Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования «Новосибирский национальный исследовательский
государственный университет» (Новосибирский государственный университет, НГУ)

Факультет информационных технологий

СОГЛАСОВАНО
Декан ФИТ НГУ
_____ М.М. Лаврентьев
«18» апреля 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Симметричная криптография и криптоанализ

Направление подготовки: 09.04.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА
Направленность (профиль): Квантовые технологии и криптография

Форма обучения: очная
Год обучения: 1, семестр: 2

№	Вид деятельности	Семестр
		2
1	Лекции, час.	32
2	Практические занятия, час.	32
3	Лабораторные занятия, час.	
4	Занятий в контактной форме без учета промежуточной аттестации, час, из них	64
5	в электронной форме, час.	
6	из них аудиторных занятий, час.	64
7	из них в активной и интерактивной форме, час.	64
8	консультаций, час.	
9	Самостоятельная работа, час.	150
10	в том числе на выполнение письменных работ, час	70
11	Форма аттестации (экзамен, зачет, дифференцированный зачет), час	ДЗ 2
12	Всего зачетных единиц[1]	6

Новосибирск 2022

[1] С учетом выделенных часов на промежуточную аттестацию

Рабочая программа дисциплины составлена на основании федерального государственного образовательного стандарта (ФГОС) высшего образования - магистратура по направлению подготовки 09.04.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА.

Федеральный государственный образовательный стандарт (ФГОС) высшего образования по направлению подготовки магистратуры 09.04.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА введен в действие приказом Минобрнауки 19.09.2017 № 918.

Место дисциплины в структуре учебного плана: Блок 1 Дисциплины (модули), часть, формируемая участниками образовательных отношений; дисциплина по выбору

Рабочая программа дисциплины утверждена решением Ученого совета факультета информационных технологий от 28.03.2022, протокол № 84.

Программу разработали:

ст. преподаватель кафедры теоретической кибернетики ММФ НГУ
кандидат физико-математических наук — Н.А.Коломеец

ассистент кафедры компьютерных систем ФИТ НГУ — Ю.П.Максимлюк

Заведующий кафедрой систем информатики ФИТ,
доктор физико-математических наук — М.М. Лаврентьев

Ответственный за образовательную программу:
доцент КвЭл ФФ НГУ ФФ НГУ
кандидат физико-математических наук — И.И.Бетеров

Аннотация к рабочей программе дисциплины

Дисциплина **Симметричная криптография и криптоанализ** реализуется в рамках образовательной программы высшего образования – программы магистратуры 09.04.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА, направленность (профиль): КВАНТОВЫЕ ТЕХНОЛОГИИ И КРИПТОГРАФИЯ по очной форме обучения на английском языке.

Место в образовательной программе: Дисциплина **Симметричная криптография и криптоанализ** развивает знания, умения и навыки, сформированные у обучающихся по результатам изучения следующих дисциплин: Дискретная математика.

Дисциплина **Симметричная криптография и криптоанализ** реализуется во 2 семестре в рамках части, формируемой участниками образовательных отношений, Блока 1 дисциплин (модулей) и является дисциплиной по выбору.

Дисциплина **Симметричная криптография и криптоанализ** направлена на формирование компетенций:

Способен выполнять фундаментальные и прикладные работы поискового, теоретического и экспериментального характера (ПКС-1), в части следующих индикаторов достижения компетенции:

ПКС-1.1. Применяет актуальные модели и подходы в области профессиональной деятельности

ПКС-1.2. Комбинирует и адаптирует существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности

ПКС-1.3 Применяет на практике программные средства и платформы информационных технологий для разработки и реализации математических моделей, проведение их анализа при решении задач в области профессиональной деятельности

Перечень основных разделов дисциплины:

Тема 1. Введение в симметричную криптографию и криптоанализ.

Тема 2. Псевдослучайные числа. Методы генерации. Использование в криптографии.

Тема 3. Генераторы псевдослучайных чисел и поточные шифры. Базовые конструкции. Принципы проектирования. Методы криптоанализа. Корреляционные атаки и др.

Тема 4. Блочные шифры. Основные схемы. Режимы шифрования. Общие методы криптоанализа.

Тема 5. Линейный и разностный криптоанализ. Алгебраический криптоанализ.

Тема 6. Построение шифров с гарантированной оценкой стойкости к линейному и дифференциальному методам. The Wide Trail Design Strategy.

