Министерство науки и высшего образования Российской Федерации
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)

Механико-математический факультет

УТВЕРЖДАЮ:
Декан
_____ Л. В.Гензе
«30» 06 2022 г.

Рабочая программа дисциплины

Основы криптографии

по направлению подготовки

01.03.01 Математика, 02.03.01 Математика и компьютерные науки

Направленность (профиль) подготовки :
Основы научно-исследовательской деятельности в области математики
Основы научно-исследовательской деятельности в области математики и компьютерных наук

Форма обучения
Очная

Квалификация
Бакалавр

Год приема
2022

Код дисциплины в учебном плане: Б1.В.3.ДВ.02.01

СОГЛАСОВАНО:
Руководитель ОП
_____ Л. В.Гензе

Председатель УМК
_____ Е.А. Тарасов

Томск – 2022

1. Цель и планируемые результаты освоения дисциплины

Целью освоения дисциплины является формирование следующих компетенций:

ОПК-4 Способен проводить под научным руководством исследование на основе существующих методов в конкретной области профессиональной деятельности.

ПК-1 Способен проводить научно-исследовательские разработки по отдельным разделам выбранной темы.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК 4.1 Проводит поиск и обработку научной и научно-технической информации, необходимой для решения исследовательских задач

ИОПК 4.2 Оценивает полученные результаты и формулирует выводы по итогам проведенных исследований

ИПК 1.1 Проводит работы по обработке и анализу научно-технической информации и результатов исследований

ИПК 1.2 Подготавливает планы и программы проведения отдельных этапов научно-исследовательской работы

ИПК 1.3 Проводит отдельные этапы научно-исследовательской работы

2. Задачи освоения дисциплины

– Освоить аппарат теории шифрования данных (ОПК-4, ПК-1).

– Научиться применять понятийный аппарат криптографии для решения практических задач профессиональной деятельности (ИОПК 4.1, ИОПК 4.2, ИПК 1.1, ИПК 1.2, ИПК 1.3).

3. Место дисциплины в структуре образовательной программы

Дисциплина относится к Блоку 1 «Дисциплина (модули)».

Дисциплина относится к части образовательной программы, формируемой участниками образовательных отношений, предлагается обучающимся на выбор.

4. Семестр(ы) освоения и форма(ы) промежуточной аттестации по дисциплине

Седьмой семестр, зачет

5. Входные требования для освоения дисциплины

Для успешного освоения дисциплины требуются результаты обучения по следующим дисциплинам: алгебра, математическая логика, дискретная математика, теория чисел.

6. Язык реализации

Русский

7. Объем дисциплины

Общая трудоемкость дисциплины составляет 2 з.е., 72 часов, из которых:

-практические занятия: 32 ч.

в том числе практическая подготовка: 0 ч.

Объем самостоятельной работы студента определен учебным планом.

8. Содержание дисциплины, структурированное по темам

Тема 1. Математические модели открытых текстов

Детерминированная модель. Вероятностная модель (ИОПК 4.1, ИОПК 4.2, ИПК 1.1, ИПК 1.2, ИПК 1.3).

Тема 2. Исторические шифры

Одноалфавитные шифры замены. Многоалфавитные шифры замены. Шифры сдвига (ИОПК 4.1, ИОПК 4.2, ИПК 1.1, ИПК 1.2, ИПК 1.3).

Тема 3. Надежность шифров

Формальные модели шифров. Математические модели некоторых шифров. Совершенные шифры. Вопросы стойкости шифров (ИОПК 4.1, ИОПК 4.2, ИПК 1.1, ИПК 1.2, ИПК 1.3).

Тема 4. Симметричные шифры

Итеративные блочные шифры. Шифры Фейстеля. Построение раундовой функции. Входное и выходное отображения. Слабые ключи. Режимы использования блочных шифров. ГОСТ Р 34.12-2005. AES (ИОПК 4.1, ИОПК 4.2, ИПК 1.1, ИПК 1.2, ИПК 1.3).

