МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Ярославский государственный университет им. П.Г. Демидова

Кафедра компьютерной безопасности и математических методов обработки информации

УТВЕРЖДАЮ

Декан математического факультета

_____ П.Н.Нестеров

«18» мая 2021 г.

Рабочая программа дисциплины
«Методы комбинаторной теории групп в криптографии»

Направление подготовки
10.06.01 Информационная безопасность

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

Форма обучения очная

Программа рассмотрена
на заседании кафедры компьютерной безопасности
и математических методов обработки информации
от «16» апреля 2021 года, протокол № 8

Ярославль

1. Цели освоения дисциплины

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.

2. Место дисциплины в структуре программы аспирантуры

Дисциплина «Методы комбинаторной теории групп в криптографии» является дисциплиной по выбору вариативной части. Она играет важную роль для общематематической и общепрофессиональной подготовки специалиста. При ее изучении используются знания, полученные при изучении таких математических дисциплин, как “Алгебра”, "Теория чисел", "Дискретная математика", "Топология", "Математическая логика" и "Теория алгоритмов".

3. Планируемые результаты обучения по дисциплине – знания, умения, навыки и (или) опыт деятельности, характеризующие этапы формирования компетенций и обеспечивающие достижение планируемых результатов освоения программы аспирантуры, и критерии их оценивания

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Общепрофессиональными компетенции

- способностью формулировать научные задачи в области обеспечения информационной безопасности, применять для их решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность (ОПК-1);
- способностью разрабатывать частные методы исследования и применять их в самостоятельной научно-исследовательской деятельности для решения конкретных исследовательских задач в области обеспечения информационной безопасности (ОПК-2);

Профессиональные компетенции:

- способностью разрабатывать защитные механизмы и средства обеспечения информационной безопасности, осуществлять их настройку, регулировку, восстановление работоспособности (ПК-2);

Результаты обучения выпускника формулируются в следующих категориях:
«знать» – означает способность выпускника воспроизводить учебный материал с требуемой степенью научной точности (формулировать определение, с достаточной полнотой описывать процесс и явление);

«уметь» – означает способность выпускника решать типовые (адаптированные) задачи на основе воспроизведения алгоритма решения и его применения в конкретных стандартных условиях;
«владеть» – означает способность выпускника решать усложненные, в том числе комплексные задачи. Задачи данного уровня решаются на основе ранее приобретенных знаний и умений, с их трансформацией и применением в новых нетиповых условиях.

Код компетенции	**Планируемые результаты обучения**	**Критерии оценивания результатов обучения**		
		Пороговый уровень	**Продвинутый уровень**	**Высокий Уровень**
способностью формулировать научные задачи в области обеспечения информационной безопасности, применять для их решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность (ОПК-1)	**Знать:** - методологию научного познания в области физико-математических и технических наук (З-7.1); - научные подходы к обеспечению информационной безопасности и характеристику ее составляющих (З-7.2); - научную классификацию источников и угроз информационной безопасности (З-7.3). **Уметь:** - обоснованно классифицировать защищаемую информацию по видам тайны и степени конфиденциальности (У-7.1); - обоснованно классифицировать и оценивать угрозы информационной безопасности компьютерных систем (У-7.2). **Владеть:** - специальной	**Знает:** - методологию научного познания в области физико-математических и технических наук (З-7.1); - научные подходы к обеспечению информационной безопасности и характеристику ее составляющих (З-7.2); - научную классификацию источников и угроз информационной безопасности (З-7.3).	**Знает:** - методологию научного познания в области физико-математических и технических наук (З-7.1); - научные подходы к обеспечению информационной безопасности и характеристику ее составляющих (З-7.2); - научную классификацию источников и угроз информационной безопасности (З-7.3). **Умеет:** - обоснованно классифицировать защищаемую информацию по видам тайны и степени конфиденциальности (У-7.1); - обоснованно классифицировать и оценивать угрозы информационной безопасности компьютерных систем (У-7.2).	**Знает:** - методологию научного познания в области физико-математических и технических наук (З-7.1); - научные подходы к обеспечению информационной безопасности и характеристику ее составляющих (З-7.2); - научную классификацию источников и угроз информационной безопасности (З-7.3). **Умеет:** - обоснованно классифицировать защищаемую информацию по видам тайны и степени конфиденциальности (У-7.1); - обоснованно классифицировать и оценивать угрозы информационной безопасности компьютерных систем (У-7.2). **Владеет:** - специальной

