УТВЕРЖДАЮ
Проректор по учебной работе
И.А. Кузнецова
23 июня 2020 г
Прием 2020 года

Аннотация дисциплины
«История и философия науки»

Направление 10.06.01 Информационная безопасность
Направленность (профиль) «Методы и системы защиты информации, информационная безопасность»

1. Дисциплина «История и философия науки» относится к базовой части блока Б1.

2. Целью освоения данной дисциплины является формирование у аспирантов целостного понимания предмета и основных концепций современной философии науки, развитию философского подхода к проблеме возникновения науки и основных стадий ее исторической эволюции.

3. Общая трудоемкость дисциплины составляет 5 зачетных единиц, 180 часов.

4. Содержание дисциплины:

Часть 1. Общие проблемы философии науки

1. Предмет и основные концепции современной философии науки.

Три аспекта бытия науки: наука как генерация нового знания, как социальный институт, как особая сфера культуры.

Логико-эпистемологический подход к исследованию науки. Позитивистская традиция в философии науки. Расширение поля философской проблематики в постпозитивистской философии науки**.** Концепции К.Поппера, И.Лакатоса, Т.Куна, П.Фейерабенда, М.Полани.

Социологический и культурологический подходы к исследованию развитии науки. Проблема интернализма и экстернализма в понимании механизмов научной деятельности. Концепции М.Вебера, А.Койре, Р.Мертона, М.Малкея.

2. Наука в культуре современной цивилизации

Традиционалистский и техногенный типы цивилизационного развития и их базисные ценности. Ценность научной рациональности.

Наука и философия. Наука и искусство. Роль науки в современном образовании и формировании личности. Функции науки в жизни общества (наука как мировоззрение, как производительная и социальная сила).

3. Возникновение науки и основные стадии её исторической эволюции.

Преднаука и наука в собственном смысле слова. Две стратегии порождения знаний: обобщение практического опыта и конструирование теоретических моделей, обеспечивающих выход за рамки наличных исторически сложившихся форм производства и обыденного опыта.

Культура античного полиса и становление первых форм теоретической науки. Античная логика и математика. Развитие логических норм научного мышления и организаций науки в средневековых университетах. Роль христианской теологии в изменении созерцательной позиции ученого: человек творец с маленькой буквы; манипуляция с природными объектами – алхимия, астрология, магия. Западная и восточная средневековая наука.

Становление опытной науки в новоевропейской культуре. Формирование идеалов математизированного и опытного знания: оксфордская школа, Роджер Бэкон, Уильям Оккам. Предпосылки возникновения экспериментального метода и его соединения с математическим описанием природы. Г.Галилей, Френсис Бэкон, Р.Декарт. Мировоззренческая роль науки в новоевропейской культуре. Социокультурные предпосылки возникновения экспериментального метода и его соединения с математическим описанием природы.

Формирование науки как профессиональной деятельности. Возникновение дисциплинарно-организованной науки. Технологические применения науки. Формирование технических наук.

Становление социальных и гуманитарных наук. Мировоззренческие основания социально-исторического исследования.

4. Структура научного знания.

Научное знание как сложная развивающаяся система. Многообразие типов научного знания. Эмпирический и теоретический уровни, критерии их различения. Особенности эмпирического и теоретического языка науки.

Структура эмпирического знания. Эксперимент и наблюдение. Случайные и систематические наблюдения. Применение естественных объектов в функции приборов в систематическом наблюдении. Данные наблюдения как тип эмпирического знания. Эмпирические зависимости и эмпирические факты. Процедуры формирования факта. Проблема теоретической нагруженности факта.

Структуры теоретического знания. Первичные теоретические модели и законы. Развитая теория. Теоретические модели как элемент внутренней организации теории. Ограниченность гипотетико-дедуктивной концепции теоретических знаний. Роль конструктивных методов в дедуктивном развертывании теории. Развертывание теории как процесса решения задач. Парадигмальные образцы решения задач в составе теории. Проблемы генезиса образцов. Математизация теоретического знания. Виды интерпретации математического аппарата теории.

Основания науки. Структура оснований. Идеалы и нормы исследования и их социокультурная размерность. Система идеалов и норм как схема метода деятельности.

Научная картина мира. Исторические формы научной картины мира. Функции научной картины мира (картина мира как онтология, как форма систематизации знания, как исследовательская программа).

Операциональные основания научной картины мира. Отношение онтологических постулатов науки к мировоззренческим доминантам культуры.

Философские основания науки. Роль философских идей и принципов в обосновании научного знания. Философские идеи как эвристика научного поиска. Философское обоснование как условие включения научных знаний в культуру.

5. Динамика науки как процесс порождения нового знания.

Историческая изменчивость механизмов порождения научного знания. Взаимодействие оснований науки и опыта как начальный этап становления новой дисциплины. Проблема классификации. Обратное воздействие эмпирических фактов на основания науки.

Формирование первичных теоретических моделей и законов. Роль аналогий в теоретическом поиске. Процедуры обоснования теоретических знаний. Взаимосвязь логики открытия и логики обоснования. Механизмы развития научных понятий.

Становление развитой научной теории. Классический и неклассический варианты формирования теории. Генезис образцов решения задач.

Проблемные ситуации в науке. Перерастание частных задач в проблемы. Развитие оснований науки под влиянием новых теорий.

Проблема включения новых теоретических представлений в культуру.

6. Научные традиции и научные революции. Типы научной рациональности.

Взаимодействие традиций и возникновение нового знания. Научные революции как перестройка оснований науки. Проблемы типологии научных революций. Внутридисципли-

нарные механизмы научных революций. Междисциплинарные взаимодействия и "парадигмальные прививки" как фактор революционных преобразований в науке. Социокультурные предпосылки глобальных научных революций. Перестройка оснований науки и изменение смыслов мировоззренческих универсалий культуры. Прогностическая роль философского знания. Философия как генерация категориальных структур, необходимых для освоения новых типов системных объектов.

Научные революции как точки бифуркации в развитии знания. Нелинейность роста знаний. Селективная роль культурных традиций в выборе стратегий научного развития. Проблема потенциально возможных историй науки.

Глобальные революции и типы научной рациональности. Историческая смена типов научной рациональности: классическая, неклассическая, постнеклассическая наука.

7. Особенности современного этапа развития науки. Перспективы научно-технического прогресса.

Главные характеристики современной, постнеклассической науки. Современные процессы дифференциации и интеграции наук. Связь дисциплинарных и проблемно-ориентированных исследований. Освоение саморазвивающихся "синергетических" систем и новые стратегии научного поиска. Роль нелинейной динамики и синергетики в развитии современных представлений об исторически развивающихся системах. Глобальный эволюционизм как синтез эволюционного и системного подходов. Глобальный эволюционизм и современная научная картина мира. Сближение идеалов естественнонаучного и социально-гуманитарного познания. Осмысление связей социальных и внутринаучных ценностей как условие современного развития науки. Включение социальных ценностей в процесс выбора стратегий исследовательской деятельности. Расширение этоса науки. Новые этические проблемы науки в конце XX столетия. Проблема гуманитарного контроля в науке и высоких технологиях. Экологическая и социально-гуманитарная экспертиза научно-технических проектов. Кризис идеала ценностно-нейтрального исследования и проблема идеалогизированной науки. Экологическая этика и ее философские основания. Философия русского космизма и учение В.И.Вернадского о биосфере, техносфере и ноосфере. Проблемы экологической этики в современной западной философии (Б.Калликот, О.Леопольд, Р.Аттфильд).

Постнеклассическая наука и изменение мировоззренческих установок техногенной цивилизации. Сциентизм и антисциентизм. Наука и паранаука. Поиск нового типа цивилизационного развития и новые функции науки в культуре. Научная рациональность и проблема диалога культур. Роль науки в преодолении современных глобальных кризисов.

8. Наука как социальный институт.

Различные подходы к определению социального института науки. Историческое развитие институциональных форм научной деятельности. Научные сообщества и их исторические типы (республика ученых 17 века; научные сообщества эпохи дисциплинарно организованной науки; формирование междисциплинарных сообществ науки XX столетия). Научные школы. Подготовка научных кадров. Историческое развитие способов трансляции научных знаний (от рукописных изданий до современного компьютера). Компьютеризация науки и ее социальные последствия. Наука и экономика. Наука и власть. Проблема секретности и закрытости научных исследований. Проблема государственного регулирования науки.

Часть 2. Философия техники и технических наук
Философские проблемы информатики

1. История становления информатики как междисциплинарного направления во второй половине XX века.

Теория информации К.Шеннона. Кибернетика Норберта Винера, Росса Эшби. Уорренга Мак-Каллока, Алана Тьюринга, Джулиана Бигелоу, Джона фон Неймана, Грегори

Бэйтсона, Маргарет Мид, Артуро Розенблюта,Уолтера Питтса, Стаффорда Бира. Общая теория систем Л.фон Берталанфи, А.Раппорта.

Концепция гипертекста Ваневара Буша. Конструктивная кибернетическая эпистемология Хайнца фон Ферстера и Валентина Турчина. Синергетический подход в информатике. Герман Хакен и Дмитрий Сергеевич Чернавский. Информатика в контексте постнеклассической науки и представлений о развивающихся человекомерных системах.

2. Информатика как междисциплинарная наука о функционировании и развитии информационно-коммуникативной среды и ее технологизации посредством компьютерной техники

Моделирование и вычислительный эксперимент как интеллектуальное ядро информатики. Конструктивная природа информатики и ее синергетический коэволюционный смысл. Взаимосвязь искусственного и естественного в информатике, нейрокомпьютинг, процессоры Хопфилда, Гроссберга, аналогия между мышлением и распознаванием образов.

Концепция информационной безопасности: гуманитарная составляющая. Проблема реальности в информатике. Виртуальная реальность. Понятие информационно-коммуникативной реальности как междисциплинарный интегративный концепт.

3. Интернет как метафора глобального мозга

Понятие киберпространства ИНТЕРНЕТ и его философское значение. Синергетическая парадигма «порядка и хаоса» в ИНТЕРНЕТ. Наблюдаемость, фрактальность, диалог. Феномен зависимости от Интернета. Интернет как инструмент новых социальных технологий.

Интернет как информационно-коммуникативная среда науки 21 века и как глобальная среда непрерывного образования.

4. Эпистемологическое содержание компьютерной революции

Концепция информационной эпистемологии и ее связь с кибернетической эпистемологией. Компьютерная этика, инженерия знаний проблемы интеллектуальной собственности. Технологический подход к исследованию знания. Проблема искусственного интеллекта и ее эволюция.

5. Социальная информатика

Концепция информационного общества: от Питирима Сорокина до Эмануэля Кастельса. Происхождение информационных обществ. Синергетический подход к проблемам социальной информатики. Информационная динамика организаций в обществе. Сетевое общество и задачи социальной информатики. Проблема личности в информационном обществе. Современные психотехнологии и психотерапевтические практики консультирования как составная часть современной социогуманитарной информатики.

Часть 3. История науки
История информатики

1.Методологические и дидактические принципы изучения истории информатики

1.1 Цели и задачи изучения истории информатики. Место истории информатики в системе вузовского и послевузовского преподавания, в системе необходимых профессиональных знаний. Современное понимание разделения знания на учебное и научное. Историзм как необходимый компонент современной культуры мышления; история информатики как основа новой информационной культуры. Современное вероятностное понимание истории. Логика истории информатики, логика ее восприятия и принципы научной оценки истории.

1.2. Предмет и методы истории информатики. Межпредметный характер информатики и его проявления в истории информатики. Многозначность понимания социальной истории информатики. Неполнота когнитивной истории информатики. Основные методы в ис-

следованиях по истории информатики. Новые информационно-коммуникационные технологии и перспективы истории информатики. Этические проблемы исследований по истории информатики.

1.3. Источниковая база истории информатики. Структура и характеристики традиционных источников. Возможности и пределы конструирования новых (модельных, в том числе виртуальных) видов источников. Основные правила и ограничения идентификации и интерпретации источников по истории информатики.

1.4. Принципы оценки и самооценки уровня понимания истории информатики. Структура и содержание тестово-контрольного блока по истории информатики. Темы возможных рефератов, докладов, самостоятельных работ. Музеи, историко-научные центры, интернет-ресурсы истории информатики.

2. Информатика в системе наук. Историческое осмысление

2.1. Понятие «информатика». Дефиниции понятия «информатика» как в России, так и за рубежом в историческом аспекте. Предмет информатики. Роль зарубежных и отечественных ученых в становлении информатики как науки в современном ее представлении. Место и роль вычислительной техники, средств связи и другой оргтехники в развитии информатики как науки.

2.2. «Информация» как базовое понятие информатики. Историческое развитие определений понятия «информация». Современное представление об информации. Виды информации. Общие свойства информации. Методы оценки информации: качественные и количественные. Жизненный цикл информации. Кодирование информации.

2.3. Место информатики как науки в ряду других наук. История становления теоретических основ информатики.

Семиотические основания информатики: «знак», «знаковая система», естественные и искусственные знаковые системы; естественный язык и искусственный язык как знаковые системы, синтактика, семантика и прагматика знаковых систем; проблема значения и означаемого; проблема коммуникации знаковых систем.

Математические основания информатики: вычислительная математика, дискретная математика, математическая логика, теория вероятности; проблема представления в ЭВМ числовой и символьной информации и процессов ее преобразования.

Лингвистические основания информатики: современная лингвистическая парадигма, структуризация естественно-языковых конструкций, модели текстов на естественном языке; проблема представления текстов на естественном языке в ЭВМ.

Когнитивно-психологические основания информатики: системность мышления, современные модели организации памяти, модели восприятия информации, модели понимания.

Теория систем: понятие «система», структуры систем, свойства систем, системная совместимость, системный подход, системный анализ.

Искусственный интеллект: искусственные языки, развитие языков программирования; проблема понимания человека и компьютера, проблема решения интеллектуальных задач, проблема понимания и генерация текстов на естественном языке.

2.4. Формирование современного понятийного аппарата информатики: информационные ресурсы, информационные системы, информационные технологии, базы данных, хранилища данных, базы знаний. Современные информационные технологии: операционные системы, системы редактирования текстов и таблиц, системы управления базами данных, локальные и глобальные информационно-вычислительные сети, экспертные системы, case-технологии. Основные научно-технические и гуманитарные проблемы информатики. Перспективы развития информатики.

