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
«28» сентября 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ДОКАЗУЕМО «НЕВСКРЫВАЕМЫЕ» КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ

Научная специальность: 2.3.5 Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей
Направленность (профиль): Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей

Форма обучения: очная

Разработчик:
доцент кафедры систем информатики ФИТ,
доктор технических наук Б.Я. Рябко

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

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

Новосибирск 2022

Аннотация к рабочей программе дисциплины
«Доказуемо "невскрываемые" криптографические методы»

Дисциплина «Доказуемо "невскрываемые" криптографические методы**»** реализуется в рамках программы аспирантуры по научной специальности 2.3.5 «Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей» и направленности (профилю): Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей по очной форме обучения на русском языке.

Дисциплина «Доказуемо "невскрываемые" криптографические методы**»** входит в блок элективных дисциплин, реализуемых в рамках программы аспирантуры и направлен на формирование знаний и умений, связанных с возникшим в последнее десятилетие направлением криптографии – энтропийно-стойкими системами, которое уже признано способным радикально изменить эту науку и ее приложения к системам защиты информации. Энтропийно-стойкие системы относятся к той группе методов, надежность которых строго математически доказана, а не опирается на какие-либо недоказанные предположения (такие, как "P не равно NP", "отсутствие алгоритма полиномиальной сложности для задачи факторизации" и т.п.). Интерес к таким методам вызван еще и тем, что они не вскрываемы при любой вычислительной мощности «злоумышленника», включая и гипотетические квантовые компьютеры, появление которых предсказывают многие исследователи в этой области. В курсе дается систематизированное описание энтропийно-стойких методов, базирующееся на теоретико-информационном подходе. Все результаты доказываются и реализуются в виде программ.

Целью курса является освоение основных понятий энтропийно-стойких шифров и других подобных систем, представлять их возможности. Курс интересен аспирантам в силу его большой важности для информатики, т.к. по отзывам специалистов, энтропийно-стойкие шифры станут основным аппаратом криптографической защиты информации.

Перечень основных разделов дисциплины: энтропия и информация, энтропия эргодических процессов и теорема Шеннона-Макмиллана-Бреймана, Шенноновская теория секретных систем, энтропийно-надежные шифры

Общий объем дисциплины – 2 зачетных единицы (72 часа). Из которых лекции составляют 16 часов, практические занятия 16 часов, самостоятельная работа 36 часов, консультации 2 часа.

Правила аттестации по дисциплине. Промежуточная аттестация по дисциплине «Доказуемо "невскрываемые" криптографические методы» проводится в форме дифференцированного зачета.

1. Результаты освоения дисциплины:

- Знакомство с теорией доказуемо стойких методов криптографии, понимание возможностей и пределов их применения.

2. Трудоемкость дисциплины по видам учебной деятельности

Трудоемкость дисциплины – 2 з.е. (72 ч)
Форма промежуточной аттестации: диф.зачет.

№	Вид деятельности	Количество часов
1	Лекции, час.	16
2	Практические занятия, час.	16
3	Лабораторные занятия, час	
4	Занятий в контактной форме без учета промежуточной аттестации, час, из них	34
5	в электронной форме, час.	
6	аудиторных занятий, час.	32
7	из них в активной и интерактивной форме, час.	
8	консультаций, час.	2
9	Самостоятельная работа, час.	36
10	Всего, ч	72

3. Содержание дисциплины

Лекции (16 ч)

Наименование тем и их содержание	Объем час
Основы теории информации	
1. Энтропия и информация	2
2. Энтропия эргодических процессов и теорема Шеннона-Макмиллана-Бреймана	2
Шенноновская теория секретных систем	
3. Шифр Вернама и его обобщения	2
4. Идеальные криптографические системы	2
Энтропийно-надежные шифры	
5. Шифр Рассела и Вонга	2
6. Применение сжатия данных для повышения стойкости шифра	2
7. Повышение стойкости шифра при помощи рандомизации	2
8. Энтропийно-надежные шифры с секретным ключом постоянной длины	2

Практические занятия (16 ч)

Содержание практического занятия	Объем час
1. Основы теории информации	4
2. Шифр Вернама и его обобщения	4
3. Омофонные коды и их использование в криптографии	4
4. Сжатие данных и рандомизация для повышения надежности криптосистем	2
5. Оценивание параметров энтропийно-надежных шифров	2

Самостоятельная работа студентов (36 ч)

Перечень занятий на СР аспиранта	Объем час
1. Энтропия и информация.	8
2. Стационарные и эргодические процессы	6
3. Совершенные секретные системы	8
4. Энтропийно- надежные шифры	6
5. Конструкции энтропийно-надежных шифров с секретным ключом конечной длины	8

4. Перечень учебно-методического обеспечения по самостоятельной работе аспирантов

1. Рябко Б.Я., Фионов А.Н. Криптография в информационном мире., М. «Телеком», 2018 (18 экз.)