	профессиональной терминологией в области информационной безопасности (В-7.1); - научно обоснованными методами обеспечения информационной безопасности и построения систем защиты информации от несанкционированного доступа (В-7.2).			профессиональной терминологией в области информационной безопасности (В-7.1); - научно обоснованными методами обеспечения информационной безопасности и построения систем защиты информации от несанкционированного доступа (В-7.2).
способностью разрабатывать частные методы исследования и применять их в самостоятельной научно-исследовательской деятельности для решения конкретных исследовательских задач в области обеспечения информационной безопасности (ОПК-2)	**Знать:** - принципы и инструментарий научно-исследовательской деятельности в области обеспечения информационной безопасности (З-8.1); - средства и методы научного исследования (З-8.2); - математический аппарат и инструментарий обработки результатов исследований (З-8.3). **Уметь:** - применять философско-методологические принципы и установки для решения частных научных задач (У-8.1); - применять систему математических	**Знает:** - принципы и инструментарий научно-исследовательской деятельности в области обеспечения информационной безопасности (З-8.1); - средства и методы научного исследования (З-8.2); - математический аппарат и инструментарий обработки результатов исследований (З-8.3).	**Знает:** - принципы и инструментарий научно-исследовательской деятельности в области обеспечения информационной безопасности (З-8.1); - средства и методы научного исследования (З-8.2); - математический аппарат и инструментарий обработки результатов исследований (З-8.3). **Умеет:** - применять философско-методологические принципы и установки для решения частных научных задач (У-8.1);	**Знает:** - принципы и инструментарий научно-исследовательской деятельности в области обеспечения информационной безопасности (З-8.1); - средства и методы научного исследования (З-8.2); - математический аппарат и инструментарий обработки результатов исследований (З-8.3). **Умеет:** - применять философско-методологические принципы и установки для решения частных научных задач (У-8.1); - применять систему математических

	моделей и методов при осуществлении научно-исследовательской деятельности (У-8.2); - оценивать достоверность результатов, полученных в ходе исследований (У-8.3). **Владеть:** - методами проведения теоретических исследований (В-8.1); - методами планирования и проведения экспериментов (В-8.2); - методами использования средств обработки результатов исследований (В-8.3).		- применять систему математических моделей и методов при осуществлении научно-исследовательской деятельности (У-8.2); - оценивать достоверность результатов, полученных в ходе исследований (У-8.3).	моделей и методов при осуществлении научно-исследовательской деятельности (У-8.2); - оценивать достоверность результатов, полученных в ходе исследований (У-8.3). **Владеет:** - методами проведения теоретических исследований (В-8.1); - методами планирования и проведения экспериментов (В-8.2);- методами использования средств обработки результатов исследований (В-8.3).
Способностью разрабатывать защитные механизмы и средства обеспечения информационной безопасности, осуществлять их настройку, регулирование, восстановление работоспособности (ПК-2)	**Знать:** защитные механизмы и средства обеспечения информационной безопасности. **Уметь:** осуществлять настройку, регулирование и восстановление работоспособности защитных механизмов и средств обеспечения информационной безопасности. **Владеть:**	**Знает:** защитные механизмы и средства обеспечения информационной безопасности, основные понятия, результаты и методы комбинаторной теории групп.	**Знает:** защитные механизмы и средства обеспечения информационной безопасности, основные понятия, результаты и методы комбинаторной теории групп. **Умеет:** осуществлять настройку, регулирование и восстановление	**Знает:** защитные механизмы и средства обеспечения информационной безопасности, основные понятия, результаты и методы комбинаторной теории групп. **Умеет:** осуществлять настройку, регулирование и восстановление работоспособности защитных

	навыками настройки, регулирования и восстановления работоспособности защитных механизмов и средств обеспечения информационной безопасности.		работоспособности защитных механизмов и средств обеспечения информационной безопасности.	механизмов и средств обеспечения информационной безопасности. **Владеет:** навыками настройки, регулирования и восстановления работоспособности защитных механизмов и средств обеспечения информационной безопасности.

4. Объем, структура и содержание дисциплины

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

Дисциплина изучается в течение четвертого семестра. Формой итоговой промежуточной аттестации по дисциплине является зачет.

