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
«25» апреля 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Криптография и протоколы безопасности

Направление подготовки: 09.04.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА
Направленность (профиль): Интернет вещей

Форма обучения: очная
Год обучения: 1, 2, семестр: 2, 3

№	Вид деятельности	Семестр	
		2	3
1	Лекции, час.	32	16
2	Практические занятия, час.	32	32
3	Лабораторные занятия, час.		
4	Занятий в контактной форме без учета промежуточной аттестации, час, из них	64	48
5	в электронной форме, час.		
6	из них аудиторных занятий, час.	64	48
7	из них в активной и интерактивной форме, час.	64	48
8	консультаций, час.		
9	Самостоятельная работа, час.	78	58
10	в том числе на выполнение письменных работ, час	30	30
11	Форма аттестации (экзамен, зачет, дифференцированный зачет), час	ДЗ 2	ДЗ 2
12	Всего зачетных единиц[1]	4	3

Новосибирск 2023

[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), обязательная дисциплина.

Рабочая программа дисциплины утверждена решением Ученого совета факультета информационных технологий от 24.04.2023, протокол №91.

Программу разработали:

Старший преподаватель
кафедры систем информатики ФИТ  Р.А. Пермяков

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

Ответственный за образовательную программу
Заведующий кафедрой Систем информатики ФИТ,
доктор физико-математических наук  М.М. Лаврентьев

Аннотация к рабочей программе дисциплины
«Криптография и протоколы безопасности»

Дисциплина «Криптография и протоколы безопасности» реализуется в рамках образовательной программы высшего образования – программы магистратуры 09.04.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА, направленность (профиль): ИНТЕРНЕТ ВЕЩЕЙ по очной форме обучения на русском языке.

Место в образовательной программе: Дисциплина «Криптография и протоколы безопасности» реализуется в 2 и 3 семестре в рамках базовой части дисциплин (модулей) Блока 1 и является обязательной дисциплиной.

Дисциплина **«Криптография и протоколы безопасности»** является базовой для выполнения работы в рамках практики и выполнением выпускной квалификационной работы.

Дисциплина **«Криптография и протоколы безопасности»** направлена на формирование компетенций:

Способен самостоятельно приобретать, развивать и применять математические, естественнонаучные, социально-экономические и профессиональные знания для решения нестандартных задач, в том числе в новой или незнакомой среде и в междисциплинарном контексте (ОПК-1), в части следующих индикаторов достижения компетенции:

ОПК-1.1. Знать: математические, естественнонаучные и социально-экономические методы для использования в профессиональной деятельности

ОПК-1.2. Уметь: решать нестандартные профессиональные задачи, в том числе в новой или незнакомой среде и в междисциплинарном контексте, с применением математических, естественнонаучных, социально-экономических и профессиональных знаний

ОПК-1.3. Владеть: навыками теоретического и экспериментального исследования объектов профессиональной деятельности, в том числе в новой или незнакомой среде и в междисциплинарном контексте

Перечень основных разделов дисциплины:

Тема 1. Введение в теорию информации.
Тема 2. Подходы к измерению сложности сообщения. Понятие энтропии, ее свойства.
Тема 3. Передача сообщений по каналу связи с искажением. Коды с малой плотностью проверок на четность.
Тема 4. Методы сжатия информации.
Тема 5. Основные задачи криптографии. Теория секретности Шеннона.
Тема 6. Симметричная криптография. Принципы построения симметричных шифров.
Тема 7. Введение в криптографические свойства булевых функций.
Тема 8. Общие методы криптоанализа симметричных шифров.
Тема 9. Хэш-функции. Базовые принципы.
Тема 10. Асимметричная криптография. Основные принципы построения и анализа асимметричных криптосистем.
Тема 11. Новые направления криптографии: квантовая и постквантовая криптография.
Тема 12. Обзор приложений теории информации.

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.

Предусмотрено проведение занятий с использованием дистанционных образовательных технологий.

Общий объем дисциплины – 7 зачетных единицы (252 часа).

Правила аттестации по дисциплине. Текущий контроль по дисциплине «Криптография и протоколы безопасности» осуществляется на практических занятиях на основании оценки за портфолио (задания по темам практических занятий). По результатам защиты портфолио выставляется оценка «зачтено» или «не зачтено».

