Приложение к ОПОП «Безопасность и этика искусственного интеллекта»

СПбГЭТУ «ЛЭТИ»
ПЕРВЫЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ

МИНОБРНАУКИ РОССИИ

федеральное государственное автономное образовательное учреждение высшего образования
«Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И.Ульянова (Ленина)»
(СПбГЭТУ «ЛЭТИ»)

РАБОЧАЯ ПРОГРАММА

дисциплины

«КРИПТОГРАФИЯ И КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ»

для подготовки магистров

по направлению

09.04.01 «Информатика и вычислительная техника»

по программе

«Безопасность и этика искусственного интеллекта»

Санкт-Петербург

2023

ЛИСТ СОГЛАСОВАНИЯ

Разработчики:

доцент, к.ф.-м.н., доцент Левина А.Б.

Рабочая программа рассмотрена и одобрена на заседании кафедры ВТ 02.09.2021, протокол № 6

Рабочая программа рассмотрена и одобрена учебно-методической комиссией ФКТИ, 16.09.2021, протокол № 6

Согласовано в ИС ИОТ

Начальник ОМОЛА Загороднюк О.В.

1 СТРУКТУРА ДИСЦИПЛИНЫ

Обеспечивающий факультет	ФКТИ
Обеспечивающая кафедра	ИБ
Общая трудоемкость (ЗЕТ)	4
Курс	1
Семестр	2
Виды занятий	
Лекции (академ. часов)	17
Практические занятия (академ. часов)	17
Иная контактная работа (академ. часов)	1
Все контактные часы (академ. часов)	35
Самостоятельная работа, включая часы на контроль (академ. часов)	109
Всего (академ. часов)	144
Вид промежуточной аттестации	
Экзамен (курс)	1

2 АННОТАЦИЯ ДИСЦИПЛИНЫ

«КРИПТОГРАФИЯ И КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ»

Данная дисциплина формирует знания и умения, необходимые для разработки криптографических алгоритмов и криптографических протоколов, а так же формирует компетенции для анализа устойчивости криптопроколов/криптоалгорит к различного видам криптоатакам.

В рамках дисциплины изучаются следующие основные темы: основные криптоалгоритмы, принципы построения криптопротоколов, алгоритмы создания и проверки электронной цифровой подписи, гибридные криптосистемы, наиболее применяемые протоколы, используемые для защиты информации в интернете, протоколы видео конференций на примере WhatsApp, принципы построения криптопротоколов.

Практические часть курса, в составе практических работ нацелена на изучение принципов работы криптоалгоритмов/криптопротоколов и анализ их криптостойкости.

SUBJECT SUMMARY

«CRYPTOGRAPHY AND CRYPTOGRAPHIC PROTOCOLS»

This discipline forms the knowledge and skills necessary for the development cryptographic algorithms and cryptographic protocols, as well as forms competencies for analyzing the stability of cryptographic protocols/cryptographic algorithms to various types of cryptographic attacks.

Within the framework of the discipline, the following main topics are studied: the main cryptoalgorithms, the principles of building cryptoprotocols, the main algorithms of symmetric block and stream ciphers, the main algorithms of asymmetric encryption, hash functions, algorithms for creating and validating electronic digital signatures, hybrid cryptosystems, the main encryption protocols, the key distribution

structure, attacks on cryptoalgorms and cryptoprotocols considered in the course, the principles of building cryptoprotocols.

The practical part of the course, as part of practical works, is aimed at studying the principles of cryptomodules and analyzing their ability to stand against the attack.

3 ОБЩИЕ ПОЛОЖЕНИЯ

3.1 Цели и задачи дисциплины

1. Предметом изучения данного курса является криптографические алгоритмы и криптографические протоколы, используемые для обеспечения целостности и конфиденциальности хранимых и передаваемых данных. Курс даст необходимые умения и навыки для самостоятельного построения криптопротоколов и навыки для анализа существующих. Теоретический базис дисциплины основывается на знаниях из теории чисел, дискретной математики, теории вероятности, теории алгоритмов. Способность разрабатывать и модернизировать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности в различных предметных областях.

