**Факультет** **вычислительной математики и кибернетики**

**Межфакультетский курс**

**"Задача защиты информации в истории, политике и математике"**

**Лекции: 30 часов**

**Лектор: д.ф.-м.н., доцент факультета ВМК Черепнёв Михаил Алексеевич**

**Аннотация.**

В исторической ретроспективе раскрыты мотивы возникновения и способы решения задачи защиты информации. Раскрываются взаимосвязи коммерции, военных и разведывательных операций, а также методов создания защищённых информационных каналов в разных странах. Выделены результаты и преимущества, полученные за счёт использования и вскрытия защищённых каналов связи. Изложены математические основания работы криптографических протоколов.

Annotation

We describe a history of cryptography and it's relation with finance and army. We present features obtained with the help of cryptographic protocols and their breaking. We explain mathematical background of cryptographic protocols.

**Программа лекций.**

1. История научных знаний и мировых цивилизаций. Методы защиты информации в древнем Китае, Индии, Месопотамии, Персии, Греции, Египте, Риме, Европпе.
2. История средневековых военных операций. Оружие Китая, Персии, Греции (шифр «квадрат Полибия»), Рима. Походы Александра Македонского. Спарта (шифр «Сциталь») Готы и Гунны. Разгром Скифии, Рима, Персии, Хорезма, Хозарии, Ся. Катары. Крестовые походы (первые биометрические документы). Использование достижений древней науки (компас, порох, метательные орудия, греческий огонь, оптика, рычаги, вуц, шёлк). Появление фальшивых и бумажных денег, кредитные обязательства, брактеаты. Вооружение и экипировка крестоносцев.
3. Средневековая наука западной европпы. Разработка европейцами месторождений серебра, железа, каменного и бурого угля, соли. Производство оружия, фортификация. Начало книгопечатания. Шифр «Таблица Тритемия». Европейские государства и религия. Военные и монашествующие ордена, их отношения к науке, финансам, юриспруденции, религиям, колониям. Православие в Византии, Англии, Руси. Государственное управление в Хозарии. Трактат Константина Багрянородного. Природа Каспийского моря. Русская правда. Русский календарь и праздники. Лествичное право. Яссы.
4. Теорема о парадоксе дней рождения. Расчёт вероятности случайного совпадения слов. Заимствованные средневековые слова и выражения (русский, английский, татарский). Глаголица, кирилица. Неиспользуемые буквы кирилического алфавита. Имена, географические названия и «иностранные» слова Повести временных лет, Сказания о битве Игоря с половцами, Сокровенного сказания монголов. Новгород и Старая Ладога (география, генетика). Рюрик, Синеус, Трувор, Олег, Святослав, Игорь, Ольга, Владимир – красно солнышко, Ярослав мудрый, Андрей Боголюбский, Владимир Мономах.
5. Разгром Волжской Булгарии, Владимирской руси, Киевской руси, Польши, Венгрии. Окончание нашествия «тартар». Европейские колонии на территории РФ. Оружие «тартар», производство металла, оружие и фортификация средневековой руси. Липецкая битва, битва при Калке, Разгром Резани (её границы, Коловрат), взятие Владимира, вазятие Киева. Денежное обращение в средневековой руси. Вычисления и письменность средневековой руси. Измаилтяне, агаряне, маршруты Батыя. Ярослав, Александр Ярославович (Невский), Михаил (Черниговский), Михаил (Тверской), Народы средневековой руси. Русские пути (волоки, дороги, структура провозимых товаров, таможенные и торговые пункты). Шелковый путь. Хождение за три моря А.Никитина.
6. Куликовская битва. Митрополит Алексий. Походы Дмитрия (Донского), политика, канонизация, монеты. Оружие, стратегия, разведка, география (сурожане, гребневые казаки, дороги, границы), состав войска и его численность. Татарская летопись. Столетняя война в Европпе.
7. Иван III и Софья Палеолог, переписка со святым престолом. Иван Грозный и московская торговая компания. Мангазея. Первые криптографические примитивы в русской письменности (вязь, литорея, цыфры, азбука Варкоча). Верхняя типография, Сильвестр Медведев. Шифрование испанских завоевателей (кодноменклатор). Становление английской разведки. Шифр Ф.Бэкона. Елизавета 1 и Мария Стюарт. Петр Первый и его цыфирная азбука. Екатерина II и шифр Виженера. Создание криптографической службы в России, Гольдбах, школы. Шифры Котельникова, Шеннона. Энигма и первая ЭВМ.
8. Лабораторя Белла США и английская телефонная служба. Определение односторонней функции, примеры. Принципиальные схемы шифрования и электронной подписи.
9. Кольца и поля вычетов. Расширенный алгоритм Евклида. Малая теорема Ферма.
10. Решение систем линейных сравнений. Задача о безопасном хранении ключа.
11. Простейшие тесты простоты. Простейшие свойства конечных полей. Неприводимые многочлены над конечным полем (по Лидл, Нидеррайтор).
12. Линейные рекуррентные последовательности (по Лидл, Нидеррайтор). Криптосхемы Мессей-Омуры, Фейденбаума, “Подбрасывание монеты по телефону”.
13. Схемы с открытым ключом и электронной подписи Эль-Гамаля. Российский стандарт. DSA. Криптоанализ РСА. Схемы распределения ключа Кояма-Охта.
14. Аутентификация. Цифровая подпись. Интерактивные протоколы.
15. Простейшие алгоритмы дискретного логарифмирования. Коды, исправляющие ошибки.

**Вопросы.**

1. Как вскрыть шифр простой замены?
2. Что такое книжный шифр?
3. Структура военного руководства в средневековой европпе.
4. География шелкового пути.
5. Сравнительная характеристика вооружения и военного строительства в европпе 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 распологались на территории современной РФ в средние века.
10. Приоритеты внешней политики России до и после убийства Павла 1.
11. Найти 41-1(mod 53)
12. Доказать, что 561 является числом Кармайкла.
13. Решить рекуррентное уравнение: xm= xm-1+ xm-2 , x0=1, x1=1.
14. Чем отличается аутентификация от цифровой подписи.
15. Определение кодового расстояния.
16. Решить: 2x = 3 (mod 53)

**Литература**

1. Повесть временных лет.
2. Русская правда.
3. Wikipedia
4. Н.А.Морозов «Новый взгляд на историю русского госудорства» 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. М.А.Черепнев Криптографические протоколы. Изд.-во центра Прикладных исследований. 2006. 72с.
20. Е.П.Романов (М.А.Черепнев) Памятная книга Богучара. Книга вторая. Воронеж, АО «Воронежская областная типография», 2017, 272с.
21. Столпаков Б.В., Никонов В. Чтоб было в тех землях не знатно. М.: Медиа Группа «Авангард», 2016, 236с.
22. Бабаш А.В., Шанкин Г.П. История Криптографии М.: Гелиос, АРВ, 2002, 240с.  [ISBN 5-85438-043-9](https://ru.wikipedia.org/wiki/%D0%A1%D0%BB%D1%83%D0%B6%D0%B5%D0%B1%D0%BD%D0%B0%D1%8F%3A%D0%98%D1%81%D1%82%D0%BE%D1%87%D0%BD%D0%B8%D0%BA%D0%B8_%D0%BA%D0%BD%D0%B8%D0%B3/5854380439).
23. Гашков С.Б., Применко Э.А., Черепнев М.А. Криптографичкские методы защиты информации. М.: Издательский центр «Академия», 2010, 304с., ISBN 978-5-7695-4962-5