Промежуточная аттестация по дисциплине «Криптография и протоколы безопасности» 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 (итоговой по дисциплине) аттестации определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Оценки «отлично», «хорошо», «удовлетворительно» означают успешное прохождение промежуточной аттестации.

Учебно-методическое обеспечение дисциплины.

www.crypto.nsu.ru

1. **Внешние требования к дисциплине**

Таблица 1.1

Компетенция ОПК-1 Способен самостоятельно приобретать, развивать и применять математические, естественнонаучные, социально-экономические и профессиональные знания для решения нестандартных задач, в том числе в новой или незнакомой среде и в междисциплинарном контексте, *в части следующих индикаторов достижения компетенции*:	
ОПК-1.1	Знать: математические, естественнонаучные и социально-экономические методы для использования в профессиональной деятельности
ОПК-1.2	Уметь: решать нестандартные профессиональные задачи, в том числе в новой или незнакомой среде и в междисциплинарном контексте, с применением математических, естественнонаучных, социально-экономических и профессиональных знаний
ОПК-1.3	Владеть: навыками теоретического и экспериментального исследования объектов профессиональной деятельности, в том числе в новой или незнакомой среде и в междисциплинарном контексте

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**
ОПК-1.1 Знать: математические, естественнонаучные и социально-экономические методы для использования в профессиональной деятельности			
1 Знать основной набор понятий современной теории информации, сжатия данных, теории кодирования и криптографии, наиболее часто используемые математические принципы в криптографии;	+	+	+
ОПК-1.2 Уметь: решать нестандартные профессиональные задачи, в том числе в новой или незнакомой среде и в междисциплинарном контексте, с применением математических, естественнонаучных, социально-экономических и профессиональных знаний			
2. Уметь ориентироваться в современных и классических методах теории информации и криптографии;	+	+	+
ОПК-1.3 Владеть: навыками теоретического и экспериментального исследования объектов профессиональной деятельности, в том числе в новой или незнакомой среде и в междисциплинарном контексте			
3. Владеть навыками общего выбора методов для решения конкретных задач теории информации и 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 теорию информации.	4	4	1, 2, 3
Тема 2. Подходы к измерению сложности сообщения. Понятие энтропии, ее свойства.	4	4	1, 2, 3
Тема 3. Передача сообщений по каналу связи с искажением. Коды с малой плотностью проверок на четность.	10	10	1, 2, 3
Тема 4. Методы сжатия информации.	4	4	1, 2, 3
Тема 5. Основные задачи криптографии. Теория секретности Шеннона.	6	6	1, 2, 3
Тема 6. Симметричная криптография. Принципы построения симметричных шифров.	4	4	1, 2, 3
Итого:	32	32	
Семестр: 3			
Тема 7. Введение в криптографические свойства булевых функций.	2	2	1, 2, 3
Тема 8. Общие методы криптоанализа симметричных шифров.	2	2	1, 2, 3
Тема 9. Хэш-функции. Базовые принципы.	4	4	1, 2, 3
Тема 10. Асимметричная криптография. Основные принципы построения и анализа асимметричных криптосистем.	4	4	1, 2, 3
Тема 11. Новые направления криптографии: квантовая и постквантовая криптография.	2	2	1, 2, 3
Тема 12. Обзор приложений теории информации.	2	2	1, 2, 3
Итого:	**16**	**16**	

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. Введение в теорию информации. История вопроса и современное состояние. Разделы теории информации. Приложения теории информации. Источники информации, методы преобразования непрерывного сигнала в цифровую форму. Теорема дискретизации Котельникова.	4	4	1, 2, 3	Разбор представленного теоретического материала, решение задач, практическое применение изученной темы
Тема 2. Подходы к измерению сложности сообщения. Понятие энтропии, ее свойства. Модели источников сообщений. Подходы к измерению сложности сообщения. Энтропия и ее свойства.	4	4	1, 2, 3	Разбор представленного теоретического материала, решение задач, практическое применение изученной темы
Тема 3. Передача сообщений по каналу связи с искажением. Коды с малой плотностью проверок на четность. Модель канала связи, пропускная способность. Ошибка декодирования. Линейные коды. Код Хэмминга. Циклические коды. Теорема Шеннона о скорости кодирования. Коды с малой плотностью проверок на четность, достигающие оценку теоремы Шеннона. Коды Галлагера. Графы Таннера	12	12	1, 2, 3	Разбор представленного теоретического материала, решение задач, практическое применение изученной темы
Тема 4. Методы сжатия информации. Методы сжатия информации. Сжатие без потерь. Метод Хаффмана. Метод Фано. Энтропийное кодирование. Теорема Шеннона о блочном энтропийном кодировании. Арифметическое кодирование. Словарные методы. Сжатие с потерями. Формат JPEG. Достоинства и недостатки популярных методов. Обзор современных архиваторов.	4	4	1, 2, 3	Разбор представленного теоретического материала, решение задач, практическое применение изученной темы
Тема 5. Основные задачи криптографии. Теория секретности Шеннона. История вопроса. Обзор современных направлений в криптографии и	12	12	1, 2, 3	Разбор представленного теоретического материала, решение задач, практическое применение изученной темы

