МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рабочая программа дисциплины (модуля)

МАТЕМАТИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Специальность и специализация
10.05.03 Информационная безопасность автоматизированных систем. Безопасность открытых информационных систем

Год набора на ОПОП
2024

Форма обучения
очная

Владивосток 2025

Рабочая программа дисциплины (модуля) «Математические методы защиты информации» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем (утв. приказом Минобрнауки России от 26.11.2020г. №1457) и Порядком организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры (утв. приказом Минобрнауки России от 06.04.2021 г. N245).

Составитель(и):

Мартышенко Н.С., старший преподаватель, Кафедра информационной безопасности, Nikolay.Martyshenko@vvsu.ru

Шумик Е.Г., кандидат экономических наук, заведующий кафедрой, Кафедра информационной безопасности, Ekaterina.Shumik1@vvsu.ru

Утверждена на заседании кафедры информационной безопасности от 15.05.2025 , протокол № 9

СОГЛАСОВАНО:

Заведующий кафедрой (разработчика)

Шумик Е.Г.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат	eg_1575874368
Номер транзакции	0000000000EAAFE3
Владелец	Шумик Е.Г.

1 Цель, планируемые результаты обучения по дисциплине (модулю)

Целью дисциплины является освоение студентами методов, способов и средств программной и аппаратной реализации алгоритмов теории чисел

Задачами освоения дисциплины являются:

− изучение математических основ криптографии;

− получение студентами знаний о простейших системах шифрования;

− приобретение навыков использования алгоритмов теории чисел.

Планируемыми результатами обучения по дисциплине (модулю), являются знания, умения, навыки. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы, представлен в таблице 1.

Таблица 1 – Компетенции, формируемые в результате изучения дисциплины (модуля)

Название ОПОП ВО, сокращенное	Код и формулировка компетенции	Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине		
			Код результата	Формулировка результата	
10.05.03 «Информационная безопасность автоматизированных систем» (ИБ)	ОПК-3 : Способен использовать математические методы, необходимые для решения задач профессиональной деятельности	ОПК-3.2к : использует теорию фундаментальной математики и при решении прикладных задач;	РД1	Знание	алгоритмы теории чисел и простейших систем шифрования и особенности их реализации
			РД2	Умение	решать прикладные задачи криптологии с использованием алгоритмов теории чисел, составлять и реализовывать алгоритмы
			РД3	Навык	навыками решения прикладных задач криптологии с использованием алгоритмов теории чисел

В процессе освоения дисциплины решаются задачи воспитания гармонично развитой, патриотичной и социально ответственной личности на основе традиционных российских духовно-нравственных и культурно-исторических ценностей, представленные в таблице 1.2.

Таблица 1.2 – Целевые ориентиры воспитания

Воспитательные задачи	**Формирование ценностей**	**Целевые ориентиры**
Формирование гражданской позиции и патриотизма		
Развитие патриотизма и гражданской ответственности	Гражданственность	Внимательность к деталям
Формирование духовно-нравственных ценностей		
Воспитание чувства долга и ответственности перед семьей и обществом	Гражданственность	Системное мышление

Формирование научного мировоззрения и культуры мышления		
Развитие познавательного интереса и стремления к знаниям	Патриотизм	Доброжелательность и открытость
Формирование коммуникативных навыков и культуры общения		
Развитие умения эффективно общаться и сотрудничать	Взаимопомощь и взаимоуважение	Системное мышление

2 Место дисциплины (модуля) в структуре ОПОП

Дисциплина «Математические методы защиты информации» относится к базовой части «Блока 1 Дисциплины (модули)» учебного плана специальности 10.05.03 «Информационная безопасность автоматизированных систем». Входными требованиями, необходимыми для освоения дисциплины, является наличие у обучающихся компетенций, сформированных при изучении дисциплин и/или прохождении практик «Алгебра и геометрия», «Математический анализ модуль 1». На данную дисциплину опираются «Криптографические протоколы».

3. Объем дисциплины (модуля)

Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу с обучающимися (по видам учебных занятий) и на самостоятельную работу, приведен в таблице 2.

