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
«26» апреля 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Криптографические проекты

Направление подготовки: 09.03.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА
Направленность (профиль): Программная инженерия и компьютерные науки

Форма обучения: очная
Год обучения: 3 семестр: 5, 6

№	Вид деятельности	Семестр	
		5	6
1	Лекции, час.		
2	Практические занятия, час.		
3	Лабораторные занятия, час.	32	32
4	Занятий в контактной форме без учета промежуточной аттестации, час, из них	32	32
5	в электронной форме, час.		
6	из них аудиторных занятий, час.	32	32
7	из них в активной и интерактивной форме, час.	32	32
8	консультаций, час.		
9	Самостоятельная работа, час.	40	40
10	в том числе на выполнение письменных работ, час		
11	Форма аттестации (экзамен, зачет, дифференцированный зачет), час	ДЗ	ДЗ
12	Всего зачетных единиц[1]	2	2

Новосибирск 2021

[1] С учетом выделенных часов на промежуточную аттестацию

Рабочая программа дисциплины составлена на основании федерального государственного образовательного стандарта (ФГОС) высшего образования - бакалавриат по направлению подготовки 09.03.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА.

Федеральный государственный образовательный стандарт (ФГОС) высшего образования - бакалавриат по направлению подготовки 09.03.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА введен в действие приказом Минобрнауки от 19.09.2017 № 929.

Место дисциплины в структуре учебного плана: Блок ФТД Факультативы, факультативная дисциплина.

Рабочая программа дисциплины утверждена решением Ученого совета факультета информационных технологий от 26.04.2021, протокол № 10.

Программу разработал:

доцент кафедры компьютерных систем ФИТ
кандидат физико-математических наук — Н.Н. Токарева

ассистент кафедры теоретической кибернетики ММФ,
кандидат физико-математических наук — Н.А.Коломеец

ассистент кафедры систем информатики ФИТ — Д.О.Кондырев

преподаватель кафедры фундаментальной и
прикладной лингвистики ГИ — Ю.П.Максимлюк

Заведующий кафедрой компьютерных систем ФИТ,
кандидат технических наук — Б.Н.Пищик

Ответственный за образовательную программу:

доцент кафедры систем информатики ФИТ,
кандидат технических наук — А.А. Романенко

Аннотация к рабочей программе дисциплины
«Криптографические проекты»

Дисциплина «Криптографические проекты» реализуется в рамках образовательной программы высшего образования – программы бакалавриата 09.03.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА, направленность (профиль): ПРОГРАММНАЯ ИНЖЕНЕРИЯ И КОМПЬЮТЕРНЫЕ НАУКИ; по очной форме обучения на русском языке.

Место в образовательной программе: Дисциплина «Криптографические проекты» развивает знания, умения и навыки, сформированные у обучающихся по результатам изучения следующих дисциплин: «Информатика», «Программирование», «Дискретная математика».

Дисциплина «Криптографические проекты» реализуется в 5,6 семестрах в рамках в рамках Блока ФТД Факультативы и является факультативной дисциплиной.

Дисциплина «Криптографические проекты» направлена на формирование компетенций:

Способен применять естественнонаучные и общеинженерные знания, методы математического анализа и моделирования, теоретического и экспериментального исследования в профессиональной деятельности (ОПК-1), в части следующих индикаторов достижения компетенции:

ОПК-1.1 Знать: основы математики, физики, вычислительной техники и программирования

ОПК-1.2 Уметь: решать стандартные профессиональные задачи с применением естественнонаучных и общеинженерных знаний, методов математического анализа и моделирования

ОПК-1.3 Владеть: навыками теоретического и экспериментального исследования объектов профессиональной деятельности

Способен использовать современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности (ОПК-2), в части следующих индикаторов достижения компетенции:

ОПК-2.3 Владеть: навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности.

Способен разрабатывать компоненты системных программных продуктов (ПКС-2), в части следующих индикаторов достижения компетенции:

ПКС-2.1 Владеть: навыками разработки программ на языках высокого уровня

Перечень основных разделов дисциплины: древние шифры, статистические методы криптоанализа примитивных шифров, качество шифртекста и тесты на случайность, симметричная криптография, основные методы криптоанализа симметричных шифров, криптография с открытым ключом, методы анализа асимметричных шифров, основы криптографических протоколов и блокчейн технологий.

