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

Криптография и криптоанализ

Направление подготовки: 09.06.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА
Направленность (профиль): Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей

Форма обучения: очная
Год обучения: 2, семестр: 3,4

№	Вид деятельности	Семестр 3	Семестр 4
1	Лекции, час.		
2	Практические занятия, час.	32	32
3	Лабораторные занятия, час.		
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.		
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	З	З
12	Всего зачетных единиц[1]	2	2

Новосибирск 2021

[1] С учетом выделенных часов на промежуточную аттестацию

Рабочая программа составлена на основании образовательного стандарта высшего образования по направлению подготовки научно-педагогических кадров в аспирантуре 09.06.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА, самостоятельно устанавливаемого НГУ (СУОС).

Федеральный государственный образовательный стандарт (ФГОС) высшего образования по направлению подготовки научно-педагогических кадров в аспирантуре 09.06.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА введен в действие приказом Минобнауки № 875 от 30.07.2014 (в ред. приказа Минобрнауки России от 30.04.2015 № 464).

СУОС утвержден решением Ученого совета НГУ от 06.07.2015, протокол № 3 (273) (редакция 2).

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 № 80.

Программу разработал:

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

ассистент кафедры теоретической кибернетики ММФ А.В. Куценко

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

Ответственный за образовательную программу:

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

Аннотация к рабочей программе дисциплины
«Криптография и криптоанализ»

Дисциплина «Криптография и криптоанализ» реализуется в рамках основной профессиональной образовательной программы (ОПОП) высшего образования – программы подготовки научно-педагогических кадров в аспирантуре по направлению подготовки 09.06.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА, направленность (профиль): МАТЕМАТИЧЕСКОЕ И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ВЫЧИСЛИТЕЛЬНЫХ МАШИН, КОМПЛЕКСОВ И КОМПЬЮТЕРНЫХ СЕТЕЙ по очной форме обучения на русском языке.

Место в образовательной программе: знания, умения и навыки, сформированные у обучающихся по результатам изучения дисциплины «Криптография и криптоанализ», могут быть использованы для дальнейшей научно-исследовательской деятельности и подготовки научно-квалификационной работы (диссертации).

Дисциплина «Криптография и криптоанализ» реализуется в 3, 4 семестрах в рамках Блока ФТД Факультативы и является факультативной дисциплиной.

Дисциплина «Криптография и криптоанализ» направлена на формирование следующих компетенций:
ОПК-5. Способностью объективно оценивать результаты исследований и разработок, выполненных другими специалистами и в других научных учреждениях:

- ОПК-5.1. Уметь: проводить сравнительный анализ современных достижений в области профессиональной деятельности, в том числе и в междисциплинарных областях.

Основная цель факультатива – познакомить слушателей с последними научными результатами в области криптографии, в частности – в области математических методов криптографии, выработка у студентов навыков и компетенций, необходимых при проведении научно-исследовательской деятельности, представления результатов собственных научных изысканий. Рассматриваются задачи, связанные с построением криптографических булевых функций, стойких блочных и поточных шифров, схем разделения секрета, а также методы их анализа. Факультатив предполагает активное участие студентов в подготовке докладов и реферировании статей. Кроме того, к проведению факультатива подключаются работающие в области криптографии специалисты, с которыми удается достичь договоренности о выступлении. Так, в разное время на факультативе выступали ученые из России (Иркутск, Омск), США (Нью-Йорк), Норвегии (Берген) и др.

Тематика дисциплины включает в себя широкий спектр задач, связанных с построением криптографических булевых функций, стойких блочных и поточных шифров, схем разделения секрета, а также методами их анализа, в том числе:

- задачи построения криптографических булевых функций,
- задачи построения стойких блочных и поточных шифров,
- задачи криптоанализа симметричных криптосистем,
- задачи криптоанализа асимметричных криптосистем,
- задачи анализа протоколов постквантовой криптографии и т.д.

При освоении дисциплины студенты выполняют следующие виды учебной работы: практические занятия, самостоятельная работа. Самостоятельная работа включает:

самостоятельное изучение публикаций по тематике факультатива, подготовку презентаций докладов.