Таблица 2 – Общая трудоемкость дисциплины

Название ОПОП ВО	Форма обучения	Часть УП	Семестр (ОФО) или курс (ЗФО, ОЗФО)	Трудоемкость	Объем контактной работы (час)						СРС	Форма аттестации
				(З.Е.)	Всего	Аудиторная			Внеаудиторная			
						лек.	прак.	лаб.	ПА	КСР		
10.05.03 Информационная безопасность автоматизированных систем	ОФО	С1.Б	6	5	91	36	36	0	1	18	89	Э

4 Структура и содержание дисциплины (модуля)

4.1 Структура дисциплины (модуля) для ОФО

Тематический план, отражающий содержание дисциплины (перечень разделов и тем), структурированное по видам учебных занятий с указанием их объемов в соответствии с учебным планом, приведен в таблице 3.1

Таблица 3.1 – Разделы дисциплины (модуля), виды учебной деятельности и формы текущего контроля для ОФО

№	Название темы	Код результата обучения	Кол-во часов, отведенное на				Форма текущего контроля
			Лек	Практ	Лаб	СРС	

1	Теория чисел и алгебраические основы	РД1, РД2, РД3	6	6	0	18	практическое задание
2	Криптографические примитивы	РД1, РД2, РД3	6	6	0	18	практическое задание
3	Симметричное шифрование	РД1, РД2, РД3	6	6	0	18	практическое задание
4	Асимметричные криптосистемы	РД1, РД2, РД3	6	6	0	18	практическое задание
5	Приложения криптографии и управление ключами	РД1, РД2, РД3	6	6	0	18	практическое задание
6	Криптоанализ	РД1, РД2, РД3	6	6	0	18	практическое задание
Итого по таблице			**36**	**36**	**0**	**108**	

4.2 Содержание разделов и тем дисциплины (модуля) для ОФО

Тема 1 Теория чисел и алгебраические основы.

Содержание темы: Основные понятия теории чисел: делимость, сравнение по модулю, расширенный алгоритм Евклида. Факторизация и вычисления в конечных полях. Применение теоремы Эйлера-Ферма и китайской теоремы об остатках. Введение в абстрактную алгебру: группы, кольца, поля. .

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция, практическое занятие.

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

Тема 2 Криптографические примитивы.

Содержание темы: Хеш-функции и их свойства. Генерация случайных чисел и псевдослучайных последовательностей. Блочные и потоковые шифры: общие принципы и отличия. Односторонние функции и схемы разделения секрета. .

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция, практическое занятие.

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

Тема 3 Симметричное шифрование.

Содержание темы: История развития симметричного шифрования. Современные блочные шифры: DES, AES. Режимы работы блочных шифров (ECB, CBC, OFB, CTR). Потоковые шифры: RC4, ChaCha20.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция, практическое занятие.

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

Тема 4 Асимметричные криптосистемы.

Содержание темы: Принцип асимметричной криптографии. RSA-шифрование и цифровая подпись. Эллиптические кривые и ECC-криптография. Примеры реализаций и областей применения. .

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция, практическое занятие.

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

Тема 5 Приложения криптографии и управление ключами.

Содержание темы: Аутентификация пользователей и обмен сообщениями. Инфраструктура открытых ключей (PKI) и цифровые сертификаты. Управление ключами и жизненным циклом ключей. Электронная почта и веб-протоколы с использованием SSL/TLS.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция, практическое занятие.

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

Тема 6 Криптоанализ.

Содержание темы: Типичные атаки на криптосистемы: дифференциальный и линейный криптоанализ. Атаки на хэш-функции и генераторы случайных чисел. Оценка эффективности атак и меры противодействия. Анализ слабых мест существующих стандартов шифрования. .

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция, практическое занятие.

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

5 Методические указания для обучающихся по изучению и реализации дисциплины (модуля)

5.1 Методические рекомендации обучающимся по изучению дисциплины и по обеспечению самостоятельной работы