№ п/п	Темы (разделы) дисциплины, их содержание	Семестр	Виды учебных занятий и их трудоемкость (в академических часах)					Формы текущего контроля успеваемости Форма промежуточной аттестации *(по семестрам)*
			Лекции	практические	лабораторные	консультации	самостоятельная работа	
1	Базовые сведения по теории групп.					0,5	7	Собеседование на консультации
2	Задание групп образующими и определяющими соотношениями.	4	1				7	
3	Фундаментальные проблемы М. Дэна.	4	1				7	
4	Свободные группы.	4	1				7	
5	Преобразования Тице.	4	1				7	
6	Граф Кэли группы.	4					7	
7	Фундаментальные группы топологических пространств.	4				0,5	7	Собеседование на консультации
8	Задание факторгрупп и подгрупп.	4	1				7	

9	Факторгруппы по коммутанту.	4	1				7	
10	Свободное дифференциальное исчисление.	4				0,5	7	Собеседование на консультации
11	Свободное произведение групп и свободное произведение групп с объединенной подгруппой. HNN-расширения групп.	4	1				7	
12	Группы с условием малого сокращения.	4				0,5	7	Собеседование на консультации
13	Некоторые криптографические протоколы на группах.	4	1				14	
		4						Зачет
	Всего		**8**			**2**	**98**	

Содержание разделов 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 Бритона.

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. Образовательные технологии, используемые при осуществлении образовательного процесса по дисциплине

В процессе обучения используются следующие образовательные технологии:
Академическая лекция (или лекция общего курса) – последовательное изложение материала, осуществляемое преимущественно в виде монолога преподавателя.
Требования к академической лекции: современный научный уровень и насыщенная информативность, убедительная аргументация, доступная и понятная речь, четкая структура и логика, наличие ярких примеров, научных доказательств, обоснований, фактов. Академическая лекция, как правило, состоит из трех частей: вступления (введения), изложения и заключения:

- вступление (введение) определяет тему, план и цель лекции. Оно призвано заинтересовать и настроить аудиторию, сообщить, в чём заключается предмет лекции и (или) её актуальность, основная идея (проблема, центральный вопрос), связь с предыдущими и последующими занятиями, поставить её основные вопросы. Введение должно быть кратким и целенаправленным.

- изложение является основной частью лекции, в которой реализуется научное содержание темы, ставятся все узловые вопросы, приводится вся система доказательств с использованием наиболее целесообразных методических приемов. Каждое теоретическое положение должно быть обосновано и доказано, приводимые формулировки и определения должны быть четкими, насыщенными глубоким содержанием.

- заключение обобщает в кратких формулировках основные идеи лекции, логически ее завершая. В заключении могут даваться рекомендации о порядке дальнейшего изучения основных вопросов лекции самостоятельно по указанной литературе.

Вводная лекция – дает первое целостное представление о дисциплине (или ее разделе) и ориентирует студента в системе изучения данной дисциплины. Обучающиеся знакомятся с назначением и задачами курса, его ролью и местом в системе учебных дисциплин и в системе подготовки специалиста. Дается краткий обзор курса, история развития науки и практики, достижения в этой сфере, имена известных ученых, излагаются перспективные направления исследований. На этой лекции высказываются методические и организационные особенности работы в рамках курса, а также дается анализ рекомендуемой учебно-методической литературы.

6. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения и информационных справочных систем (при необходимости).

В процессе осуществления образовательного процесса используются:

– для формирования текстов материалов для промежуточной и текущей аттестации – программы Microsoft Office, издательская система MikTex;

– для поиска учебной литературы библиотеки ЯрГУ – Автоматизированная библиотечная информационная система "БУКИ-NEXT" (АБИС "Буки-Next").

7. Перечень основной и дополнительной учебной литературы, необходимых для освоения дисциплины

а) основная литература

1. Адян С.И., Дурнев В.Г. Алгоритмические проблемы для групп и полугрупп // Успехи матем. наук. - 2000. - Том 55, № 2. - С. 3-94.

2. Адян С.И. Алгоритмическая неразрешимость проблем распознавания некоторых свойств групп // Докл. АН СССР. 1955. Т. 103. № 4. С. 533-535.

3. Адян С.И. Неразрешимость некоторых алгоритмических проблем теории групп // Тр. Моск. матем. о-ва. 1957. Т. 6. С. 231-298.

4. Дурнев В.Г. О системах уравнений на свободных нильпотентных группах // Вопросы теории групп и гомолог. алгебры. Ярославль. ЯрГУ. 1981. С.66-69.