3. Информационное общество — история концепции и становления

3.1. Изменение понимания роли информации в обществе. Явление «информационного взрыва». Индустриальное и постиндустриальное общество. Понятие информационного общества. Признаки информационного общества. Основные характеристики информационного

общества. Причины и условия возникновения информационного общества. Информационная потребность. Человек в информационном пространстве.

3.2. Основные этапы информатизации общества. Влияние информатики на развитие наук и материального производства. Понятие «информатизация общества». Этапы информатизации. Общественный прогресс и новые реалии информационного общества. Понятие: «национальный информационный потенциал».

3.3. Историческая оценка становления мирового информационного рынка. Понятие информационного рынка. Основные участники информационного рынка. Понятие информационного продукта и информационной услуги. Классификация информационных продуктов и услуг. Жизненный цикл информационного продукта. Отечественные и зарубежные рынки информационных продуктов. Основные тенденции мирового информационного рынка информационных технологий: стандартизация, ликвидация промежуточных звеньев, глобализация, конвергенция.

3.4. Основные закономерности становления современного информационного пространства и его институтов. Понятие «информационное пространство». Основные объекты и субъекты информационного пространства. ИНТЕРНЕТ как составная часть мирового информационного пространства. Национальные концепции вхождения в мировое информационное общество.

4. Информационная безопасность — история проблемы и ее решение

4.1. Антиобщественные аспекты и формы использования информации: информационные агрессии, информационные войны, информационный голод, дезинформация, утечка и уничтожение информации. Социальные последствия антиобщественных форм использования информации. Формирование информационной этики.

4.2. Психологические проблемы взаимодействия человека и современной информационной среды. Человек в информационном пространстве. Здоровье нации в информационном пространстве. Методы психологический защиты человека в информационной среде.

4.3. Правовые проблемы информатизации. Информационное право.

Проблемы правового регулирования интеллектуальной собственности. Законодательные и нормативные акты (государственные и международные), направленные против хищения информационных ресурсов и продуктов. Законодательные акты по легализации и защите электронных документов. Государственная политика в области защиты информационных ресурсов общества. Международный обмен информацией. Международное сотрудничество в области защиты интеллектуальной собственности.

5. Информатика и образование — историзм и современность

5.1. Информатика как предмет обучения. Уровни и модели образования в области информатики в России и за рубежом. Основные квалификации специалистов в области информатики. Объекты профессиональной деятельности специалистов в области информатики различных квалификаций и уровней подготовки: вычислительные машины, сети и системы коммуникаций; информационные и функциональные процессы, которые определяются спецификой предметной области; новые направления деятельности и области применения средств информатизации. Государственные образовательные стандарты по подготовке специалистов в области информатики, их роль и значение для подготовки специалистов в области информатики. Перечень и характеристика вузовских специальностей и специальностей послевузовского обучения. Виды и задачи профессиональной подготовки. Квалификационные требования к подготовке информатиков. Общие требования к образовательным программам по специальностям в области информатики.

5.2. Информатика как метод обучения. Информационные технологии в обучении: дистанционное образование, автоматизированные обучающие системы, образовательные мультимедиа технологии. Цели и задачи дистанционного образования; классификация форм дистанционного обучения; методы организации; информационное и документационное обеспечение; сетевые технологии в дистанционном обучении; использование Internet-технологий в

образовании; методы текущего и итогового контроля с использованием компьютерных технологий; оценка качества дистанционных систем обучения. Назначение автоматизированных обучающих систем, история возникновения, типы используемых автоматизированных обучающих систем, их классификация и перспективы использования.

6. История доэлектронной информатики

Механические и электромеханические устройства и машины.

6.1. Аналитическая машина Ч. Бэбиджа (1837) и первая машинная программа А.

6.2. Аналоговая вычислительная техника. Дифференциальные анализаторы А. Н. Крылова (1911) и В. Буша (1931). Гидроинтегратор В. С. Лукьянова (1936).

6.3. Алгебра логики (Дж. Буль, 1947). Логические машины У. Джевонса (1869), П. Д. Хрущева (ок. 1900) и А. Н. Щукарева (1911).

6.4. Доказательство возможностей и первые результаты в области анализа и синтеза релейных схем на основе алгебры логики в независимых исследованиях (ок. 1938) Кл. Шеннона, В. А. Розенберга. Последующие исследования и результаты, полученные М. А. Гавриловым.

6.5. Формализация понятия «алгоритм». Абстрактная машина Тьюринга (1936).

6.6. Программно-управляемые ЦВМ на электромеханических реле: Ц-3 (1941) К. Цузе, МАРК-1 (1944) Г. Айкена, машины серии «Белл» Дж. Стибица. Первый эксперимент по автоматическому выполнению вычислений на больших расстояниях (между штатами Нью-Йорк — Нью-Гемпшир, 1940).

7. Зарождение электронной информатики.

7.1. Технические и социальные предпосылки. Изобретение лампового триггера (М. А. Бонч-Бруевич, 1918). Электронные счетчики импульсов. Рост объемов необходимых вычислений в научно-исследовательских и опытно-конструкторских работах.

7.2. Первые проекты ЭВМ. Работающая модель машины Атанасова-Берри (1939) и постройка опытного образца (1939–1942). Памятная записка Г. Шрейера (1939) и постройка арифметического устройства (1942) Г. Шрейром и К. Цузе. Машины «Колосс» (1943) и «Колосс Марк-2» (1944). Памятная записка Дж. Маучли (1942) и постройка ЭНИАК (1943–1945).

7.3. Концепция машины с хранимой программой Дж. Неймана (1946).

7.4. Первые несерийные ЭВМ с хранимой программой. Британские машины МАРК-1 (1948) и ЭДСАК (1949); проект АКЕ (А. Тьюринг). США: работы над проектами ЭДВАК и ИАС с участием Дж. Фон Неймана и их влияние на развитие ЭВМ; машины СЕАК, БИНАК, ЭРА-1101, «Вихрь» (1950). СССР: независимое развитие и сходные результаты. Роль С. А. Лебедева. Машины МЭСМ (1951) и БЭСМ (1952). И. С. Брук. Машины М-1 (1951) и М-2 (1952).

7.5. Зарождение программирования. Программирование на языке машины и символьных обозначениях. Метод библиотечных подпрограмм (М. Уилкс, 1951). Планкалькюль К. Цузе (1945) Операторный метод программирования (1952–1953, А. А. Ляпунов). Концепция крупноблочного программирования (1953–1954, Л. В. Канторович).

8. Развитие ЭВМ, проблемного и системного программирования

8.1. Поколение ЭВМ. Обоснование критерия периодизации. Поколения: 1-е (50-е гг.), 2-е (первая половина 60-х гг.), 3-е (вторая половина 60-х гг.– первая половина 70-х гг.), 4-е (вторая половина 70-х гг. – 80-е гг.), 5-е (90-е и 2000-е гг.). Характеристика поколений по схеме: технические параметры, классы машин и сфера их применения, языки программирования и математическое обеспечение ЭВМ, архитектурные особенности, элементная база, парк ЭВМ. Особенности смены поколений и развития электронной вычислительной техники в России.

8.2. Проекты ЭВМ исторического значения — международного и национального. Гамма-60, Франция (1959), Стретч, США (1961), Атлас, Великобритания (1962), СДС-6600, США (1964), БЭСМ-6, СССР (1967), ИБМ-360, США (1965–1969), Иллиак-4, США (1972), Крей, США (1976), Японский проект ЭВМ пятого поколения (1980).

8.3. Тенденции и закономерности развития. Эволюция технических и технико-экономических характеристик ЭВМ. Тенденции в области проблемного и системного программирования, архитектуры и структуры ЭВМ. Некоторые общие закономерности развития средств переработки информации.

9. Формирование и развитие индустрии средств переработки информации

9.1. Машины и программы — составные части конечного продукта информационной индустрии. Эволюция пропорций.

9.2. Мировая информационная индустрия. Изменения на протяжении 50–90-х гг.

10. Развитие технологических основ информатики

10.1. Миниатюризация элементов на протяжении всей истории вычислительной техники — от первых счетных приборов до современных ЭВМ.

10.2. Полупроводниковые интегральные схемы — технологическая основа развития информатики с 1965 г. до наших дней. Закон Мура. Ограниченность спектра возможностей любых средств повышения эффективности (программных, структурных, сетевых, с помощью интеллектуальных моделей и т.п.) по сравнению с возможностями, обусловленными интеграцией полупроводниковых схем.

10.3. Первое десятилетие XXI в. Возможности технологии интегральных схем и проекты в области информатики, находящейся в стадии реализации.

11. Формирование и эволюция информационно-вычислительных сетей

11.1. Смена наиболее динамично развивающихся направлений в области сетей.

11.2. Многомашинные территориальные комплексы для решения специальных крупномасштабных задач (противовоздушная оборона, космические полеты и т.п.) и рационального использования вычислительных ресурсов. Система ПВО Североамериканского континента «Сейдж».

11.3. Идея разделения времени (К. Стрейчи, 1959).

Концепция всеобщего информационно-вычислительного обслуживания (Дж. Маккарти, 1961). Проект МАК (1963).

Работа в диалоговом режиме и графоаналитическое взаимодействие человека с машиной.

11.4. Первые универсальные информационно-вычислительные сети: Марк II (1968), Инфонет (1970), Тимнет (1970). Сеть Арпанет (1971).

11.5. Развитие специализированных сетей.

Информационно-вычислительные сети в СССР. Проект Государственной сети вычислительных центров (В. М. Глушков, 1963). Формирование ГСВЦ.

Локальные вычислительные сети.

11.6. Интернет, «всемирная паутина», и процессы глобализации.

12. Искусственный интеллект: научный поиск и проектно-технологические решения.

12.1. Первые исследования и первые машинные программы решения интеллектуальных задач. Машинный перевод. Джорджтаунский эксперимент (1954). Исследования в СССР (А. А. Ляпунов, Ю. Д. Апресян, О. С. Кулагина и др.). Доказательство теорем. Метод резолюций (Дж. Робинсон, 1965) и обратный метод Ю. С. Маслова (1967). Эвристическое программирование. Распознавание образов. Персептрон (Ф. Розенблатт, 1957). Игровые программы: идеи Кл. Шеннона (1947), метод граней и оценок (А. Брудно), программа М. М. Ботвинника «Пионер». Сочинение музыки и текстов. «Иллиак-сюита» (Л. Хиллер и Л, Айзексон, 1955). Исследования Р. Х. Зарипова.

12.2. Формирование общих подходов к решению интеллектуальных задач. Лабиринтная модель и Универсальный решатель задач А. Ньюэлла и Г. Саймона (1959). Реляционная модель и ситуационное управление (Д. А. Поспелов и В. Н. Пушкин). Информационный (феноменологическое моделирование) и бионический (структурное моделирование) подходы к решению интеллектуальных задач.

12.3. Развитие теории и практики искусственного интеллекта. Теория представления знаний фреймы (М. Минский, 1974), сценарии (Р. Шенк), продукционные системы, семантические

сети. Теория вопросно-ответных и диалоговых систем. Развитие практического применения: интеллектуальные пакеты прикладных программ, расчетно-логические, обучающие системы (тьюторы), экспертные системы.

5. **Форма промежуточной аттестации:** кандидатский экзамен.

Аннотация дисциплины
«Иностранный язык»

Направление 10.06.01 Информационная безопасность
Направленность (профиль) «Методы и системы защиты информации, информационная безопасность»

1. Дисциплина «Иностранный язык» относится к базовой части блока Б1.

2. Целью освоения дисциплины «Иностранный язык» является формирование у аспирантов необходимого для сдачи кандидатского экзамена уровня знаний, умений и навыков в области чтения, говорения, аудирования, перевода, аннотирования, реферирования и письма.

3. Общая трудоемкость дисциплины составляет 4 зачетных единиц, 144 часа.

4. Содержание дисциплины:

1. Виды речевой коммуникации

1.1.Говорение. Аспирант должен владеть подготовленной, а также неподготовленной монологической речью, уметь делать резюме, сообщения, доклад на иностранном языке; диалогической речью в ситуациях научного, профессионального и бытового общения в пределах изученного языкового материала и в соответствии с избранной специальностью.

1.2.Аудирование. Аспирант должен уметь понимать на слух оригинальную монологическую и диалогическую речь по специальности, опираясь на изученный языковой материал, фоновые страноведческие и профессиональные знания, навыки языковой и контекстуальной догадки.

1.3.Чтение. Аспирант должен уметь читать, понимать и использовать в своей научной работе оригинальную научную литературу по специальности, опираясь на изученный языковой материал, фоновые страноведческие и профессиональные знания и навыки языковой и контекстуальной догадки. Владеть всеми видами чтения (изучающее, ознакомительное, поисковое и просмотровое).

1.4.Письмо. Аспирант должен владеть умениями письма в пределах изученного языкового материала, в частности уметь составить план (конспект) прочитанного, изложить содержание прочитанного в форме резюме; написать сообщение или доклад по темам проводимого исследования.

2. Языковой материал

2.1. Виды речевых действий и приемы ведения общения

При отборе конкретного языкового материала необходимо руководствоваться следующими функциональными категориями:

Передача фактуалъной информации: средства оформления повествования, описания, рассуждения, уточнения, коррекции услышанного или прочитанного, определения темы сообщения, доклада и т.д.

Передача эмоциональной оценки сообщения: средства выражения одобрения/неодобрения, удивления, восхищения, предпочтения и т.д.

Передача интеллектуальных отношений: средства выражения согласия/несогласия, способности/неспособности сделать что-либо, выяснение возможности/невозможности сделать что-либо, уверенности/неуверенности говорящего в сообщаемых им фактах.

Структурирование дискурса: оформление введения в тему, развитие темы, смена темы, подведение итогов сообщения, инициирование и завершение разговора, приветствие, выражение благодарности, разочарования и т.д.;

владение основными формулами этикета при ведении диалога, научной дискуссии, при построении сообщения и т.д.