криптоанализе. Задачи криптографии. Понятие криптографического протокола. Вероятностная модель шифрсистемы. Полная избыточность языка сообщений и избыточность на букву сообщения. Теоремы Шеннона об избыточности языка сообщений, о числе ложных ключей, о совершенной секретности				
Тема 6. Симметричная криптография. Принципы построения симметричных шифров. Блочные и поточные шифры. Математические модели, принципы построения. Примеры шифров: DES, Magma, AES, Kuznechik. Криптографические примитивы симметричных шифров	4	4	1, 2, 3	Разбор представленного теоретического материала, решение задач, практическое применение изученной темы
Семестр: 3				
Тема 7. Введение в криптографические свойства булевых функций. Принципы построения криптографических булевых функций. Нелинейные булевы функции. Алгебраически иммунные функции. APN-функции.	4	4	1, 2, 3	Разбор представленного теоретического материала, решение задач, практическое применение изученной темы
Тема 8. Общие методы криптоанализа симметричных шифров. Введение в основы симметричного криптоанализа. Универсальные методы криптоанализа. Статистические и аналитические методы криптоанализа симметричных шифров.	4	4	1, 2, 3	Разбор представленного теоретического материала, решение задач, практическое применение изученной темы
Тема 9. Хэш-функции. Базовые принципы. Основы конструирования криптографических хэш-функций. Требования к ним. Базовые примеры современных хэш-функций.	4	4	1, 2, 3	Разбор представленного теоретического материала, решение задач, практическое применение изученной темы
Тема 10. Асимметричная криптография. Основные принципы построения и анализа асимметричных криптосистем. Математические вопросы асимметричной криптографии. Вопросы существования односторонних функций и псевдослучайных генераторов.	4	4	1, 2, 3	Разбор представленного теоретического материала, решение задач, практическое применение изученной темы

Задачи факторизации и дискретного логарифмирования. Вопросы теории чисел. Проверка простоты числа. Протокол Диффи-Хеллмана. Криптосистемы RSA, Эль-Гамаля, Шамира и другие. Электронная цифровая подпись.				
Тема 11. Новые направления криптографии: квантовая и постквантовая криптография.	4	4	1, 2, 3	Разбор представленного теоретического материала, решение задач, практическое применение изученной темы
Тема 12. Обзор приложений теории информации. Цифровая сотовая связь. Система безопасности GSM. Алгоритмы A5. Безопасность телефонных переговоров. Беспроводные сети WiFi. Методы шифрования WEP и WPA. Криптографические методы в противоугонных системах безопасности. Криптосистемы на основе биометрических данных.	4	4	1, 2, 3	Разбор представленного теоретического материала, решение задач, практическое применение изученной темы
Итого за 1 и 2 семестры:	**64**	**64**		

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	30	
	Выполнение заданий			
3	Подготовка к дифференцированному зачету	1, 2, 3	6	
	Повторение теоретического материала по вопросам, совпадающим с темами лекций			
			76	0
Семестр: 3				
1	**Изучение разделов дисциплины по учебной литературе, в том числе вопросов, не освещаемых на лекциях**	1, 2, 3	22	
	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	30	
	Выполнение заданий			
3	Подготовка к дифференцированному зачету	1, 2, 3	6	
	Повторение теоретического материала по вопросам, совпадающим с темами лекций			
	Итого		136	0

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, по вопросам, вызывающим затруднения, проводятся консультации на практических занятиях.