При освоении дисциплины студенты выполняют следующие виды учебной работы: лабораторные занятия, самостоятельная работа. В учебном процессе предусматривается использование активных и интерактивных форм проведения занятий. В том числе, предполагаются создание и анализ своих игрушечных примитивов.

Самостоятельная работа включает: подготовку к лабораторным занятиям по разделам дисциплины, подготовку к диф.зачету.

Общий объем дисциплины – 4 зачетных единиц (144 часа).

Правила аттестации по дисциплине. Текущий контроль по дисциплине «Криптографические проекты» осуществляется во время лабораторных занятий по количеству выполненных и защищенных лабораторных работ.

Промежуточная аттестация по дисциплине «Криптографические проекты» проводится по завершению каждого периода ее освоения (семестра) в форме дифференцированного зачёта. Оценка за освоение дисциплины выставляется по результатам оценивания портфолио работ студента, которое включает выполненные и защищенные лабораторные работы.

Результаты промежуточной аттестации по дисциплине оцениваются по шкале «неудовлетворительно», «удовлетворительно», «хорошо», «отлично». Оценки «отлично», «хорошо», «удовлетворительно» означают успешное прохождение промежуточной аттестации.

Оценка «отлично» соответствует 80% и более выполненным и защищенным лабораторным работам.

Оценка «хорошо» соответствует от 65% до 80% (не включительно) выполненным и защищенным лабораторным работам.

Оценка «удовлетворительно» соответствует от 50% до 65% (не включительно) выполненным и защищенным лабораторным работам.

Оценка «неудовлетворительно» соответствует менее 50% выполненным и защищенным лабораторным работам.

Учебно-методическое обеспечение дисциплины.

Учебно-методическое обеспечение дисциплины представлено в рабочей программе дисциплины в виде методических рекомендаций по подготовке и выполнению лабораторных работ.
Методические рекомендации по дисциплине «Криптографические проекты» в электронной информационно-образовательной среде НГУ:
https://drive.google.com/drive/folders/19yKeCBej1QCb0OWeRceDb5k6JE3YVSP8

1. Внешние требования к дисциплине

Таблица 1.1

Компетенция ОПК-1 Способен применять естественнонаучные и общеинженерные знания, методы математического анализа и моделирования, теоретического и экспериментального исследования в профессиональной деятельности, *в части следующих индикаторов достижения компетенции:*
ОПК-1.1 Знать: основы математики, физики, вычислительной техники и программирования
ОПК-1.2 Уметь: решать стандартные профессиональные задачи с применением естественнонаучных и обще-инженерных знаний, методов математического анализа и моделирования
ОПК-1.3 Владеть: навыками теоретического и экспериментального исследования объектов профессиональной деятельности.
Компетенция ОПК-2 Способен использовать современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности, *в части следующих индикаторов достижения компетенции:*
ОПК-2.3 Владеть: навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности
Компетенция ПКС-2 Способен разрабатывать компоненты системных программных продуктов, *в части следующих индикаторов достижения компетенции:*
ПКС-2.1 Владеть: навыками разработки программ на языках высокого уровня

2. Требования к результатам освоения дисциплины

Таблица 2.1

Результаты изучения дисциплины по уровням освоения (иметь представление, знать, уметь, владеть)	**Формы организации занятий**	
	лабораторные работы	**самостоятельная работа**
ОПК-1.1 Знать: основы математики, физики, вычислительной техники и программирования		
1.Знать основные особенности современной криптографии	+	+
2.Знать основные задачи, которые решает современная криптография	+	+
ОПК-1.2 Уметь: решать стандартные профессиональные задачи с применением естественнонаучных и общеинженерных знаний, методов математического анализа и моделирования		
3.Знать требования надежности и главные уязвимые компоненты криптографических примитивов в зависимости от их назначения	+	+
ОПК-1.3 Владеть: навыками теоретического и экспериментального исследования объектов профессиональной деятельности		
4.Владеть основными алгоритмами криптоанализа криптографических примитивов в зависимости от их назначения	+	+
5.Уметь применять общий алгоритм для конкретного примитива	+	+