Тема 7. Перемешивающие свойства преобразований, используемых при шифровании. Branch numbers.

Тема 8. Подробный разбор алгоритмов AES, Кузнечик. Оценки стойкости.

Тема 9. Хэш-функции, MAC, их приложения. Базовые схемы. Криптоанализ.

Тема 10. Подробный разбор алгоритмов SHA-3, Стрибог. Оценки стойкости.

Тема 11. Криптоанализ по сторонним каналам.

Тема 12. ARX-схемы. Достоинства и недостатки. Особенности криптоанализа.

При освоении дисциплины студенты выполняют следующие виды учебной работы: лекции, практические занятия, самостоятельная работа. В учебном процессе предусматривается использование активных и интерактивных форм проведения занятий.

Самостоятельная работа включает: подготовку к практическим занятиям по разделам дисциплины, выполнение заданий, подготовку к дифференцированному зачету.

Общий объем дисциплины – 6 зачетных единиц (216 часов).

Правила аттестации по дисциплине. Текущий контроль по дисциплине Симметричная криптография и криптоанализ осуществляется на практических занятиях на основании оценки за портфолио (задания по темам практических работ). По результатам защиты портфолио выставляется оценка «зачтено» или «не зачтено».

Промежуточная аттестация по дисциплине «Симметричная криптография и криптоанализ» проводится по завершению периода ее освоения (семестра). Промежуточная аттестация по дисциплине включает 2 этапа:

1) портфолио (задания по темам практических работ);

2) дифференцированный зачет.

Оценка «зачтено» за портфолио является необходимым условием для прохождения промежуточной аттестации. Результаты промежуточной (итоговой по дисциплине) аттестации определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Оценки «отлично», «хорошо», «удовлетворительно» означают успешное прохождение промежуточной аттестации.

Учебно-методическое обеспечение дисциплины.

Учебно-методические материалы по дисциплине «Симметричная криптография и криптоанализ» в электронной информационно-образовательной среде НГУ создаются и выкладываются для каждого нового набора

1. Внешние требования к дисциплине

Таблица 1.1

Компетенция ПКС-1 Способен выполнять фундаментальные и прикладные работы поискового, теоретического и эксперименального характера, *в части следующих индикаторов достижения компетенции*:	
ПКС-1.1	Применяет актуальные модели и подходы в области профессиональной деятельности
ПКС-1.2	Комбинирует и адаптирует существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности
ПКС-1.3	Применяет на практике программные средства и платформы информационных технологий для разработки и реализации математических моделей, проведение их анализа при решении задач в области профессиональной деятельности

2. Требования к результатам освоения дисциплины

Таблица 2.1

Результаты изучения дисциплины по уровням освоения (иметь представление, знать, уметь, владеть)	**Формы организации занятий**		
	Лекции	**Практики / семинары**	**Самостоятельная работа**
ПКС-1.1. Применяет актуальные модели и подходы в области профессиональной деятельности			
1 Знать основной набор понятий современной симметричной криптографии, наиболее часто используемые математические принципы в алгоритмах шифрования и их криптоанализе	+	+	+
ПКС-1.2. Комбинирует и адаптирует существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности			
2. Уметь ориентироваться в современных и классических методах криптографии	+	+	+
ПКС-1.3 Применяет на практике программные средства и платформы информационных технологий для разработки и реализации математических моделей, проведение их анализа при решении задач в области профессиональной деятельности			
3. Владеть навыками общего выбора методов для решения конкретных задач криптографии	+	+	+

3. Содержание и структура учебной дисциплины

Таблица 3.1

Темы лекций	**Активные формы, час. (входит в общее кол-во часов)**	**Часы**	**Ссылки на результаты обучения**
Семестр: 2			
Тема 1. Введение в симметричную криптографию и криптоанализ.	2	2	1, 2, 3