2. Дисциплина формирует знания и умения, необходимые для разработки криптографических протоколов и исследования их стойкости к различным атакам в составе средств защиты. компьютерных систем. Умение разрабатывать программное и аппаратное обеспечение технологий и систем искусственного интеллекта для решения профессиональных задач с учетом требований информационной безопасности в различных предметных областях.

3. Дисциплина формирует знания, необходимые для разработки криптографических протоколов и исследования их стойкости к различным атакам в составе средств защиты компьютерных систем.

4. Дисциплина формирует умения, необходимые для анализа, выбора и разработки криптографических алгоритмов и криптографических протоколов, умения модернизировать программное и аппаратное обеспечение технологий и систем искусственного интеллекта для решения профессиональных задач с учетом требований информационной безопасности в различных предметных обла-

стях.

5. Результатом освоения дисциплины является приобретение практических навыков, включающих настройки программных и аппаратных средств построение компьютерных сетей, использующих криптографическую защиту информации.

3.2 Место дисциплины в структуре ОПОП

Дисциплина изучается на основе ранее освоенных дисциплин учебного плана:

1. «Машинное обучение»

и обеспечивает изучение последующих дисциплин:

1. «Производственная практика (технологическая (проектно-технологическая) практика)»

2. «Аппаратно-программные средства защиты информации в компьютерных системах»

3. «Защищенное исполнение искусственного интеллекта»

4. «Квантовые вычисления и квантовая криптография»

5. «Основы построения защищенных компьютерных сетей»

6. «Теория информации и теория кодирования»

7. «Производственная практика (преддипломная практика)»

3.3 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

В результате освоения образовательной программы обучающийся должен достичь следующие результаты обучения по дисциплине:

Код компетенции/ индикатора компетенции	**Наименование компетенции/индикатора компетенции**
ПК-30	Способен разрабатывать и модернизировать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности в различных предметных областях
ПК-30.1	*Разрабатывает программное и аппаратное обеспечение технологий и систем искусственного интеллекта для решения профессиональных задач с учетом требований информационной безопасности в различных предметных областях*
ПК-30.2	*Модернизирует программное и аппаратное обеспечение технологий и систем искусственного интеллекта для решения профессиональных задач с учетом требований информационной безопасности в различных предметных областях*

4 СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1 Содержание разделов дисциплины

4.1.1 Наименование тем и часы на все виды нагрузки

№ п/п	Наименование темы дисциплины	Лек, ач	Пр, ач	ИКР, ач	СР, ач
1	Введение	1	0	0	5
2	Тема 1. Симметричное шифрование	3	3	0	20
3	Тема 2. Асимметричное шифрование	3	3	0	20
4	Тема 3. Протоколы гибридного шифрования	2	3	0	15
5	Тема 4. Протоколы аутентификации	2	3	0	16
6	Тема 5. Протоколы индивидуальной и коллективной цифровой подписи	2	2	0	16
7	Тема 6. Криптоанализ и криптостойкость	3	3	0	17
8	Заключение	1	0	1	0
	Итого, ач	17	17	1	109
	Из них ач на контроль	0	0	0	35
	Общая трудоемкость освоения, ач/зе	144/4			

4.1.2 Содержание

№ п/п	Наименование темы дисциплины	Содержание
1	Введение	В введении будут представлены основные понятия, определения, свойства и классификация криптоалгоритмов и криптопротоколов. Объяснены их цели и задачи, представлены основные объекты, рассмотрена модель взаимодействия. Рассмотрены требования, предъявляемые к протоколам, понятие уязвимости и атаки на криптографические алгоритмы/протоколы. Подходы к классификации криптографических алгоритмов и подходы к моделированию криптографических протоколов.
2	Тема 1. Симметричное шифрование	Будут рассмотрены основные алгоритмы блочного и поточного симметричного шифрования (DES, Rijndael, A5), изучены проблема распределения и аутентификации секретных ключей. Рассмотрены протоколы передачи ключей через ЦД, схемы построения ключа. Изучены пороговые схемы разделения секрета на основе китайской теоремы об остатках и схема Шамира, построение протоколов шифрования на основе пороговых схем разделения секрета.