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

Правила аттестации по дисциплине.
Аттестация по дисциплине «Криптография и криптоанализ» проводится по завершению каждого периода ее освоения (семестра) в форме зачета. По результатам аттестации за освоение дисциплины выставляется оценка «зачтено» или «не зачтено». Оценка «зачтено» выставляется при условии наличия выступления с устным докладом на выбранную тематику, а также систематического посещения занятий в ходе периода ее освоения.

Учебно-методическое обеспечение дисциплины.
Учебно-методическое обеспечение дисциплины представлено в рабочей программе дисциплины в виде методических рекомендаций по подготовке докладов.

1. Внешние требования к дисциплине

Таблица 1.1

Компетенция ОПК-5 Способностью объективно оценивать результаты исследований и разработок, выполненных другими специалистами и в других научных учреждениях, *в части следующих индикаторов достижения компетенции:*
ОПК-5.1 Уметь: проводить сравнительный анализ современных достижений в области профессиональной деятельности, в том числе и в междисциплинарных областях.

2. Требования к результатам освоения

Таблица 2.1

Результаты изучения дисциплины по уровням освоения (иметь представление, знать, уметь, владеть)	**Формы организации занятий**	
	Практические занятия	**Самостоятельная работа**
ОПК-5.1 Уметь: проводить сравнительный анализ современных достижений в области профессиональной деятельности, в том числе и в междисциплинарных областях.		
1. Уметь проводить анализ современных научных результатов в области криптографии и криптоанализа.	+	+

3. Содержание и структура учебной дисциплины

Таблица 3.1

Темы практических занятий	**Активные формы, час.**	**Часы**	**Ссылки на результаты обучения**	**Учебная деятельность**
Семестр: 1				
Тема. Современные результаты в области криптографии и криптоанализа	32	32	1	Участие в работе научного семинара, в том числе представление собственных результатов и рефератов статей по тематике семинара.
Итого	**32**	**32**		
Семестр: 2				
Тема. Современные результаты в области криптографии и криптоанализа	32	32	1	Участие в работе научного семинара, в том числе представление собственных результатов и рефератов статей по тематике семинара.
Итого	**32**	**32**		

4. Самостоятельная работа обучающихся

Таблица 4.1

№	**Виды самостоятельной работы**	**Ссылки на результаты обучения**	**Часы на выполнение**	**Часы на консультации**
Семестр: 1				
1	Подготовка к выступлению с	1	40	-

	докладом.			
	Обучающийся самостоятельно выбирает тему доклада, согласует ее с преподавателем. Знакомится с необходимой литературой по выбранной тематике, формулирует постановку рассматриваемой задачи, анализирует результаты, полученные в рассматриваемой тематике. Для удобства при проведении доклада оформляется презентация. Методические рекомендации по подготовке докладов представлены в рабочей программе дисциплины.			
Семестр: 2				
1	Подготовка к выступлению с докладом.	1	40	-
	Обучающийся самостоятельно выбирает тему доклада, согласует ее с преподавателем. Знакомится с необходимой литературой по выбранной тематике, формулирует постановку рассматриваемой задачи, анализирует результаты, полученные в рассматриваемой тематике. Для удобства при проведении доклада оформляется презентация. Методические рекомендации по подготовке докладов представлены в рабочей программе дисциплины.			

5. Образовательные технологии

Реализация учебного процесса по дисциплине осуществляется в форме научного семинара, в ходе которого применяются такие формы организации занятий, как дискуссия, обсуждение новых результатов, а также используются следующие интерактивные формы организации учебного процесса (таблица 5.1).

Таблица 5.1

1	Междисциплинарное обучение	ОПК-5.1
Формируемые умения: 1. Уметь проводить анализ современных научных результатов в области криптографии и криптоанализа.		
Краткое описание применения: использование знаний из разных областей, их группировка и концентрация в контексте решаемой задачи.		

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

Таблица 5.2

Информирование	https://crypto.nsu.ru/ru/news/
Консультирование	tokareva@math.nsc.ru a.kutsenko@g.nsu.ru

6. Правила аттестации обучающихся по учебной дисциплине

По дисциплине «Криптография и криптоанализ» проводится текущая и промежуточная аттестация (итоговая по дисциплине).