Тема 2. Псевдослучайные числа. Методы генерации. Использование в криптографии.	2	2	1, 2, 3
Тема 3. Генераторы псевдослучайных чисел и поточные шифры. Базовые конструкции. Принципы проектирования. Методы криптоанализа. Корреляционные атаки и др.	4	4	1, 2, 3
Тема 4. Блочные шифры. Основные схемы. Режимы шифрования. Общие методы криптоанализа.	2	2	1, 2, 3
Тема 5. Линейный и разностный криптоанализ. Алгебраический криптоанализ.	4	4	1, 2, 3
Тема 6. Построение шифров с гарантированной оценкой стойкости к линейному и дифференциальному методам. The Wide Trail Design Strategy.	2	2	1, 2, 3
Тема 7. Перемешивающие свойства преобразований, используемых при шифровании. Branch numbers.	4	4	1, 2, 3
Тема 8. Подробный разбор алгоритмов AES, Кузнечик. Оценки стойкости.	2	2	1, 2, 3
Тема 9. Хэш-функции, MAC, их приложения. Базовые схемы. Криптоанализ.	4	4	1, 2, 3
Тема 10. Подробный разбор алгоритмов SHA-3, Стрибог. Оценки стойкости.	2	2	1, 2, 3
Тема 11. Криптоанализ по сторонним каналам.	2	2	1, 2, 3
Тема 12. ARX-схемы. Достоинства и недостатки. Особенности криптоанализа.	2	2	1, 2, 3
Итого:	**32**	**32**	

Таблица 3.2

Темы практических занятий	Активные формы, час. (входит в общее кол-во часов)	Часы	Ссылки на результаты обучения	Учебная деятельность
Семестр: 2				
Тема 1. Статистические методы криптоанализа. Теория и реализация метода криптоанализа для шифра Виженера.	4	4	1, 2, 3	Разбор представленного теоретического материала, практическое применение изученной темы
Тема 2. Линейная сложность последовательностей. Реализация алгоритма Берлекэмпа-Мэсси.	4	4	1, 2, 3	Разбор представленного теоретического материала, практическое применение изученной темы
Тема 3. Реализация поточного шифра на выбор. Анализ отдельных компонент.	4	4	1, 2, 3	Разбор представленного теоретического материала, практическое применение изученной темы
Тема 4. Реализация блочного шифра на выбор. Тестирование различных режимов шифрования.	4	4	1, 2, 3	Разбор представленного теоретического материала, практическое применение изученной темы
Тема 5. Реализация линейного криптоанализа игрушечного шифра. Оценка необходимого	4	4	1, 2, 3	Разбор представленного теоретического материала, практическое применение

объема статистики.				изученной темы
Тема 6. Реализация разностного криптоанализа игрушечного шифра. Оценка необходимого объема статистики.	4	4	1, 2, 3	Разбор представленного теоретического материала, практическое применение изученной темы
Тема 7. Реализация хэш-функции на выбор. Анализ отдельных компонент.	4	4	1, 2, 3	Разбор представленного теоретического материала, практическое применение изученной темы
Тема 8. Анализ криптографических примитивов используя тесты на случайность.	4	4	1, 2, 3	Разбор представленного теоретического материала, практическое применение изученной темы
Итого:	**32**	**32**		

4. Самостоятельная работа студентов

Таблица 4.1

№	Виды самостоятельной работы	Ссылки на результаты обучения	Часы на выполнение	Часы на консультации
Семестр: 2				
1	Изучение разделов дисциплины по учебной литературе, в том числе вопросов, не освещаемых на лекциях	1, 2, 3	40	
	Изучение предлагаемых теоретических разделов в соответствии с настоящей Программой. Учебно-методические материалы по дисциплине выложены на странице курса в сети Интернет			
2	Подготовка к практическим занятиям, к текущему контролю знаний	1, 2, 3	70	
	Выполнение заданий			
3	Подготовка к дифференцированному зачету	1, 2, 3	40	
	Повторение теоретического материала по вопросам, совпадающим с темами лекций			
	Итого		150	

5. Образовательные технологии

В ходе реализации учебного процесса по дисциплине проводятся лекционные и практические занятия. Темы, рассматриваемые на лекциях и изучаемые самостоятельно, закрепляются на практических занятиях. Применяются такие формы проведения практических занятий, как обсуждение и защита результатов работы, а также используются следующие интерактивные формы обучения (таблица 5.1).

Таблица 5.1

Технологии проблемного обучения	ПКС-1
Формируемые умения: уметь ориентироваться в современных и классических методах теории криптографии;	
Краткое описание применения: Постановка под руководством преподавателя проблемных задач и активная самостоятельная деятельность обучающихся по их разрешению, сопровождающаяся обсуждением результатов.	