2.2. Фонетика

Интонационное оформление предложения: словесное, фразовое и логическое ударения, мелодия, паузация; фонологические противопоставления, релевантные для изучаемого языка: долгота/краткость, закрытость/открытость гласных звуков, звонкость/глухость конечных согласных и т.п.

2.3. Лексика

Лексический запас сдающего кандидатский экзамен должен составить не менее 5500 лексических единиц с учетом вузовского минимума и потенциального словаря, включая примерно 500 терминов профилирующей специальности.

2.4. Грамматика

Английский язык

Порядок слов простого предложения. Сложное предложение: сложносочиненное и сложноподчиненное предложения. Союзы и относительные местоимения. Эллиптические предложения. Бессоюзные придаточные. Употребление личных форм глагола в активном и пассивном залогах. Согласование времен. Функции инфинитива: инфинитив в функции подлежащего, определения, обстоятельства. Синтаксические конструкции: оборот «дополнение с инфинитивом» (объектный падеж с инфинитивом); оборот «подлежащее с инфинитивом» (именительный падеж с инфинитивом); инфинитив в функции вводного члена; инфинитив в составном именном сказуемом *(be + инф.)* и в составном модальном сказуемом; (оборот *«for + smb. To do smth..»*), Сослагательное наклонение. Модальные глаголы. Модальные глаголы с простым и перфектным инфинитивом. Атрибутивные комплексы (цепочки существительных). Эмфатические (в том числе инверсионные) конструкции в форме *Continuous* или пассива; инвертированное придаточное уступительное или причины; двойное отрицание. Местоимения, слова-заместители *(that (of),those (of), this, these, do, one, ones),* сложные и парные союзы, сравнительно-сопоставительные обороты (as…as, not so…as, the…the*).*

Французский язык

Порядок слов простого предложения. Сложное предложение: сложносочиненное и сложноподчиненное предложения. Союзы. Употребление личных форм глаголов в активном залоге. Согласование времен. Пассивная форма глагола. Возвратные глаголы в значении пассивной формы. Безличные конструкции. Конструкции с инфинитивом: *avoir à + infinitif, être à + infinitif, laisser + infinitf, faire + infinitif.* Неличные формы глагола: инфинитив настоящего и прошедшего времени; инфинитив, употребляемый с предлогами; инфинитивный оборот. Причастие настоящего времени; причастие прошедшего времени; деепричастие; сложное причастие прошедшего времени. Абсолютный причастный оборот. Условное наклонение. Сослагательное наклонение. Степени сравнения прилагательных и наречий. Местоимения: личные, относительные, указательные; местоимение среднего рода *1e,* местоимения-наречия *en и y.*

Немецкий язык

Простые распространенные, сложносочиненные и сложноподчиненные предложения. Рамочная конструкция и отступления от нее. Место и порядок слов придаточных предложений. Союзы и корреляты. Бессоюзные придаточные предложения. Распространенное определение. Причастие I с *zu* в функции определения. Приложение. Степени сравнения прилагательных. Указательные местоимения в функции замены существительного. Однородные члены предложения разного типа. Инфинитивные и причастные обороты в различных функциях. Модальные конструкции *sein* и *haben* + *zu* + infinitiv. Модальные глаголы с инфинитивом I и II актива и пассива. Конъюнктив и кондиционалис в различных типах предложений. Футурум I и II в модальном значении. Модальные слова. Функции пассива и конструкции *sein* + *Partizip II* (статива). Трехчленный, двучленный и одночленный (безличный пассив). Сочетания с послелогами, предлогами с уточнителями. Многозначность и синонимия союзов, пред-

логов, местоимений, местоименных наречий и т.д. Коммуникативное членение предложения и способы его выражения.

5. **Форма промежуточной аттестации:** кандидатский экзамен.

Аннотация дисциплины
«Педагогика и психология высшей школы»

Направление 10.06.01 Информационная безопасность
Направленность (профиль) «Методы и системы защиты информации, информационная безопасность»

1. Дисциплина «Педагогика и психология высшей школы» относится к обязательным дисциплинам вариативной части блока Б1.

2. Основной целью освоения дисциплины «Педагогика и психология высшей школы» является подготовка к преподавательской деятельности, в том числе:

- формирование представлений об особенностях педагогической деятельности в высшей школе;
- приобретение знаний по педагогике и психологии высшей школы: формирование мотивации учения, управление познавательной деятельностью обучающихся.
- изучение общих принципов организации учебного процесса в высшей школе.

3. Общая трудоемкость дисциплины составляет 3 зачетных единиц, 108 часов.

4. Содержание дисциплины:

Тема 1: Цели и задачи высшей школы на современном этапе.

Тенденции развития современного высшего образования в России.

Подходы к определению целей образования: обучение как формирование опыта; обучение как формирование личности профессионала.

Модель личности профессионала: профессиональная направленность, профессиональный опыт, профессионально-важные качества, индивидуальный стиль деятельности. Этапы формирования профессионала, цели и задачи работы на каждом этапе. Классификация методов обучения и воспитания в вузе.

Нормативное обеспечение образовательного процесса в высшей школе. Федеральный государственный образовательный стандарт: его структура и содержание.

Тема 2: Технология знаково-контекстного подхода А.А.Вербицкого.

Учебная деятельность. Противоречия учебной и профессиональной деятельности. Контекстное обучение. Информация и знание. Основные принципы контекстного обучения. Модель динамического движения деятельности в контекстном обучении. Два этапа и три вида учебной деятельности: учебная деятельность академического типа, квазипрофессиональная деятельность, учебно-профессиональная деятельность. Педагогические технологии контекстного обучения. Активные методы обучения: обмен вопросами в малых группах, анализ ситуаций профессиональной деятельности, кейс-метод, деловые игры, разработка проектов и мини-проектов, взаимодействие подгрупп с раной ролевой определенностью, дискуссии, демонстрации с привлечением студентов, социально-психологический тренинг.

*Тема 3: Мотивы учения***.**

Структура учебной деятельности. Концепции мотивации учебной деятельности. Виды мотивов учения: познавательные и социальные мотивы. Формирование мотивов учения. Мотивация на изучение предмета, мотивация на выполнение отдельных заданий. Методические приемы: связь с практикой, ориентация на успех, принцип выбора заданий, связь с другими областями знаний, разъяснение учебных целей, личностная и профессиональная значимость целей, использование активных методов обучения, методическое разнообразие.

Тема 4: Психолого-педагогические аспекты организации учебной деятельности студентов.

Лекция как форма учебной деятельности в высшей школе. Виды лекций. Лекторское

мастерство. Условия превращения лекции в интерактивную. Имидж преподавателя. Практические занятия. Формы проведения семинаров. Психолого-педагогические цели семинарских занятий. Семинар рефератов. Семинар по типу круглого стола. Психологические контакты с аудиторией: личностный, эмоциональный, познавательный контакт. Психологические барьеры, условия преодоления барьеров. Учет познавательных возможностей слушателей. Управление вниманием аудитории. Восприятие и понимание учебного материала. Организация запоминания. Развитие мышления студентов. Организация самостоятельной работы студентов: формы и методы. Формы контроля. Понятие фонда оценочных средств и его разработка. Виды оценочных средств. Проведение зачетов и экзаменов.

Тема 5: Воспитательная работа

Роль воспитательной работы со студентами. Психологическая характеристика студенчества как социальной группы: ценностные ориентации, интересы, профессиональные планы. Возрастно-психологические особенности студентов. Психологические характеристики студенческой группы.

Тема 6: Учебно-методическая работа в ВУЗе

Методическое обеспечение учебного процесса в ВУЗе. Основная образовательная программа и ее структура. Учебный план. Рабочая программа дисциплины и ее содержание. Проектирование и разработка рабочих программ дисциплин. Технологии анализа учебного занятия. Методика разработки учебных занятий.

Тема 7: На итоговой консультации разбираются выполненные аспирантами задания для самостоятельной работы по темам дисциплины (в том числе и тест для самопроверки по дисциплине), преподаватель отвечает на вопросы аспирантов.

5. **Форма промежуточной аттестации:** зачет.

Аннотация дисциплины
«Электронное обучение и дистанционные образовательные технологии»

Направление 10.06.01 Информационная безопасность
Направленность (профиль) «Методы и системы защиты информации, информационная безопасность»

1. Дисциплина «Электронное обучение и дистанционные образовательные технологии» относится к обязательным дисциплинам вариативной части блока Б1.

2. **Цели освоения дисциплины**
   Ознакомление с компьютерными методами формирования информационно-образовательной среды и применением электронного обучения и дистанционных технологий

3. Общая трудоемкость дисциплины составляет 3 зачетные единицы, 108 часов.

4. Содержание дисциплины:

1. Информационно-образовательная среда учебного процесса. Формирование понятия электронной информационно-образовательной среды. Применяемые модели. Информационно-образовательное пространство, построенное с помощью интеграции информации на традиционных и электронных носителях, компьютерно-телекоммуникационных технологиях взаимодействия, включающее в себя виртуальные библиотеки, распределенные базы данных, учебно-методические комплексы и расширенный аппарат дидактических подходов
2. Компьютерные технологии в образовательном процессе. Применения компьютерных технологий в образовательном процессе. Компьютерное тестирование. Информационное обеспечение и иллюстративная поддержка образовательного процесса. Электронные обучающие системы. Виртуальный практикум
3. Электронный учебный контент: жанры. Курсы для ВУЗовского образования. Корпоративные курсы. Курсы для поддержки очных и.заочных тренингов.Курсы широкого профиля для коммерческой продажи. Курсы от вендоров («Основы фотошопа») и др.
4. Структура электронной обучающей системы. Структура электронной обучающей системы. Современное состояние электронных обучающих комплексов. Параметры, определяющие качество системы. Примеры реализации.
5. Виртуальный практикум. Виртуальный практикум. Компьютерные симуляторы. Примеры реализации.
6. Структура применения современной электронной обучающей системы. Структура применения современной электронной обучающей системы. Обучающая траектория. Методическое сопровождение.
7. Разработка электронного ресурса. Разработка электронного ресурса. Подходы и среды. Состав команды. Оформление. Создание и применение отдельных компонентов. Создание гипертекстовых документов. Специализированные среды.
8. Специализированные среды. Moodle. WebTutor. Moodle – модулярная объектно-ориентированная динамическая обучающая среда. Участники образовательного процесса. Порог доступности для различных групп. Виды ресурсов теоретической части курса. Виды ресурсов практической части. Доступ к системе. Разработка использование образовательных ресурсов в среде Moodle. WebTutor – возможности применения.

5. **Форма промежуточной аттестации:** зачет.

Аннотация дисциплины
«Методы и системы защиты информации, информационная безопасность»

Направление 10.06.01 Информационная безопасность
Направленность (профиль) «Методы и системы защиты информации, информационная безопасность»

1. Дисциплина «Методы и системы защиты информации, информационная безопасность» относится к обязательным дисциплинам вариативной части блока Б1.

2. Дисциплина «Методы и системы защиты информации, информационная безопасность» обеспечивает приобретение фундаментальных и профессиональных знаний, умений и навыков, содействует дальнейшей фундаментализации образования, развитию логического мышления и формированию математического и общенаучного мировоззрения. Целью изучения дисциплины является овладение базовыми понятиями и методами в области защиты информации, прежде всего криптографическими методами, овладение современным математическим аппаратом, используемым в криптографии для дальнейшего использования в приложениях.

3. Общая трудоемкость дисциплины составляет 6 зачетных единиц, 216 часов.

4. Содержание дисциплины:

1. Методы и системы защиты информации

1.1.Законодательные и правовые основы защиты компьютерной информации информационных технологий.

Безопасность информационных ресурсов и документирование информации; государственные информационные ресурсы;
персональные данные о гражданах; права на доступ к информации;
разработка и производство информационных систем;
вычислительные сети и защита информации;
нормативно-правовая база функционирования систем защиты информации; компьютерные преступления и особенности их расследования;
российское законодательство по защите информационных технологий;
промышленный шпионаж и законодательство, правовая защита программного обеспечения авторским правом.

1.2.Проблемы защиты информации в информационных системах.

Меры по обеспечению сохранности информации и угрозы ее безопасности в информационных системах;
основные задачи обеспечения безопасности информации в информационных системах; защита локальных сетей и операционных систем;
интеграция систем защиты;
Internet в структуре информационно-аналитического обеспечения информационных систем;
рекомендации по защите информации в Internet.

1.3.Содержание системы средств защиты компьютерной информации в информационных системах.

Защищенная информационная система и система защиты информации;
принципы построения систем защиты информации и их основы;
законодательная, нормативно-методическая и научная база системы защиты информации;
требования к содержанию нормативно-методических документов по защите информации;
научно-методологический базис, стратегическая направленность и инструментальный базис

защиты информации;
структура и задачи (типовой перечень) органов, выполняющих защиту информации;
организационно-правовой статус службы информационной безопасности; организационно-технические и режимные меры;
политика безопасности: организация секретного делопроизводства и мероприятий по защите информации;
программно-технические методы и средства защиты информации; программно-аппаратные методы и средства ограничения доступа к компонентам компьютера;
типы несанкционированного доступа и условия работы средств защиты;
вариант защиты от локального несанкционированного доступа и от удаленного ИСД;
средства защиты, управляемые модемом, надежность средств защиты.

2 . Информационная безопасность

2.1.Изучение традиционных симметричных криптосистем.

Основные этапы становления криптографии.

Теоретические основы криптографии: основные понятия и определения; общее понятие шифра, алгебраическая и вероятностная модели шифра; простейшие исторические шифры и их криптоанализ; основные классы шифров и их свойства: шифры перестановки и шифры замены; шифр перестановки «скитала»; шифрующие таблицы; применение магических квадратов; шифры простой замены; полибианский квадрат; система шифрования Цезаря; система шифрования Вижинера; шифр «двойной квадрат» Уитстона; одноразовая система шифрования; шифрование методом Вернама; роторные машины; шифрование методом гаммирования; методы генерации псевдослучайных последовательностей чисел.

2.2.Применение симметричных криптосистем для защиты компьютерной информации в информационных системах.