Текущая аттестация по дисциплине проводится на практических занятиях и заключается в представлении устного доклада на выбранную тематику с учётом систематического посещения занятий в ходе периода освоения дисциплины и регулярного участия в обсуждении представленных докладов. Для представления доклада, как правило, дается около 45 минут, затем следует обсуждение с остальными участниками факультатива.

Промежуточная аттестация (итоговая по дисциплине) проводится по завершению каждого периода ее освоения (семестра) в форме зачета.

Зачёт проводится по результатам оценивания портфолио, которое включает:

1. Посещение обучающимся не менее 50% семинаров.
2. Регулярное участие в обсуждении представленных докладов.
3. Представление одного или нескольких докладов в течение семестра.

По результатам освоения дисциплины «Криптография и криптоанализ» выставляется оценка «зачтено» или «не зачтено». Оценка «зачтено» означает успешное прохождение дисциплины.

Для получения оценки «зачтено» в каждом семестре портфолио должно быть выполнено в полном соответствии с предъявляемыми требованиями.

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

Таблица 6.1

Коды компетенций ФГОС	**Результаты обучения**	**Форма аттестации**	
		Семестр 3	**Семестр 4**
		Зачет	**Зачет**
		Портфолио	**Портфолио**
ОПК.5	**ОПК-5.1** Уметь: проводить сравнительный анализ современных достижений в области профессиональной деятельности, в том числе и в междисциплинарных областях	+	+

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
2. Васильева, Мария Александровна (лингвист (англ. яз.)). Обучение реферированию научной литературы / М.А. Васильева, Е.И. Закгейм. М. : Изд-во МГУ, 1976. 260 с.

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, электронную почту.

Таблица 8.1

№ п/п	Наименование Интернет-ресурса	Краткое описание

1	Журнал «Вестник НГУ. Серия: Информационные технологии» [Электронный ресурс]. – Режим доступа: https://journals.nsu.ru/jit/ . – Загл. с экрана	Полнотекстовые электронные копии статей в области вычислительный методов (с 2006 года).
2	Курс «Cryptography: Boolean functions and related problems» на платформе Coursera от НГУ. – Режим доступа: https://www.coursera.org/learn/cryptography-boolean-functions	Электронный курс от НГУ на платформе Coursera. Курс посвящён изложению основных известных результатов касательно использования булевых функций в криптографии.
3	Сайт Криптографического Центра (Новосибирск) https://crypto.nsu.ru/ru/	Сайт содержит материалы, посвященные криптографическим курсам и семинарам, научным исследованиям в области криптографии и др.

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 рекомендации по подготовке докладов.

Методические рекомендации по подготовке докладов.

Обучающийся самостоятельно выбирает тему доклада, с которым будет выступать на научном семинаре, согласует ее с преподавателем. Темы семинаров никогда не повторяются. Доклад должен быть о новых результатах в области криптографии.

Перечень тем докладов, представленных за время существования научного семинара, размещён на сайтах:

- http://math.nsc.ru/seminar/all.html;
- http://crypto.nsu.ru/ru/courses/course/(%3FP3%5B0-9%5D+)/.

Тему доклада необходимо выбрать и согласовать с преподавателем в начале семестра. После согласования темы преподаватель включает доклад в расписание проведения научного семинара, а обучающийся приступает к подготовке доклада. Каждый обучающийся в течение семестра готовит и представляет один или несколько докладов. Доклад может быть посвящён изложению научных результатов, полученных обучающимся лично, при соответствии темы исследований обучающегося тематике семинара.

Подготовка доклада должна начинаться со знакомства с необходимой литературой по выбранной тематике. Далее обучающийся формулирует постановку рассматриваемой задачи, анализирует известные или полученные им лично результаты в рамках рассматриваемой тематики, делает вывод о современном состоянии рассматриваемой области. Также в рамках доклада необходимо отметить возможное междисциплинарное взаимодействие, прямое или косвенное влияние представленных результатов на положение дел в смежных областях. В докладе должны быть отражены актуальные нерешённые проблемы и открытые вопросы из соответствующей области.