№ п/п	Наименование темы дисциплины	Содержание
3	Тема 2. Асимметричное шифрование	Будут рассмотрены основные задачи ловушки, используемые в криптографии, принципы построения задач ловушек, их применимость. Протоколы асимметричного шифрования, алгоритм RSA, его сферы использования, сравнение с другими алгоритмами асимметричного шифрования. Алгоритм рюкзак, криптосистема Рабина, криптосистема Эль-Гамаль, их сферы применимость в различных протоколах. Сравнение протоколов использующих асимметричное и симметричное шифрование. Основные критерии выбора алгоритмов для дальнейшего построения протокола. Требование контроля корректности формирования открытого ключа.
4	Тема 3. Протоколы гибридного шифрования	Основные принципы и суть гибридного шифрования, протокол передачи ключей Диффи-Хеллмана и протоколы гибридного шифрования на основе алгоритма Диффи-Хеллмана. Изучение протоколов SSL/TLS как одних из наиболее демонстративных систем гибридного шифрования, принципы их «сбора».
5	Тема 4. Протоколы аутентификации	Изучение задачи аутентификации, как одной из составных частей криптопротокола, аутентификация пользователя и информации, простая и строгая аутентификация, достоинства и недостатки, принципы выбора алгоритма аутентификации при построение протокола. Изучение основных понятия электронной цифровой подписи (ЭЦП), использование RSA для ЭЦП. Изучение работы подписи DSA. Изучение работы и принципы построения хэш-функий, как основного примитива, используемого при построение ЭЦП. Изучение протокола «рукопожатия», протоколы установления подлинности. Протоколы «рукопожатия» с использованием симметричных и асимметричных алгоритмов.
6	Тема 5. Протоколы индивидуальной и коллективной цифровой подписи	Протоколы мультиподписи, знакомство с коллективной и композиционной подписью. Целостность коллективной подписи, атаки на протоколы коллективной подписи.
7	Тема 6. Криптоанализ и криптостойкость	Основные понятия криптоанализа, криптоатаки на пройденные алгоритмы/протоколы, классический криптоанализ, навыки для нахождения уязвимостей в криптоалгоритмах/криптомодулях. Атаки по сторонним каналам, основные понятия и принципы, изучение наиболее известных и перспективных атак. Атаки по акустике, электромагнитному излучению, времени. Способы защиты от данных атак.
8	Заключение	Подведение итогов, разбор направлений для дальнейших научных исследований, обсуждение курса.

4.2 Перечень лабораторных работ

Лабораторные работы не предусмотрены.

4.3 Перечень практических занятий

Наименование практических занятий	Количество ауд. часов
1. Симметричное шифрование	3
2. Асимметричное шифрование	3
3. Протоколы гибридного шифрования	3
4. Протоколы аутентификации	3
5. Протоколы индивидуальной и коллективной цифровой подписи	2
6. Криптоанализ и криптостойкость	3
Итого	17

4.4 Курсовое проектирование

Курсовая работа (проект) не предусмотрены.

4.5 Реферат

Реферат не предусмотрен.

4.6 Индивидуальное домашнее задание

Индивидуальное домашнее задание не предусмотрено.

4.7 Доклад

Доклад не предусмотрен.

4.8 Кейс

Кейс не предусмотрен.

4.9 Организация и учебно-методическое обеспечение самостоятельной работы

Изучение дисциплины сопровождается самостоятельной работой студентов с рекомендованными преподавателем литературными источниками и информационными ресурсами сети Интернет.

Планирование времени для изучения дисциплины осуществляется на весь период обучения, предусматривая при этом регулярное повторение пройденного материала. Обучающимся, в рамках внеаудиторной самостоятельной работы, необходимо регулярно дополнять сведениями из литературных источников материал, законспектированный на лекциях. При этом на основе изучения рекомендованной литературы целесообразно составить конспект основных положений, терминов и определений, необходимых для освоения разделов учебной дисциплины.