Самостоятельная работа студентов (СРС) — это деятельность учащихся, которую они совершают без непосредственной помощи и указаний преподавателя, руководствуясь сформировавшимися ранее представлениями о порядке и правильности выполнения операций. Цель СРС в процессе обучения заключается, как в усвоении знаний, так и в формировании умений и навыков по их использованию в новых условиях на новом учебном материале. Самостоятельная работа призвана обеспечивать возможность осуществления студентами самостоятельной познавательной деятельности в обучении, и является видом учебного труда, способствующего формированию у студентов самостоятельности. В данной учебной программе приведен перечень основных и дополнительных источников, которые предлагается изучить в процессе облучения по дисциплине. Кроме того, для расширения и углубления знаний по данной дисциплине целесообразно использовать: научные публикации в тематических журналах; полнотекстовые базы данных библиотеки; имеющиеся в библиотеках вуза и региона публикаций на электронных и бумажных носителях. Успешное освоение дисциплины предполагает активную работу студентов на всех занятиях аудиторной формы: лекций и практических занятий, выполнение аттестационный мероприятий, эффективную самостоятельную работу. В процессе изучения дисциплины студенту необходимо ориентироваться на самостоятельную проработку лекционного материала, подготовку к практическим занятиям, выполнение тестов, кейсовых заданий, самостоятельное изучение некоторых разделов курса Для проведения занятий лекционного типа используются учебно-наглядные пособия в форме презентационных материалов, обеспечивающих тематические иллюстрации, соответствующие темам лекций, представленным в пункте 4 настоящей РПД.

5.2 Особенности организации обучения для лиц с ограниченными возможностями здоровья и инвалидов

При необходимости обучающимся из числа лиц с ограниченными возможностями здоровья и инвалидов (по заявлению обучающегося) предоставляется учебная информация в доступных формах с учетом их индивидуальных психофизических особенностей:

- для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания, консультации и др.
- для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания, консультации и др.
- для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; индивидуальные задания, консультации и др.

6 Фонд оценочных средств для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине (модулю)

В соответствии с требованиями ФГОС ВО для аттестации обучающихся на соответствие их персональных достижений планируемым результатам обучения по дисциплине (модулю) созданы фонды оценочных средств. Типовые контрольные задания, методические материалы, определяющие процедуры оценивания знаний, умений и навыков, а также критерии и показатели, необходимые для оценки знаний, умений, навыков и характеризующие этапы формирования компетенций в процессе освоения образовательной программы, представлены в Приложении 1.

7 Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1 Основная литература

1. Мартыненков, Б. В. Основы криптографической защиты информации : учебно-методическое пособие / Б. В. Мартыненков, В. А. Иванов, М. Ю. Конышев. — Москва : РТУ МИРЭА, 2023. — 95 с. — ISBN 978-5-7339-1807-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/368762 (дата обращения: 27.10.2025). — Режим доступа: для авториз. пользователей.
2. Сергеева, О. А. Основы криптографии : учебно-методическое пособие / О. А. Сергеева, А. С. Кутовая. — Кемерово : КемГУ, 2024. — 160 с. — ISBN 978-5-8353-3120-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/407729 (дата обращения: 27.10.2025). — Режим доступа: для авториз. пользователей.

7.2 Дополнительная литература

1. Донгак, Ш. М. Криптография : учебное пособие / Ш. М. Донгак. — Москва : РТУ МИРЭА, 2021 — Часть 3— 2021. — 64 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/182517 (дата обращения: 27.10.2025). — Режим доступа: для авториз. пользователей.
2. Сдвижков, О. А., Основы математической логики и криптографии. Практикум в Excel. : учебное пособие / О. А. Сдвижков. — Москва : КноРус, 2024. — 356 с. — ISBN 978-

5-406-12297-6. — URL: https://book.ru/book/950673 (дата обращения: 26.10.2025). — Текст : электронный.

7.3 Ресурсы информационно-телекоммуникационной сети "Интернет", включая профессиональные базы данных и информационно-справочные системы (при необходимости):

1. Электронно-библиотечная система "BOOK.ru"
2. Электронно-библиотечная система "ЛАНЬ"
3. Open Academic Journals Index (OAJI). Профессиональная база данных - Режим доступа: http://oaji.net/
4. Президентская библиотека им. Б.Н.Ельцина (база данных различных профессиональных областей) - Режим доступа: https://www.prlib.ru/
5. Информационно-справочная система "Консультант Плюс" - Режим доступа: http://www.consultant.ru/

8 Материально-техническое обеспечение дисциплины (модуля) и перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения

Основное оборудование:

- Компьютеры

Программное обеспечение:

- Microsoft Office Professional Plus 2016

МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Фонд оценочных средств
для проведения текущего контроля
и промежуточной аттестации по дисциплине (модулю)

МАТЕМАТИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Специальность и специализация
10.05.03 Информационная безопасность автоматизированных систем. Безопасность открытых информационных систем

Год набора на ОПОП
2024

Форма обучения
очная

Владивосток 2025

1 Перечень формируемых компетенций

Название ОПОП ВО, сокращенное	Код и формулировка компетенции	Код и формулировка индикатора достижения компетенции
10.05.03 «Информационная безопасность автоматизированных систем» (ИБ)	ОПК-3 : Способен использовать математические методы, необходимые для решения задач профессиональной деятельности	ОПК-3.2к : использует теорию фундаментальной математики и при решении прикладных задач;

Компетенция считается сформированной на данном этапе в случае, если полученные результаты обучения по дисциплине оценены положительно (диапазон критериев оценивания результатов обучения «зачтено», «удовлетворительно», «хорошо», «отлично»). В случае отсутствия положительной оценки компетенция на данном этапе считается несформированной.

2 Показатели оценивания планируемых результатов обучения

Компетенция ОПК-3 «Способен использовать математические методы, необходимые для решения задач профессиональной деятельности»

Таблица 2.1 – Критерии оценки индикаторов достижения компетенции

Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине			Критерии оценивания результатов обучения
	Код рез-та	Тип рез-та	Результат	
ОПК-3.2к : использует теорию фундаментальной математики и при решении прикладных задач;	РД 1	Знание	алгоритмы теории чисел и простейших систем шифрования и особенности их реализации	решение тестовых заданий
	РД 2	Умение	решать прикладные задачи криптологии с использованием алгоритмов теории чисел, составлять и реализовывать алгоритмы	выполнение практических заданий
	РД 3	Навык	навыками решения прикладных задач криптологии с использованием алгоритмов теории чисел	выполнение практических заданий

Таблица заполняется в соответствии с разделом 1 Рабочей программы дисциплины (модуля).

3 Перечень оценочных средств

Таблица 3 – Перечень оценочных средств по дисциплине (модулю)

Контролируемые планируемые результаты обучения	Контролируемые темы дисциплины	Наименование оценочного средства и представление его в ФОС

			Текущий контроль	Промежуточная ат тестация
Очная форма обучения				
РД1	Знание : алгоритмы теор ии чисел и простейших систем шифрования и ос обенности их реализаци и	1.1. Теория чисел и алге браические основы	Опрос	Экзамен в устной форме
		1.2. Криптографические примитивы	Опрос	Экзамен в устной форме
		1.3. Симметричное шиф рование	Опрос	Экзамен в устной форме
		1.4. Асимметричные кри птосистемы	Опрос	Экзамен в устной форме
		1.5. Приложения крипто графии и управление кл ючами	Опрос	Экзамен в устной форме
		1.6. Криптоанализ	Опрос	Экзамен в устной форме
РД2	Умение : решать прикла дные задачи криптологи и с использованием алго ритмов теории чисел, со ставлять и реализовыват ь алгоритмы	1.1. Теория чисел и алге браические основы	Практическая рабо та	Экзамен в устной форме
		1.2. Криптографические примитивы	Практическая рабо та	Экзамен в устной форме
		1.3. Симметричное шиф рование	Практическая рабо та	Экзамен в устной форме
		1.4. Асимметричные кри птосистемы	Практическая рабо та	Экзамен в устной форме
		1.5. Приложения крипто графии и управление кл ючами	Практическая рабо та	Экзамен в устной форме
		1.6. Криптоанализ	Практическая рабо та	Экзамен в устной форме
РД3	Навык : навыками реше ния прикладных задач к риптологии с использов анием алгоритмов теори и чисел	1.1. Теория чисел и алге браические основы	Практическая рабо та	Экзамен в устной форме
		1.2. Криптографические примитивы	Практическая рабо та	Экзамен в устной форме
		1.3. Симметричное шиф рование	Практическая рабо та	Экзамен в устной форме
		1.4. Асимметричные кри птосистемы	Практическая рабо та	Экзамен в устной форме
		1.5. Приложения крипто графии и управление кл ючами	Практическая рабо та	Экзамен в устной форме
		1.6. Криптоанализ	Практическая рабо та	Экзамен в устной форме

4 Описание процедуры оценивания

Качество сформированности компетенций на данном этапе оценивается по результатам текущих и промежуточных аттестаций при помощи количественной оценки, выраженной в баллах. Максимальная сумма баллов по дисциплине (модулю) равна 100 баллам.