Блочные системы шифрования: изучение американских стандартов шифрования данных DES и AES;

основные режимы работы алгоритмов DES и AES;

отечественные стандарты шифрования данных ГОСТ 28147-89 и ГОСТ Р 34.12-2015;

режимы работы блочных шифров ГОСТ Р 34.13-2015: режим простой замены; режим гаммирования; режим гаммирования с обратной связью; режим выработки имитовставки;

сравнение блочных и поточных шифров; надежность шифров.

2.3.Применение ассиметричных криптосистем для защиты компьютерной информации в информационных системах.

Концепция криптосистемы с открытым ключом;
однонаправленные функции;
системы шифрования с открытым ключом: криптосистема шифрования данных RSA (процедуры шифрования и расшифрования в этой системе); безопасность и быстродействие криптосистемы RSA;
схема шифрования Полига-Хеллмана;
схема шифрования Эль-Гамаля, комбинированный метод шифрования.

2.4.Методы идентификации и проверки подлинности пользователей компьютерных систем.

Основные понятия и концепции;
идентификация и механизмы подтверждения подлинности пользователя;
взаимная проверка подлинности пользователей;
протоколы идентификации с нулевой передачей знаний; упрощенная схема идентификации с нулевой передачей знаний;
проблема аутентификации данных и электронная цифровая подпись;
однонаправленные хэш-функции; алгоритм безопасного дешифрования SHA; однонаправленные хэш-функции на основе симметричных блочных алгоритмов; отечественный стандарт хэш-функции ГОСТ Р 34.11-2012;
алгоритм цифровой подписи RSA;

алгоритм цифровой подписи Эль Гамаля (EGSA); алгоритм цифровой подписи DSA; отечественные стандарты цифровой подписи ГОСТ Р 34.10-94 и ГОСТ Р 34.10-2012; протоколы распределения ключей.

2.5.Защита компьютерных систем от удаленных атак через сеть Internet.

Режим функционирования межсетевых экранов и их основные компоненты; маршрутизаторы; шлюзы сетевого уровня; усиленная аутентификация;
основные схемы сетевой защиты на базе межсетевых экранов;
применение межсетевых экранов для организации виртуальных корпоративных сетей; программные методы защиты.

2.6.Изучение существующих аппаратно-программных средств криптографической защиты компьютерной информации серии КРИПТОН.

Основные элементы средств защиты сети от несанкционированного доступа; устройства криптографической защиты данных;
контроллер смарт-карт SCAT-200;
программно-аппаратная система защиты от НСД КРИПТОН-ВЕТО;
защита от НСД со стороны сети абонентское шифрование и ЭЦП;
шифрование пакетов, аутентификация, защита компонентов ЛВС от НСД;
защита абонентского пункта, маршрутизаторов и устройств контроля;
технология работы с ключами.

2.7.Методы защита программ от изучения и разрушающих программных воздействий (программных закладок и вирусов).

Классификация способов защиты;
защита от отладок и дизассемблирования;
способы встраивания защитных механизмов в программное обеспечение;
понятие разрушающего программного воздействия;
модели взаимодействия прикладной программы и программной закладки;
методы перехвата и навязывания информации;
методы внедрения программных закладок;
компьютерные вирусы как особый класс разрушающих программных воздействий; защита от РПВ; понятие изолированной программной среды.

2.8.Комплексная защита процесса обработки информации в компьютерных системах на основе стохастической интеллектуальной информационной технологии.

Возможности СИИТ для обеспечения комплексной
защиты программ в момент их выполнения и данных при их обработке в компьютере; метод верификации программного обеспечения для контроля корректности, реализуемости и защиты от закладок;
разработка транслятора исходного текста программ, обеспечивающего их защиту на логическом (алгоритмическом) и физическом уровне от НСД, программных закладок и вирусов;
метод защиты от НСД и разрушающих программных воздействий процесса хранения, обработки информации;
защита арифметических вычислений в компьютерных системах;
основные направления создания защищенных компьютерных систем нового поколения на основе СИИТ.

5. **Форма промежуточной аттестации:** кандидатский экзамен.

Аннотация дисциплины
«Математические модели для информационной безопасности»

Направление 10.06.01 Информационная безопасность
Направленность (профиль) «Методы и системы защиты информации, информационная безопасность»

1. Дисциплина «Математические модели для информационной безопасности» относится к дисциплинам по выбору вариативной части блока Б1.

2. Дисциплина «Математические модели для информационной безопасности» обеспечивает приобретение фундаментальных и профессиональных знаний, умений и навыков, содействует дальнейшей фундаментализации образования, развитию логического мышления и формированию математического и общенаучного мировоззрения. Целью изучения дисциплины является освоение современных подходов к построению и исследованию математических моделей систем обеспечения информационной безопасности компьютерных систем с последующим математическим доказательством их соответствия выбранной политике обеспечения информационной безопасности.

3. Общая трудоемкость дисциплины составляет 3 зачетные единицы, 108 часов.

4. Содержание дисциплины:

Тема 1. Основные понятия и определения, используемые при описании моделей безопасности компьютерных систем.

Элементы теории компьютерной безопасности. Сущность, субъект, доступ, информационный поток.

Классификация угроз безопасности информации.

Виды информационных потоков.

Виды политик управления доступом и информационными потоками.

Утечка права доступа и нарушение безопасности КС.

Математические основы моделей безопасности. Основные понятия, автоматы, графы. Алгоритмические проблемы: разрешимые и неразрешимые алгоритмические проблемы.

Основные виды формализованных моделей безопасности КС.

Проблема адекватности реализации модели безопасности в реальной КС.

Тема 2. Модели компьютерных систем с дискреционным управлением доступом.

Модель матрицы доступов Харрисона - Руззо - Ульмана (ХРУ, HRU). Описание модели, анализ безопасности систем ХРУ.

Алгоритмическая неразрешимость проблемы утечки для модели HRU.

Модель типизированной матрицы доступов.

Тема 3. Модель распространения прав доступа Take-Grant.

Основные положения классической модели Take-Grant.

Расширенная модель Take-Grant.

Представление систем Take-Grant системами HRU.

Дискреционные ДП-модели. Базовая ДП-модель

ДП-модели без кооперации доверенных и недоверенных субъектов.

Тема 4. Модели изолированной программной среды.

Субъектно-ориентированная модель изолированной программной среды.

Корректность субъектов в ДП-моделях КС с дискреционным управлением доступом.

ДП-модель с функционально ассоциированными с субъектами сущностями.

ДП-модель для политики безопасного администрирования.

ДП-модель для политики абсолютного разделения административных и пользовательских полномочий.

ДП-модель с функционально или параметрически ассоциированными с субъектаим сущностями.

Методы предотвращения утечки прав доступа и реализации запрещенных информационных потоков.

Метод предотвращения возможности получения права доступа владения недоверенным субъектом к доверенному субъекту.

Метод реализации политики безопасности администрирования.

Метод реализации политики абсолютного разделения административных и пользовательских полномочий.

Тема 5. Модели компьютерных систем с мандатным управлением доступом.

Модель Балла - ЛаПадулы: классическая модель Белла - ЛаПадулы, пример некорректного администрирования.

Политика low-watermark в модели Белла - ЛаПадулы.

Безопасность переходов.

Модель мандатной политики целостности информации Биба.

Модель систем военных сообщений: общие положения и основные понятия.

Неформальное и формальное описания модели СВС.

Мандатная ДП-модель.

Правила преобразования состояний мандатной ДП-модели.

Безопасность в смысле Белла - ЛаПадулы.

Тема 6. Модели безопасности информационных потоков.

Автоматная модель безопасности информационных потоков.

Программная модель контроля информационных потоков.

Вероятностная модель безопасности информационных потоков.

ДП-модель безопасности информационных потоков по времени.

Тема 7. Модели компьютерных систем с ролевым управлением доступом.

Понятие ролевого управления доступом.

Базовая модель ролевого управления доступом.

Модель администрирования ролевого управления доступом.

Администрирование множеств авторизованных ролей пользователей.

Администрирование множеств прав доступа, которыми обладают роли.

Администрирование иерархии ролей.

Модель мандатного ролевого управления доступом.

Защита от угрозы конфиденциальности информации.

Защита от угрозы целостности информации.

Тема 8. ДП-модели.

Базовая ролевая ДП-модель.

Состояния базовой ролевой ДП-модели.

Правила преобразования состояний базовой ролевой ДП-модели.

Условия передачи прав доступа с участием двух субъект-сессий.

Мандатная ДП-модель.

Правила преобразования состояний мандатной ДП-модели.

ДП-модель безопасности информационных потоков по времени.

5. **Форма промежуточной аттестации:** зачет.

Аннотация дисциплины
«Алгебраические и теоретико-числовые методы в криптографии»

Направление 10.06.01 Информационная безопасность
Направленность (профиль) «Методы и системы защиты информации, информационная безопасность»

1. Дисциплина «Алгебраические и теоретико-числовые методы в криптографии» относится к дисциплинам по выбору вариативной части блока Б1.

2. Дисциплина «Алгебраические и теоретико-числовые методы в криптографии» обеспечивает приобретение фундаментальных и профессиональных знаний, умений и навыков, содействует дальнейшей фундаментализации образования, развитию логического мышления и формированию математического и общенаучного мировоззрения. Целью изучения дисциплины является освоение фундаментальных понятий теории чисел, комбинаторной теории групп и алгебры, лежащих в основе современных подходов к построению криптоалгоритмов и криптопротоколов, математическому обоснованию их криптографической стойкости.

3. Общая трудоемкость дисциплины составляет 3 зачетные единицы, 108 часов.

4. Содержание дисциплины:

Тема 1. Базовые понятия теории чисел, теории множеств и теории алгоритмов.

Отношение делимости для натуральных и целых чисел. Деление с остатком.

Простые и составные числа. Основная теорема арифметики.

НОД и НОК. Алгоритм Евклида, оценка его сложности. Коэффициенты Безу. Взаимно простые числа. Функция Л. Эйлера.

Распределение простых чисел в ряду натуральных чисел. Теорема Л. Эйлера. Асимптотический закон распределения простых чисел. Теоремы П.Л. Чебышева и Ж. Адамара - Ш.-Ж. Валле-Пуссена.

Сложность проблемы проверки числа на простоту. Тесты простоты и алгоритмы.

Сравнения по натуральному модулю. Квадратичные вычеты и невычеты. Квадратичный закон взаимности.

Цепные дроби, подходящие дроби. Теорема Ж.-Л. Лагранжа.

Диофантовы уравнения. 10-ая проблема Д. Гильберта. Уравнение Пелля и метод цепных дробей.

Математическое уточнение интуитивного понятия алгоритма - машины Тьюринга и частично рекурсивные функции.

Рекурсивные, рекурсивно перечислимые и диофантовы множества.

Временная и емкостная оценки сложности выполнения алгоритма.

Сложность описания (задания) алгоритма.

Теоретико-числовые функции. Мультипликативные функции.

Сумматорные функции. Функция Мебиуса и формула обращения.

Тема 2. Полугруппы, моноиды и группы.

Алгебраические операции. Группоиды. Гомоморфизмы и изоморфизмы группоидов.

Полугруппы. Нейтральные элементы, моноиды. Гомоморфизмы и изоморфизмы полугрупп и моноидов. Задание полугрупп и моноидов образующими и определяющими соотношениями. Алгоритмические проблемы для конечно определенных полугрупп и моноидов. Теорема А.А. Маркова - Э. Поста.

Обратимые элементы, группы. Задание групп образующими и определяющими соотношениями. Алгоритмические проблемы для конечно определенных групп, фундаментальные проблемы М. Дэна. Теоремы П.С. Новикова и С.И. Адяна.

Подгруппы, нормальные подгруппы и факторгруппы. Гомоморфизмы и изоморфизмы групп. Теоремы о гомоморфизмах.

Группы подстановок. Теорема Кэли.

Действие группы на множестве, орбиты элементов и стабилизаторы.

Фундаментальные группы топологических пространств.

Группы узлов и кос.

Прямое произведение групп. Теорема о строении конечно определенной абелевой группы.

Коммутаторы и коммутанты. Нильпотентные и разрешимые группы.

Свободные группы. Уравнения и системы уравнений в группах. Неразрешимые и NP-трудные алгоритмические проблемы для уравнений в группах.

Тема 3. Кольца и многочлены.

Понятие кольца. Ассоциативные и коммутативные кольца. Кольца Ли.

Гомоморфизмы колец.

Подкольца и идеалы. Факторкольца. Теорема о гомоморфизме для колец.

Кольца с единицей. Делители нуля. Области целостности.

Кольца главных идеалов.

Евклидовы кольца.

Прямое произведение колец.

Сумма и прямая сумма идеалов. Разложение кольца в прямую сумму идеалов.

Неразложимые и простые элементы колец. Факториальные кольца.

Кольца многочленов. Корни многочленов. Кратные и простые корни.

Производная многочлена.

Многочлена от нескольких переменных.

Нетеровы кольца. Теорема Д. Гильберта.

Тема 4. Поля и многочлены над ними.

Поле, подполе, простое подполе.

Характеристика поля. Связь с полями вычетов.

Расширения полей. Конечно порожденные и простые расширения.

Расширения конечной степени (конечные расширения).

Теорема о башне полей (конечные расширения).

Алгебраические над подполем элементы. Алгебраические расширения.

Теорема о башне полей (алгебраические расширения).

Алгебраически замкнутые поля. Алгебраическое замыкание поля.

Вложение областей целостности в поля (поля отношений).

Евклидовость кольца многочленов над полем, деление с остатком.

НОД и НОК многочленов.

Алгоритм Евклида для многочленов над полем.

Факториальность кольца многочленов над полем.

Многочлены над факториальным кольцом. Лемма Гаусса о произведении примитивных многочленов.

Многочлены над кольцом целых чисел и над полем рациональных чисел.

Корни многочленов над полями. Теорема о "символическом присоединении".

Неприводимые многочлены над полями комплексных и действительных чисел.

Тема 5. Конечные поля и многочлены над ними.

Существование и единственность поля с примарным числом элементов.

Теорема о цикличности мультипликативной группы конечного поля. Примитивные элементы, их число.

Существование над конечным полем неприводимого многочлена произвольной степени.

