Федеральное государственное бюджетное образовательное учреждение
высшего образования
Московский государственный университет имени М.В. Ломоносова
Факультет вычислительной математики и кибернетики

УТВЕРЖДАЮ
декан факультета
вычислительной математики и кибернетики

_____/И.А. Соколов /
«__» _октября_____2021г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Наименование дисциплины (модуля):

Постквантовые криптосистемы с открытым ключом

Уровень высшего образования:

магистратура

Направление подготовки / специальность:

01.04.02 "Прикладная математика и информатика" (3++)

Направленность (профиль) ОПОП:

Искусственный интеллект в кибербезопасности

Форма обучения:

очная

Рабочая программа рассмотрена и утверждена
на заседании Ученого совета факультета ВМК
(протокол №_7_, от 29 сентября 2021 года)

Москва 2021

Рабочая программа дисциплины (модуля) разработана в соответствии с самостоятельно установленным МГУ образовательным стандартом (ОС МГУ) для реализуемых основных профессиональных образовательных программ высшего образования по направлению подготовки 01.04.02 "Прикладная математика и информатика" программы магистратуры в редакции приказа МГУ от 21 декабря 2021 года No 1404.

1. Место дисциплины (модуля) в структуре ОПОП ВО:
Дисциплина (модуль) относится к части дисциплин основной профессиональной образовательной программы, формируемых участниками образовательных отношений.

2. Входные требования для освоения дисциплины (модуля):
учащиеся должны владеть знаниями по математическому анализу, линейной алгебре и теории вероятностей в объеме, соответствующем программе обучения основных образовательных программ бакалавриата по укрупненным группам направлений и специальностей 01.00.00 «Математика и механика», 02.00.00 «Компьютерные и информационные науки» и другим направлениям подготовки бакалавриата, а также должны владеть знаниями по вопросам синтеза и анализа криптосистем с открытым ключом в объёме курса «Синтез и анализ криптосистем с открытым ключом», и владеть знаниями по алгебраической теории кодирования в объёме курса «Теория информации и теория кодирования».

3. Результаты обучения по дисциплине (модулю), соотнесенные с требуемыми компетенциями выпускников.

Планируемые результаты обучения по дисциплине (модулю)		
Содержание и код компетенции.	**Индикатор (показатель) достиженияkомпетенции**	**Планируемые результаты обучения по дисциплине, сопряженные с индикаторамидостижения компетенций**
ПК-1. Способен исследовать и разрабатывать архитектуры систем искусственного интеллекта для различных предметных областей на основе комплексов методов и инструментальных средств систем искусственного интеллекта	ПК-1.1. Исследует и разрабатывает архитектуры систем искусственного интеллекта для различных предметных областей	ПК-1.1. З-1. Знает архитектурные принципы построения систем искусственного интеллекта, методы декомпозиции основных подсистем (компонентов) и реализации их взаимодействия на основе методологии предметно-ориентированного проектирования ПК-1.1. У-1. Умеет выстраивать архитектуру системы искусственного интеллекта, осуществлять декомпозицию основных подсистем (компонентов) и реализации их взаимодействия на основе методологии предметно-ориентированного проектирования
	ПК-1.2. Выбирает комплексы методов и инструментальных средств искусственного интеллекта для решения задач в зависимости от особенностей предметной области	ПК-1.2. З-1. Знает методы и инструментальные средства систем искусственного интеллекта, критерии их выбора и методы комплексирования в рамках создания интегрированных гибридных интеллектуальных систем различного назначения ПК-1.2. У-1. Умеет выбирать, применять и интегрировать

		методы и инструментальные средства систем искусственного интеллекта, критерии их выбора и методы комплексирования в рамках создания интегрированных гибридных интеллектуальных систем различного назначения

4. Объем дисциплины (модуля) составляет 3 з.е., в том числе 36 академических часа, отведенных на контактную работу обучающихся с преподавателем, 72 академических часов на самостоятельную работу обучающихся.

5. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и виды учебных занятий.