Тема 5. Шифрование с открытым ключом

Основные идеи. Система Диффи-Хэллмана. Протокол Месси-Омуры. Вероятностный шифр Эль-Гамаля. Шифр RSA. Криптосистема Шора-Ривеста. Модификации на эллиптической кривой (ИОПК 4.1, ИОПК 4.2, ИПК 1.1, ИПК 1.2, ИПК 1.3).

Тема 6. Некоммутативная криптография

Предварительные сведения. Задача сопряжения. Задача декомпозиции. Задача факторизации. Протокол Аншеля-Аншеля-Гольдфельда. Возможные группы платформы (ИОПК 4.1, ИОПК 4.2, ИПК 1.1, ИПК 1.2, ИПК 1.3).

9. Текущий контроль по дисциплине

Текущий контроль по дисциплине проводится путем контроля посещаемости и фиксируется в форме контрольной точки не менее одного раза в семестр.

10. Порядок проведения и критерии оценивания промежуточной аттестации

Зачет в седьмом семестре проводится в письменной форме по билетам. Билет содержит два теоретических вопроса. Продолжительность зачета 1,5 часа.

Примерный перечень теоретических вопросов

1. Основные принципы современных симметричных шифров.
2. Вычислительно защищенная криптосистема. Абсолютно защищенная криптосистема.
3. Блочные шифры.
4. Эффективный алгоритм возведения в степень по модулю простого числа p.
5. Компрометация ключа.
6. Односторонние функции.
7. Поточные шифры.
8. Причины ненадежности криптосистем.

Зачет ставится, если студент при ответе на вопросы билета демонстрирует глубокие знания по основам криптографии и наличии удовлетворительной посещаемости.

11. Учебно-методическое обеспечение

а) Электронный учебный курс по дисциплине в электронном университете «Moodle» - https://moodle.tsu.ru/course/view.php?id=10121

б) Оценочные материалы текущего контроля и промежуточной аттестации по дисциплине.

12. Перечень учебной литературы и ресурсов сети Интернет

а) основная литература:

– Рацеев С. М. Математические методы защиты информации: учебное пособие для вузов, СПб. Лань. 2022. 544 с.

– Рацеев С. М. Математические методы защиты информации и их основы. Сборник задач: учебное пособие для вузов. СПб: Лань. 2023. 140 с.

– Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. Изд. 2. Москва. Гелиос АРВ. 2005. 480 с.

б) дополнительная литература:

– Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов М.МЦНМО. 2006. 91 с.

– Group-based cryptography A. Myasnikov, A. Ushakov, V. Shpilran. Birkhauser Basel. 2008. 183 p.

в) ресурсы сети Интернет:

– http://www.coursera.org/ – сайт обучающих курсов ведущих вузов мира

– https://ocw.mit.edu/index.htm – сайт открытых курсов MIT

– журнал «Вестник ТГУ. Математика и механика» http://journals.tsu.ru/mathematics/

13. Перечень информационных технологий

а) лицензионное и свободно распространяемое программное обеспечение:

– Microsoft Office Standart 2013 Russian: пакет программ. Включает приложения: MS Office Word, MS Office Excel, MS Office PowerPoint, MS Office On-eNote, MS Office Publisher, MS Outlook, MS Office Web Apps (Word Excel MS PowerPoint Outlook);

– публично доступные облачные технологии (Google Docs, Яндекс диск и т.п.).

б) информационные справочные системы:

– Электронный каталог Научной библиотеки ТГУ – http://chamo.lib.tsu.ru/search/query?locale=ru&theme=system

– Электронная библиотека (репозиторий) ТГУ – http://vital.lib.tsu.ru/vital/access/manager/Index

14. Материально-техническое обеспечение

Аудитории для проведения занятий лекционного типа.

Аудитории для проведения занятий семинарского типа, индивидуальных и групповых консультаций, текущего контроля и промежуточной аттестации.

Помещения для самостоятельной работы, оснащенные компьютерной техникой и доступом к сети Интернет, в электронную информационно-образовательную среду и к информационным справочным системам.

15. Информация о разработчиках

Норбосамбуев Цырендоржи Дашацыренович, к.ф.-м.н., доцент кафедры алгебры ММФ ТГУ