Формула обращения Мебиуса. Число унитарных неприводимых над конечным полем F многочленов степени n.

Примитивные многочлены и их число.

Использование в современной криптографии неприводимых и примитивных многочленов над конечными полями (Россия, США).

Тема 6. Элементы эллиптической криптографии.

Алгебраические кривые на евклидовой плоскости. Квадратичные кривые (квадрики, коники). Сложение точек, его свойства.

Кубические кривые, 2-местная операция сложения точек, ее свойства.

Понятие о проективном пространстве.

Проективная плоскость. Алгебраические кривые на проективной плоскости.

Особые и неособые кубические кривые. Форма Вейерштрасса.

Эллиптические кривые, свойства операции сложения точек на них.

Группа точек на эллиптической кривой.

Понятие об эллиптических функциях. Функция Вейерштрасса. Параметризация эллиптической кривой над полем комплексных чисел.

Эллиптические кривые над полем рациональных чисел, рациональные и целочисленные точки на них.

Эллиптические кривые над конечными полями.

Тема 7. Вычислительные алгоритмы в алгебре и теории чисел.

Проверка чисел и многочленов на простоту. Числа Мерсенна.

Факторизация П. Ферма и факторные базы.

Тест Рабина - Миллера.

Ро-метод Полларда.

Метод цепных дробей.

Метод квадратичного решета.

Тест простоты на базе эллиптических кривых.

Разложение натуральных чисел на множители с использованием эллиптических кривых.

Решение проблемы равенства и проблемы изоморфизма для конечно определенных абелевых групп.

Решение проблемы сопряженности для групп кос.

Алгоритмические проблемы для групп с условием малого налегания (сокращения).

Тема 8. Методы теории чисел и комбинаторной теории групп в современной криптографии.

"Рюкзачная" криптосистема.

Криптосистема RSA.

Дискретной логарифмирование.

Криптосистемы на эллиптических кривых.

Криптосистемы на базе групп, заданных образующими и определяющими соотношениями.

Протокол Anschel-Anschel-Goldfeld выработки общего секретного ключа на базе коммутаторов элементов групп.

Протокол Ko -- Lee -- Cheon -- Han -- Kang -- Park выработки общего секретного ключа на базе проблемы сопряженности для группы кос.

Протокол Wang -- Cao -- Okamoto -- Shao выработки общего секретного ключа на базе некоммутативного моноида.
Протокол Сидельникова В. М. -- Черепнева М. А. -- Ященко В. Ю на базе некоммутативных полугрупп.
Протокол Stickel на базе конечной (периодической) некоммутативной группы.
Протоколы, базирующиеся на групповых автоморфизмах и эндоморфизмах: протокол Mahalanobis, протокол Habeeb -- Kahrobaei -- Koupparis -- Shpilrain.

Протоколы аутентификации, основанные на некоторых "трудных" алгоритмических проблемах теории групп: протокол Романькова -- Григорьева -- Шпильрайна, протокол Шпильрайна -- Ушакова, протокол Мегрелишвили -- Джинджихадзе.

Криптосистема Росошека.

5. **Форма промежуточной аттестации:** зачет.

Аннотация дисциплины
«Теория алгоритмов и сложность вычислений»

Направление 10.06.01 Информационная безопасность
Направленность (профиль) «Методы и системы защиты информации, информационная безопасность»

1. Дисциплина «Теория алгоритмов и сложность вычислений» относится к дисциплинам по выбору вариативной части блока Б1.

2. Дисциплина «Теория алгоритмов и сложность вычислений» обеспечивает приобретение фундаментальных и профессиональных знаний, умений и навыков, содействует дальнейшей фундаментализации образования, развитию логического мышления и формированию математического и общенаучного мировоззрения. Целью изучения дисциплины является овладение базовыми понятиями и методами теории алгоритмов, ознакомление с их применениями в области обеспечения информационной безопасности, установление существования алгоритмически неразрешимых проблем и значение этого фундаментального факта теории алгоритмов для алгоритмической практики, компьютерных наук и защиты информации, ознакомление с базовыми подходами к оценке сложности алгоритмов и задач и некоторыми приемами построения эффективных алгоритмов.

3. Общая трудоемкость дисциплины составляет 3 зачетные единицы, 108 часов.

4. Содержание дисциплины:

Раздел "Теория алгоритмов"

Тема 1. Введение. История развития теории алгоритмов.
Теория алгоритмов и принципиальные возможности компьютеров.
Оценки сложности алгоритмов и их значение для практики.

Тема 2. Машины Тьюринга.
Интуитивное понятие "алгоритма" и его характерные черты. Задачи, приводящие к необходимости уточнения понятия "алгоритм".
Вычислимые в интуитивном смысле функции.
Два подхода к уточнению понятия "алгоритм".
Машины Тьюринга-Поста: внешний и внутренний алфавиты, программы и команды.
Конфигурации. Композиция и ветвление машин Тьюринга. Вычислимость и правильная вычислимость функций по Тьюрингу. Принцип Тьюринга- Поста-Черча.
Правильная вычислимость исходных функций и сложения.

Тема 3. Частично рекурсивные, рекурсивные и примитивно рекурсивные функции.
Тезис Черча.
Примитивная рекурсивность теоретико-числовых функций.
Операции суммирования и мультиплицирования.

Тема 4. Примитивно рекурсивные и рекурсивные предикаты, отношения и множества, операции над ними.
Соотношения между классами примитивно рекурсивных, общерекурсивных и частично рекурсивных функций.

Тема 5. Задание функций и предикатов.
Задание функций кусочными схемами.
Ограниченный оператор минимизации.
Примитивная рекурсивность функций, связанных с каноническим представлением натуральных чисел и с делением с остатком.

Тема 6. Нумерация.
Канторовские нумерационные функции, их примитивная рекурсивность.
Примитивная рекурсивность функции Геделя.

Тема 7. Рекурсивно перечислимые множества, отношения и предикаты.
Рекурсивно перечислимые множества, отношения и предикаты, операции над ними.
Теорема о графике функции. Ее следствия.

Тема 8. Операции над машинами Тьюринга.
Транспозиция, удвоение, циклический сдвиг, копирование

Тема 9. Вычислимость функций по Тьюрингу.
Правильная вычислимость по Тьюрингу любой частично рекурсивной функции.

Тема 10. Арифметизация теории машин Тьюринга.
Частичная рекурсивность любой вычислимой по Тьюрингу функции.

Тема 11. Нормальная форма Клини.
Универсальные частично рекурсивные функции.

Тема 12. Алгоритмическая неразрешимость.
Неразрешимость проблемы самоприменимости и применимости для машин Тьюринга.

Тема 13. Тьюрингов предикат вычислимости.
Существование рекурсивно перечислимого, но не рекурсивного множества.

Тема 14. Нумерация Клини частично рекурсивных функций. Универсальные функции Клини.
Теорема о неподвижной точке для частично рекурсивных функций.

Тема 15. Теорема Райса для частично рекурсивных функций.

Тема 16. Нумерация Поста рекурсивно перечислимых множеств.
Теорема о неподвижной точке для рекурсивно перечислимых множеств.
Теорема Райса для рекурсивно перечислимых множеств.

Тема 17. Сводимость по Тьюрингу. *m*-сводимость.
m-универсальные, креативные и продуктивные множества.

Тема 18. Нормальные алгоритмы А.А. Маркова.
Нормальные алгорифмы А.А.Маркова: схема алгорифма, заключительные и простые правила подстановки (замены). Примеры нормальных алгорифмов. Принцип нормализации А.А.Маркова. Композиция нормальных алгорифмов.
Связь с машинами Тьюринга и частично рекурсивными функциями

Тема 19. Алгоритмическая разрешимость и неразрешимость. Нумерация слов в счетном алфавите и арифметизация алгоритмов. Примеры алгоритмически разрешимых и неразре-

шимых задач из математической логики, теории алгоритмов, алгебры, теории чисел, теории формальных грамматик, теории обыкновенных дифференциальных уравнений, топологии, математического анализа и теории конечных автоматов. Теорема Черча о неразрешимости логики предикатов.
Значение существования алгоритмически неразрешимых проблем для обще математической практики, приложений в компьютерных науках и в области обеспечения информационной безопасности.

Раздел "Сложность вычислений":

Тема 1. Детерминированные многоленточные машины Тьюринга.
Внешний и внутренний алфавиты k-ленточной детерминированной машины Тьюринга. Программа и команды. Конфигурации. Описание выполнения команд в терминах преобразования конфигураций. Языки, принимаемые (допускаемые, распознаваемые) k-ленточными детерминированными машинами Тьюринга.

Тема 2. Сложность алгоритмов и вычислений. Некоторые подходы к оценкам сложности алгоритмов и вычислений. Модели вычислений. Сложность вычисления на детерминированной машине Тьюринга. Временная и емкостная меры сложности (детерминированный случай). Полиномиально ограниченные детерминированные машины Тьюринга. Классы языков **P**-TIME и **P**-SPACE. Пример языка, не входящего в класс **P**-TIME.

Тема 3. Недетерминированные многоленточные машины Тьюринга.
Внешний и внутренний алфавиты k-ленточной недетерминированной машины Тьюринга. Программа и команды недетерминированной машины Тьюринга. Их особенность. Конфигурации. Описание выполнения команд в терминах преобразования конфигураций. Языки, принимаемые (допускаемые) недетерминированными k-ленточными машинами Тьюринга.

Тема 4. Временная и емкостная меры сложности (недетерминированный случай).
Класс языков **NP**-TIME. Проблема **NP = P**?
Полиномиальная сводимость.
NP-трудные и **NP-полные** языки (задачи, проблемы).
NP-полнота проблемы выполнимости для формул логики высказываний (булевых функций).

Тема 5. Свойства функций сложности.
Нижние оценки. Сложность распознавания функциональной полноты системы булевых функций, сложность проблем вхождения в классы самодвойственных, монотонных и линейных функций. Существование сколь угодно сложно вычислимых функций.

Тема 6. Сложность проблемы разрешимости систем линейных уравнений.
Решение систем целочисленных линейных уравнений в целых, натуральных и 0-1 числах.

Тема 7. NP-полные проблемы для уравнений в свободных полугруппах и для регулярных языков.

Тема 8. NP-полные проблемы в теории графов.

Тема 9. NP-полные проблемы из различных разделов математики.

Тема 10. Алгоритмически неразрешимые проблемы в области защиты информации.
Дискреционная политика управления доступом - неразрешимый и разрешимые варианты.

Тема 11. Сложностная классификация языков. Классы TIME(f(n)) и SPACE(f(n)).
Классы TIME(n^k), P-TIME и TIME(2^n).
Сложностные иерархии.
Элементарные и неэлементарные задачи (языки).
Сложность разрешимости элементарной теории поля действительных чисел и арифметики Пресбургера.

Тема 12. Сложность описания нормального алгоритма А.А. Маркова.

Тема 13. Теория алгоритмов и задачи использования ЭВМ. Вычислительные возможности современных ЭВМ. Модель ЭВМ – машина произвольного доступа (МПД). МПД - вычислимые функции и их связь с частично рекурсивными функциями.

Тема 14. Сложность конечных объектов по А.Н.Колмогорову.

5. **Форма промежуточной аттестации:** зачет.

Аннотация дисциплины
«Нормальные алгорифмы»

Направление 10.06.01 Информационная безопасность
Направленность (профиль) «Методы и системы защиты информации, информационная безопасность»

1. Дисциплина «Нормальные алгорифмы» относится к дисциплинам по выбору вариативной части блока Б1.

2. Дисциплина «Нормальные алгорифмы» обеспечивает приобретение фундаментальных и профессиональных знаний, умений и навыков, содействует дальнейшей фундаментализации образования, развитию логического мышления и формированию математического и общенаучного мировоззрения. Целью изучения дисциплины является овладение базовыми понятиями и методами общей теории алгоритмов и теории нормальных алгоритмов, как удобного средства преобразования текстовой информации, ознакомление с применениями теории алгоритмов в области обеспечения информационной безопасности, установление существования алгоритмически неразрешимых проблем и значение этого фундаментального факта теории алгоритмов для алгоритмической практики, компьютерных наук и защиты информации, ознакомление с базовыми подходами к оценке сложности алгоритмов и задач, а так же сложности описания самого алгоритма.

3. Общая трудоемкость дисциплины составляет 3 зачетные единицы, 108 часов.

4. Содержание дисциплины:

Тема 1. Введение. История развития теории алгоритмов.
Теория алгоритмов и принципиальные возможности компьютеров.
Оценки сложности алгоритмов и их значение для практики.

Тема 2. Нормальные алгорифмы А.А. Маркова.
Нормальные алгорифмы А.А. Маркова: схема алгорифма, заключительные и простые правила подстановки (замены). Примеры нормальных алгорифмов. Принцип нормализации А.А.Маркова. Композиция нормальных алгорифмов.

Тема 3. Машины Тьюринга.
Интуитивное понятие "алгоритма" и его характерные черты. Задачи, приводящие к необходимости уточнения понятия "алгоритм".
Вычислимые в интуитивном смысле функции.
Два подхода к уточнению понятия "алгоритм".
Машины Тьюринга-Поста: внешний и внутренний алфавиты, программы и команды.
Конфигурации. Композиция и ветвление машин Тьюринга. Вычислимость и правильная вычислимость функций по Тьюрингу. Принцип Тьюринга- Поста-Черча.
Правильная вычислимость исходных функций и сложения.

Тема 4. Частично рекурсивные, рекурсивные и примитивно рекурсивные функции.
Тезис Черча.
Примитивная рекурсивность теоретико-числовых функций.
Операции суммирования и мультиплицирования.

Тема 5. Примитивно рекурсивные и рекурсивные предикаты, отношения и множества, операции над ними.
Соотношения между классами примитивно рекурсивных, общерекурсивных и частично рекурсивных функций.

Тема 6. Задание функций и предикатов.
Задание функций кусочными схемами.
Ограниченный оператор минимизации.
Примитивная рекурсивность функций, связанных с каноническим представлением натуральных чисел и с делением с остатком.

Тема 7. Нумерация.
Канторовские нумерационные функции, их примитивная рекурсивность.
Примитивная рекурсивность функции Геделя.