5. Перечень учебных изданий, необходимых для освоения дисциплины

2. Ryabko B., Fionov A. Cryptography in the Information Society.- World Scientific Publishing. - 2021. https://www.worldscientific.com/doi/epdf/10.1142/11988

6. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Для реализации дисциплины «Доказуемо «невскрываемые» криптографические методы» 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;

3. Лаборатории;

4. Помещения для хранения и профилактического обслуживания учебного оборудования.

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

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

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

- комплект лекций-презентаций по темам дисциплины;

Материально-техническое обеспечение образовательного процесса по дисциплине для аспирантов 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».

7. Оценочные средства для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

Промежуточная аттестация:

Промежуточная аттестация проводится в виде сдачи дифференцированного зачета.

Дифференцированный зачет проводится в устной форме, по билетам. Билет выбирается обучающимся случайным образом. При подготовке ответа на вопросы билета не разрешается использование каких-либо источников информации. В процессе ответа обучающегося на вопросы билета преподаватель может задавать дополнительные вопросы по темам дисциплины. Результаты промежуточной аттестации определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Оценки «отлично», «хорошо», «удовлетворительно» означают успешное прохождение промежуточной аттестации.

Описание критериев и шкал оценивания результатов освоения дисциплины:

Результат освоения дисциплины	**Критерии оценивания результатов освоения дисциплины**	**Шкала оценивания**
знать основные понятия теории секретных систем и их основные классы, включая идеальные, совершенные и энтропийно-устойчивые.	Вопросы диф.зачета категорий 1-2 Знает основные классы секретных систем, может доказывать их свойства и	Отлично

	описать алгоритмы, их реализующие	
	Вопросы диф.зачета категорий 1-2 Знает основные классы секретных системи, их свойства и алгоритмы, их алгоритмы, их реализующие	Хорошо
	Вопросы диф.зачета категорий 1-2 Знает основные классы секретных систем и их свойства	Удовлетворительно
	Вопросы диф.зачета категорий 1-2 Имеет фрагментарное представление об основных классах секретных систем и их свойствах	Неудовлетворительно

Результаты промежуточной аттестации, проводимой в форме дифференцированного зачета, определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Оценки «отлично», «хорошо», «удовлетворительно» означают успешное прохождение промежуточной аттестации.

Типовые контрольные задания и иные материалы, необходимые для оценки результатов освоения дисциплины (оценочные материалы)

Перечень вопросов диф.зачета структурированный по категориям

Категория	Формулировка вопроса
Категория 1	Вопрос 1. Энтропия и информация
	Вопрос 2. Энтропия эргодических процессов
	Вопрос 3. Теорема Шеннона-Макмиллана-Бреймана
	Вопрос 4. Шифр Вернама и его обобщения
	Вопрос 5. Идеальные криптографические системы
	Вопрос 6. Шифр Рассела и Вонга
	Вопрос 7. Применение сжатия данных для повышения стойкости шифра
	Вопрос 8. Применение рандомизации для повышения стойкости шифра
	Вопрос 9. Омофонные коды
	Вопрос 10. Энтропийно-надежные шифры с секретным ключом постоянной длины для источников информации с известной статистикой
	Вопрос 11. Энтропийно-надежные шифры с секретным

	ключом постоянной длины для источников информации с неизвестной статистикой
	Вопрос 12. Оценивание параметров энтропийно-надежных шифров
	Вопрос 13. Код Шеннона и его свойства
Категория 2	Вопрос 14. Универсальные коды
	Вопрос 15. Код Фитингофа
	Вопрос 16. Код Кричевского
	Вопрос 17. Избыточность кода
	Вопрос 18. Избыточность омофонного кода