Наименование и краткое содержание разделов и тем дисциплины (модуля), **Форма промежуточной аттестации по дисциплине (модулю)**	**Всего (часы)**	В том числе			
		Контактная работа (работа во взаимодействии с преподавателем) Виды контактной работы, часы			**Самостоятельная работа обучающегося, часы** *(виды самостоятельной работы – эссе, реферат, контрольная работа и пр. – указываются при необходимости)*
		Занятия лекционного типа*	Занятия семинарского типа*	**Всего**	
1. Неоднородная модель квантовых вычислений. Дискретное преобразование Фурье и квантовое дискретное преобразование Фурье. Квантовый алгоритм Дойча—Йожи и квантовый алгоритм Шора для факторизации целых чисел.	**10**	5	0	**5**	**5** **Чтение литературы по теме, чтение конспектов лекции или просмотр видео записи лекции**
2. Постквантовые криптографические алгоритмы, построенные на основе хэш-функций. Алгоритм электронной цифровой подписи Меркля.	**2**	1	0	**1**	**1** **Чтение литературы по теме, чтение конспектов лекции или просмотр видео записи лекции**

3. Постквантовые криптографические алгоритмы, построенные на основе кодов, исправляющих ошибки. Сложные задачи в теории кодов, исправляющих ошибки. Задача о тройкосочетаниях, её NP-полнота. Базовые понятия теории кодов, исправляющих ошибки. NP-полнота задачи декодирования кода общего положения. NP-полнота задачи о весовом спектре линейного кода.	**12**	6	0	**6**	**6** **Чтение литературы по теме, чтение конспектов лекции или просмотр видео записи лекции**
4. Эквивалентность кодов. Понятие протокола интерактивного доказательства. Протокол Артура--Мерлина. Протокол интерактивного доказательства для задачи неэквивалентности кодов. Следствие из существования такого протокола. Эквивалентность кодов. Эквивалентность графов. Связь задачи эквивалентности кодов с задачей эквивалентности графов.	**12**	6	0	**6**	**6** **Чтение литературы по теме, чтение конспектов лекции или просмотр видео записи лекции**
5. Криптосистема Мак-Элиса и Ниддерайтера, построенные на основе произвольного класса кодов.	**12**	6	0	**6**	**6** **Чтение литературы по теме, чтение конспектов лекции или просмотр видео записи лекции**
6. Криптосистема Мак-Элиса, построенная на фиксированном коде. Криптосистема Мак-Элиса, построенная на кодах Хэмминга. Атака декодирования на эту криптосистему. Понятие группы автоморфизмов кода. Изоморфизм группы автоморфизмов кода и подгруппы	**12**	6	0	**6**	**6** **Чтение литературы по теме, чтение конспектов лекции или просмотр видео записи лекции**

полной линейной группы GLk (матрицы, задающие автоморфизм кода). Понятие эквивалентности секретных ключей. Структура класса эквивалентности секретного ключа криптосистемы Мак-Элиса.					
7. Коды Рида--Маллера первого порядка. Строение группы автоморфизмов кода Рида--Маллера первого порядка. Алгоритм их быстрого декодирования. Строение группы автоморфизмов кода Рида--Маллера первого порядка. Криптосистема Мак-Элиса, построенная на кодах Рида--Маллера первого порядка. Структура класса эквивалентности криптосистемы Мак-Элиса, построенной на кодах Рида--Маллера первого порядка. Структурные атаки на криптосистему Мак-Элиса. Структурная атака на криптосистему Мак-Элиса, построенную на кодах Рида--Маллера первого порядка	**12**	6	0	**6**	**6** **Чтение литературы по теме, чтение конспектов лекции или просмотр видео записи лекции**
Промежуточная аттестация: устный экзамен	**36**	0	0	**0**	**36**
Итого	**108**	**36**	**0**	**0**	**72**

6. Фонд оценочных средств (ФОС) для оценивания результатов обучения по дисциплине (модулю)

6.1. Типовые контрольные задания или иные материалы для проведения текущего контроля успеваемости.

Типовые задачи для проведения контрольных работ.

Типовое задание 1:

Помогите Анне расшифровать сообщение 0x53, зашифрованное Борисом криптосистемой Мак-Элиса, построенной на основе кодов Хэмминга H3, если её секретный ключ равен

{[12, 6, 9, 11]; (4, 5, 1, 3, 6, 2, 0)}.

