меньше 50 баллов	«не зачтено»

8 семестр

Лекции

Оценивается посещаемость, активность, умение выделить главную мысль и др. Преподаватель выдает красивые именные карточки с изображением болот и равнин (а также островов) за попытки студентов сказать что-то умное и поучаствовать в дискуссии. В конце семестра карточки подсчитываются и пропорционально начисляются баллы. Максимальный балл (20) получает обладатель наибольшего числа карточек.

Лабораторные работы

Оценивается самостоятельность при выполнении работы, грамотность в оформлении, правильность выполнения и т.д. Заработать можно максимум 20 баллов, которые начисляются преподавателем за решение поставленных задач (программирование, работа в программах и т.д.)

Практические занятия

Оценивается самостоятельность при выполнении работы, грамотность в оформлении, правильность выполнения и т.д. Заработать можно максимум 20

баллов, которые начисляются преподавателем за решение поставленных задач (программирование, работа в программах и т.д.)

Промежуточная аттестация

Проходит в виде устного ответа по билетам. Максимально возможный балл 40.

При проведении промежуточной аттестации

ответ на «отлично» оценивается от 31 до 40 баллов;

ответ на «хорошо» оценивается от 21 до 30 баллов;

ответ на «удовлетворительно» оценивается от 11 до 20 баллов;

ответ на «неудовлетворительно» оценивается от 0 до 10 баллов.

Таким образом, максимально возможная сумма баллов за все виды учебной деятельности студента за 8 семестр по дисциплине «Математические основы информационной безопасности» составляет 100 баллов.

Таблица пересчета полученной студентом суммы баллов по дисциплине «Математические основы информационной безопасности» за 8 семестр в оценку (экзамен):

100-81 баллов	«отлично»
80-61 баллов	«хорошо»
60-41 баллов	«удовлетворительно»
40-0 баллов	«не удовлетворительно»

8. Учебно-методическое и информационное обеспечение дисциплины

а) литература:

- Ярочкин В.И. Информационная безопасность [Текст] : учеб. для студентов вузов, обучающихся по гуманитар. и социал.-экон. специальностям / В. И. Ярочкин. - М. : Гаудеамус : Акад. Проект, 2008.

- Информационная безопасность и защита информации [Текст] : учеб. пособие для студентов вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков. - 4-е изд., стер. - М. : Изд. центр "Академия", 2009.

- Информационная безопасность и защита информации [Электронный ресурс] : учебное пособие / Башлы П. Н. – Москва: Евразийский открытый институт, 2012. -311 с. 978-5-374-00301-7

Книга находится в базовой версии ЭВС IPRbooks/

- А. А. Малюк. Информационная безопасность: концептуальные и методологические основы защиты информации [Текст] : учеб. пособие / А. А. Малюк. - М. : Горячая линия - Телеком, 2004.

- Информационная безопасность систем организационного управления. Теоретические основы [Текст] : в 2 т. / Н. А. Кузнецов [и др.] ; под ред. Н. А. Кузнецова, В. В. Кульбы ; Рос. акад. наук, Ин-т проблем передачи информ. - М. : Наука, 2006.

б) программное обеспечение и Интернет-ресурсы:

- ОС Windows (лицензионное ПО) или ОС Unix/Linux (свободное ПО)
- Microsoft Office (лицензионное ПО) или Open Office/Libre Office (свободное ПО)
- Браузеры Internet Explorer, Google Chrome, Opera и др. (свободное ПО).
- Среда программирования Java на платформе Eclipse (свободное ПО).
- Портал по информационной безопасности <http://www.securitylab.ru/>
- Учебные ресурсы центра «Новые информационные технологии» <http://nto.immpu.sgu.ru>

8. Учебно-методическое и информационное обеспечение дисциплины

а) литература:

- Ярочкин В.И. Информационная безопасность [Текст] : учеб. для студентов вузов, обучающихся по гуманитар. и социал.-экон. специальностям / В. И. Ярочкин. - М. : Гаудеамус : Акад. Проект, 2008.
- Информационная безопасность и защита информации [Текст] : учеб. пособие для студентов вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков. - 4-е изд., стер. - М. : Изд. центр "Академия", 2009.
- Информационная безопасность и защита информации [Электронный ресурс] : учебное пособие / Башлы П. Н. – Москва: Евразийский открытый институт, 2012. -311 с. 978-5-374-00301-7

Книга находится в базовой версии ЭВС IPRbooks.

б) программное обеспечение и Интернет-ресурсы:

- ОС Windows (лицензионное ПО) или ОС Unix/Linux (свободное ПО)
- Microsoft Office (лицензионное ПО) или Open Office/Libre Office (свободное ПО)
- Браузеры Internet Explorer, Google Chrome, Opera и др. (свободное ПО).
- Среда программирования Java на платформе Eclipse (свободное ПО).
- Портал по информационной безопасности <http://www.securitylab.ru/>
- Учебные ресурсы центра «Новые информационные технологии» <http://nto.immpu.sgu.ru>