5. Каргаполов М.И., Мерзляков Ю.И. Основы теории групп. М.: Наука, 1982.

6. Коксетер Г.С.М., Мозер У.О.Дж. Порождающие элементы и определяющие соотношения дискретных групп. М.: Наука. 1980.

7. Курош А.Г. Теория групп. М.: Наука. 1967

8. Линдон Р., Шупп П. Комбинаторная теория групп. М.: Мир. 1980.

9. Магнус В., Каррас А., Солитэр Д. Комбинаторная теория групп. М.: Наука. 1974.

10. Маканин Г.С. Проблема сопряженности в группе кос // Докл. АН СССР. 1968. Т. 182. № 3. С.495-496.

11. Маканин Г.С. Уравнения в свободной группе // Изв. АН СССР. Сер. мат. 1982. Т. 46. № 6. С.1199-1273.

12. Мальцев А.И. Алгоритмы и рекурсивные функции. М.: Наука. 1965.

13. Марков А.А. Основы алгебраической теория кос. Труды МИАН им. В.А.Стеклова, 1945. Том 16. II. 10.

14. Матиясевич Ю.В. Простые примеры неразрешимых ассоциативных исчислений // Докл. АН СССР. 1967. Т. 173. № 6. С. 1264-1266.

15. Новиков П.С. Об алгоритмической неразрешимости проблемы тождества теории групп // Докл. АН СССР. 1952. Т. 85. № 4. С. 709-712.

16. Новиков П.С. Неразрешимость проблемы сопряженности в теории групп // Изв. АН СССР. Сер. матем. 1954. Т. 18. № 6. С. 485-524.

17. Новиков П.С. Об алгоритмической неразрешимости проблемы тождества слов в теории групп // М.: Наука. 1955. Труды МИАН. Т. 44.

18. Ольшанский А.Ю., Шмелькин А.Л. Бесконечные группы. Итоги науки и техники. ВИНИТИ. Современные проблемы математики. Фундаментальные направления. 1989. Том 37. С. 5-113.

19. Павлов Р.Д. К проблеме распознавания групповых свойств // Матем. заметки. 1971. Т. 10. № 2. С. 169-180.

20. Разборов А.А. О системах уравнений в свободной группе // Изв. АН СССР. Сер. мат. 1984. Т. 48. № 4.

21. Романьков В.А. О неразрешимости проблемы эндоморфной сводимости в свободных нильпотентных группах и в свободных кольцах // Алгебра и логика. 1977. Т. 16. № 4. С.457-471.

22. Романьков В.А. Об уравнениях в свободных метабелевых группах // Сиб. матем. журн. 1979. Т. 20. № 3. С.671-673.

23. Романьков В.А. Алгебраическая криптография. Омск. Изд-во. Ом. гос. ун-та., 2013. 136 с.

24. Сидельников В.М., Черепнев М.А., Ященко В.В. Системы открытого распределения ключей на основе некоммутативных полугрупп // Докл. РАН. 1993. Том 332. № 5. С. 566 -- 567.

25. Тартаковский В.А. О проблеме тождества для некоторых типов групп // Докл. АН СССР. 1947. Т. 58. С. 1909-1910.

26. Тартаковский В.А. Решение проблемы тождества для группы с k-сократимым базисом при k=6 // Изв. АН СССР. Сер. матем. 1949. Т. 13. С. 483-494.

27. Фридман А.А. О взаимоотношении между проблемой тождества и проблемой сопряженности в конечно определенных группах // Тр. Моск. матем. о-ва. 1960. Т. 9. С. 329-356.

28. Хмелевский Ю.И. Решение уравнений в словах с тремя неизвестными // Докл. АН СССР. 1967. Т. 177. № 5. С.1023-1025.

29. Хмелевский Ю.И. Системы уравнений в свободной группе. I, II // Изв. АН СССР. Сер. мат. 1971. Т. 35. № 6. С.1237-1268. 1972. Т. 36. № 1. С.110-179.

30. Шпильрайн В.Э. Об уравнениях в группах вида F_n(R) // Алгоритмические проблемы теории групп и полугрупп. Тула. ТГПИ. 1990. С.164-183.

31. Artin E. Theorie der Zopfe. // Abh. Math. Sem. Hamburg. Univ. - 1925. - Bd. 4. - S. 47-72.

32. Artin E. Theory of braids // Ann. Math. 1947. Vol. 48. Pp.101-126.

33. Boone W.W. Certain simple unsolvable problems in group theory // Proc. Kon. ned. akad. wetensch. A, 1957. V. 60. P. 22-27, 227-232.