Портфолио	ПКС-1
Формируемые умения: Уметь ориентироваться в современных и классических методах симметричной криптографии; владеть навыками общего выбора методов для решения конкретных задач криптографии.	
Краткое описание применения: студенты ведут портфолио (коллекцию работ), которое является основой для проведения аттестации по дисциплине.	

Для организации и контроля самостоятельной работы студентов применяются информационно-коммуникационные технологии (таблица 5.2).

Таблица 5.2

Информирование	www.crypto.nsu.ru www.crypto-master.nsu.ru
Консультирование	www.crypto.nsu.ru www.crypto-master.nsu.ru
Контроль	www.crypto.nsu.ru www.crypto-master.nsu.ru
Размещение учебных материалов	www.crypto.nsu.ru www.crypto-master.nsu.ru

6. Правила аттестации студентов по учебной дисциплине

По дисциплине **Симметричная криптография и криптоанализ** проводится текущая и промежуточная аттестация (итоговая по дисциплине).

Текущая аттестация по дисциплине Симметричная криптография и криптоанализ осуществляется на практических занятиях и представлена защитой практических работ. В ходе обучения каждый студент должен выполнить задания. По результатам текущей аттестации выставляется оценка «зачтено» или «не зачтено». Оценка «зачтено» по результатам защиты заданий является одним из условий успешного прохождения промежуточной аттестации.

Для получения оценки «зачтено» каждое задание должно быть выполнено и защищено в полном соответствии с предъявляемыми требованиями.

Промежуточная аттестация по дисциплине Симметричная криптография и криптоанализ проводится по завершению периода ее освоения (семестра). Промежуточная аттестация по дисциплине включает 2 этапа:

1) портфолио (задания по темам практических занятий);

2) дифференцированный зачет.

Оценка «зачтено» за портфолио является необходимым условием для прохождения промежуточной аттестации. Результаты промежуточной аттестации определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Оценки «отлично», «хорошо», «удовлетворительно» означают успешное прохождение промежуточной аттестации.

В таблице 6.1 представлено соответствие форм аттестации заявляемым требованиям к результатам освоения дисциплины.

Таблица 6.1

Коды компетенций ФГОС	Результаты обучения	Формы аттестации	
		1 этап - портфолио	2 этап – дифференцированный зачет
ПКС-1	ПКС-1.1. Применяет актуальные модели и подходы в области профессиональной деятельности	+	+
	ПКС-1.2. Комбинирует и адаптирует существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности	+	+
	ПКС-1.3 Применяет на практике программные средства и платформы информационных технологий для разработки и реализации математических моделей, проведение их анализа при решении задач в области профессиональной деятельности	+	+

Требования к структуре и содержанию портфолио, оценочные средства, а также критерии оценки сформированности компетенций и освоения дисциплины в целом, представлены в Фонде оценочных средств, являющемся приложением 1 к настоящей рабочей программе дисциплины.

7. Перечень учебной литературы

1) Токарева, Наталья Николаевна. Симметричная криптография : краткий курс : учебное пособие : М-во образования и науки РФ, Новосиб гос. ун-т, Мех.-мат. фак., Каф. теорет. кибернетики. - Новосибирск : Редакционно-издательский центр НГУ, 2012 – 234с. https://e-lib.nsu.ru/reader/bookView.html?params=UmVzb3VyY2UtMTIyMg/cGFnZTAwMQ
2) Мак-Вильямс, Ф. Дж. Теория кодов, исправляющих ошибки = The theory of error-correcting codes / Ф. Дж. Мак-Вильямс, Н. Дж. А. Слоэн ; пер. с англ. И.И. Грушко, В.А. Зиновьева; под ред. Л. А. Бассалыго. Москва : Связь, 1979. 744 с. : ил. ; 22 см. (2 экз.)
3) Смарт, Найджел. Криптография / Н. Смарт ; пер. с англ. С.А. Кулешова ; под ред. С.К. Ландо. Москва : Техносфера, 2005. 525 с. ; 24 см. (Мир программирования ; VIII; 05) . ISBN 5-94836-043-1. (15 экз.)

8. Перечень ресурсов информационно-коммуникационной сети «Интернет», необходимых для освоения дисциплины

При освоении дисциплины используются следующие ресурсы:

- электронная информационно-образовательная среда НГУ (ЭИОС);
- образовательные интернет-порталы;
- информационно-телекоммуникационная сеть Интернет.

