Федеральное государственное бюджетное образовательное
учреждение высшего образования
Московский государственный университет имени М.В. Ломоносова
Механико-математический факультет

УТВЕРЖДАЮ
декан механико-
математического факультета
_____/А.И.
Шафаревич /
«_14_» _октября__2021г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Наименование дисциплины:

Криптографические протоколы (на англ. языке)

Уровень высшего образования:
специалитет, магистратура

Направление подготовки / специальность:

02.04.01 "Математика и компьютерные науки" (3++)

Направленность (профиль)/специализация ОПОП:

Интеллектуальные системы. Теория и приложения

Форма обучения:
очная

Рабочая программа рассмотрена и одобрена

на заседании Ученого совета механико- математического факультета

(протокол № 7 от 14 октября 2021 года)

Москва 2021

Рабочая программа дисциплины (модуля) разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) для реализуемых основных профессиональных образовательных программ высшего образования по направлению подготовки 02.04.01 "Математика и компьютерные науки" утвержденного Приказом Министерства образования и науки РФ от 10 января 2018 г. N 13.

1. Место дисциплины (модуля) в структуре ОПОП ВО:
дисциплина относится к блоку профессиональной подготовки вариативной части ОПОП ВО.

2. Входные требования для освоения дисциплины (модуля), предварительные условия (если есть):
Для того чтобы изучение дисциплины было возможно, обучающийся должен обладать следующими компетенциями:
Знать: основные понятия, концепции, результаты и методы дискретной математики, математического анализа, линейной алгебры, математической логики.
Уметь: решать стандартные задачи математической логики и дискретной математики.

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

Планируемые результаты обучения по дисциплине (модулю)		
Содержание и код компетенции.	**Индикатор (показатель) достижения компетенции**	**Планируемые результаты обучения по дисциплине, сопряженные с индикаторами достижения компетенций**
ОПК-5. Способен анализировать профессиональную информацию для решения задач в области применения технологий и систем искусственного интеллекта, выделять в ней главное, структурировать, оформлять и представлять в виде аналитических обзоров и презентаций с обоснованными выводами и рекомендациями	ОПК-5.1. Применяет принципы, методы и средства анализа и структурирования профессиональной информации для решения задач области применения технологий и систем искусственного интеллекта ОПК-5.2. Анализирует профессиональную информацию, выделяет в ней главное, структурирует, оформляет и представляет в виде аналитических обзоров	ОПК-5.1. З-1. Знает способы обобщения и оценки результатов научных исследований ОПК-5.1. У-1. Умеет обобщать и критически оценивать результаты исследований, полученные отечественными и зарубежными исследователями ОПК-5.2. З-1. Знает методы анализа профессиональной информации, структурирования, оформления и разработки аналитических обзоров ОПК-5.2. У-1. Умеет анализировать профессиональную информацию, выделять в ней главное, структурировать, оформлять и представлять в виде аналитических обзоров
ПК-1. Способен исследовать применение интеллектуальных систем для различных предметных областей	ПК-1.1. Исследует направления применения систем искусственного интеллекта для различных предметных областей ПК-1.2. Выбирает комплексы методов и инструментальных средств искусственного интеллекта	ПК-1.1. З-1. Знает направления развития систем искусственного интеллекта, методы декомпозиции решаемых задач с использованием искусственного интеллекта ПК-1.1. У-1. Умеет осуществлять декомпозицию решаемых задач с использованием искусственного интеллекта ПК-1.2. З-1. Знает методы и инструментальные средства систем искусственного интеллекта, критерии их выбора и методы

	для решения задач в зависимости от особенностей предметной области	комплексирования в рамках применения интегрированных гибридных интеллектуальных систем различного назначения ПК-1.2. У-1. Умеет выбирать и комплексно применять методы и инструментальные средства систем искусственного интеллекта, критерии их выбора

4. Объем дисциплины (модуля) составляет 4 з.е., в том числе 36 академических часов, отведенных на контактную работу обучающихся с преподавателем, 108 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:
5.1. Структура дисциплины (модуля) по темам (разделам) с указанием отведенного на них количества академических часов и виды учебных занятий (в строгом соответствии с учебным планом)

Наименование разделов и тем дисциплины (модуля), **Форма промежуточной аттестации по дисциплине (модулю)**	**Номинальные трудозатраты обучающегося**			**Всего академических часов**	**Форма текущего контроля успеваемости* (наименование)**
	Контактная работа (работа во взаимодействии с преподавателем) Виды контактной работы, академические часы		**Самостоятельная работа обучающегося, академические часы**		
	Занятия лекционного типа	Занятия семинарского типа			
Тема 1 Криптографические примитивы: системы шифрования, хэш-функции, электронная подпись.	4		20	24	опрос
Тема 2 Протоколы аутентификации	8		20	28	опрос