34. Boone W.W. The word problem // Ann. Math. 1959. V. 70. N 2. P. 207-265.

35. Britton J.L. The word problem for groups // Proc. London Math. Soc. 1958. V. 8. P. 493-506.

36. Britton J.L. The word problem // Ann. Math. 1963. V. 77. № 1. P. 16-32.

37. Dehn M. \"Uber unendliche diskontinuerliche Gruppen // Math.Ann. 1911. Bd. 71. S. 116-144.

38. Diffie W., Hellman M.E. New directions in cryptography // IEEE Transaction Information Theory. 1976. Vol. 22. № 6. P. 644 - 654.

39. Garside F.A. On the braid group and other groups // Quart. J. Math. 1969. Vol. 20. № 78. Pp.235-254.

40. Greendlinger M. Dehn's algorithm for the word problem // Comm. Pure and Appl. Math. 1960. V. 13. P. 67-83.

41. Greendlinger M. On Dehn's algoriths for the conjugacy and word problems with applications // Comm. Pure and Appl. Math. 1960. V. 13. P. 641-677.

42. Higman G. Subgroups of finitely presented groups // Proc. Roy. Soc. London A. 1961. V. 262. № 1311. P. 455-475.

43. Ko K.H., Lee S.J., Cheon J.H. New public-key cryptosistem using braid groups // Advances in cryptology -- CRYPTO 2000 (Santa Barbara, CA). Lecture Notes in Comput. Sci. 1880. 2000. P. 166 - 183. Springer, Berlin.

44. Magnus W. Das Identitats problem fur Gruppen mit einer definierenden Relation // Math. Ann. 1932. Bd. 106. S. 295-307. Рус. пер.: Успехи мат. наук. 1941. Вып. 8. С. 365-376.

45. Miller C.F. III. Some connection between Hilbert's 10th problem and the theory of groups // Word Probl. Decis. Probl. Group Theory. Amsterdam. London. P. 483-506.

46. Myasnikov A., Shpilrain V., Ushakov A. Group-based cryptography. Advances courses in Math. CRM, Barselona. Basel-Berlin-New York: Birkhauser Verlag, 2008. 183 p.

47. Myasnikov A., Shpilrain V., Ushakov A. Non-commutative cryptography and complexity of group-theoretic problems // Amer. Math. Soc. Surveys and Monographs. Providence R.I.: Amer. Math. Soc., 2001. 385 p.

48. Rabin M.O. Recursive unsolvability of group theoretic problems // Ann. Math. 1958. V. 67. № 1. P. 172-194.

49. Rivest R.L., Shamir A., Adleman L. A method for obtaining digital signatures and public-key cryptosistems // Comm. ACM. 1978. Vol. 21. № 2. P. 120 - 126.

б) дополнительная литература

1. Ахо А., Хопкрофт Дж., Ульман Дж. Построение и анализ вычислительных алгоритмов. М.: Мир, 1983.
2. Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи. М.: Мир, 1979.

3. Безверхний В.Н. Решение проблемы вхождения для одного класса групп // Вопросы теории групп и полугрупп. Тула. ТГПИ имени Л.Н.Толстого. 1972. Вып. 2. С.3-86.

4. Борисов В.В. Простые примеры групп с неразрешимой проблемой тождества // Матем. заметки. 1969. Т. 6. Вып. 5. С. 521-532.

5. Валиев М.К. Примеры универсальных конечно определенных групп // Докл. АН СССР. 1973. Т. 211. С. 265-268.

6. Гольберг А.И. О невозможности усиления некоторых результатов Гриндлингера и Линдона // Успехи матем. наук. 1978. Т. 33. № 6. С. 201-202.

7. Косневски Ч. Начальный курс алгебраической топологии. М.: Мир. 1983.
8. Кроуэл Р., Фокс Р. Введение в теорию узлов. М.: Мир. 1967.

9. Маканина Т.А. Проблема вхождения для группы кос B(n) при n>4 // Матем. заметки. 1981. Т. 29. № 1. С.31-33.

10. Мальцев А.И. О гомоморфизмах на конечные группы // Уч. зап. Ивановск. гос. пед. ин-та. 1958. Т. 18. № 5. С. 49-60.