Взаимодействие обучающегося с преподавателем (синхронное и (или) асинхронное) осуществляется через личный кабинет студента в ЭИОС

Таблица 8.1

№ п/п	Наименование Интернет-ресурса	Краткое описание
1	www.crypto.nsu.ru	Cryptographic center (Novosibirsk) Sobolev Institute of Mathematics Mathematical Center in Akademgorodok Laboratory of Cryptography JetBrains Research Novosibirsk State University

9. Учебно-методическое и программное обеспечение дисциплины

9.1. Перечень учебно-методических материалов по самостоятельной работе обучающихся

Учебно-методическое обеспечение самостоятельной работы студентов включает в себя следующие учебно-методические материалы:

1. Рабочая программа дисциплины, соответствующие разделы.
2. Учебники, учебные пособия и дополнительные материалы, указанные в соответствующих разделах настоящей рабочей программы
3. Перечень ресурсов информационно-коммуникационной сети «Интернет», указанные в соответствующих разделах настоящей рабочей программы.
4. Методические указания для обучающихся по освоению дисциплины, обеспечивающие самостоятельную работу студента при подготовке к учебным занятиям, выполнении домашних работ, подготовке к контрольным мероприятиям и аттестациям, приведенные в соответствующих разделах настоящей рабочей программы и приложения к ней.

9.2. Программное обеспечение

Для обеспечения реализации дисциплины используется стандартный комплект программного обеспечения (ПО), включающий регулярно обновляемое лицензионное ПО Windows и MS Office.

Перечень специализированного программного обеспечения для изучения дисциплины представлен в таблице 9.1.

Специализированное программное обеспечение

Таблица 9.1

№	Наименование ПО	Назначение
1	Microsoft Visual Studio 2013	Среда разработки приложений

10. Профессиональные базы данных и информационные справочные системы

1. Полнотекстовые электронные ресурсы Freedom Collection издательства Elsevier (Нидерланды) (2 предметные коллекции – Computer Science, Mathematics)

2. БД Scopus (Elsevier)

11. Материально-техническое обеспечение

Для реализации дисциплины используются специальные помещения:

1. Учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля, промежуточной и итоговой аттестации;

2. Помещения для самостоятельной работы обучающихся;

Учебные аудитории укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду НГУ.

Для проведения занятий лекционного типа предлагаются следующие наборы демонстрационного оборудования и учебно-наглядных пособий:

- комплект лекций-презентаций по темам дисциплины;

Таблица 11.1

№	Наименование	Назначение
1	Презентационное оборудование (мультимедиа-проектор, экран, компьютер для управления)	Для проведения лекционных и практических занятий
2	Компьютерный класс (с выходом в Internet)	Для организации самостоятельной работы обучающихся

Материально-техническое обеспечение образовательного процесса по дисциплине для обучающихся из числа лиц с ограниченными возможностями здоровья осуществляется согласно «Порядку организации и осуществления образовательной деятельности по образовательным программам для инвалидов и лиц с ограниченными возможностями здоровья в Новосибирском государственном университете».

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования «Новосибирский национальный исследовательский
государственный университет» (Новосибирский государственный университет, НГУ)

Факультет информационных технологий

СОГЛАСОВАНО
Декан ФИТ НГУ
М.М. Лаврентьев
«18» апреля 2022 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ
по дисциплине Симметричная криптография и криптоанализ

Направление подготовки: 09.04.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА

Направленность (профиль): Квантовые технологии и криптография
Квалификация: Магистр

Форма обучения: очная

Год обучения: 1, семестр 2

Форма аттестации	Семестр
Дифзачет	2

Новосибирск 2022

Фонд оценочных средств промежуточной аттестации является **Приложением 1** к рабочей программе дисциплины «Симметричная криптография и криптоанализ», реализуемой в рамках образовательной программы высшего образования – программы магистратуры 09.04.01 Информатика и вычислительная техника, направленность (профиль): Квантовые технологии и криптография

Фонд оценочных средств промежуточной аттестации по дисциплине утвержден решением Ученого совета факультета информационных технологий протокол № 84 от 28.03.2022

Разработчик:
ст. преподаватель кафедры теоретической кибернетики ММФ НГУ
кандидат физико-математических наук Н.А.Коломеец

ассистент кафедры компьютерных систем ФИТ НГУ
Ю.П.Максимлюк

Заведующий кафедрой систем информатики ФИТ,
доктор физико-математических наук М.М. Лаврентьев

Ответственный за образовательную программу:
Доцент кафедры квантовой электроники ФФ,
кандидат физико-математических наук И.И.Бетеров

1. Содержание и порядок проведения промежуточной аттестации по дисциплине

1.1. Общая характеристика содержания промежуточной аттестации

Промежуточная аттестация по дисциплине «Симметричная криптография и криптоанализ» проводится по завершению периода освоения образовательной программы (семестра) для оценки сформированности компетенций, в части следующих индикаторов достижения компетенции (таблица П1.1).