ОПК-2.3 Владеть: навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности		
6.Знать основные статистические тесты	+	+
7.Уметь применять существующие реализации тестов на практике	+	+
8.Уметь делать выводы о надежности шифрования по результатам статистического тестирования	+	+
ПКС-2.1 Владеть: навыками разработки программ на языках высокого уровня, при решении задач профессиональной деятельности		
9.Уметь делать эффективные программные реализации примитивов симметричной криптографии на языке высокого уровня	+	+
10.Уметь делать эффективные программные реализации примитивов криптографии с открытым ключом	+	+
11.Уметь эффективно реализовывать основные алгоритмы криптоанализа на языке высокого уровня	+	+

3. Содержание и структура учебной дисциплины

Таблица 3.1

Темы лабораторных занятий	Активные формы, час.	Часы	Ссылки на результаты обучения	Учебная деятельность
Семестр: 5				
Тема 1. Древние шифры	6	6	1, 3	Реализация шифра Виженера и шифра простой замены. Реализация алгоритмов, которые при условии шифрования данных с высокой избыточностью определяют: длину использованного ключа в шифра Виженера; полное восстановление ключа шифра Виженера; ключевую подстановку шифра простой замены.
Тема 2. Реализация примитивов симметричной криптографии	8	8	1,2,9	Особенности применения блочных шифров, хэш-функций, поточных шифров и генераторов псевдослучайных чисел.. Особенности их программной реализации.
Тема 3. Тесты на случайность	4	4	6,7,8	Тесты NIST и другие. Основная роль тестов. Тестирование выхода криптографических примитивов. Сравнение результатов для надежных и

				ненадежных шифров.
Тема 4. Универсальные методы криптоанализа симметричных шифров	4	4	4,5,9,11	Реализация метода встречи посередине для игрушечного шифра, использование парадокса дней рождений для хэш-функций.
Тема 5. Линейный и дифференциальный криптоанализ блочных шифров	10	10	11	Реализация игрушечного шифра и алгоритмов поиска оптимальных линейных приближений и цепочек минимального веса. Определения части используемого ключа при наличии требуемого объема статистики
Итого	**32**	**32**		
Семестр: 6				
Тема 6. Основы алгебраического криптоанализа	4	4	11	Составление системы уравнений для нескольких раундов выбранного низкоресурсного шифра.
Тема 7. Поиск коллизий хэш-функций	6	6	2,3,11	Реализация алгоритма поиска коллизий игрушечной хэш-функции.
Тема 8. Реализация алгоритмов криптографии с открытым ключом	6	6	2,10	Программная реализация алгоритмов асимметричного шифрования и алгоритмов электронной подписью. Эллиптические кривые.
Тема 9. Криптоанализ асимметричных алгоритмов	6	6	2,10	Метод больших и малых шагов, реализация атак на слабые ключи.
Тема 10. Криптографические протоколы	6	6	2,3,10	Реализация протокола Диффи-Хэллмана на эллиптических кривых, протоколы с нулевым разглашением.
Тема 11. Блокчейн-технологии	4	4	2,3	Знакомство с технологией блокчейн.
Итого	**32**	**32**		

4. Самостоятельная работа студентов

Таблица 4.1

№	Виды самостоятельной работы	Ссылки на результаты обучения	Часы на выполнение	Часы на консультации
Семестр: 5				
1	Подготовка к лабораторным занятиям.	1-11	40	0
	Дополнительный самостоятельный разбор материалов, необходимых для выполнения			

	лабораторных работ. https://drive.google.com/drive/folders/19yKeCBej1QCb0OWeRceDb5k6JE3YVSP8			
Семестр: 6				
2	Подготовка к лабораторным занятиям.	1-11	40	0
	Дополнительный самостоятельный разбор материалов, необходимых для выполнения лабораторных работ. https://drive.google.com/drive/folders/19yKeCBej1QCb0OWeRceDb5k6JE3YVSP8			

5. Образовательные технологии

В ходе реализации учебного процесса по дисциплине проводятся лабораторные занятия.