11. Мальцев А.И. Об одном соответствии между кольцами и группами // Мат. сб. 1960. Т. 50. № 2. С. 257-266.

12. Мальцев А.И. Алгоритмы и рекурсивные функции. М.: Наука. 1965.

13. Мальцев А.И. О свободных разрешимых группах // ДАН СССР. 1960. Т. 130. № 3. С.495-498.
14. Масси У., Столлингс Дж. Алгебраическая топология. Введение. М.: Мир. 1977.

15. Матиясевич Ю.В. Диофантовость перечислимых множеств // ДАН СССР. - 1970. - Том 130, № 3. - С. 495-498.

16. Матиясевич Ю.В. Десятая проблема Гильберта. М.: Наука, 1993.

17. Михайлова К.А. Проблема вхождения для прямых произведений групп // Докл. АН СССР. 1958. Т. 119. С. 1103-1105.

18. Михайлова К.А. Проблема вхождения для свободных произведений групп // Докл. АН СССР. 1959. Т. 127. С. 746-748.

19. Ольшанский А.Ю. Геометрия определяющих соотношений в группах. М.: Наука. 1989.

20. Ремесленников В.Н. Пример группы, конечно-определенной в многообразии A^5, с неразрешимой проблемой равенства слов // Алгебра и логика. 1973. Т. 12. № 5. С. 577-602.

21. Репин Н.Н. Уравнения с одной неизвестной в нильпотентной группе // Мат. заметки. 1983. Т. 34. № 2. С.201-206.

22. Романовский Н.С. О некоторых алгоритмических проблемах для разрешимых групп // Алгебра и логика. 1974. Т. 13. № 1. С. 26-34.

23. Стышнев В.Б. Извлечение корня в группе кос // Изв. АН СССР. Сер. мат. 1978. Т. 42. № 5. С.1120-1131.

24. Тайцлин М.А. О проблеме изоморфизма для коммутативных полугрупп // Матем. сборник. 1974. Т. 93. № 1. С. 103-128.

25. Тайцлин М.А. Проблема изоморфизма для коммутативных полугрупп решается положительно // Теория моделей и ее применения. Алма-Ата. 1980. С. 75-81.

26. Харлампович О.Г. Конечно определенная разрешимая группа с неразрешимой проблемой равенства // Изв. АН СССР. Сер. матем. 1981. Т. 45. № 4. С. 852-873.

27. Цейтин Г.С. Ассоциативное исчисление с неразрешимой проблемой эквивалентности // Труды матем. ин-та. АН СССР. 1958. Т. 52. С. 172-189.

28. Чеботарь А.А. Подгруппы групп с одним определяющим соотношением // Известия высших учебных заведений. Математика. 1978. N 8(195). С. 109-110.

29. Aanderaa S. A proof of Higman's embedding theorem using Britton extentions of groups // Word Problems I. Studies in Logic and the Foundations of Mathematics. 1973.

30. Garside F.A. On the braid group and other groups // Quart. J. Math. 1969. Vol. 20. № 78. Pp.235-254.

31. Grunewald F., Segal D. Some general algorithms. I. Arithmetic groups. II. Nilpotent groups // Ann. Math. 1980. V. 112. № 3. P. 531-583. P. 585-617.

32. Higman G., Neumann B.H., Neumann H. Embedding theorems for groups // J. London Math. Soc. 1949. V. 24. P. 247-254.

33. Higman G. Subgroups of finitely presented groups // Proc. Roy. Soc. London A. 1961. V. 262. № 1311. P. 455-475.

34. van Kampen E.R. On the connection between the fundamental groups of some related spaces // Amer. J. Math. 1933. V. 55. P. 261-267.

35. van Kampen E.R. On some lemmas in the theory of groups of some related spaces // Amer. J. Math. 1933. V. 55. P. 268-273.

36. Macintyre A. On algebraically closed groups // Ann. Math. 1972. V. 96. № 1. P. 53-97.

37. Neumann B.H. A note on algebraically closed groups // J. London. Math. Soc. 1952. Vol.27. Pp. 227-242.

38. Newman B.B. Some results on one-relator groups // Bull. Amer. Math. Soc. 1968. V. 74. P. 568-571.

39. Rips E. Another characterization of finitely generated groups with a solvable word problem // Bull. London. Math. Soc. 1982. Vol.14. № 1. P.43-44.

40. Turing A.M. On computable numbers, with an application to the Entscheidugsproblem // Proceedings of London Mathematical Society. Ser. 2. 1936. V. 42. № 3,4. P. 230-265.