Предусмотрено проведение занятий с использованием дистанционных образовательных технологий. При проведении практических занятий студенты подключаются к онлайн сессии. На занятии разбираются теоретические темы и формулировки практических заданий. Для сдачи выполненного задания студент включает демонстрацию экрана, показывает результаты, обосновывает решение, отвечает на вопросы преподавателя

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	ОПК-1
Формируемые умения: уметь ориентироваться в современных и классических методах теории информации и криптографии;	
Краткое описание применения: Постановка под руководством преподавателя проблемных задач и активная самостоятельная деятельность обучающихся по их разрешению, сопровождающаяся обсуждением результатов.	
Портфолио	ОПК-1
Формируемые умения: Уметь ориентироваться в современных и классических методах теории информации и криптографии; владеть навыками общего выбора методов для решения конкретных задач теории информации и криптографии.	
Краткое описание применения: студенты ведут портфолио (коллекцию работ), которое является основой для проведения аттестации по дисциплине.	

Для организации и контроля самостоятельной работы студентов, а также проведения консультаций применяются информационно-коммуникационные технологии (таблица 5.2).

Таблица 5.2

Практические занятия	www.crypto.nsu.ru www.crypto-master.nsu.ru
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 «Криптография и протоколы безопасности» проводится текущая и промежуточная аттестация (итоговая по дисциплине).

Текущая аттестация по дисциплине «Криптография и протоколы безопасности» осуществляется на практических занятиях и представлена защитой заданий на практических занятиях. 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 «Криптография и протоколы безопасности» 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**
ОПК-1	**ОПК-1.1.** Знать: математические, естественнонаучные и социально-экономические методы для использования в профессиональной деятельности	+	+
	ОПК-1.2. Уметь: решать нестандартные профессиональные задачи, в том числе в новой или незнакомой среде и в междисциплинарном контексте, с применением математических, естественнонаучных, социально-экономических и профессиональных знаний	+	+
	ОПК-1.3. Владеть: навыками теоретического и экспериментального исследования объектов профессиональной деятельности, в том числе в новой или незнакомой среде и в междисциплинарном контексте	+	+

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. Литература

Основная литература

1) Материалы международных конференций по теории информации и криптографии: ISIT, EUROCRYPT, CRYPTO, FSE, ASIACRYPT, SIBECRYPT, BFCA и др.
2) Cover T.M. *Elements of Information Theory.*Wiley Series in Telecommunications and Signal Processing (Book 20), Wiley-Interscience, ISBN: 978-0471062592, 1991, 576 pages.
3) Gallager R.G. Information Theory and Reliable Communication, Wiley, ISBN: 978-0471290483, 1968, 608 pages.
4) Ifeachor I.C., Jervis B.W. *Digital Signal Processing: A Practical Approach.* Pearson Education, ISBN 978-0201596199, 2002, 960 pages.
5) MacWilliams F.J., Sloane N.J.A. *The Theory of Error-Correcting Codes*. Elsevier/North-Holland Publishing Company, 1977, 782 pages.
6) Mao W. *Modern Cryptography: Theory and Practice.* Prentice Hall, ISBN 9780132887410, 2003, 752 pages.
7) Menezes A.J, Van Oorschot P.C., Vanstone S.A. *Handbook of Applied Cryptography*. CRC Press, ISBN 0-8493-8523-7, 1996, 816 pages.
8) Moon T. K., *Error Correction Coding, Mathematical Methods and Algorithms*. Wiley, ISBN 0-471-64800-0, 2005, 800 pages.
9) Salomon D. *Data Compression: The Complete Reference*. Springer-Verlag London, ISBN 978-1-84628-603-2, 2007, 1092 pages.
10) Schneier B. *Applied Cryptography. Protocols, Algorithms, and Source Code in C.* John Wiley & Sons. ISBN 978-1-119-09672-6, 1996, 784 pages.
11) Shannon C. *Collected papers (Edited by N.J.A.Sloane, A.D.Wyner).* Wiley, ISBN 978-0-7803-0434-5, 1993, 968 pages.
12) Smart N. *Cryptography: An Introduction.* Mcgraw-Hill College, ISBN 978-0077099879, 2004, 433 pages.
13) Stinson D.R. *Cryptography: Theory and Practice, Third Edition (Discrete Mathematics and Its Applications*). Chapman and Hall/CRC, ISBN 978-1584885085, 2005, 616 pages.
14) Tokareva N. *Bent Functions, Results and Applications to Cryptography.* Academic Press Elsevier, ISBN 978-0-12-802318-1, 2015, 220 pages.