Пояснение: матрица задана списком (в квадратных скобках) целых чисел, двоичное представление которых равно строкам матрицы; подстановка (в круглых скобках) задана

Типовое задание 2:

Помогите Семёну-Редиске восстановить секретный ключ Анны, если она пользуется криптосистемой Мак-Элиса, построенной на основе кодов Рида--Маллера первого порядка RM(1, 4), и её открытый ключ равен

[59154, 53972, 16859, 43095, 61793].

Пояснение: матрица задана списком (в квадратных скобках) целых чисел, двоичное представление которых равно строкам матрицы.

Типовое задание 3:

Помогите Семёну-Редиске дешифровать сообщение 0x38, зашифрованное Борисом криптосистемой Мак-Элиса, построенной на основе кодов Хэмминга H3, для Анны, если её открытый ключ равен

[52, 75, 23, 82].

Пояснение: матрица задана списком (в квадратных скобках) целых чисел, двоичное представление которых равны строкам матрицы.

Типовое задание 4:

Помогите Анне расшифровать сообщение 0xCF5E, зашифрованное Борисом криптосистемой Мак-Элиса, построенной на основе кодов Рида--Маллера первого порядка RM(1,4), если её секретный ключ равен {[5, 15, 18, 14, 27]; (10, 3, 14, 0, 7, 15, 8, 6, 5, 9, 12, 4, 13, 11, 1, 2)}.

Пояснение: матрица задана списком (в квадратных скобках) целых чисел, двоичное представление которых равно строкам матрицы; подстановка (в круглых скобках) задана обычным образом.

Типовое задание 5:

Помогите Семёну-Редиске восстановить секретный ключ Анны, если она пользуется криптосистемой Мак-Элиса, построенной на основе кодов Хэмминга H3, и её открытый ключ равен

[14, 77, 84, 43].

Пояснение: матрица задана списком (в квадратных скобках) целых чисел, двоичное представление которых равно строкам матрицы.

6.2. Типовые контрольные задания или иные материалы для проведения промежуточной аттестации.

Вопросы к экзамену.

1. Неоднородная модель квантовых вычислений. Квантовые операторы. Операторы с управляющим кубитом. Квантовая схема. Оператор CNOT.
2. Неоднородная модель квантовых вычислений. Квантовый алгоритм Дойча--Йожи.
3. Дискретное преобразование Фурье. Квантовое дискретное преобразование Фурье. Схема квантового дискретного преобразования Фурье (без вывода)
4. Квантовое дискретное преобразование Фурье. Вывод схемы квантового ДПФ.
5. Алгоритм Шора. Схема доказательства корректности.
6. Постквантовые криптографические алгоритмы, построенные на основе хэш-функций. Алгоритм электронной цифровой подписи Меркля.
7. Задача о тройкосочетаниях, её NP-полнота
8. Постквантовые криптографические алгоритмы, построенные на основе кодов, исправляющих ошибки. Базовые понятия теории кодов, исправляющих ошибки. Сложные задачи теории кодов, исправляющих ошибки. NP-полнота задачи декодирования кода общего положения.
9. Постквантовые криптографические алгоритмы, построенные на основе кодов, исправляющих ошибки. Базовые понятия теории кодов, исправляющих ошибки. Сложные задачи теории кодов, исправляющих ошибки. NP-полнота задачи о весовом спектре кодов.
10. Эквивалентность кодов. Понятие протокола интерактивного доказательства. Протокол Артура--Мерлина. Протокол интерактивного доказательства для задачи неэквивалентности кодов. Следствие из существования такого протокола.
11. Эквивалентность кодов. Эквивалентность графов. Связь задачи эквивалентности кодов с задачей эквивалентности графов.
12. Криптосистема Мак-Элиса и Нидеррайтера, построенные на основе произвольного класса кодов. Эквивалентность стойкости этих криптосистем.
13. Криптосистема Мак-Элиса, построенная на кодах Хэмминга. Атака декодирования на эту криптосистему.
14. Коды Рида--Маллера первого порядка. Алгоритм их быстрого декодирования.
15. Понятие группы автоморфизмов кода. Изоморфизм группы автоморфизмов кода и подгруппы линейной группы GLk (матрицы, задающие автоморфизм кода).
16. Строение группы автоморфизмов кода Рида--Маллера первого порядка.