Тема 8. Рекурсивно перечислимые множества, отношения и предикаты.
Рекурсивно перечислимые множества, отношения и предикаты, операции над ними.
Теорема о графике функции. Ее следствия.

Тема 9. Операции над машинами Тьюринга.
Транспозиция, удвоение, циклический сдвиг, копирование

Тема 10. Вычислимость функций по Тьюрингу.
Правильная вычислимость по Тьюрингу любой частично рекурсивной функции.

Тема 11. Арифметизация теории машин Тьюринга.
Частичная рекурсивность любой вычислимой по Тьюрингу функции.

Тема 12. Нормальная форма Клини.
Универсальные частично рекурсивные функции.

Тема 13. Алгоритмическая неразрешимость.
Неразрешимость проблемы самоприменимости и применимости для машин Тьюринга.

Тема 14. Тьюрингов предикат вычислимости.
Существование рекурсивно перечислимого, но не рекурсивного множества.

Тема 15. Нумерация Клини частично рекурсивных функций. Универсальные функции Клини.
Теорема о неподвижной точке для частично рекурсивных функций.

Тема 16. Теорема Райса для частично рекурсивных функций.

Тема 17. Нумерация Поста рекурсивно перечислимых множеств.
Теорема о неподвижной точке для рекурсивно перечислимых множеств.
Теорема Райса для рекурсивно перечислимых множеств.

Тема 18. Сводимость по Тьюрингу. *m*-сводимость.
m-универсальные, креативные и продуктивные множества.

Тема 19. Алгоритмическая разрешимость и неразрешимость. Нумерация слов в счетном алфавите и арифметизация алгоритмов. Примеры алгоритмически разрешимых и неразрешимых задач из математической логики, теории алгоритмов, алгебры, теории чисел, теории

формальных грамматик, теории обыкновенных дифференциальных уравнений, топологии, математического анализа и теории конечных автоматов. Теорема Черча о неразрешимости логики предикатов.
Значение существования алгоритмически неразрешимых проблем для обще математической практики, приложений в компьютерных науках и в области обеспечения информационной безопасности.

Тема 20. Связь между нормальными алгоритмами, машинами Тьюринга и частично рекурсивными функциями. Совпадение класса вычислимых по Маркову функций с классом частично рекурсивных функций и с классом вычислимых по Тьюрингу функций.

Тема 21. Детерминированные многоленточные машины Тьюринга.
Внешний и внутренний алфавиты k-ленточной детерминированной машины Тьюринга. Программа и команды. Конфигурации. Описание выполнения команд в терминах преобразования конфигураций. Языки, принимаемые (допускаемые, распознаваемые) k-ленточными детерминированными машинами Тьюринга.
Некоторые подходы к оценкам сложности алгоритмов и вычислений. Модели вычислений. Сложность вычисления на детерминированной машине Тьюринга. Временная и емкостная меры сложности (детерминированный случай). Полиномиально ограниченные детерминированные машины Тьюринга. Классы языков **P**-TIME и **P**-SPACE. Пример языка, не входящего в класс **P**-TIME.

Тема 22. Недетерминированные многоленточные машины Тьюринга.
Внешний и внутренний алфавиты k-ленточной недетерминированной машины Тьюринга. Программа и команды недетерминированной машины Тьюринга. Их особенность. Конфигурации. Описание выполнения команд в терминах преобразования конфигураций. Языки, принимаемые (допускаемые) недетерминированными k-ленточными машинами Тьюринга.

Тема 23. Временная и емкостная меры сложности (недетерминированный случай).
Класс языков **NP**-TIME. Проблема **NP = P**?
Полиномиальная сводимость.
NP-трудные и **NP-полные** языки (задачи, проблемы).
NP-полнота проблемы выполнимости для формул логики высказываний (булевых функций).
Свойства функций сложности.
Нижние оценки. Сложность распознавания функциональной полноты системы булевых функций, сложность проблем вхождения в классы самодвойственных, монотонных и линейных функций. Существование сколь угодно сложно вычислимых функций.

Тема 24. Сложность проблемы разрешимости систем линейных уравнений.
Решение систем целочисленных линейных уравнений в целых, натуральных и 0-1 числах.

Тема 25. NP-полные проблемы для уравнений в свободных полугруппах и для регулярных языков.

Тема 26. NP-полные проблемы в теории графов.

Тема 27. NP-полные проблемы из различных разделов математики.

Тема 28. Алгоритмически неразрешимые проблемы в области защиты информации.
Дискреционная политика управления доступом - неразрешимый и разрешимые варианты.

Тема 29. Сложностная классификация языков. Классы TIME(f(n)) и SPACE(f(n)).

Классы TIME(n^k), P-TIME и TIME(2^n).
Сложностные иерархии.
Элементарные и неэлементарные задачи (языки).
Сложность разрешимости элементарной теории поля действительных чисел и арифметики Пресбургера.

Тема 30. Сложность описания нормального алгоритма А.А.Маркова.

Тема 31. Теория алгоритмов и задачи использования ЭВМ. Вычислительные возможности современных ЭВМ. Модель ЭВМ – машина произвольного доступа (МПД). МПД - вычислимые функции и их связь с частично рекурсивными функциями.

Тема 32. Сложность конечных объектов по А.Н.Колмогорову.

5. **Форма промежуточной аттестации:** зачет.

Аннотация дисциплины
«Дискретные функции»

Направление 10.06.01 Информационная безопасность
Направленность (профиль) «Методы и системы защиты информации, информационная безопасность»

1. Дисциплина «Дискретные функции» относится к факультативным дисциплинам.

2. Дисциплина «Дискретные функции» обеспечивает приобретение фундаментальных и профессиональных знаний, умений и навыков, содействует дальнейшей фундаментализации образования, развитию логического мышления и формированию математического и общенаучного мировоззрения. Целью изучения дисциплины является овладение базовыми понятиями и методами теории дискретных функций, ознакомление с их применениями в области обеспечения информационной безопасности, ознакомление с базовыми подходами к оценке сложности задания и сложности вычисления дискретной функции.

3. Общая трудоемкость дисциплины составляет 2 зачетные единицы, 72 часа.

4. Содержание дисциплины:

Тема № 1. Булевы функции.

Способы задания булевых функций. Существенные и несущественные переменные. Термы. Задание булевых функций термами. Элементарные функции и их свойства. Разложение функций по переменной.

Совершенные дизъюнктивная и конъюнктивная нормальные формы.

Полиномы Жегалкина. Представление булевых функций полиномами.

Замыкание произвольного класса булевых функций. Свойства операции замыкания. Замкнутые классы. Полные системы булевых функций.

Классы C_0 и C_1.

Линейные функции. Лемма о нелинейной функции.

Самодвойственные функции. Принцип двойственности. Лемма о несамодвойственной функции.

Монотонные функции. Лемма о немонотонной функции.

Теорема Поста о полноте систем булевых функций.

Предполные классы. Базисы, примеры базисов.

Дизъюнктивные нормальные формы (ДНФ). Тупиковая, минимальная и сокращенная ДНФ. Геометрическая интерпретация. Алгоритм нахождения всех минимальных ДНФ. Свойство сокращенной ДНФ для монотонных булевых функций. Методы построения сокращенной ДНФ: градиентный алгоритм, локальные алгоритмы.

Тема № 2. Функции к-значной логики.

Элементарные функции.

Полнота систем функций. Алгоритм распознавания полноты конечных систем функций в P_k.

Представление функций из P_k полиномами.

Особенности функций к-значной логики. Пример замкнутого класса в P_k, не имеющего базиса. Пример замкнутого класса в P_k, имеющего счетный базис. Пример континуального семейства замкнутых классов в P_k.

Теорема Кузнецова о функциональной полноте в P_k.

Существенные функции. Теорема Слупецкого.

Тема № 3. Схемы из функциональных элементов.

Сложность схем. Синтез схем из функциональных элементов для индивидуальных функций.

Схемы сложения и умножения n-разрядных чисел.

Простейшие универсальные методы синтеза. Метод Шеннона.

Мощностной метод получения оценок сложности.

Функция L (n). Порядок роста функции L (n).

Асимптотически наилучший метод синтеза схем из функциональных элементов в базисе {V, &, -- }. Асимптотика функции L (n).

Контактные схемы. Простейшие методы синтеза. Контактное дерево.

Универсальный многополюсник. Метод Шеннона для контактных схем.

Нижняя оценка сложности линейной функции в классе контактных схем (метод Кардо).

Тема № 4. Автоматные функции.

Конечные автоматы с выходом и без выхода. Входной, выходной и внутренний алфавиты. Функция переходов и выхода. Эквивалентность состояний автомата. Теорема об эквивалентности состояний конечного автомата. Эквивалентность автоматов. Построение автомата, эквивалентного данному, с минимальным числом состояний. Преобразование автоматными функциями периодических последовательностей.

. Операция суперпозиции. Отсутствие полных относительно операций суперпозиции конечных систем автоматных функций.

Схемы из логических элементов и элементов задержки. Реализация автоматных функций.

Регулярные выражения и регулярные языки. Теорема С. Клини.

Пример нерегулярного языка.

Тема № 5. Вычислимые по Тьюрингу функции.

Машины Тьюринга. Внешний и внутренний алфавиты, команды и программа машины Тьюринга. Различные варианты машин Тьюринга: многоленточные и одноленточные, с одномерной и многомерной лентой, с потенциально бесконечной в обе стороны лентой, с непродолжаемой влево лентой и т. д.

Словарные алгоритмы, реализуемые машинами Тьюринга. Вычислимые по Тьюрингу функции. Правильная вычислимость по Тьюрингу. Вычислимость по Тьюрингу элементарных теоретико-числовых функций.

Разрешимые и перечислимые множества слов.

Операции над машинами Тьюринга. Композиция машин Тьюринга. Разветвление. Зацикливание. Диаграммы машин Тьюринга. Циклический сдвиг, копирование.

Тезис Тьюринга. Замкнутость класса правильно вычислимых по Тьюрингу функций относительно операций суперпозиции, примитивной рекурсии и минимизации. Тезис А.Тьюринга.

Тема № 6. Частично рекурсивные функции.

Простейшие (исходные) функции. Операции суперпозиции, примитивной рекурсии и минимизации.

Примитивно рекурсивные функции. Примеры примитивно рекурсивных теоретико-числовых функций.

Частично рекурсивные и рекурсивные функции, примеры.

Операции над примитивными, рекурсивными и частично рекурсивными функциями. Тезис А. Черча.

Нумерация пар и n-ок натуральных чисел. Нумерационные функции.

Рекурсивные и рекурсивно перечислимые множества и предикаты. Теорема Э. Поста.

Теорема о графике функции.

Правильная вычислимость по Тьюрингу любой частично рекурсивной функции.

Тема 7. Универсальные функции.

Арифметизация теории машин Тьюринга. Геделева нумерация слов в конечных и счетных алфавитах.

Нумерация команд и программ машин Тьюринга. Нумерация конфигураций.

Построение примитивно рекурсивных функций, описывающих работу машин Тьюринга.

Частичная рекурсивность любой вычислимой по Тьюрингу функции.

Универсальные частично рекурсивные функции.

Неразрешимость проблем останова, самоприменимости и бессмертия для машин Тьюринга.

Нормальная форма С. Клини.

Универсальные машины Тьюринга.

Неразрешимые алгоритмические проблемы. Неразрешимость проблемы выводимости для полусистем Туэ.

Неразрешимость проблемы равенства для полугрупп и групп.

Теоремы А.А. Маркова и С.И. Адяна об алгоритмической неразрешимости проблем распознавания полугрупповых и групповых свойств. Неразрешимые проблемы в математической логике.

Тема № 8. Функции, характеризующие сложность алгоритмов.

Многоленточные машины Тьюринга: внешний и внутренний алфавиты, программы.

Сложностные характеристики работы машины Тьюринга: временная (число шагов) и емкостная (объем памяти), связь между ними.

Сложностные характеристики работы машины Тьюринга в худшем случае: временная и емкостная сигнализирующие функции (сложности, характеристики алгоритма), связь между ними.

Сложностные классы. Другие сложностные характеристики.

Сложность описания нормального алгорифма А.А.Маркова.

Сложность конечных объектов по А.Н.Колмогорову.

5. **Форма промежуточной аттестации:** зачет.

Аннотация дисциплины
«Диофантова криптография»

Направление 10.06.01 Информационная безопасность
Направленность (профиль) «Методы и системы защиты информации, информационная безопасность»

1. Дисциплина «Диофантова криптография» относится к дисциплинам по выбору вариативной части блока Б1.

2. Дисциплина «Диофантова криптография» обеспечивает приобретение фундаментальных и профессиональных знаний, умений и навыков, содействует дальнейшей фундаментализации образования, развитию логического мышления и формированию математического и общенаучного мировоззрения. Целью изучения дисциплины является овладение базовыми понятиями и методами теории диофантовых уравнений, ознакомление с их применениями в области обеспечения информационной безопасности, установление существования алгоритмически неразрешимых проблем в теории диофантовых уравнений и значение этого фундаментального факта для алгоритмической практики, компьютерных наук и защиты информации.

3. Общая трудоемкость дисциплины составляет 2 зачетные единицы, 72 часа.

4. Содержание дисциплины:

   Тема 1. Диофантовы уравнения. Десятая проблема Д. Гильберта.
   Общее понятие диофантового уравнения, связь между решениями в целых числах и решениями в натуральных числах.
   Линейные диофантовы уравнения и их системы.
   Диофантовы уравнения второй степени с двумя неизвестными. Уравнение Пелля, существование натурального решения, общий вид его решения в натуральных и целых числах. Нахождение наименьшего натурального решения методом цепных дробей.
   Теорема Лагранжа о разложении квадратичной иррациональности в цепную дробь.
   Теорема Туэ.
   Десятая проблема Д. Гильберта.
   Проблемы Д. Гильберта и их историческое значение для развития математики в XX веке.

   Тема 2. Частично рекурсивные, рекурсивные и примитивно рекурсивные функции.
   Тезис Черча.
   Примитивная рекурсивность теоретико-числовых функций.
   Операции суммирования и мультиплицирования.