Интернет-ресурсы

Таблица 7.1

№ 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

8. Учебно-методическое и программное обеспечение дисциплины

8.1. Учебно-методическое обеспечение

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.

8.2. 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 8.1.

Специализированное программное обеспечение

Таблица 8.1

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

9. 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)

10. Материально-техническое обеспечение

Таблица 10.1

№	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

Лист актуализации рабочей программы дисциплины
«Криптография и протоколы безопасности»

№	Характеристика внесенных изменений (с указанием пунктов документа)	Дата и № протокола Ученого совета ФИТ	Подпись ответственного
1.	Внесены изменения в п.5 в части проведения занятий с использованием дистанционных образовательных технологий	05.02.2024 №94	

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
«25» апреля 2023 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ
по дисциплине Криптография и протоколы безопасности

Направление подготовки: 09.04.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА.

Направленность (профиль): Интернет вещей
Квалификация: Магистр

Форма обучения: очная Год обучения: 1, 2 семестр 2, 3

Форма аттестации	Семестр
Дифференцированный зачет	2, 3

Новосибирск 2023

Фонд оценочных средств промежуточной аттестации является **Приложением 1** к рабочей программе дисциплины «Криптография и протоколы безопасности», реализуемой в рамках образовательной программы высшего образования – программы магистратуры 09.04.01 Информатика и вычислительная техника, направленность (профиль): Интернет вещей

Фонд оценочных средств промежуточной аттестации по дисциплине утвержден решением ученого совета факультета информационных технологий, протокол №91 от 24.04.2023.

Разработчик:
Старший преподаватель
кафедры систем информатики ФИТ  Р.А. Пермяков

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

Ответственный за образовательную программу:

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

1. Содержание и порядок проведения промежуточной аттестации по дисциплине

1.1. Общая характеристика содержания промежуточной аттестации

Промежуточная аттестация по дисциплине «Криптография и протоколы безопасности» 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 «Криптография и протоколы безопасности»	Семестр 1	
		портфолио	дифференцированный зачет
ОПК-1 Способен самостоятельно приобретать, развивать и применять математические, естественнонаучные, социально-экономические и профессиональные знания для решения нестандартных задач, в том числе в новой или незнакомой среде и в междисциплинарном контексте			
ОПК-1.1	Знать: математические, естественнонаучные и социально-экономические методы для использования в профессиональной деятельности	+	+
ОПК-1.2	Уметь: решать нестандартные профессиональные задачи, в том числе в новой или незнакомой среде и в междисциплинарном контексте, с применением математических, естественнонаучных, социально-экономических и профессиональных знаний	+	+
ОПК-1.3	Владеть: навыками теоретического и экспериментального исследования объектов профессиональной деятельности, в том числе в новой или незнакомой среде и в междисциплинарном контексте	+	+

Тематика вопросов к дифференцированному зачету соответствует избранным разделам (темам) дисциплины «Криптография и протоколы безопасности»

Тема 1. Введение в теорию информации.

Тема 2. Подходы к измерению сложности сообщения. Понятие энтропии, ее свойства.

Тема 3. Передача сообщений по каналу связи с искажением. Коды с малой плотностью проверок на четность.

Тема 4. Методы сжатия информации.

Тема 5. Основные задачи криптографии. Теория секретности Шеннона.

Тема 6. Симметричная криптография. Принципы построения симметричных шифров.

Тема 7. Введение в криптографические свойства булевых функций.

Тема 8. Общие методы криптоанализа симметричных шифров.

Тема 9. Хэш-функции. Базовые принципы.

Тема 10. Асимметричная криптография. Основные принципы построения и анализа асимметричных криптосистем.

Тема 11. Новые направления криптографии: квантовая и постквантовая криптография.

Тема 12. Обзор приложений теории информации.

Промежуточная аттестация включает 2 этапа:

1. Портфолио.
2. Дифференцированный зачет.

Все компетенции, формируемые в рамках дисциплины, оцениваются как через портфолио, так и на устном дифференцированном зачете.