41. Sapir M.V. On the word problem in periodic group varieties // International Journal of Algebra and Computation. 1991. V. 1. № 1. P. 115-126.

42. Scott D. A short recursively unsolvable problem (abstract) // J. Symbol. Log. 1956. V. 21. № 1. P. 11-112.

43. Scott W.R. Algebraically closed groups // Proc. Amer. Math. Soc. 1951. Vol.2. Pp.118-121.

в) ресурсы сети «Интернет»

1.Электронные каталоги НБ ЯрГУ

(http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php) содержат библиографические записи всех видов документов, составляющих фонд библиотеки, на русском и иностранных языках.

2. Личный кабинет (http://lib.uniyar.ac.ru/opac/bk_login.php) возможность получения on-line доступа к списку выданной в автоматизированном режиме литературы, просмотра и копирования электронных версий изданий сотрудников университета (учеб. и метод. пособия, тексты лекций и т.д.) Для работы в «Личном кабинете» необходимо зайти на сайт Научной библиотеки ЯрГУ с любой точки, имеющей доступ в Internet, в пункт меню *«Электронный каталог»*; пройти процедуру авторизации, выбрав вкладку *«Авторизация»*, и заполнить представленные поля информации.

3.Электронная библиотека учебных материалов ЯрГУ

(http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php) содержит более 2500 полных текстов учебных и учебно-методических материалов по основным изучаемым дисциплинам, изданных в университете. Доступ в сети университета, либо по логину/паролю.

4.Электронный архив ЯрГУ

(http://elar.uniyar.ac.ru/jspui/community-list**)** представляет собой коллекцию полнотекстовых электронных публикаций в области научных исследований. База данных предназначена для использования в учебных и научных целях, облегчая доступ к информации о научных работах и их содержанию.

5. Электронная картотека «Книгообеспеченность»

(http://www.lib.uniyar.ac.ru/opac/bk_bookreq_find.php)

раскрывает учебный фонд научной библиотеки ЯрГУ, предоставляет оперативную информацию о состоянии книгообеспеченности дисциплин основной и дополнительной литературой, а также цикла дисциплин и специальностей. Электронная картотека «Книгообеспеченность» доступна в сети университета и через Личный кабинет.

Русскоязычные электронные ресурсы (внешние)

1. Научная электронная библиотека (НЭБ) (http://elibrary.ru) – это крупнейший российский информационный портал, содержащий рефераты и полные тексты более 12 млн. научных статей и публикаций. **ЯрГУ выписывает в электронном виде 66 журналов,** более 2 500 наименований журналов на английском и русском языках находятся в свободном доступе. Для работы с полными текстами необходимо зарегистрироваться. Доступ к полным текстам журналов в сети университета.

2. Электронная библиотека диссертаций Российской государственной библиотеки (http://diss.rsl.ru) содержит более 580 000 полных текстов диссертаций и авторефератов. Доступ осуществляется в сети университета.

8. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине включает в свой состав специальные помещения:
-учебные аудитории для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации;
-помещения для самостоятельной работы;
-помещения для хранения и профилактического обслуживания оборудования.

Специальные помещения укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления информации большой аудитории.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации.

Число посадочных мест в лекционной аудитории больше либо равно списочному составу потока, а в аудитории для практических занятий (семинаров) – списочному составу группы обучающихся.

Автор(ы) :

Зав. кафедрой компьютерной безопасности и математических методов обработки информации, д.ф.-м.н. Дурнев В.Г.

_____

(подпись)

Приложение к №1 к рабочей программе дисциплины
«Методы комбинаторной теории групп в криптографии»

Оценочные средства
для проведения текущей и/или промежуточной аттестации аспирантов
по дисциплине

1. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Домашние задания по теме № 2 **"Задание групп образующими и определяющими соотношениями."**

Задания для самостоятельного решения № 1 - 14 из параграфа 1.1 и № 1-21 параграфа 1.2 главы I монографии Магнус В. Комбинаторная теория групп / В. Магнус, А. Каррас, Д. Солитэр. М.: Наука. 1974. 456 с.

Домашние задания по теме № 3 **"Фундаментальные проблемы М. Дэна."**

Задания для самостоятельного решения № 1 - 16 из параграфа 1.3 главы I монографии Магнус В. Комбинаторная теория групп / В. Магнус, А. Каррас, Д. Солитэр. М.: Наука. 1974. 456 с.