17. Криптосистема Мак-Элиса, построенная на фиксированном коде. Понятие эквивалентности секретных ключей. Структура класса эквивалентности секретного ключа криптосистемы Мак-Элиса.
18. Криптосистема Мак-Элиса, построенная на кодах Рида--Маллера первого порядка.
19. Структура класса эквивалентности криптосистемы Мак-Элиса, построенной на кодах Рида--Маллера первого порядка.
20. Структурные атаки на криптосистему Мак-Элиса. Структурная атака на криптосистему Мак-Элиса, построенную на кодах Рида--Маллера первого порядка.

ШКАЛА И КРИТЕРИИ ОЦЕНИВАНИЯ результатов обучения (РО) по дисциплине (модулю)				
Оценка РО и соответствующие виды оценочных средств	2	3	4	5
Знания *Экзамен*	Отсутствие знаний	Фрагментарные знания	Общие, но не структурированные знания	Сформированные систематические знания
Умения *Задачи в экзаменационном билете*	Отсутствие умений	В целом успешное, но не систематическое умение	В целом успешное, но содержащее отдельные пробелы умение (допускает неточности непринципиального характера)	Успешное и систематическое умение
Навыки (владения, опыт деятельности) *Экзамен*	Отсутствие навыков (владений, опыта)	Наличие отдельных навыков (наличие фрагментарного опыта)	В целом, сформированные навыки (владения), но используемые не в активной форме	Сформированные навыки (владения), применяемые при решении задач

Соответствие результатов обучения и компетенций, в развитии которых участвует дисциплина (модуль)	
Результаты обучения	Компетенция, с частичным формированием которой связано достижение результата обучения
Знать: 1. Основы квантовых вычислений; 2. Квантовый алгоритм Шора для факторизации и дискретного логарифмирования 3. Основы построения постквантовых схем электронной подписи на основе хэш-функций;	СПК-ПКОК-1.М
Знать: 1. Основы применения алгебраической теории кодирования для построения постквантовых криптосистем с открытым ключом; 2. Математические методы криптографического анализа криптосистем Мак-Элиса и Нидеррайтера, построенных на основе кодов Хэмминга и кодов Рида-Маллера первого порядка. **Уметь:** 1. Применять математические методы для анализа кодовых криптографических систем. 2. Проводить криптографический анализ криптосистем Мак-Элиса и Нидеррайтера, построенных на основе двоичных кодов Хэмминга. 3. Проводить криптографический анализ криптосистем Мак-Элиса и Нидеррайтера, построенных на основе двоичных кодов Рида-Маллера первого порядка.	СПК-ПКОК-2.М

7. Ресурсное обеспечение:
7.1. Перечень основной и дополнительной литературы

Основная литература:

1. Кудряшов Б.Д. Основы теории кодирования. Учебное пособие. СПБ:БВХ-Петерург, 2016г.

Дополнительная литература:

1. Алгоритм Дойча — Йожи // Википедия. — 21.12.2019. — URL: https://ru.wikipedia.org/w/index.php?title=%D0%90%D0%BB%D0%B3%D0%BE%D1%80%D0%B8%D1%82%D0%BC_%D0%94%D0%BE%D0%B9%D1%87%D0%B0_%E2%80%94_%D0%99%D0%BE%D0%B6%D0%B8&oldid=104069340 (дата обр. 28.12.2019) ; Page Version ID: 104069340.
2. Garey M. R., Johnson D. S. Computers and intractability. T. 29. — wh freeman New York, 2002.
3. Сидельников В.М. Теория кодирования.ФИЗМАТЛИТ,Москва, 2008, с. 322.
4. Логачев О.А., Сальников А.А., Смышляев С.В., Ященко В.В. Булевы функции в теории кодирования и криптологии. ЛЕНАНД, Москва, 2015, с. 576.
5. Э. Берлекэмп. Алгебраическая теория кодирования. Москва «Мир», 1971.
6. Т. Касами, Н. Токура, Ё. Ивадари, Я. Инагаки. Теория кодирования. Москва «Мир», 1978.
7. Китаев А., Шень А., Вялый М. Классические и квантовые вычисления. — Москва : МЦНМО, ЧеРо, 1999. — 192 с. — ISBN 5-900916-35-9.
8. Мак-Вильямс Ф. Д., Слоэн Н. Д. А. Теория кодов, исправляющих ошибки / под ред. Л. А. Бассалыго ; пер. И. И. Грушко, В. А. Зиновьев. — Москва : Связь, 1979. — 744 с.
9. Berlekamp E., McEliece R. J., Tilborg H. C. van. On the Inherent Intractability of Certain Coding Problems // Information Theory, IEEE Transactions on. — 1978. — Т. 24, No 3. — С. 384—386. — DOI: 10.1109/TIT.1978.1055873.
10. Petrank E., Roth R. M. Is code equivalence easy to decide? // IEEE Transactions on Information Theory. — 1997. — DOI: 10.1109/18.623157.
11. Repka M., Zajac P. Overview of the Mceliece Cryptosystem and its Security // Tatra Mountains Mathematical Publications. — 2014. — Sept. 1. — Vol. 60, no. 1. — P. 57–83. — DOI: 10.2478/tmmp-2014-0025. — URL: https://content.sciendo.com/view/journals/tmmp/60/1/article-p57.xml (visited on 12/27/2019).