1.2. Порядок проведения промежуточной аттестации по дисциплине

Промежуточная аттестация проводится в форме дифференцированного зачета и включает 2 этапа: портфолио и дифференцированный зачет. 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.

Дифференцированный зачет проводится в устной форме, в аудитории, студентам разрешено пользоваться бумагой для записей и авторучкой. Во время проведения дифференцированного зачета студенту разрешается использовать справочники, учебную и научную литературу, компьютеры. В процессе ответа на вопросы дифференцированного зачета 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 – Дифференцированный зачет			
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 «Криптография и протоколы безопасности» проводится в форме портфолио. Промежуточная аттестация проводится в формате дифференцированного зачета

2.1.1 Требования к структуре и содержанию портфолио

Портфолио включает защиту заданий на практических занятиях.

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

2.1.2 Перечень вопросов дифференцированного зачета 2 семестра

Тема 1. Введение в теорию информации.

Тема 2. Подходы к измерению сложности сообщения. Понятие энтропии, ее свойства.

Тема 3. Передача сообщений по каналу связи с искажением. Коды с малой плотностью проверок на четность.

Тема 4. Методы сжатия информации.

Тема 5. Основные задачи криптографии. Теория секретности Шеннона.

Тема 6. Симметричная криптография. Принципы построения симметричных шифров.

2.1.3 Перечень вопросов дифференцированного зачета 3 семестра

Тема 7. Введение в криптографические свойства булевых функций.

Тема 8. Общие методы криптоанализа симметричных шифров.

Тема 9. Хэш-функции. Базовые принципы.

Тема 10. Асимметричная криптография. Основные принципы построения и анализа асимметричных криптосистем.

Тема 11. Новые направления криптографии: квантовая и постквантовая криптография.

Тема 12. Обзор приложений теории информации.

Набор вопросов для дифференцированного зачета формируется и утверждается в установленном порядке в начале учебного года при наличии контингента обучающихся, завершающих освоение дисциплины «Криптография и протоколы безопасности» 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
ОПК-1	Портфолио (этап 1), Дифференцированный зачет (этап 2)	ОПК-1.1. Знать: математические, естественнонаучные и социально-экономические методы для использования в профессиональной деятельности	Не знает математические, естественнонаучные и социально-экономические методы для использования в профессиональной деятельности	Допускает грубые ошибки, слабо знает основной набор понятий современной теории информации, сжатия данных, теории кодирования и криптографии, наиболее часто используемые математические принципы в криптографии	Знает на базовом уровне основной набор понятий современной теории информации, сжатия данных, теории кодирования и криптографии, наиболее часто используемые математические принципы в криптографии	Уверенно знает основной набор понятий современной теории информации, сжатия данных, теории кодирования и криптографии, наиболее часто используемые математические принципы в криптографии
ОПК-1	Портфолио (этап 1), Дифференцированный зачет (этап 2)	ОПК-1.2. Уметь: решать нестандартные профессиональные задачи, в том числе в новой или незнакомой среде и в междисциплинарном контексте, с применением математических, естественнонаучных, социально-экономических и профессиональных знаний	Не умеет решать нестандартные профессиональные задачи, в том числе в новой или незнакомой среде и в междисциплинарном контексте, с применением математических, естественнонаучных, социально-экономических и профессиональных знаний	Демонстрирует слабые умения ориентироваться в современных и классических методах теории информации и криптографии	Умеет ориентироваться в современных и классических методах теории информации и криптографии	Умеет грамотно ориентироваться в современных и классических методах теории информации и криптографии

ОПК-1	Портфолио (этап 1), Дифференцированный зачет (этап 2)	ОПК-1.3. Владеть: навыками теоретического и экспериментального исследования объектов профессиональной деятельности, в том числе в новой или незнакомой среде и в междисциплинарном контексте	Не владеет навыками теоретического и экспериментального исследования объектов профессиональной деятельности, в том числе в новой или незнакомой среде и в междисциплинарном контексте	Слабо владеет навыками общего выбора методов для решения конкретных задач теории информации и криптографии	Владеет навыками общего выбора методов для решения конкретных задач теории информации и криптографии, для решения учебных задач	Уверенно владеет навыками общего выбора методов для решения конкретных задач теории информации и криптографии

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 дифференцированный зачет.