Вид учебной деятельности	Оценочное средство			
	Опрос	Практическая работа	Экзамен	Итого
Лекционные занятия	20			20
Промежуточная аттестация		60	20	80
Итого	80	80	20	100

Сумма баллов, набранных студентом по всем видам учебной деятельности в рамках дисциплины, переводится в оценку в соответствии с таблицей.

Сумма баллов по дисциплине	Оценка по промежуточной аттестации	Характеристика качества сформированности компетенции
от 91 до 100	«зачтено» / «отлично»	Студент демонстрирует сформированность дисциплинарных компетенций, обнаруживает всестороннее, систематическое и глубокое знание учебного материала, усвоил основную литературу и знаком с дополнительной литературой, рекомендованной программой, умеет свободно выполнять практические задания, предусмотренные программой, свободно оперирует приобретенными знаниями, умениями, применяет их в ситуациях повышенной сложности.
от 76 до 90	«зачтено» / «хорошо»	Студент демонстрирует сформированность дисциплинарных компетенций: основные знания, умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
от 61 до 75	«зачтено» / «удовлетворительно»	Студент демонстрирует сформированность дисциплинарных компетенций: в ходе контрольных мероприятий допускаются значительные ошибки, проявляется отсутствие отдельных знаний, умений, навыков по некоторым дисциплинарным компетенциям, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.
от 41 до 60	«не зачтено» / «неудовлетворительно»	У студента не сформированы дисциплинарные компетенции, проявляется недостаточность знаний, умений, навыков.
от 0 до 40	«не зачтено» / «неудовлетворительно»	Дисциплинарные компетенции не сформированы. Проявляется полное или практически полное отсутствие знаний, умений, навыков.

5 Примерные оценочные средства

5.1 Примеры заданий для выполнения практических работ

Цель : закрепление навыков работы с базовыми элементами криптографии.

- **Задания** :
    1. Провести экспериментальное исследование свойств хеш-функций MD5 и SHA-256.
    2. Проверить выполнение односторонних функций на примере простых моделей.
    3. Реализовать генератор псевдослучайных чисел на основе известного стандарта.
    4. Создать простую схему разделения секрета по схеме Шамира.

---

3. Симметричное шифрование

Цель : понимание механизмов симметричных шифров и режимов их работы.

- **Задания** :

1. Расшифровка сообщений, зашифрованных с помощью шифра Вернама (одноразового блоканотного шифра).
2. Моделирование процесса шифрования и расшифровки в режиме электронной книги (ECB) и цепочки блоков (CBC).
3. Исследование уязвимости режима ECB на конкретном примере.
4. Реализация шифра AES на Python/C++ и проверка его работоспособности.

---

4. Асимметричные криптосистемы

Цель : обучение принципам работы асимметричных схем шифрования и цифровых подписей.

- **Задания** :
  1. Создание пары открытый-закрытый ключи для алгоритма RSA и демонстрация процессов шифрования и дешифрации.
  2. Подписание сообщения с помощью RSA и проверка подлинности цифровой подписи.
  3. Вычислить эллиптическую кривую над простым полем и провести операции на ней.
  4. Демонстрация работы алгоритма ECDSA (цифровой подписи на основе эллиптических кривых).

---

5. Приложения криптографии и управление ключами

Цель : развитие навыков управления криптографическими ключами и организации инфраструктуры открытых ключей.

- **Задания** :
  1. Организация простого центра сертификации (CA) и создание цифрового сертификата.
  2. Генерация ключей и сертификатов для модели клиент-сервер с использованием TLS/SSL.
  3. Имитация процедуры распределения и обновления ключей в сетевом приложении.
  4. Оценка рисков и разработка плана резервного копирования и восстановления закрытых ключей.

---

6. Криптоанализ

Цель : приобретение начальных навыков анализа и взлома простейших криптосистем.

- **Задания** :
  1. Осуществить атаку полного перебора на простой шифр замены.
  2. Реализовать дифференциальный криптоанализ для упрощённого варианта блочного шифра (например, Speck).