В ходе реализации учебного процесса по дисциплине применяются следующие интерактивные формы организации учебных занятий (таблица 5.1).

Таблица 5.1

1	Портфолио	ОПК-1, ОПК-2, ПКС-2
Формируемые умения: 1.Знать основные особенности современной криптографии. 2.Знать основные задачи, которые решает современная криптография. 3.Знать требования надежности и главные уязвимые компоненты криптографических примитивов в зависимости от их назначения. 4.Владеть основными алгоритмами криптоанализа криптографических примитивов в зависимости от их назначения. 5.Уметь применять общий алгоритм для конкретного примитива. 6.Знать основные статистические тесты. 7.Уметь применять существующие реализации тестов на практике. 8.Уметь делать выводы о надежности шифрования по результатам статистического тестирования. 9.Уметь делать эффективные программные реализации примитивов симметричной криптографии на языке высокого уровня. 10.Уметь делать эффективные программные реализации примитивов криптографии с открытым ключом. 11.Уметь эффективно реализовывать основные алгоритмы криптоанализа на языке высокого уровня		
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

Информирование	n.kolomeets@g.nsu.ru
Консультирование	n.kolomeets@g.nsu.ru
Контроль	n.kolomeets@g.nsu.ru
Размещение учебных материалов	https://crypto.nsu.ru https://drive.google.com/drive/folders/19yKeCBej1QCb0OWeRceDb5k6JE3YVSP8

6. Правила аттестации студентов по учебной дисциплине

По дисциплине «Криптографические проекты» проводится текущая и промежуточная аттестация (итоговая по дисциплине).

Текущий контроль осуществляется во время лабораторных занятий по количеству выполненных и защищенных лабораторных работ.

Промежуточная аттестация проводится по завершению каждого периода ее освоения (семестра). Оценка за освоение дисциплины выставляется по результатам оценивания портфолио работ студента, которое включает выполненные и защищенные лабораторные работы.

Результаты промежуточной аттестации по дисциплине оцениваются по шкале «неудовлетворительно», «удовлетворительно», «хорошо», «отлично». Оценки «отлично», «хорошо», «удовлетворительно» означают успешное прохождение промежуточной аттестации.

Оценка «отлично» соответствует 80% и более выполненным и защищенным лабораторным работам.

Оценка «хорошо» соответствует от 65% до 80% (не включительно) выполненным и защищенным лабораторным работам.

Оценка «удовлетворительно» соответствует от 50% до 65% (не включительно) выполненным и защищенным лабораторным работам.

Оценка «неудовлетворительно» соответствует менее 50% выполненным и защищенным лабораторным работам.

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

Таблица 6.1

Коды компетенций	**Результаты обучения**	**Формы аттестации**	
		Семестр 5	**Семестр 6**
		диф. зачет	диф. зачет
		портфолио	портфолио
ОПК.1	**ОПК-1.1** Знать: основы математики, физики, вычислительной техники и программирования	+	+
ОПК.1	**ОПК-1.2** Уметь: решать стандартные профессиональные задачи с применением естественнонаучных и общеинженерных знаний, методов математического анализа и моделирования.	+	+
ОПК.1	**ОПК-1.3** Владеть: навыками теоретического и экспериментального исследования объектов профессиональной деятельности	+	+
ОПК.2	**ОПК-2.3** Владеть: навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности	+	+
ПКС.2	**ПКС-2.1** Владеть: навыками разработки программ на языках высокого уровня	+	+

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 Н.Н. Симметричная криптография: краткий курс. Учебное пособие. М-во образования и науки РФ, Новосиб гос. ун-т, Мех.-мат. фак., Каф. теорет. кибернетики. Новосибирск, 2012. 234 с. http://e-lib.nsu.ru/dsweb/Get/Resource-1222/page001.pdf

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 и электронную почту.