   Тема 3. Примитивно рекурсивные и рекурсивные предикаты, отношения и множества, операции над ними.
   Соотношения между классами примитивно рекурсивных, общерекурсивных и частично рекурсивных функций.

   Тема 4. Задание функций и предикатов.
   Задание функций кусочными схемами.
   Ограниченный оператор минимизации.

Примитивная рекурсивность функций, связанных с каноническим представлением натуральных чисел и с делением с остатком.

Тема 5. Нумерация.
Канторовские нумерационные функции, их примитивная рекурсивность.
Примитивная рекурсивность функции Геделя.

Тема 6. Рекурсивно перечислимые и диофантовы множества, отношения и предикаты.
Рекурсивно перечислимые множества, отношения и предикаты, операции над ними.
Теорема о графике функции. Ее следствия.
Диофантовы множества, отношения и предикаты. Связь диофантовости с рекурсивной перечислимостью. Гипотеза М. Дэвиса.

Тема 7. Теорема М. Дэвиса - Дж. Робинсон - Х. Путнам - Ю.В. Матиясевича о совпадении классов рекурсивно перечислимых и диофантовых множеств.

Тема 8. Арифметизация теории диофантовых уравнений.
Нумерация уравнений. Построение универсального диофантового уравнения и множества.

Тема 9. Диофантовы уравнения и криптография.
Диофантовы функции с нерекурсивной областью значений как "претенденты" на роль односторонних функций (В.А. Романьков).

Тема 10. Элементы теории групп - базовые сведений по теории групп.
Двуместные алгебраические операции. Группоиды, гомоморфизмы и изоморфизмы группоидов. Ассоциативность, полугруппы. Обобщенная ассоциативность, натуральные степени элемента полугруппы. Нейтральные элементы, моноиды. Обратимые элементы, группы. Целочисленные степени элемента группы. Примеры групп: симметрические группы, фундаментальные группы многообразий, группы узлов, группы кос, группы движений метрических пространств, матричные группы, аддитивные и мультипликативные группы колец с единицей и полей, группы вычетов. Подгруппы, строение подгруппы, порожденной множеством элементов группы. Циклические подгруппы. Образующие элементы группы. Нормальные подгруппы, строение нормальной подгруппы, порожденной множеством элементов группы. Факторгруппы, теоремы о гомоморфизмах. Порядок элемента группы. Циклические группы. Сопряженные элементы. Коммутаторы, коммутант, ряды коммутантов. Абелевы, нильпотентные и разрешимые группы.

Тема 11. Задание групп образующими и определяющими соотношениями.
Групповые алфавиты, элементарные преобразования. Построение группы, заданной образующими и определяющими соотношениями. Представление (задание, генетический код) группы. Некоторые подходы к нахождению задания группы. Примеры заданий групп. Задания для групп узлов, групп кос, симметрических и знакопеременных групп.

Тема 12. Фундаментальные проблемы М. Дэна.
Конечно порожденные и конечно определенные задания групп. Проблема тождества для групп. Проблема сопряженности для групп. Проблема изоморфизма для групп. Массовые (алгоритмические) проблемы, их положительное и отрицательное решение.

Общая проблема о распознавании групповых свойств по заданию группы. Понятие о фундаментальных результатах П.С. Новикова и С.И. Адяна.

Тема 13. Свободные группы.
Определение свободных групп, различные способы задания их элементов: классы эквивалентности и несократимые слова. Решение проблемы тождества для свободных групп. Решение проблемы сопряженности для свободных групп. Подгруппы свободных групп. Убывающие цепочки подгрупп свободных групп и теоремы об их пересечении. Хопфовость свободных групп. Финитная аппроксимируемость свободных групп.

Тема 14. Преобразования Тице.
Преобразования Тице T1, T2, T3 и T4. Изоморфность групп, задания которых получаются друг из друга преобразованиями Тице. Теорема, о возможности перейти с помощью преобразований Тице от одного задания группы к любому другому ее заданию. Построение инвариантов групп.
Граф Кэли группы. Построение графа Кэли по заданию группы образующими и определяющими соотношениями. Граф Кэли свободной группы, некоторых симметрических групп. Связь между группами и графами.

Тема 15. Фундаментальные группы топологических пространств.
Определение топологического пространства, примеры. Непрерывные отображения топологических пространств. Непрерывные пути и петли в топологическом пространстве. Умножение путей. Гомотопическая эквивалентность путей. Фундаментальная группа топологического пространства. Группы узлов. Группы кос. Связь между непрерывными отображениями топологических пространств и гомоморфизмами их фундаментальных групп. Гомеоморфизмы топологических пространств и изоморфизмы фундаментальных групп.

Тема 16. Задание факторгрупп и подгрупп.
Нахождение задания факторгруппы по заданию исходной группы и ее нормальной подгруппы. Вербальные подгруппы и приведенные свободные группы. Тождества в группах, многообразия групп. Абелевы, нильпотентные и разрешимые тождества и многообразия. Метод Рейдемейстера - Шрейера для нахождения задания подгруппы по заданию исходной группы. Система представителей правых смежных классов группы по подгруппе. Переписывающий процесс Рейдемейстера - Шрейера. Шрейеровская система представителей правых смежных классов группы по подгруппе.

Тема 17. Факторгруппы по коммутанту.
Специальные системы образующих для конечно порожденных подгрупп свободных абелевых групп конечного ранга. Прямое произведение групп. Теорема о строении конечно порожденных абелевых групп. Тест для изоморфизма групп. Факторгруппы групп узлов.
Свободное дифференциальное исчисление. Групповое кольцо. Свободное дифференциальное исчисление Фокса. Частные производные Фокса в свободной группе. Основная формула свободного дифференциального исчисления. Матрица Александера. Элементарные идеалы, их цепочки. Полиномы узлов.

Тема 18. Свободное произведение групп и свободное произведение групп с объединенной подгруппой. HNN-расширения групп.
Определение свободного произведения групп. Каноническая форма элементов свободного произведения групп. Подгруппы свободного произведения групп, понятие о

теореме А.Г. Куроша. Решение алгоритмических проблем для свободного произведения групп. Определение свободного произведения групп с объединенной подгруппой, каноническая форма элементов. Понятие о теореме Зейферта - ван Кампена**.** HNN-расширение группы, каноническая форма элементов, лемма Британа.

Тема 19. Некоторые криптографические протоколы на группах.
Интерпретация диофантовых уравнений в свободных нильпотентных и свободных разрешимых группах.
Протокол аутентификации В.А. Романькова на базе свободной метабелевой группы ранга два.

Протокол Anschel-Anschel-Goldfeld: начальная установка - группа G (платформа протокола). Выбор Алисой и Бобом открытых наборов элементов группы G и секретных элементов. Выработка общего секретного ключа - коммутатора элементов.
Протокол Ko-Lee-Cheon-Han-Kang-Park: начальная установка - корреспонденты Алиса и Боб выбирают (открыто) группу G - платформу протокола, два конечных подмножества попарно коммутирующих элементов и элемент g группы G.
Выработка материалов для создания общего секретного ключа: Алиса и Боб "случайным образом" выбирают секретные элементы.
Выработка общего секретного ключа.
Протокол Wang-Cao-Okamoto-Shao: начальная установка: корреспонденты Алиса и Боб выбирают (открыто) некоммутативный моноид G - платформу протокола, элемент g из G и обратимый элемент x в G.
Выработка материалов для создания общего секретного ключа.
Выработка общего секретного ключа.
Протокол Сидельников В.М.-Черепнев М.А.-Ященко В.Ю.: начальная установка - корреспонденты Алиса и Боб выбирают (открыто) полугруппу (моноид, группу) G - платформу протокола, два конечных подмножества попарно коммутирующих элементов и элемент g в G.
Выработка материалов для создания общего секретного ключа.
Выработка общего секретного ключа.
Протокол Stickel: начальная установка - G - неабелева конечная группа и два ее коммутирующих элемента. Выработка материалов для создания общего секретного ключа. Выработка общего секретного ключа.

Протоколы базируются на групповых автоморфизмах и эндоморфизмах.
Протокол Mahalanobis: начальная установка - корреспонденты Алиса и Боб выбирают (открыто) группу G - платформу протокола, два конечных подмножества попарно коммутирующих элементов группы автоморфизмов Aut (G) и элемент g в G.
Выработка материалов для создания общего секретного ключа.
Выработка общего секретного ключа.
Протокол Mahalanobis: начальная установка - корреспонденты Алиса и Боб выбирают (открыто) группу G -- платформу протокола, два конечных подмножества попарно коммутирующих элементов группы автоморфизмов Aut (G) и элемент g в G.
Выработка материалов для создания общего секретного ключа.
Выработка общего секретного ключа.
Протокол Habeeb-Kahrobaei-Koupparis-Shpilrain: начальная установка - корреспонденты Алиса и Боб выбирают (открыто) полугруппу или группу G - платформу протокола, ее автоморфизм и элемент. Выработка материалов для создания общего секретного ключа. Выработка общего секретного ключа.

Протоколы аутентификации, основанные на некоторых алгоритмических проблемах теории групп, которые можно отнести к сложным алгоритмическим проблемам.

Протокол Романькова-Григорьева-Шпильрайна: начальная установка - открыто выбирается бесконечная "эффективно заданная" группа G - платформа протокола с разрешимой проблемой равенства, но с алгоритмически неразрешимой проблемой эндоморфной сводимости.
Выбор "Системой" ("Доказывающим") открытого элемента g в G.
Выбор "Доказывающим" "Секретного" ключа - эндоморфизм группы G.
Построение "Открытого" ключа.
Раунд аутентификации.

Протокол Шпильрайна-Ушакова на базе проблемы скрученной сопряженности для групп.Начальная установка: открыто выбирается группа G - платформа протокола, два ее эндоморфизма и элемент w в G.
"Секретный"' ключ "Доказывающего" и "Открытый" ключ.
Раунд аутентификации.
Протокол Мегрелишвили-Джинджихадзе: начальная установка - корреспонденты Алиса и Боб выбирают (открыто) векторное пространство V над полем F - платформу протокола, квадратную матрицу A и вектор v в V.
Выработка материалов для создания общего секретного ключа.
Выработка общего секретного ключа.
Система Росошека: сообщения -- элементы группового (полугруппового) кольца K[G] группы (полугруппы) G с коэффициентами из кольца K.
Начальная установка: Алиса выбирает эндоморфизмы.
Открытый ключ Алисы - эндоморфизмы, обратимый элемент x группового кольца K[G] и элемент. Шифрование: зашифрование, расшифрование.

5. **Форма промежуточной аттестации:** зачет.

Аннотация дисциплины
«Методы комбинаторной теории групп в криптографии»

Направление 10.06.01 Информационная безопасность
Направленность (профиль) «Методы и системы защиты информации, информационная безопасность»

1. Дисциплина «Методы комбинаторной теории групп в криптографии» относится к дисциплинам по выбору вариативной части блока Б1.

2. Дисциплина «Методы комбинаторной теории групп в криптографии» обеспечивает приобретение фундаментальных и профессиональных знаний, умений и навыков, содействует дальнейшей фундаментализации образования, развитию логического мышления и формированию математического и общенаучного мировоззрения. Целью изучения дисциплины является овладение базовыми понятиями и методами комбинаторной теории групп, ознакомление с их применениями в области обеспечения информационной безопасности, установление существования алгоритмически неразрешимых проблем в области комбинаторной теории групп и значение этого фундаментального факта для алгоритмической практики, компьютерных наук и защиты информации.

3. Общая трудоемкость дисциплины составляет 2 зачетные единицы, 72 часа.

4. Содержание дисциплины:

Тема 1. Базовые сведений по теории групп.

Двуместные алгебраические операции. Группоиды, гомоморфизмы и изоморфизмы группоидов. Ассоциативность, полугруппы. Обобщенная ассоциативность, натуральные степени элемента полугруппы. Нейтральные элементы, моноиды. Обратимые элементы, группы. Целочисленные степени элемента группы. Примеры групп: симметрические группы, фундаментальные группы многообразий, группы узлов, группы кос, группы движений метрических пространств, матричные группы, аддитивные и мультипликативные группы колец с единицей и полей, группы вычетов. Подгруппы, строение подгруппы, порожденной множеством элементов группы. Циклические подгруппы. Образующие элементы группы. Нормальные подгруппы, строение нормальной подгруппы, порожденной множеством элементов группы. Факторгруппы, теоремы о гомоморфизмах. Порядок элемента группы. Циклические группы. Сопряженные элементы. Коммутаторы, коммутант, ряды коммутантов. Абелевы, нильпотентные и разрешимые группы.

Тема 2. Задание групп образующими и определяющими соотношениями.

Групповые алфавиты, элементарные преобразования. Построение группы, заданной образующими и определяющими соотношениями. Представление (задание, генетический код) группы. Некоторые подходы к нахождению задания группы. Примеры заданий групп. Задания для групп узлов, групп кос, симметрических и знакопеременных групп.

Тема 3. Фундаментальные проблемы М. Дэна.

Конечно порожденные и конечно определенные задания групп. Проблема тождества для групп. Проблема сопряженности для групп. Проблема изоморфизма для групп. Массовые (алгоритмические) проблемы, их положительное и отрицательное решение. Общая проблема о распознавании групповых свойств по заданию группы. Понятие о фундаментальных результатах П.С. Новикова и С.И. Адяна.

Тема 4. Свободные группы.

Определение свободных групп, различные способы задания их элементов: классы эквивалентности и несократимые слова. Решение проблемы тождества для свободных групп. Решение проблемы сопряженности для свободных групп. Подгруппы свободных групп. Убывающие цепочки подгрупп свободных групп и теоремы об их пересечении. Хопфовость свободных групп. Финитная аппроксимируемость свободных групп.

Тема 5. Преобразования Тице.

Преобразования Тице T1, T2, T3 и T4. Изоморфность групп, задания которых получаются друг из друга преобразованиями Тице. Теорема, о возможности перейти с помощью преобразований Тице от одного задания группы к любому другому ее заданию. Построение инвариантов групп.

Тема 6. Граф Кэли группы.

Построение графа Кэли по заданию группы образующими и определяющими соотношениями. Граф Кэли свободной группы, некоторых симметрических групп. Связь между группами и графами.

Тема 7. Фундаментальные группы топологических пространств.

Определение топологического пространства, примеры. Непрерывные отображения топологических пространств. Непрерывные пути и петли в топологическом пространстве. Умножение путей. Гомотопическая эквивалентность путей. Фундаментальная группа топологического пространства. Группы узлов. Группы кос. Связь между непрерывными отображениями топологических пространств и гомоморфизмами их фундаментальных групп. Гомеоморфизмы топологических пространств и изоморфизмы фундаментальных групп.

Тема 8. Задание факторгрупп и подгрупп.

Нахождение задания факторгруппы по заданию исходной группы и ее нормальной подгруппы. Вербальные подгруппы и приведенные свободные группы. Тождества в группах, многообразия групп. Абелевы, нильпотентные и разрешимые тождества и многообразия. Метод Рейдемейстера - Шрейера для нахождения задания подгруппы по заданию исходной группы. Система представителей правых смежных классов группы по подгруппе. Переписывающий процесс Рейдемейстера - Шрейера. Шрейеровская система представителей правых смежных классов группы по подгруппе.

Тема 9. Факторгруппы по коммутанту.

Специальные системы образующих для конечно порожденных подгрупп свободных абелевых групп конечного ранга. Прямое произведение групп. Теорема о строении конечно порожденных абелевых групп. Тест для изоморфизма групп. Факторгруппы групп узлов.

Тема 10. Свободное дифференциальное исчисление.

Групповое кольцо. Свободное дифференциальное исчисление Фокса. Частные производные Фокса в свободной группе. Основная формула свободного дифференциального исчисления. Матрица Александера. Элементарные идеалы, их цепочки. Полиномы узлов.

Тема 11. Свободное произведение групп и свободное произведение групп с объединенной подгруппой. HNN-расширения групп.

Определение свободного произведения групп. Каноническая форма элементов свободного произведения групп. Подгруппы свободного произведения групп, понятие о теореме А.Г. Куроша. Решение алгоритмических проблем для свободного произведения групп. Определение свободного произведения групп с объединенной подгруппой, каноническая форма

элементов. Понятие о теореме Зейферта - ван Кампена**.** HNN-расширение группы, каноническая форма элементов, лемма Британа.

Тема 12. Группы с условием малого сокращения.

Условие малого налегая определяющих слов, классы групп C'(1/k) и C(k). Решение для классов групп с условием малого сокращения проблем тождества и сопряженности. Результаты В.А. Тартаковского, М.Д. Гриндлингера, Р. Линдона и А.И. Гольберга.

Тема 13. Некоторые криптографические протоколы на группах.

Протокол Anschel-Anschel-Goldfeld: начальная установка - группа G (платформа протокола). Выбор Алисой и Бобом открытых наборов элементов группы G и секретных элементов.
Выработка общего секретного ключа - коммутатора элементов.
Протокол Ko-Lee-Cheon-Han-Kang-Park: начальная установка - корреспонденты Алиса и Боб выбирают (открыто) группу G - платформу протокола, два конечных подмножества попарно коммутирующих элементов и элемент g группы G.
Выработка материалов для создания общего секретного ключа: Алиса и Боб "случайным образом" выбирают секретные элементы.
Выработка общего секретного ключа.
Протокол Wang-Cao-Okamoto-Shao: начальная установка: корреспонденты Алиса и Боб выбирают (открыто) некоммутативный моноид G - платформу протокола, элемент g из G и обратимый элемент x в G.
Выработка материалов для создания общего секретного ключа.
Выработка общего секретного ключа.
Протокол Сидельников В.М.-Черепнев М.А.-Ященко В.Ю.: начальная установка - корреспонденты Алиса и Боб выбирают (открыто) полугруппу (моноид, группу) G - платформу протокола, два конечных подмножества попарно коммутирующих элементов и элемент g в G.
Выработка материалов для создания общего секретного ключа.
Выработка общего секретного ключа.
Протокол Stickel: начальная установка - G - неабелева конечная группа и два ее коммутирующих элемента.
Выработка материалов для создания общего секретного ключа.
Выработка общего секретного ключа.

Протоколы базируются на групповых автоморфизмах и эндоморфизмах.
Протокол Mahalanobis: начальная установка - корреспонденты Алиса и Боб выбирают (открыто) группу G - платформу протокола, два конечных подмножества попарно коммутирующих элементов группы автоморфизмов Aut (G) и элемент g в G.
Выработка материалов для создания общего секретного ключа.
Выработка общего секретного ключа.
Протокол Mahalanobis: начальная установка - корреспонденты Алиса и Боб выбирают (открыто) группу G -- платформу протокола, два конечных подмножества попарно коммутирующих элементов группы автоморфизмов Aut (G) и элемент g в G.
Выработка материалов для создания общего секретного ключа.
Выработка общего секретного ключа.
Протокол Habeeb-Kahrobaei-Koupparis-Shpilrain: начальная установка - корреспонденты Алиса и Боб выбирают (открыто) полугруппу или группу G - платформу протокола, ее автоморфизм и элемент.
Выработка материалов для создания общего секретного ключа.
Выработка общего секретного ключа.

Протоколы аутентификации, основанные на некоторых алгоритмических проблемах теории групп, которые можно отнести к сложным алгоритмическим проблемам.
Протокол Романькова-Григорьева-Шпильрайна: начальная установка - открыто выбирается бесконечная "эффективно заданная" группа G - платформа протокола с разрешимой проблемой равенства, но с алгоритмически неразрешимой проблемой эндоморфной сводимости.
Выбор "Системой" ("Доказывающим") открытого элемента g в G.
Выбор "Доказывающим" "Секретного" ключа - эндоморфизм группы G.
Построение "Открытого" ключа.
Раунд аутентификации.

Протокол Шпильрайна-Ушакова на базе проблемы скрученной сопряженности для групп.
Начальная установка: открыто выбирается группа G - платформа протокола, два ее эндоморфизма и элемент w в G.
"Секретный"' ключ "Доказывающего" и "Открытый" ключ.
Раунд аутентификации.
Протокол Мегрелишвили-Джинджихадзе: начальная установка - корреспонденты Алиса и Боб выбирают (открыто) векторное пространство V над полем F - платформу протокола, квадратную матрицу A и вектор v в V.
Выработка материалов для создания общего секретного ключа.
Выработка общего секретного ключа.
Система Росошека: сообщения -- элементы группового (полугруппового) кольца K[G] группы (полугруппы) G с коэффициентами из кольца K.
Начальная установка: Алиса выбирает эндоморфизмы.
Открытый ключ Алисы - эндоморфизмы, обратимый элемент x группового кольца K[G] и элемент.
Шифрование: зашифрование, расшифрование.

5. **Форма промежуточной аттестации:** зачет.

Аннотация дисциплины
«Избранные вопросы ассиметричной криптографии»

Направление 10.06.01 Информационная безопасность
Направленность (профиль) «Методы и системы защиты информации, информационная безопасность»

1. Дисциплина «Избранные вопросы ассиметричной криптографии» относится к факультативным дисциплинам.

2. Дисциплина «Избранные вопросы асимметричной криптографии» обеспечивает приобретение фундаментальных и профессиональных знаний, умений и навыков, содействует дальнейшей фундаментализации образования, развитию логического мышления и формированию математического и общенаучного мировоззрения. Целью изучения дисциплины является овладение базовыми понятиями и методами асимметричной криптографии (криптографии с открытым ключом), ознакомление с применениями в области обеспечения информационной безопасности, решения проблем конфиденциальности, целостности и аутентификации.

3. Общая трудоемкость дисциплины составляет 2 зачетные единицы, 72 часа.

4. Содержание дисциплины:

Тема № 1. Системы шифрования с открытым ключом.

Понятие односторонней функции и односторонней функции с «лазейкой».

Криптосистемы с открытым ключом - асимметричные системы шифрования. Вычислительно сложные задачи математики.

Ранцевые алгоритмы шифрования с открытым ключом, криптосистема Меркля-Хеллмана.

Криптосистема RSA и ее анализ. Система RSA и задача разложения натурального числа на множители.

Детерминированные методы разложения: метод пробного деления, метод “giant step – babe step”, метод Ферма, метод диофантовой аппроксимации.

Вероятностные методы разложения: p-метод Полларда (метод «Монте-Карло»), метод непрерывных дробей, метод квадратичного решета, разложение на эллиптической кривой.

Атаки на систему RSA, не требующие разложения: случай малого секретного показателя, случай специальных открытых показателей. Атаки на основе эндоморфизмов.

Шифрование с открытым ключом для группы вычислимого порядка: бесключевое шифрование Месси – Омуры, протокол Эль-Гамаля шифрования с открытым ключом.

Криптосистема Мак-Эллиса.

Шифрование с открытым ключом для группы трудновычислимого порядка: протокол шифрования Рабина, вероятностное шифрование.

Генераторы псевдослучайных последовательностей.

Тема № 2. Цифровая подпись документов.

Подписи на группе трудновычислимого порядка.
Схема подписи RSA.
Схема подписи Рабина.
Схема подписи Фиата – Шамира.
Подписи на группе вычислимого порядка.

Схема подписи Эль-Гамаля.
Схема подписи Шнора.
Стандарты ГОСТ Р 34.10-94, ГОСТ Р 34.10-2001 и
ГОСТ Р 34.10-2012.
Другие схемы подписи: схема "неоспоримой" подписи.
Схема подписи "вслепую".
Сравнительный анализ схем подписи.
Скрытый канал.
Электронные платежи.
Схема подписи с восстановлением сообщения.

Тема № 3. Хеш-функции.

Ключевые и бесключевые хеш-функции. Итеративные способы построения хеш-функций. Конструкции хеш-функций.

Использование хеш-функций и блочных шифров в системах аутентификации сообщений.

Коды аутентификации сообщений MAC и коды обнаружения ошибок MDC и MIC.

Изучение стандартов современных хеш-функций ГОСТ Р 34.11-2012.

Тема № 4. Криптосистемы на эллиптических кривых.

Алгебраические кривые на евклидовой плоскости. Квадратичные кривые (квадрики, коники). Сложение точек, его свойства.

Кубические кривые, 2-местная операция сложения точек, ее свойства.

Понятие о проективном пространстве.

Проективная плоскость. Алгебраические кривые на проективной плоскости.

Особые и неособые кубические кривые. Форма Вейерштрасса.

Эллиптические кривые, свойства операции сложения точек на них.

Группа точек на эллиптической кривой.

Эллиптические кривые над конечными полями.

Порядок группы точек эллиптической кривой над конечным полем, алгоритм Чуфа.

Протоколы на эллиптических кривых: аналог системы RSA, установление сеансового ключа.

Встраивание открытого текста в координату точки.

Шифрование. Цифровая подпись.

Понятие об эллиптических функциях. Функция Вейерштрасса. Параметризация эллиптической кривой над полем комплексных чисел.

Эллиптические кривые над полем рациональных чисел, рациональные и целочисленные точки на них.

Расчет числа точек эллиптической кривой в общем случае: многочлены деления, алгоритм Чуфа

Расчет числа точек эллиптической кривой над расширенным полем.

Расчет числа точек эллиптической кривой над простыми полями.

Эллиптические кривые с комплексным умножением.

Протоколы для электронных платежей.

Тема № 5. Дискретное логарифмирование в мультипликативной группе конечного поля.

Метод базы разложения.

Логарифмирование в простом поле методом решета числового поля.

Логарифмирование в расширенном поле.

Группа классов квадратичного поля.

Логарифмирование в группе функций Лукаша.

Связь между задачами Диффи – Хеллмана и дискретного логарифмирования.

Тема № 6. Дискретное логарифмирование в группе точек эллиптической кривой над конечным полем.

Задача дискретного логарифмирования на эллиптической кривой.

Универсальные методы логарифмирования.

Метод Гельфонда.

Метод встреч посередине и “giant step – babe step”.

Метод Полларда.

Метод встречи на случайном дереве.

Сравнение сложности логарифмирования на эллиптической кривой и в конечном поле.

Влияние комплексного умножения на сложность логарифмирования.

Логарифмирование с использованием функции Вейля.

Время жизни общего открытого ключа криптосистемы, основанной на дискретном логарифмировании: мультипликативная группа поля, группа точек эллиптической кривой.

Логарифмирование якобиане гиперэллиптической кривой.

Требования к эллиптической кривой.

Тема № 7. Протоколы распределения ключей.

Понятие криптографического протокола.

Передача ключей с использованием симметричной системы шифрования. Двусторонние и трехсторонние протокола. Протокол Kerberos.

Передача ключей с использованием асимметричной системы шифрования. Сертификаты открытых ключей.

Открытое распределение ключей.

Предварительное распределение ключевых материалов, схема Блома.

Возможные атаки на протоколы распределения ключей. Управление ключами.

Тема № 8. Некоторые современные направления криптографических исследований.

Криптография, базирующаяся на группах.

Задание групп образующими и определяющими соотношениями. .

Группы кос и криптопротоколы на их основе.

Криптосистемы на базе групп, заданных образующими и определяющими соотношениями.

Протокол Anschel-Anschel-Goldfeld выработки общего секретного ключа на базе коммутаторов элементов групп.

Протокол Ko -- Lee -- Cheon -- Han -- Kang -- Park выработки общего секретного ключа на базе проблемы сопряженности для группы кос.

Протокол Wang -- Cao -- Okamoto -- Shao выработки общего секретного ключа на базе некоммутативного моноида.

Протокол Сидельникова В. М. -- Черепнева М. А. -- Ященко В. Ю на базе некоммутативных полугрупп.

Протокол Stickel на базе конечной (периодической) некоммутативной группы.

Протоколы, базирующиеся на групповых автоморфизмах и эндоморфизмах: протокол Mahalanobis, протокол Habeeb -- Kahrobaei -- Koupparis -- Shpilrain.

Протоколы аутентификации, основанные на некоторых "трудных" алгоритмических проблемах теории групп: протокол Романькова -- Григорьева -- Шпильрайна, протокол

Шпильрайна -- Ушакова, протокол Мегрелишвили -- Джинджихадзе.
Криптосистема Росошека.

5. **Форма промежуточной аттестации:** зачет.