Таблица П1.1

Коды компетенций ФГОС	Компетенции, формируемые в рамках дисциплины «Симметричная криптография и криптоанализ»	Семестр 2	
		портфолио	дифзачет
ПКС-1 Способен выполнять фундаментальные и прикладные работы поискового, теоретического и экспериментального характера			
ПКС-1.1	Применяет актуальные модели и подходы в области профессиональной деятельности	+	+
ПКС-1.2	Комбинирует и адаптирует существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности	+	+
ПКС-1.3	Применяет на практике программные средства и платформы информационных технологий для разработки и реализации математических моделей, проведение их анализа при решении задач в области профессиональной деятельности	+	+

Тематика вопросов к диф.зачету соответствует избранным разделам (темам) дисциплины «Симметричная криптография и криптоанализ»

Псевдослучайные числа. Методы генерации. Использование в криптографии.

Генераторы псевдослучайных чисел и поточные шифры. Базовые конструкции. Принципы проектирования. Методы криптоанализа. Корреляционные атаки и др.

Блочные шифры. Основные схемы. Режимы шифрования. Общие методы криптоанализа.

Линейный и разностный криптоанализ. Алгебраический криптоанализ.

Построение шифров с гарантированной оценкой стойкости к линейному и дифференциальному методам. The Wide Trail Design Strategy.

Перемешивающие свойства преобразований, используемых при шифровании. Branch numbers.

Подробный разбор алгоритмов AES, Кузнечик. Оценки стойкости.

Хэш-функции, MAC, их приложения. Базовые схемы. Криптоанализ.

Подробный разбор алгоритмов SHA-3, Стрибог. Оценки стойкости.

Криптоанализ по сторонним каналам.

ARX-схемы. Достоинства и недостатки. Особенности криптоанализа.

Промежуточная аттестация включает 2 этапа:

1. Портфолио.
2. Дифзачет.

Все компетенции, формируемые в рамках дисциплины, оцениваются как через портфолио, так и на дифзачете.

1.2. Порядок проведения промежуточной аттестации по дисциплине

Промежуточная аттестация проводится в форме дифзачета и включает 2 этапа: портфолио и дифзачет. Необходимым условием для прохождения промежуточной аттестации является оценка «зачтено» по результатам выполненного портфолио. Для оценивания портфолио студенту необходимо сдать все работы, входящие в структуру портфолио.

Портфолио включает выполнение заданий по темам практических занятий.

Дифзачет проводится в устной форме, в аудитории, студентам разрешено пользоваться бумагой для записей и авторучкой. Во время проведения дифзачета студенту разрешается использовать справочники, учебную и научную литературу, компьютеры. В процессе ответа на вопросы дифзачета студенту могут быть заданы дополнительные вопросы по темам дисциплины.

2. Требования к структуре и содержанию фонда оценочных средств промежуточной аттестации по дисциплине

Перечень оценочных средств, применяемых на каждом этапе проведения промежуточной аттестации по дисциплине, представлен в таблице П1.2.

Таблица П1.2

№ п/п	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде
Этап 1 - портфолио			
1.	Портфолио	Целевая подборка работ студента, раскрывающая его индивидуальные образовательные достижения в одной или нескольких учебных дисциплинах	Структура портфолио
Этап 2 – Дифзачет			
2	Собеседование	Средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.п.	Вопросы по темам/разделам дисциплины

2.1. Требования к структуре и содержанию оценочных средств аттестации в семестре

Текущая аттестация по дисциплине «Симметричная криптография и криптоанализ» проводится в форме портфолио. Промежуточная аттестация проводится в формате дифзачета.

2.1.1 Требования к структуре и содержанию портфолио

Портфолио включает защиту заданий на практических занятиях.