Таблица 8.1

№ п/п	Наименование Интернет-ресурса	Краткое описание
1	Handbook of Applied Cryptography[Электронный ресурс]. – Режим доступа: https://cacr.uwaterloo.ca/hac/ . – Загл. с экрана	Главы книги Handbook of Applied Cryptography
2	Bit Hacks [Электронный ресурс]. – Режим доступа: https://graphics.stanford.edu/~seander/bithacks.html . – Загл. с экрана	Реализация функций с помощью битовых операций

9. Учебно-методическое и программное обеспечение дисциплины

9.1. Перечень учебно-методических материалов по самостоятельной работе обучающихся

Для обеспечения самостоятельной работы обучающихся при изучении дисциплины используются методические рекомендаций по подготовке и выполнению лабораторных работ.
https://drive.google.com/drive/folders/19yKeCBej1QCb0OWeRceDb5k6JE3YVSP8

Описание основ симметричной криптографии, некоторых современных шифров и методов криптоанализа, а также информацию по истории криптографии и древним шифрам можно найти в пособии
Токарева Н.Н. Симметричная криптография: краткий курс. Учебное пособие. М-во образования и науки РФ, Новосиб гос. ун-т, Мех.-мат. фак., Каф. теорет. кибернетики. Новосибирск, 2012. 234 с. http://e-lib.nsu.ru/dsweb/Get/Resource-1222/page001.pdf

Методические рекомендаций по подготовке и выполнению лабораторных работ.

Процесс подготовки лабораторной работы выглядит следующим образом.

1. Каждое занятие в терминальном классе посвящено одной из лабораторных работ. На нем излагается необходимая для выполнения работы теория и обговариваются сложности, которые могут возникнуть в ходе выполнения работы. На занятии можно проконсультироваться с преподавателем по поводу неясных студенту деталей работы.
2. Описание лабораторной работы и необходимые для её выполнения материалы (описание алгоритмов, использующийся математический аппарат, криптографические термины и теория) доступны по ссылке в методических материалах.
3. Лабораторная работа может быть реализована на любом языке программирования, но наиболее подходящие языки могут разниться в зависимости от работы. Например, удобно использовать Python для лабораторных, в которых используется длинная арифметика, но не требуется производительность.
4. По лабораторной работе необходимо написать отчет и отправить его преподавателю. В отчете должна содержаться информация о лабораторной работе и об особенностях ее реализации, ссылка на код (если лабораторная работа сдается очно на занятии, то ссылка не обязательна), инструкция, позволяющая провести тестирование работы, временная сложность (в зависимости от конкретной работы, это может быть теоретическая оценка сложности алгоритма или время выполнения на какой-либо машине при входных данных некоторой длины).
5. При защите лабораторной студент должен рассказать о проделанной работе и ответить на вопросы, касающиеся смысла работы, минимальной необходимой теории, а также на вопросы по коду. Преподаватель также может попросить внести небольшие изменения в код.

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 Professional 2019	Среда разработки приложений

10. Профессиональные базы данных и информационные справочные системы

1. Полнотекстовые журналы Springer Journals, электронные книги, коллекция научных биомедицинских и биологических протоколов SpringerProtocols, коллекция научных материалов в области физических наук и инжиниринга SpringerMaterials, реферативная БД по чистой и прикладной математике zbMATH.
2. Электронные ресурсы Web of Science Core Collection (Thomson Reuters Scientific LLC.), Journal Citation Reports + ESI
3. БД Scopus (Elsevier)
4. Лицензионные материалы на сайте eLibrary.ru

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.

Таблица 11.1

№	Наименование	Назначение
1	Компьютерный класс (с выходом в Internet)	Для организации лабораторных занятий и 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».

Лист актуализации рабочей программы дисциплины
«Криптографические проекты»

№	Характеристика внесенных изменений (с указанием пунктов документа)	Дата и № протокола Ученого совета ФИТ	Подпись ответственного

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
«26» апреля 2021 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ
по дисциплине «Криптографические проекты»

Направление подготовки: 09.03.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА

Направленность (профиль): Программная инженерия и компьютерные науки

Квалификация: бакалавр

Форма обучения: очная Год обучения: 3, семестр 5, 6

Форма аттестации	Семестр
Дифференцированный зачет	5
Дифференцированный зачет	6

Новосибирск 2021

Фонд оценочных средств промежуточной аттестации по дисциплине является **Приложением 1** к рабочей программе дисциплины «**Криптографические проекты**», реализуемой в рамках образовательной программы высшего образования – программы бакалавриата 09.03.01 Информатика и вычислительная техника, направленность (профиль): Программная инженерия и компьютерные науки.

Фонд оценочных средств промежуточной аттестации по дисциплине утвержден решением ученого совета факультета информационных технологий, протокол № 80 от 26.04.2021.

Разработчики:

доцент кафедры компьютерных систем ФИТ
кандидат физико-математических наук — Н.Н. Токарева

ассистент кафедры теоретической кибернетики ММФ,
кандидат физико-математических наук — Н.А.Коломеец

ассистент кафедры систем информатики ФИТ — Д.О.Кондырев

преподаватель кафедры фундаментальной и
прикладной лингвистики ГИ — Ю.П.Максимлюк

Заведующий кафедрой компьютерных систем ФИТ,
кандидат технических наук — Б.Н.Пищик

Ответственный за образовательную программу:

доцент кафедры систем информатики ФИТ,
кандидат технических наук — А.А. Романенко

1. Содержание и порядок проведения промежуточной аттестации по дисциплине

1.1. Общая характеристика содержания промежуточной аттестации

Промежуточная аттестация по дисциплине «**Криптографические проекты**» проводится по завершению периода освоения образовательной программы (семестра) для оценки сформированности компетенций в части следующих индикаторов достижения компетенции (таблица П1.1).

Таблица П1.1

Код	Компетенции, формируемые в рамках модуля «Криптографические проекты»	Семестр 5	Семестр 6
		Диф.зачет	Диф.зачет
		портфолио	портфолио
	ОПК-1 Способен применять естественнонаучные и общеинженерные знания, методы математического анализа и моделирования, теоретического и экспериментального исследования в профессиональной деятельности		
ОПК-1.1	**ОПК-1.1** Знать: основы математики, физики, вычислительной техники и программирования	+	+
ОПК-1.2	**ОПК-1.2** Уметь: решать стандартные профессиональные задачи с применением естественнонаучных и общеинженерных знаний, методов математического анализа и моделирования	+	+
ОПК-1.3	**ОПК-1.3** Владеть: навыками теоретического и экспериментального исследования объектов профессиональной деятельности	+	+
	ОПК-2 Способен использовать современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности		
ОПК-2.3	**ОПК-2.3** Владеть: навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности	+	+
	ПКС-2 Способен разрабатывать компоненты системных программных продуктов		
ПКС-2.1	**ПКС-2.1** Владеть: навыками разработки программ на языках высокого уровня	+	+

Все компетенции, формируемые в рамках дисциплины, оцениваются через портфолио, которое включает выполненные и защищенные в течение семестра лабораторные работы.

1.2. Порядок проведения промежуточной аттестации по дисциплине

Промежуточная аттестация в 5-ом и 6-ом семестрах проводится в форме **дифференцированного зачета.**

Оценка за освоение дисциплины выставляется по результатам оценивания портфолио работ студента, которое включает выполненные и защищенные лабораторные работы.

Оценка «отлично» соответствует 80% и более выполненным и защищенным лабораторным работам.

Оценка «хорошо» соответствует от 65% до 80% (не включительно) выполненным и защищенным лабораторным работам.

Оценка «удовлетворительно» соответствует от 50% до 65% (не включительно) выполненным и защищенным лабораторным работам.

Оценка «неудовлетворительно» соответствует менее 50% выполненным и защищенным лабораторным работам.

Во время сдачи лабораторной работы студентам также необходимо продемонстрировать владение необходимой теорией.