Доклад представляется в устной форме на научном семинаре в соответствии с расписанием представления докладов. Для удобства участников научного семинара доклад сопровождается компьютерной презентацией. Доклад

представляется на русском языке (по согласованию с преподавателем факультатива допускается представление доклада на иностранном языке).

При подготовке реферата научной публикации необходимо учитывать требования к его содержанию. Слайды презентации должны содержать:

1. информацию об авторах работы, выходных данных реферируемых публикаций (при наличии);
2. формулировки целей и задач исследования (реферируемой работы);
3. краткое описание известных результатов по тематике исследований (реферируемой работы);
4. перечень основных докладываемых результатов;
5. текст доклада, включающий доказательства (схемы доказательства), описание применяемых методов исследований.

Для представления доклада, как правило, дается около 45 минут, затем следует обсуждение изложенного материала с остальными участниками факультатива.

9.2. Программное обеспечение

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

Специализированное программное обеспечение для изучения дисциплины не требуется.

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. Электронная библиотека диссертаций Российской государственной библиотеки (ЭБД РГБ)
3. Полнотекстовые электронные ресурсы Freedom Collection издательства Elsevier (Нидерланды) (предметные коллекции Discrete Mathematics, Discrete Applied Mathematics)
4. Электронные ресурсы Web of Science Core Collection (Thomson Reuters Scientific LLC.), Journal Citation Reports + ESI
5. Электронные БД JSTOR (США). Предметная коллекция: Mathematics & Statistics
6. БД Scopus (Elsevier)
7. Лицензионные материалы на сайте eLibrary.ru
8. Правовая БД «Консультант Плюс»
9. Правовая БД «Гарант»

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	Презентационное оборудование (мультимедиа-проектор, экран, компьютер для управления)	Для проведения 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».

Лист актуализации рабочей программы дисциплины
«Криптография и криптоанализ»

№	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 «Криптография и криптоанализ»

Направление подготовки: 09.06.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА

Направленность (профиль): Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей
Квалификация: Исследователь. Преподаватель-исследователь.

Форма обучения: очная Год обучения: 2, семестр 3, 4

Форма аттестации	Семестр
Зачет	3
Зачет	4

Новосибирск 2021

Фонд оценочных средств промежуточной аттестации по дисциплине является **Приложением 1** к рабочей программе дисциплины «Криптография и криптоанализ», реализуемой в рамках образовательной программы высшего образования – программы подготовки научно-педагогических кадров в аспирантуре по направлению 09.06.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА, направленность (профиль): МАТЕМАТИЧЕСКОЕ И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ВЫЧИСЛИТЕЛЬНЫХ МАШИН, КОМПЛЕКСОВ И КОМПЬЮТЕРНЫХ СЕТЕЙ.

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 А.В. Куценко

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

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 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

Код	Компетенции, формируемые в рамках дисциплины «Криптография и криптоанализ»	Семестр 3	Семестр 4
		зачёт	зачёт
		портфолио	портфолио
	ОПК-5 Способностью объективно оценивать результаты исследований и разработок, выполненных другими специалистами и в других научных учреждениях		
ОПК-5.1	Уметь: проводить сравнительный анализ современных достижений в области профессиональной деятельности, в том числе и в междисциплинарных областях	+	+

Компетенции, формируемые в рамках дисциплины, оцениваются через портфолио, в которое входят работы, выполненные на протяжении каждого семестра.

1.2. Порядок проведения промежуточной аттестации по дисциплине

Промежуточная аттестация по дисциплине «Криптография и криптоанализ» проводится по завершению каждого периода ее освоения (семестра) в форме зачёта. Зачёт проводится по результатам оценивания портфолио, которое включает:

1. Посещение обучающимся не менее 50% семинаров.
2. Регулярное участие в обсуждении представленных докладов.
3. Представление одного или нескольких докладов в течение семестра.

По результатам освоения дисциплины «Криптография и криптоанализ» выставляется оценка «зачтено» или «не зачтено». Оценка «зачтено» означает успешное прохождение дисциплины.