Тема 3 Протоколы электронной подписи и передачи криптографических ключей.	8		20	28	опрос
Тема 4 Протоколы голосования и электронных платежей	8		20	28	опрос
Тема 5 Верификация криптографических протоколов	8		28	36	опрос
Другие виды самостоятельной работы (отсутствуют)	—	—			—
Промежуточная аттестация (экзамен)					
Итого	*36*		*108*	144	—

5.2. Содержание разделов (тем) дисциплины

№ п/п	Наименование разделов (тем) дисциплины	Содержание разделов (тем) дисциплин
1.	Тема 1 Криптографические примитивы: системы шифрования, хэш-функции, электронная подпись.	Понятие криптографического протокола. Шифрование сообщений. Системы шифрования. Электронная подпись. Формальные описания и примеры криптографических протоколов. Понятие уязвимости протокола. Примеры уязвимости протоколов. Вероятностный алгоритм проверки целых чисел на простоту. Криптографические примитивы. Симметричные системы шифрования. Асимметричные системы шифрования. Хэш-функции. Пример построения хэш-функции. Стандарт хэш-функции SHS. Понятие схемы разделения секрета. (n, k)-пороговая схема разделения секрета. Схемы разделения секрета с двумя группами
2.	Тема 2 Протоколы аутентификации	Протоколы аутентификации. Протоколы односторонней аутентификации. Протоколы двусторонней аутентификации. Протоколы двусторонней аутентификации с передачей сеансового ключа.
3.	Тема 3 Протоколы электронной подписи и передачи криптографических ключей.	Электронная подпись (ЭП). Протоколы ЭП, получаемые из протоколов аутентификации. Протокол ЭП Шнорра. Протокол ЭП Фиата-Шамира. Протокол ЭП DSA. Протокол ЭП ГОСТ. Протокол ЭП Эль-Гамаля. Стираемая электронная подпись. Слепая ЭП. Протоколы совместной ЭП. Генерация и передача ключей. Протокол Диффи-Хеллмана. Протоколы STS и MTI. Генерация ключа несколькими агентами. Протокол обновления сеансового ключа без аутентификации. Протокол обновления сеансового ключа с аутентификацией. Протокол квантовой передачи ключа.
4.	Тема 4 Протоколы голосования и электронных платежей	Понятие протокола голосования. Примеры протоколов голосования. Протокол голосования с использованием слепой ЭП. Протокол голосования без доверенного посредника.

		Протоколы электронных платежей. Примеры протоколов электронных платежей, распознающих мошенника.
5.	Тема 5 Процессная модель криптографических протоколов. Верификация криптографических протоколов	Моделирование и верификация криптографических протоколов на основе модели распределенных процессов. Верификация протокола аутентификации Yahalom на основе процессной модели. Верификация протокола передачи ключей на основе процессной модели. Моделирование протоколов передачи сообщений через среду с потерей сообщений. Протоколы с чередованием битов. Протоколы скользящего окна. Верификация протокола с чередованием битов. Верификация протокола скользящего окна.

6. Фонд оценочных средств (ФОС, оценочные и методические материалы) для оценивания результатов обучения по дисциплине (модулю).

6.1. Типовые контрольные задания или иные материалы для проведения текущего контроля успеваемости, критерии и шкалы оценивания (в отсутствие утвержденных соответствующих локальных нормативных актов на факультете)

Примеры задач для контрольных работ и экзамена:

1. Доказать корректность систем шифрования RSA и Эль-Гамаля.
2. Доказать корректность протоколов электронной подписи.
3. Доказать отсутствие уязвимостей в протоколе обедающих криптографов.
4. Построить обобщение протокола обедающих криптографов на случай произвольного количества участников и доказать его корректность и безопасность.
5. Доказать корректность вероятностного алгоритма распознавания простоты чисел.
6. Построить схему разделения секрета с заданным количеством групп.
7. Доказать корректность заданного протокола аутентификации на основе процессной модели.
8. Доказать корректность протокола передачи сообщений по ненадежному каналу на основе процессной модели.
9. Построить протокол передачи сообщений по каналу с искажениями, потерей пакетов, дублированием и переупорядочением сообщений, и доказать его корректность.
10. Доказать корректность модифицированного протокола аутентификации Нидхэма-Шредера.