Особое место уделяется консультированию, как одной из форм обучения и контроля самостоятельной работы. Консультирование предполагает особым образом организованное взаимодействие между преподавателем и студентами, при этом предполагается, что консультант либо знает готовое решение, которое он может предписать консультируемому, либо он владеет способами деятельности, которые указывают путь решения проблемы

Текущая СРС	**Примерная трудоемкость, ач**
Работа с лекционным материалом, с учебной литературой	39
Опережающая самостоятельная работа (изучение нового материала до его изложения на занятиях)	10
Самостоятельное изучение разделов дисциплины	9
Выполнение домашних заданий, домашних контрольных работ	0
Подготовка к лабораторным работам, к практическим и семинарским занятиям	7
Подготовка к контрольным работам, коллоквиумам	6
Выполнение расчетно-графических работ	0
Выполнение курсового проекта или курсовой работы	0

Текущая СРС	Примерная трудоемкость, ач
Поиск, изучение и презентация информации по заданной проблеме, анализ научных публикаций по заданной теме	3
Работа над междисциплинарным проектом	0
Анализ данных по заданной теме, выполнение расчетов, составление схем и моделей, на основе собранных данных	0
Подготовка к зачету, дифференцированному зачету, экзамену	35
ИТОГО СРС	109

5 Учебно-методическое обеспечение дисциплины

5.1 Перечень основной и дополнительной литературы, необходимой для освоения дисциплины

№ п/п	Название, библиографическое описание	К-во экз. в библ.
Основная литература		
1	Столлингс, Вильям. Криптография и защита сетей. Принципы и практика [Текст] : монография / В.Столлингс; [Пер. с англ. А.Г.Сивака, А.А.Шпака], 2001. -669 с.	42
2	Дернова, Евгения Сергеевна. Элементы теоретических основ криптографии [Текст] : учеб. пособие / Е.С. Дернова, Н.А. Молдовян, П.А. Молдовяну, 2009. -91 с.	77
3	Молдовян, Александр Андреевич. Криптография [Текст] : учебное пособие / А.А.Молдовян, Н.А.Молдовян, Б.Я.Советов, 2001. -218 с.	19
4	Молдовян, Александр Андреевич. Практичные протоколы цифровых мультиподписей [Текст] : учеб. пособие / А. А. Молдовян, А. Н. Березин, Д. Н. Молдовян, 2018. -71 с.	35
Дополнительная литература		
1	Масленников, Михаил Е. Практическая криптография [Текст] : монография / М.Е.Масленников, 2003. -V, 458 с.	7

5.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», используемых при освоении дисциплины

№ п/п	Электронный адрес
1	В. В. Ященко. Введение в криптографию: Москва: МЦНМО, 2012http://cryptography.ru/wp-content/uploads/2013/09/intro_to_crypto.pdf
2	Криптосистемы: интернет ресурс, 2018https://coderlessons.com/tutorials/akademicheskii/izuchite-kriptografiiu/kriptosistemy
3	А. М. Миронов. Криптографичсекие протоколыhttp://intsys.msu.ru/staff/mironov/kp.pdf

5.3 Адрес сайта курса

Адрес сайта курса: https://vec.etu.ru/moodle/course/view.php?id=7512

6 Критерии оценивания и оценочные материалы

6.1 Критерии оценивания

Для дисциплины «Криптография и криптографические протоколы» формой промежуточной аттестации является экзамен. Оценивание качества освоения дисциплины производится с использованием рейтинговой системы.

Экзамен

Оценка	Количество баллов	Описание
Неудовлетворительно	0 – 51	теоретическое содержание курса не освоено, необходимые практически навыки и умения не сформированы, выполненные учебные задания содержат грубые ошибки, дополнительная самостоятельная работа над курсом не приведет к существенному повышению качества выполнения учебных заданий
Удовлетворительно	52 – 67	теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые практические навыки и умения работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий содержат ошибки
Хорошо	68 – 84	теоретическое содержание курса освоено полностью, без пробелов, некоторые практические навыки и умения сформированы недостаточно, все предусмотренные программой обучения учебные задания выполнены, качество выполнения ни одного из них не оценено минимальным числом баллов, некоторые виды заданий выполнены с ошибками
Отлично	85 – 100	теоретическое содержание курса освоено полностью, без пробелов, необходимые практические навыки и умения сформированы, все предусмотренные программой обучения учебные задания выполнены, качество их выполнения оценено количеством баллов, близким к максимальному

Особенности допуска

Допуск к экзамену включает в себя посещение не менее 80% лекционных и практических занятий, выполнение всех практических работ и защиту их на коллоквиумах.