3. Продемонстрировать коллизионную атаку на простом хеш-функционале (MD4).
4. Определить стойкость шифра Verge (XOR-перемешивания) к статистическому анализу.

Краткие методические указания

на выполнение практической работы отводится не менее двух двухчасовых занятий

Шкала оценки

Оценка	Баллы	Описание
5	14-20	Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программны й материал исчерпывающе, последовательно, четко и логически стройно его излагает , умеет тесно увязывать теорию с практикой.
4	8-12	Оценка «хорошо» выставляется студенту, если он твердо знает материал, грамотно и по с уществу излагает его, не допуская существенных неточностей в ответе на вопрос, правил ьно применяет теоретические положения при решении практических вопросов и задач.
3	2-6	Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основ ного материала, но не усвоил его деталей, допускает неточности, недостаточно правильн ые формулировки.
2	0-2	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной ч асти программного материала, допускает существенные ошибки.

5.2 Примерные темы для опроса

1. Что такое сравнительные уравнения по модулю и почему они важны в криптографии?
2. Объясните понятие одной стороны функции и приведите примеры.
3. Какие существуют типы колец и полей, используемые в криптографии?
4. Опишите китайский остаток теоремой и его использование в криптографии.
5. Как связаны мультипликативные порядки элементов в конечных полях и криптостойкость?

Краткие методические указания

Для подготовки к опросу студенту необходимо изучить лекционный материал, а так же материал представленный в дополнительных источниках.

Шкала оценки

Оценка	Баллы	Описание
5	14-20	Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программны й материал исчерпывающе, последовательно, четко и логически стройно его излагает , умеет тесно увязывать теорию с практикой.
4	8-12	Оценка «хорошо» выставляется студенту, если он твердо знает материал, грамотно и по с уществу излагает его, не допуская существенных неточностей в ответе на вопрос, правил ьно применяет теоретические положения при решении практических вопросов и задач.
3	2-6	Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основ ного материала, но не усвоил его деталей, допускает неточности, недостаточно правильн ые формулировки.
2	0-2	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной ч асти программного материала, допускает существенные ошибки.

5.3 Вопросы к экзамену

1. Что такое однонаправленные функции и как они применяются в криптографии?
2. Дайте определение сравнительных уравнений по модулю и покажите их связь с задачей нахождения обратных элементов.
3. Объясните разницу между группами, кольцами и полями и приведите примеры их использования в криптографии.
4. Что такое шифр Вернама и почему он считается абсолютно надежным?
5. Перечислите известные вам блочные шифры и охарактеризуйте их особенности.

6. Чем отличаются потоки потоков и блочные шифры? Укажите достоинства и недостатки каждого типа.
7. Охарактеризуйте механизм работы симметричных шифров и обозначьте область их применения.
8. Объясните, как работают современные стандарты симметричного шифрования (AES).
9. Что такое хеш-функции и какие условия они должны удовлетворять?
10. Приведите определение и назначение генератора псевдослучайных чисел. Какие критерии качества для него установлены?
11. Объясните идею и устройство протокола Диффи-Хеллмана для обмена ключами.
12. Опишите принципы работы криптосистемы RSA и назовите ключевые этапы шифрования и дешифрования.
13. В чем состоит различие между стандартами DSA и RSA применительно к цифровому подписыванию?
14. Опишите конструкцию эллиптических кривых и их применение в криптографии.
15. Что такое Infrastructure Public Key (PKI) и какова её структура?
16. Какие основные проблемы безопасности присутствуют в работе SSL/TLS-протокола?
17. Объясните концепцию коллизии в хеш-функциях и причины их возникновения.
18. В чём заключаются атаки на основе анализа побочных каналов и как предотвратить подобные атаки?
19. Объясните механизмы работы метода полной переборки и дифференциального криптоанализа.
20. Каким образом осуществляется оценка стойкости современных криптографических алгоритмов?

Краткие методические указания

Для подготовки к экзамену студенту необходимо изучить лекционный материал, а так же материал представленный в дополнительных источниках.

Шкала оценки

Оценка	Баллы	Описание
5	14-20	Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой.
4	8-12	Оценка «хорошо» выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач.
3	2-6	Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки.
2	0-2	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки.