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

УТВЕРЖДАЮ
Декан факультета ВМК

_____ / Соколов И.А. /
«__09__» _____ 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Наименование дисциплины:

Задача защиты информации в истории, политике и математике

Уровень высшего образования:

бакалавриат, магистратура, специалитет

указывается: бакалавриат, магистратура или специалитет

Направление подготовки (специальность):

(код и название направления/специальности)

Направленность (профиль) ОПОП:

(если дисциплина (модуль) относится к вариативной части программы)

Форма обучения:

очная с использованием дистанционных образовательных технологий

очная, очно-заочная, заочная

Рабочая программа рассмотрена и одобрена
на заседании Ученого совета факультета
(протокол № 5, 30.06.2022)

Москва 2022

1. Место дисциплины (модуля) в структуре ОПОП реализуется в рамках МФК.

2. Входные требования для освоения дисциплины (модуля), предварительные условия: не требуются.

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

Компетенции выпускников (коды)	**Индикаторы (показатели) достижения компетенций**	**Планируемые результаты обучения по дисциплине (модулю), сопряженные с компетенциями**
Новая УК ОС МГУ Способен осуществлять коммуникацию, поиск, обработку и анализ данных с применением цифровых инструментов, в том числе с элементами программирования и технологий искусственного интеллекта.	УК-N (Ин.1ук) Знает основные понятия и методы программирования, виды и форматы хранения данных, этапы проведения анализа данных и основные понятия искусственного интеллекта и машинного обучения	**Знать:** Основные понятия программирования Этапы решения задач и применением средств вычислительной техники Виды и форматы хранения данных Этапы проведения анализа данных Стандартные алгоритмы обработки и анализа данных Основные понятия искусственного интеллекта и машинного обучения **Уметь** Применять средства и технологии программирования для решения задач связанных с анализом данных Проводить поиск, обработку и анализ данных для решения профессиональных задач, в том числе открытых данных Использовать технологии искусственного интеллекта и машинного обучения для решения профессиональных задач **Владеть:** методами и технологиями использования средств вычислительной техники для решения профессиональных задач, в том
	УК-N (Ин.2ук) Умеет применять стандартные алгоритмы и средства программирования для решения задач, связанных с анализом данных, в том числе с использованием технологий искусственного интеллекта и машинного обучения	
	УК-N (Ин.3ук) Владеет методами и технологиями использования средств вычислительной техники для решения профессиональных задач, в том числе с применением технологий искусственного интеллекта	

		числе с применением технологий искусственного интеллекта

4. Объем дисциплины (модуля) 1 з.е., в том числе 24 академических часа на контактную работу обучающихся с преподавателем, 12 академических часа на самостоятельную работу обучающихся.

5. Формат обучения асинхронное обучение с использованием *дистанционных образовательных технологий*

6. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических или астрономических 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** ***Виды самостоятельной работы, часы***	
		Занятия лекционного типа	Занятия семинарского типа	Групповые консультации	Индивидуальные консультации	**Всего**	**Работа в среде электронного обучения**	**Всего**
Тема 1. Происхождение письменности и криптографии	4	4				4	2	2
Тема 2. Древние цивилизации и конфликты	4	4				4	2	2
Тема 3. Развитие государственности и криптографиина русской равнине	4	4				4	2	2

Тема 4. Развитие государственности и криптографии в европе	6	6				6	3	3
Тема 5. Новейшее развитие криптографии	6	6				6	3	3
Промежуточная аттестация	*Тестирование*						Зачет	
Итого	36	24				24	12	12

** Текущий контроль успеваемости может быть реализован в рамках занятий семинарского типа, групповых или индивидуальных консультаций*

*** Практическая подготовка (при наличии) осуществляется на базе кафедры информационной безопасности МГУ, практическая подготовка на базе которого осуществляется на основании Договора)*

**** Часы на проведение промежуточной аттестации выделяются из часов самостоятельной работы обучающегося.*

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

РЕЗУЛЬТАТ ОБУЧЕНИЯ по дисциплине (модулю)	**СРЕДСТВА ОЦЕНИВАНИЯ**	**ШКАЛА И КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТА ОБУЧЕНИЯ по дисциплине (модулю)** *Шкалы и критерии оценивания могут быть сформулированы как общие для всех дисциплин (модулей) и размещены в документе ««Оценочные и методические материалы для контроля формирования компетенций у обучающихся в процессе освоения образовательной программы», входящем в состав ОПОП*			
		2 (не зачтено)	3 (зачтено)	4 (зачтено)	5 (зачтено)
Знать:					
Основные мировые цивилизации и их письменность	Тестирование	Отсутствие знаний	Фрагментарные знания	Общие, но не структурированные знания	Сформированные систематические знания
Основные мировые войны	Тестирование	Отсутствие знаний	Фрагментарные знания	Общие, но не структурированные знания	Сформированные систематические знания

Основные известные криптографические алгоритмы древности	Тестирование	Отсутствие знаний	Фрагментарные знания	Общие, но не структурированные знания	Сформированные систематические знания
Структуру денежного обращения в древних государствах	Тестирование	Отсутствие знаний	Фрагментарные знания	Общие, но не структурированные знания	Сформированные систематические знания
Систему государственного и религиозного управления в европе	Тестирование	Отсутствие знаний	Фрагментарные знания	Общие, но не структурированные знания	Сформированные систематические знания
Основные криптопротоколы	Тестирование	Отсутствие знаний	Фрагментарные знания	Общие, но не структурированные знания	Сформированные систематические знания
Уметь					
Выстроить единую цепочку развития мировых цивилизаций и войн	Тестирование	Отсутствие знаний	Фрагментарные знания	Общие, но не структурированные знания	Сформированные систематические знания
Объяснить причины возникновения алфавитного письма и кириллицы в частности.	Тестирование	Отсутствие знаний	Фрагментарные знания	Общие, но не структурированные знания	Сформированные систематические знания
Оценивать необходимость применения криптографических протоколов для решения задач защиты информации.	Тестирование	Отсутствие знаний	Фрагментарные знания	Общие, но не структурированные знания	Сформированные систематические знания
Владеть					
методами и технологиями защиты информации, а также правоустанавливающими документами в этой области	Тестирование	Отсутствие знаний	Фрагментарные знания	Общие, но не структурированные знания	Сформированные систематические знания

Типовые задания и иные материалы, необходимые для оценки результатов обучения

Примерные тестовые задания

Вопрос 1.
Где впервые возникла письменность?
Месопотамия
Египет
Китай
Южная америка

Вопрос 2.
Где впервые возникло алфавитное письмо?
Рим
Персия
Микенское царство
Финикия

Вопрос 3
Где впервые возникла криптография?
Индия
Китай
Рим
Европа

Вопрос 4
Где впервые использовалось автоматическое шифрование?
Франция
Испания
Рим
Греция

Вопрос 5
Что такое «брактеаты»?
Буквы шифртекста
Технология денежного обращения

Процедуры шифрования
Метки аутентификации

Вопрос 6
Когда вышла первая книга по криптографии?
16в.
17в.
15в.
14в.

Вопрос 7
Когда вышла первая книга по бухучету?
16в.
17в.
15в.
14в.

Вопрос 8
Что такое вязь?
Рисунок на обложке библии
Шифр многозначной замены
Элемент стеганографии
Орнамент на ткани

Вопрос 9
Кто такие стрельцы?
Бунтари и разбойники
Воссьавшие крестьяне
Государственные служащие
Солдаты царской армии

Вопрос 10
Как изменилось население Руси при Петре 1?
Не изменилось

Увеличилось на 25%
Уменьшилось на 25%
Постарело

Вопросы к зачету:

1. Как вскрыть шифр простой замены?
2. Что такое книжный шифр?
3. Структура военного руководства в средневековой Европе.
4. География шелкового пути.
5. Сравнительная характеристика вооружения и военного строительства в Европе и на Руси в 13 веке.
6. Принципы шифрования на Руси в 15 веке.
7. Принципы шифрования в других странах к 15 веку.
8. Что такое Московская торговая компания?
9. Какие государства располагались на территории современной РФ в средние века.
10. Приоритеты внешней политики России до и после убийства Павла 1.
11. Найти $41^{-1} (\mathrm{mod}\ 53)$
12. Доказать, что 561 является числом Кармайкла.
13. Решить рекуррентное уравнение: $x_m = x_{m-1} + x_{m-2}$, $x_0=1$, $x_1=1$.
14. Чем отличается аутентификация от цифровой подписи.
15. Определение кодового расстояния.
16. Решить: $2^x = 3 \ (\mathrm{mod}\ 53)$

8. Ресурсное обеспечение:

- Перечень основной и дополнительной учебной литературы
    - Основная литература

1. Линдер И.Б., Чуркин С.А. Спецслужбы России за 1000 лет, ООО ГК «Рипол классик», 2016, 784 с.
2. А.В.Бабаш, Г.П.Шанкин История криптографии М., Гелиос, АРВ 2002, 240с.
3. М.А.Черепнев Криптографические протоколы. Изд.-во центра Прикладных исследований. 2006. 72с.

- Дополнительная литература

1. Повесть временных лет.

2. Русская правда.

3. Wikipedia

4. Н.А.Морозов «Новый взгляд на историю русского государства» Изд.-во С-Пб Университета 2007г.
5. «Сокровенное сказание монголов» Труды членов Российской духовной миссии в Пекине. С-Пб 1866г.
6. Л.Н.Гумилёв «В поисках вымышленного царства».
7. Г.В.Носовский, А.Т.Фоменко. Русь и Рим. (т.2 Новая хронология Руси. Хронология китайской истории и ее параллели с европейской)
8. В.В.Кожинов «Против кого боролся Дмитрий Донской» Наука и Религия, 2000, №8.
9. «Задонщина»
10. В.И.Рассадин «Тюркские элементы в языке «Сокровенного сказания монголов» Новосибирск 1995.
11. Древнетюркский словарь. Институт языкознания АН СССР, издательство «Наука» Ленинград, 1969.
12. Латинско-русский словарь. И.Х.Дворецкий, издательство «Русский язык», Москва 1976г.
13. Католическая энциклопедия. Издательство Францисканцев, 2002г.
14. Nouveau petit Larousse illustrè, 290 edition, Paris, 1939, 1771 p.
15. Книга большому чертежу
16. Э. Ртвеладзе “Великий шёлковый путь” Гос. Науч. Изд-во «Узбекистон милий энциклобеяси» Ташкент.
17. Григорьев А.П. К реконструкции текстов золотоордынских ярлыков. // Историография и источниковедение истории стран Азии и Африки. Л., 1980. Вып. 5. С. 36-37.
18. В.И. Матузова, Е.Л. Назарова Крестоносцы и Русь. М., 2002.
19. С.А.Плетнева «Очерки хазарской археологии»М., «Мосты культуры 1999
20. Е.П.Романов (М.А.Черепнев) Памятная книга Богучара. Книга вторая. Воронеж, АО «Воронежская областная типография», 2017, 272с.

- Перечень лицензионного программного обеспечения
  - Zoom
- Перечень профессиональных баз данных и информационных справочных систем

1. Система федеральных образовательных порталов. Информационно-коммуникационные технологии в образовании. http://www.ict.edu.ru/lib/
2. Интернет университет информационных технологий. http://www.intuit.ru/
3. Система федеральных образовательных порталов. Информационно-коммуникационные технологии в образовании. http://www.ict.edu.ru/lib/
4. Российская национальная библиотека (РНБ). www. hbl-russia.ru http://www. nlr. ru.
5. Российская государственная библиотека (РГБ). http://www. rsl. ru.
6. ЭБС « Университетская библиотека онлайн» http:www.biblioclub.ru
7. ЭБС «Znanium.com» http://znanium.com/
8. ЭБС «Юрайт» https://biblio-online.ru/

- Перечень ресурсов информационно-телекоммуникационной сети «Интернет» (при необходимости)
- Описание материально-технической базы.

9. Язык преподавания.
Русский

10. Преподаватель (преподаватели).

11. Разработчики программы.
Черепнев М.А.,д..ф. м. н., профессор, факультет ВМК МГУ