Для получения оценки «зачтено» в каждом семестре портфолио должно быть выполнено в полном соответствии с предъявляемыми требованиями.

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 3,4			
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 Описание оценочного средства - портфолио.

Портфолио в 3 и 4 семестрах должно содержать:

1. Посещение обучающимся не менее 50% семинаров.
2. Регулярное участие в обсуждении представленных докладов.
3. Представление одного или нескольких докладов в течение семестра в соответствии с предъявляемыми требованиями.

Требования к структуре и содержанию доклада.

Доклад должен быть выполнен по теме, выбранной обучающимся самостоятельно и согласованной с преподавателем.

Доклад представляется в устной форме на научном семинаре в соответствии с расписанием представления докладов. Доклад сопровождается компьютерной презентацией, представляется на русском языке (по согласованию с преподавателем факультатива допускается представление доклада на иностранном языке).

Доклад должен содержать:

1. информацию об авторах работы, выходных данных реферируемых публикаций (при наличии);
2. формулировки целей и задач исследования (реферируемой работы);
3. краткое описание известных результатов по тематике исследований (реферируемой работы);
4. перечень основных докладываемых результатов;
5. текст доклада, включающий доказательства (схемы доказательства), описание применяемых методов исследований.

Слайды презентации должны отражать структуру и содержание доклада.

Для представления доклада, как правило, дается около 45 минут, затем следует обсуждение с остальными участниками факультатива.

Примеры тем докладов

Тема 1. Обзор методов криптоанализа по сторонним каналам.
Тема 2. Алгебраический криптоанализ шифров: перспективы.
Тема 3. Максимально-нелинейные булевы функции: открытые проблемы.
Тема 5. Криптоанализ шифра AES. Обзор результатов.
Тема 6. Обзор докладов конференции Boolean Functions and Applications (BFA) текущего года.
Тема 7. Современные методы стеганографии.
Тема 8. Обзор развития способов проектирования блочных шифров
Тема 9. Криптография в программных продуктах: PGP, Skype, WhatsApp, Zoom и др.
Тема 10. Дифференциальный (разностный) криптоанализ и его применение на практике.
Тема 11. Современные способы обеспечения информационной безопасности.
Тема 12. Постквантовая криптография: обзор криптосистем, основанных на кодах, исправляющих ошибки.
Тема 13. Технология блокчейн и распределенные реестры: современное состояние.
Тема 14. Квантовый криптоанализ и квантовая криптография: перспективы, последние результаты.
Тема 15. Конкурсы криптографических стандартов: NIST Post Quantum.

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

Таблица П1.3

Шифр компетенций	Структурные элементы оценочных средств	Показатель сформированности	Не сформирован	Пороговый уровень	Базовый уровень	Продвинутый уровень
ОПК-5	Портфолио 3 и 4 семестров	ОПК-5.1 УМЕТЬ: проводить сравнительный анализ современных достижений в области профессиональной деятельности, в том числе и в междисциплинарных областях	Имеет фрагментарное представление о методиках исследования в области профессиональной деятельности	Имеет представление о методиках исследования в области профессиональной деятельности, но затрудняется при проведении их критического анализа	Знает методики исследования в области профессиональной деятельности. Демонстрирует в целом успешные, но содержащее отдельные пробелы навыки критического анализа современных достижений в области профессиональной деятельности	Знает методики исследования в области профессиональной деятельности. Демонстрирует успешные навыки критического анализа современных достижений в области профессиональной деятельности

4. Критерии выставления оценок по результатам промежуточной аттестации по дисциплине

По результатам освоения дисциплины «Криптография и криптоанализ» в 3 и 4 семестрах выставляется оценка «зачтено» или «не зачтено». Оценка «зачтено» выставляется, если обучающийся продемонстрировал сформированность оцениваемых через портфолио компетенций на уровне, не ниже порогового.

Оценка «зачтено» означает успешное освоение дисциплины. Оценка «не зачтено» означает, что дисциплина не освоена и выставляется, если компетенция не сформирована.

Лист актуализации фонда оценочных средств промежуточной аттестации по дисциплине «Криптография и криптоанализ»

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