Оценка за курс выставляется по результатам дифзачета. Оценки «отлично», «хорошо», «удовлетворительно» означают успешное прохождение промежуточной аттестации.

2.1.2 Перечень вопросов дифзачета 2 семестра

Псевдослучайные числа. Методы генерации. Использование в криптографии.

Генераторы псевдослучайных чисел и поточные шифры. Базовые конструкции. Принципы проектирования. Методы криптоанализа. Корреляционные атаки и др.

Блочные шифры. Основные схемы. Режимы шифрования. Общие методы криптоанализа.

Линейный и разностный криптоанализ. Алгебраический криптоанализ.

Построение шифров с гарантированной оценкой стойкости к линейному и дифференциальному методам. The Wide Trail Design Strategy.

Перемешивающие свойства преобразований, используемых при шифровании. Branch numbers.

Подробный разбор алгоритмов AES, Кузнечик. Оценки стойкости.

Хэш-функции, MAC, их приложения. Базовые схемы. Криптоанализ.

Подробный разбор алгоритмов SHA-3, Стрибог. Оценки стойкости.

Криптоанализ по сторонним каналам.

ARX-схемы. Достоинства и недостатки. Особенности криптоанализа

Набор вопросов к дифзачету формируется и утверждается в установленном порядке в начале учебного года при наличии контингента обучающихся, завершающих освоение дисциплины «Симметричная криптография и криптоанализ» в текущем учебном году.

3. **Критерии оценки сформированности компетенций в рамках промежуточной аттестации по дисциплине**

Таблица П1.5

Шифр компетенций	**Структурные элементы оценочных средств**	**Показатель сформированности**	**Не сформирован**	**Пороговый уровень**	**Базовый уровень**	**Продвинутый уровень**
ПКС-1	Портфолио (этап 1), Дифзачет (этап 2)	ПКС-1.1. Применяет актуальные модели и подходы в области профессиональной деятельности	Не знает актуальные модели и подходы в области профессиональной деятельности	Допускает грубые ошибки, слабо знает основной набор понятий современной симметричной криптографии	Знает на базовом уровне основной набор понятий современной симметричной криптографии, наиболее часто используемые математические принципы в алгоритмах шифрования и их криптоанализе	Уверенно знает основной набор понятий современной симметричной криптографии, наиболее часто используемые математические принципы в алгоритмах шифрования и их криптоанализе
ПКС-1	Портфолио (этап 1), Дифзачет (этап 2)	ПКС-1.2. Комбинирует и адаптирует существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности	Не умеет комбинировать и адаптировать существующие информационно-коммуникационные технологии для решения задач в области	Демонстрирует слабые умения ориентироваться в современных и классических методах криптографии	Умеет самостоятельно ориентироваться в современных и классических методах криптографии, допускает несущественные погрешности	Умеет самостоятельно ориентироваться в современных и классических методах криптографии

			профессиональной деятельности с учетом требований информационной безопасности			
ПКС-1	Портфолио (этап 1), Дифзачет (этап 2)	ПКС-1.3 Применяет на практике программные средства и платформы информационных технологий для разработки и реализации математических моделей, проведение их анализа при решении задач в области профессиональной деятельности	Не умеет применять на практике программные средства и платформы информационных технологий для разработки и реализации математических моделей, проведение их анализа при решении задач в области	Слабо владеет навыками общего выбора методов для решения конкретных задач криптографии, допускает множественные ошибки	Владеет навыками общего выбора методов для решения конкретных задач криптографии для решения учебных задач	Уверенно владеет навыками общего выбора методов для решения конкретных задач криптографии

			профессиональной деятельности			

4. **Критерии выставления оценок по результатам промежуточной аттестации по дисциплине**

В соответствии с учебным планом устанавливаются следующие формы контроля:

Результаты промежуточной аттестации определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Оценки «отлично», «хорошо», «удовлетворительно» означают успешное прохождение промежуточной аттестации.

Оценка «отлично» соответствует продвинутому уровню сформированности компетенции.

Оценка «хорошо» соответствует базовому уровню сформированности компетенции.

Оценка «удовлетворительно» соответствует пороговому уровню сформированности компетенции.

Оценка «неудовлетворительно» выставляется, если хотя бы одна компетенция не сформирована.

Итоговая оценка результатов промежуточной аттестации выставляется как оценка за дифзачет.