6.2. Типовые контрольные задания или иные материалы для проведения промежуточной аттестации по дисциплине, критерии и шкалы оценивания

Программа экзамена:

1. Понятие криптографического протокола. Шифрование сообщений. Системы шифрования. Электронная подпись.
2. Формальные описания и примеры криптографических протоколов.
3. Понятие уязвимости протокола. Примеры уязвимости протоколов
4. Вероятностный алгоритм проверки целых чисел на простоту
5. Криптографические примитивы. Симметричные системы шифрования. Асимметричные системы шифрования.
6. Хэш-функции. Пример построения хэш-функции. Стандарт хэш-функции SHS.
7. Понятие схемы разделения секрета. (n, k)-пороговая схема разделения секрета. Схемы разделения секрета с двумя группами

8. Протоколы аутентификации. Протоколы односторонней аутентификации. Протоколы двусторонней аутентификации. Протоколы двусторонней аутентификации с передачей сеансового ключа.
9. Электронная подпись (ЭП). Протоколы ЭП, получаемые из протоколов аутентификации. Протокол ЭП Шнорра. Протокол ЭП Фиата-Шамира. Протокол ЭП DSA. Протокол ЭП ГОСТ. Протокол ЭП Эль-Гамаля
10. Стираемая электронная подпись. Слепая ЭП. Протоколы совместной ЭП.
11. Генерация и передача ключей. Протокол Диффи-Хеллмана. Протоколы STS и MTI. Генерация ключа несколькими агентами. Протокол обновления сеансового ключа без аутентификации. Протокол обновления сеансового ключа с аутентификацией. Протокол квантовой передачи ключа.
12. Понятие протокола голосования. Примеры протоколов голосования. Протокол голосования с использованием слепой ЭП. Протокол голосования без доверенного посредника.
13. Протоколы электронных платежей. Примеры протоколов электронных платежей, распознающих мошенника.
14. Процессная модель криптографических протоколов.
15. Моделирование и верификация криптографических протоколов на основе модели распределенных процессов.
16. Верификация протокола аутентификации Yahalom на основе процессной модели.
17. Верификация протокола передачи ключей на основе процессной модели.
18. Моделирование протоколов передачи сообщений через среду с потерей сообщений. Протоколы с чередованием битов. Протоколы скользящего окна.
19. Верификация протокола с чередованием битов.
20. Верификация протокола скользящего окна.

ШКАЛА И КРИТЕРИИ ОЦЕНИВАНИЯ результатов обучения (РО) по дисциплине				
Оценка виды оценочных средств	2 (не зачтено)	3 (зачтено)	4 (зачтено)	5 (зачтено)
Знания	Отсутствие знаний	Фрагментарные знания	Общие, но не структурированные знания	Сформированные систематические знания

(виды оценочных средств: опрос, тесты)				
Умения *(виды оценочных средств: практические задания)*	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) *(виды оценочных средств: выполнение и защита курсовой работы, отчет по практике, отчет по НИР и т.п.)*	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

7. Ресурсное обеспечение:

7.1. Перечень основной и дополнительной литературы

Перечень основной и дополнительной учебной литературы:

[1] Миронов А.М., Протоколы безопасности, часть 1,
http://intsysjournal.ru/pdfs/21-3/65-105-Mironov.pdf

[2] Миронов А.М., Криптографические протоколы, часть 1.
Ташкент, издательство филиала МГУ в Узбекистане, 2010. 129 с.,
http://intsys.msu.ru/staff/mironov/kp.pdf ,

[3] Миронов А.М., Новая математическая модель протоколов аутентификации и основанный на ней метод верификации,
http://intsysjournal.ru/pdfs/22-4/Mironov.pdf

[4] Шнайер Б.: Прикладная криптография. М.: Триумф, 2002.

[5] Черемушкин А.В.: Криптографические протоколы. Основные свойства и уязвимости. Учебное пособие.
М.: Изд. центр Академия, 2009. 272 с.

[6] Menezes A.J., van Oorschot P.C., Vanstone S.A.: Handbook of applied cryptography.
Boca Raton, New York, London, Tokyo: CRC Press, 1997.

[7] Stinson D.R.: Cryptography, theory and practice. London etc., CRC Press, 1995.

[8] Мао В.: Современная криптография: теория и практика. М.: Вильямс, 2005.

[9] Столлингс В.: Криптография и защита сетей: принципы и практика, 2-е издание. М.: Вильямс, 2001.
[10] Столингс В.: Основы защиты сетей. Приложения и стандарты. М.: Вильямс, 2002.

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

нет

7.3. Перечень профессиональных баз данных и информационных справочных систем

нет

7.4. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. http://intsys.msu.ru/
2. http://intsys.msu.ru/science/books/

7.5. Описание материально-технического обеспечения.

Аудитории для проведения лекционных занятий.

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

9. Разработчик (разработчики) программы.

к.ф.-м.н., доцент А.М.Миронов.