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
Семестр 5			
Дифференцированный зачет			
1	Портфолио	Целевая подборка работ студента, раскрывающая его индивидуальные образовательные достижения в одной или нескольких учебных дисциплинах.	Структура портфолио
Семестр 6			
Дифференцированный зачет			
1	Портфолио	Целевая подборка работ студента, раскрывающая его индивидуальные образовательные достижения в одной или нескольких учебных дисциплинах.	Структура портфолио

2.1 Требования к структуре и содержанию оценочных средств аттестации

2.1.1 Требования к структуре и содержанию портфолио (5 семестр)

Портфолио должно содержать результаты выполненных лабораторных работ по следующим темам:

1. Реализация определения длины ключа в шифре Виженера.
2. Реализация определения ключа в шифре Виженера.
3. Реализация алгоритма нахождение ключевой подстановки при использовании перестановочного шифра.
4. Реализация шифрования с помощью таких алгоритмов, как AES, Kuznechik, MAGMA, Present, Simon, SHA-3, SHA-2, Stribog, Salsa20, A5/1, Grain.
5. Использование статистических тестов для анализа выхода блочных шифров, поточных шифров, хэш-функций.
6. Реализация метода встречи посередине для подходящего шифра.
7. Реализация алгоритмов линейного и дифференциального криптоанализа.

Пример описания лабораторной работы.

Реализуйте игрушечный блочный шифр E с длиной ключа 20 бит, за основу можно взять либо один из уже реализованных в рамках курса стандартных шифров (с поправкой на длину ключа), либо реализовать новый на основе сети Фейстеля или SP-сети.

Реализуйте надстройку над шифром E’(k1, k2, x) = E(k2, E(k1, x)), где новый ключ k = (k1, k2) имеет длину 40 бит (k1 и k2 по 20 бит).

На некотором выбранном ключе сгенерируйте множество пар (открытый текст, шифртекст), нужно шифровать ровно один блок данных для каждой пары.

Реализуйте метод встречи посередине для шифра E’, и по сгенерированным парам определите секретный ключ, который использовался при шифровании.

2.1.2 Требования к структуре и содержанию портфолио (6 семестр)
Портфолио должно содержать результаты выполненных лабораторных работ по следующим темам:

1. Реализация простейшего алгебраического криптоанализа для подходящего шифра.
2. Нахождение коллизий подходящей хэш-функции с помощью парадокса дней рождений.
3. Поиск коллизий хэш-функции с определенной структурой.
4. Реализация операций на эллиптической кривой.
5. Реализация шифрования с помощью алгоритма RSA.
6. Реализация одного из алгоритмов электронной подписи.
7. Реализация протокола Диффи-Хэллмана на эллиптических кривых.
8. Реализация атак на слабые ключи для RSA.
9. Реализация протоколов с нулевым разглашением.

Пример описания лабораторной работы.
Реализуйте операции с точками на эллиптической кривой по простому модулю, которая задана в форме Вейерштрасса с ненулевым дискриминантом. В частности, нужно реализовать сложение двух точек, отрицание точки и умножение точки на целое число.

Напишите программу, которая по заданной кривой, открытому ключу первого абонента и секретному ключу второго абонента с помощью протокола Диффи-Хэллмана на эллиптических кривых устанавливает общий секретный ключ пары. Все данные должны задаваться через файлы.

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

Таблица П1.3

Шифр компетенций	**Структурные элементы оценочных средств**	**Показатель сформированности**	**Не сформирован (2 балла)**	**Пороговый уровень (3 балла)**	**Базовый уровень (4 балла)**	**Продвинутый (5 баллов)**
ОПК-1	Портфолио	**ОПК-1.1** Знать: основы математики, физики, вычислительной техники и программирования.	Знания основных разделов современной криптографии отсутствуют или носят поверхностный характер; студент слабо ориентируется в базовых понятиях, допускает грубые ошибки.	Знания основных разделов современной криптографии присутствуют, но содержат отдельные пробелы; студент в целом ориентируется в базовых объектах дисциплины.	Знания основных разделов современной криптографии присутствуют, студент в целом владеет материалом курса, ответ содержит отдельные недочеты.	Знания основных разделов современной криптографии присутствуют, студент в полной мере владеет материалом курса.
ОПК-1	Портфолио	**ОПК-1.2** Уметь: решать стандартные профессиональные задачи с применением естественнонаучных и общеинженерных знаний, методов математического анализа и моделирования.	Умение выбирать правильные методы анализа современных криптографических примитивов отсутствует или носит фрагментарный характер; студент допускает грубые ошибки.	Умение выбирать правильные методы анализа современных криптографических примитивов присутствует, но содержит пробелы; студент испытывает затруднения при его применении, допускает ошибки, нуждается в	Умение выбирать правильные методы анализа современных криптографических примитивов в целом сформировано; студент в состоянии его применять к указанным объектам, ответ содержит	Умение выбирать правильные методы анализа современных криптографических примитивов сформировано, студент в состоянии успешно его применять