6.2 Оценочные материалы для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине

Вопросы к экзамену

№ п/п	Описание
1	Основные алгоритмы блочного и поточного симметричного шифрования, проблема распределения и аутентификации секретных ключей, протоколы передачи ключей через ЦД, какие бывают ключи, пороговые схемы разделения секрета на основе китайской теоремы об остатках и схема Шамира, протоколы шифрования на основе пороговых схем разделения секрета.
2	Задачи ловушки, протоколы асимметричного шифрования: RSA, рюкзак, криптосистема Рабина, сравнение протоколов асимметричного и симметричного шифрования.
3	Протоколы гибридного шифрования. Протоколы гибридного шифрования на основе асимметричного шифра, протокол передачи ключей Диффи-Хеллмана, протокол гибридного шифрования на основе протокола DH, протокол SSL/TLS
4	Протоколы аутентификации. Задача аутентификации информации и пользователей, простая и строгая аутентификация, достоинства и недостатки, . Основные понятие электронной цифровой подписи (ЭЦП), RSA для ЭЦП, DSA для ЭЦП, протоколы ”рукопожатия”, протоколы установления подлинности, протоколы ”рукопожатия” с использованием симметричных и асимметричных криптографических алгоритмов. Хэш-функции, как основная часть ЭЦП.
5	Протоколы индивидуальной и коллективной цифровой подписи. Протоколы мультиподписи, коллективная и композиционная подпись, целостность коллективной подписи, требование контроля корректности формирования открытого ключа, атаки на протоколы коллективной подписи.
6	Криптоанализ и криптостйкость. Основные понятия, атаки по сторонним каналам.

Форма билета

Министерство науки и высшего образования Российской Федерации

ФГАОУ ВО «Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» имени В.И. Ульянова (Ленина)»

_____

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

Дисциплина **Криптография и криптографические протоколы** ФКТИ

1. **Симметричное шифрование.** Основные алгоритмы блочного и поточного симметричного шифрования (DES, AES, A5), проблема распределения и аутентификации секретных ключей, протоколы передачи ключей через ЦД, какие бывают ключи, пороговые схемы разделения секрета на основе китайской теоремы об остатках и схема Шамира, протоколы шифрования на основе пороговых схем разделения секрета.

2. Обсуждение других вопросов курса в форме собеседования.

УТВЕРЖДАЮ

Заведующий кафедрой

Образцы задач (заданий) для контрольных (проверочных) работ

Перечень примерных вопросов к коллоквиумам:

1. Алгоритм рюкзак, криптосистема Рабина, криптосистема ЭльГамаль, их сферы применимость в различных протоколах

2. Основные критерии выбора алгоритмов для дальнейшего построения протокола. Требование контроля корректности формирования открытого ключа.

3. Основные принципы и суть гибридного шифрования, протокол передачи ключей ДиффиХеллмана и протоколы гибридного шифрования на основе алгоритма ДиффиХеллмана.

4. Протоколы мультиподписи, знакомство с коллективной и композиционной подписью.

5. Целостность коллективной подписи, атаки на протоколы коллективной подписи.

6. Основные понятия криптоанализа, криптоатаки на пройденные алгоритмы/протоколы, классический криптоанализ, навыки для нахождения уязвимостей в криптоалгоритмах/криптомодулях.

7. Атаки по сторонним каналам, основные понятия и принципы, изучение наиболее известных и перспективных атак.

8. Атаки по акустике, электромагнитному излучению, времени. Способы защиты от данных атак.

9. Системы электронной жеребьевки, тайного электронного голосования, системы электронных денег, протокол подбрасывания монет и игра в покер по телефону, защита от атак: сертификаты и PKI, семейства протоколов IPsec, протоколы Oakley, ISAKMP, IKE.