12. Эффективная атака на криптосистему Мак-Элиса, построенную на основе кодов Рида - Маллера / М. А. Бородин [и др.] // Дискретная математика. — 2014. — Т. 26, No 1. — С. 10—20. — ISSN 0234-0860, 2305-3143. — DOI: 10.4213/dm1264. — URL: http://mi.mathnet.ru/dm1264 (дата обр. 25.06.2019).

7.2. Перечень лицензионного программного обеспечения, в том числе отечественного производства

При реализации дисциплины может быть использовано следующее программное обеспечение:

Программное обеспечение для подготовки слайдов лекций MS PowerPoint, MS Word

Программное обеспечение для создания и просмотра pdf-документов Adobe Reader

Издательская система LaTeX

Язык программирования Python и среда разработки Jupiter Notebook (вместе с библиотеками numpy, scikit-learn, pandas)

Язык программирования R и среда разработки R Studio

Среда разработки MATLAB.

7.3. Перечень профессиональных баз данных и информационных справочных систем

1. http://www.edu.ru – портал Министерства образования и науки РФ
2. http://www.ict.edu.ru – система федеральных образовательных порталов «ИКТ в образовании»
3. http://www.openet.ru - Российский портал открытого образования
4. http://www.mon.gov.ru - Министерство образования и науки Российской Федерации
5. http://www.fasi.gov.ru - Федеральное агентство по науке и инновациям

7.4. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Math-Net.Ru [Электронный ресурс] : общероссийский математический портал / Математический институт им. В. А. Стеклова РАН ; Российская академия наук, Отделение математических наук. - М. : [б. и.], 2010. - Загл. с титул. экрана. - Б. ц.
URL: http://www.mathnet.ru
2. Университетская библиотека Online [Электронный ресурс] : электронная библиотечная система / ООО "Директ-Медиа" . - М. : [б. и.], 2001. - Загл. с титул. экрана. - Б. ц. URL: www.biblioclub.ru
3. Универсальные базы данных East View [Электронный ресурс] : информационный ресурс / East View Information Services. - М. : [б. и.], 2012. - Загл. с титул. экрана. - Б. ц.
URL: www.ebiblioteka.ru
4. Научная электронная библиотека eLIBRARY.RU [Электронный ресурс] : информационный портал / ООО "РУНЭБ" ; Санкт-Петербургский государственный университет. - М. : [б. и.], 2005. - Загл. с титул. экрана. - Б. ц.

URL: www.eLibrary.ru

7.5. Описание материально-технического обеспечения.

Факультет ВМК, ответственный за реализацию данной Программы, располагает соответствующей материально-технической базой, включая современную вычислительную технику, объединенную в локальную вычислительную сеть, имеющую выход в Интернет. Используются специализированные компьютерные классы, оснащенные современным оборудованием. Материальная база факультета соответствует действующим санитарно-техническим нормам и обеспечивает проведение всех видов занятий (лабораторной, практической, дисциплинарной и междисциплинарной подготовки) и научно-исследовательской работы обучающихся, предусмотренных учебным планом.

8. Соответствие результатов обучения по данному элементу ОПОП результатам освоения ОПОП указано в Общей характеристике ОПОП.

9. Разработчик (разработчики) программы.

доцент факультета ВМК МГУ И. В. Чижов.

10. Язык преподавания - русский.