				подсказках.	отдельные недочеты.	
ОПК-1	Портфолио	**ОПК-1.3** Владеть: навыками теоретического и экспериментального исследования объектов профессиональной деятельности.	Умение применять основные методы криптоанализа современных криптографических примитивов отсутствует или носит фрагментарный характер; студент допускает грубые ошибки.	Умение применять основные методы криптоанализа современных криптографических примитивов присутствует, но содержит пробелы; студент испытывает затруднения при его применении, допускает ошибки, нуждается в подсказках.	Умение применять основные методы криптоанализа современных криптографических примитивов в целом сформировано; студент в состоянии его применять к указанным объектам, ответ содержит отдельные недочеты.	Умение применять основные методы криптоанализа современных криптографических примитивов сформировано, студент в состоянии успешно его применять
ОПК-2	Портфолио	**ОПК-2.3** Владеть: навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности.	Умение применять существующие программные методы анализа качества шифрования отсутствует или носит фрагментарный характер; студент допускает грубые ошибки.	Умение применять существующие программные методы анализа качества шифрования присутствует, но содержит пробелы; студент испытывает затруднения при его применении, допускает ошибки, нуждается в подсказках.	Умение применять существующие программные методы анализа качества шифрования в целом сформировано; студент в состоянии его применять к указанным объектам, ответ содержит отдельные	Умение применять существующие программные методы анализа качества шифрования сформировано, студент в состоянии успешно его применять

					недочеты.	
ПКС-2	Портфолио	**ПКС-2.1** Владеть: навыками разработки программ на языках высокого уровня.	Владение навыками реализации алгоритмов шифрования и криптоанализа на языке высокого уровня отсутствует или носит фрагментарный характер; студент допускает грубые ошибки.	Владение навыками реализации алгоритмов шифрования и криптоанализа на языке высокого уровня присутствует, но содержит пробелы; студент испытывает затруднения при их применении, допускает ошибки, нуждается в подсказках.	Владение навыками реализации алгоритмов шифрования и криптоанализа на языке высокого уровня в целом сформировано; студент в состоянии их применять к указанным объектам, ответ содержит отдельные недочеты.	Владение навыками реализации алгоритмов шифрования и криптоанализа на языке высокого уровня сформировано, студент в состоянии успешно их применять

4. Критерии выставления оценок по результатам промежуточной аттестации по дисциплине

В 5 и 6 семестрах результаты промежуточной аттестации определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Оценки «отлично», «хорошо», «удовлетворительно» означают успешное прохождение промежуточной аттестации.

Оценка «отлично» выставляется, если 80% и более лабораторных работ выполнены и защищены. Оценка «отлично» соответствует продвинутому уровню сформированности компетенции.

Оценка «хорошо» выставляется, если от 65% до 80% (не включительно) лабораторных работ выполнены и защищены. Оценка «хорошо» соответствует базовому уровню сформированности компетенции.

Оценка «удовлетворительно» выставляется, если от 50% до 65% (не включительно) лабораторных работ выполнены и защищены. Оценка «удовлетворительно» соответствует пороговому уровню сформированности компетенции.

Оценка «неудовлетворительно» выставляется, если хотя бы одна компетенция не сформирована, менее 50% лабораторных работ выполнены и защищены.

Оценка в 6 семестре является итоговой по дисциплине.

Лист актуализации фонда оценочных средств промежуточной аттестации
по дисциплине
«Криптографические проекты»

№	Характеристика внесенных изменений (с указанием пунктов документа)	Дата и № протокола Ученого совета ФИТ	Подпись ответственного