10. Основные алгоритмы блочного и поточного симметричного шифрования, проблема распределения и аутентификации секретных ключей, протоколы передачи ключей через ЦД, какие бывают ключи, пороговые схемы разделения секрета на основе китайской теоремы об остатках и схема Шамира, протоколы шифрования на основе пороговых схем разделения секрета.

Весь комплект контрольно-измерительных материалов для проверки сформированности компетенции (индикатора компетенции) размещен в закрытой части по адресу, указанному в п. 5.3

6.3 График текущего контроля успеваемости

Неделя	Темы занятий	Вид контроля
2	Тема 1. Симметричное шифрование	
3		
4		Коллоквиум
5	Тема 2. Асимметричное шифрование	
6		
7		Коллоквиум
8	Тема 3. Протоколы гибридного шифрования	
9		
10		Коллоквиум
11	Тема 5. Протоколы индивидуальной и коллективной цифровой подписи	
12		Коллоквиум
13	Тема 6. Криптоанализ и криптостойкость	
14		Коллоквиум

6.4 Методика текущего контроля

на лекционных занятиях

Текущий контроль включает в себя контроль посещаемости (не менее ***80*** % занятий), по результатам которого студент получает допуск на экзамен.

на практических (семинарских) занятиях

Текущий контроль включает в себя контроль посещаемости (не менее ***80*** % занятий), по результатам которого студент получает допуск на экзамен.

В ходе проведения семинарских и практических занятий целесообразно привлечение студентов к как можно более активному участию в дискуссиях, решении задач, обсуждениях и т. д. При этом активность студентов также может учитываться преподавателем, как один из способов текущего контроля на практических занятиях. Сдача практических заданий будет проходить в форме коллоквиумов на которых проводится защита отчетов по практическим работам.

Критерии оценивания работы студентов на коллоквиумах:

«отлично» - тема вопроса раскрыта полностью, студент свободно владеет материалом и отвечает на дополнительные вопросы по теме.

«хорошо» - тема раскрыта не полностью, студент свободно владеет материалом, отвечает на дополнительные вопросы с несущественными ошибками.

«удовлетворительно» - в ответе имеются существенные ошибки, студент не дает ответов на дополнительные вопросы;

«неудовлетворительно» - ответ отсутствует, не соответствует теме, содержит грубые ошибки.

самостоятельной работы студентов

Контроль самостоятельной работы студентов осуществляется на лекционных и практических занятиях студентов по методикам, описанным выше.

7 Описание информационных технологий и материально-технической базы

Тип занятий	Тип помещения	Требования к помещению	Требования к программному обеспечению
Лекция	Лекционная аудитория	Количество посадочных мест – в соответствии с контингентом, рабочее место преподавателя, компьютер или ноутбук, проектор, экран, маркерная доска.	1) Windows XP и выше; 2) Microsoft Office 2007 и выше 3)CrypTool 1 и 2 4) C/C++, Java, Python
Практические занятия	Аудитория	Количество посадочных мест – в соответствии с контингентом, рабочее место преподавателя, компьютер или ноутбук, проектор, экран, маркерная доска.	1) Windows XP и выше; 2) Microsoft Office 2007 и выше 3)CrypTool 1 и 2 4) C/C++, Java, Python
Самостоятельная работа	Помещение для самостоятельной работа	Оснащено компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.	1) Windows XP и выше; 2) Microsoft Office 2007 и выше

8 Адаптация рабочей программы для лиц с ОВЗ

Адаптированная программа разрабатывается при наличии заявления со стороны обучающегося (родителей, законных представителей) и медицинских показаний (рекомендациями психолого-медико-педагогической комиссии). Для инвалидов адаптированная образовательная программа разрабатывается в соответствии с индивидуальной программой реабилитации.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ п/п	Дата	Изменение	Дата и номер протокола заседания УМК	Автор	Начальник ОМОЛА
1	14.02.2023	Программа актуальна, изменения не требуются.	14.02.2023 г., протокол заседания УМК № 2	доцент, к.ф.-м.н., доцент, А.Б. Левина	