Домашние задания по теме № 4 **"Свободные группы."**

Задания для самостоятельного решения № 1 - 31 из параграфа 1.4 главы I и № 1 - 37 из параграфа 2.4 главы II монографии Магнус В. Комбинаторная теория групп / В. Магнус, А. Каррас, Д. Солитэр. М.: Наука. 1974. 456 с.

Домашние задания по теме № 5 **"Преобразования Тице."**

Задания для самостоятельного решения № 1 - 16 из параграфа 1.5 главы I монографии Магнус В. Комбинаторная теория групп / В. Магнус, А. Каррас, Д. Солитэр. М.: Наука. 1974. 456 с.

Домашние задания по теме № **6. "Граф Кэли группы."**

Задания для самостоятельного решения № 1 - 16 из параграфа 1.6 главы I монографии Магнус В. Комбинаторная теория групп / В. Магнус, А. Каррас, Д. Солитэр. М.: Наука. 1974. 456 с.

Домашние задания по теме № **8. "Задание факторгрупп и подгрупп."**

Задания для самостоятельного решения № 1 - 8 из параграфа 2.1 и № 1 - 40 из параграфа 2.2 № 1 - 26 из параграфа 2.4 главы II монографии Магнус В. Комбинаторная теория групп / В. Магнус, А. Каррас, Д. Солитэр. М.: Наука. 1974. 456 с.

Домашние задания по теме № **9. "Факторгруппы по коммутанту."**

Задания для самостоятельного решения № 1 - 21 из параграфа 3.3 главы III монографии Магнус В. Комбинаторная теория групп / В. Магнус, А. Каррас, Д. Солитэр. М.: Наука. 1974. 456 с.

Домашние задания по теме № **10. "Свободное дифференциальное исчисление."**

Задания для самостоятельного решения № 1 - 16 из параграфа 3.4 главы III монографии Магнус В. Комбинаторная теория групп / В. Магнус, А. Каррас, Д. Солитэр. М.: Наука. 1974. 456 с.

Домашние задания по теме № **11. "Свободное произведение групп и свободное произведение групп с объединенной подгруппой. HNN-расширения групп."**

Задания для самостоятельного решения № 1 - 34 из параграфа 4.1 и № 1 - 49 из параграфа 4.2 главы IV монографии Магнус В. Комбинаторная теория групп / В. Магнус, А. Каррас, Д. Солитэр. М.: Наука. 1974. 456 с.

Домашние задания по теме № **12. "Группы с условием малого сокращения."**

Задания для самостоятельного решения № 1 - 31 из параграфа 4.4 главы IV монографии Магнус В. Комбинаторная теория групп / В. Магнус, А. Каррас, Д. Солитэр. М.: Наука. 1974. 456 с.

Домашние задания по теме № **13. "Некоторые криптографические протоколы на группах."**

Выполнить программную реализацию одного из криптопротоколов.

1.1 Список вопросов и (или) заданий для проведения промежуточной аттестации

Вопросы к зачету по дисциплине
"Методы комбинаторной теории групп в криптографии "
(4 семестр)

Тема 1. Базовые сведений по теории групп.

1. Двуместные алгебраические операции. Группоиды, гомоморфизмы и изоморфизмы группоидов.

2. Ассоциативность, полугруппы. Обобщенная ассоциативность, натуральные степени элемента полугруппы. Нейтральные элементы, моноиды.

3. 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.

4. Подгруппы, строение подгруппы, порожденной множеством элементов группы. Циклические подгруппы. Образующие элементы группы.

5. Нормальные подгруппы, строение нормальной подгруппы, порожденной множеством элементов группы. Факторгруппы, теоремы о гомоморфизмах.

6. Порядок элемента группы. Циклические группы. Сопряженные элементы.

7. Коммутаторы, коммутант, ряды коммутантов. Абелевы, нильпотентные и разрешимые группы.

Тема 2. Задание групп образующими и определяющими соотношениями.

1. Групповые алфавиты, элементарные преобразования. Построение группы, заданной образующими и определяющими соотношениями.

2. Представление (задание, генетический код) группы. Некоторые подходы к нахождению задания группы. Примеры заданий групп.

3. Задания для групп узлов, групп кос, симметрических и знакопеременных групп.

Тема 3. Фундаментальные проблемы М. Дэна.

1. Конечно порожденные и конечно определенные задания групп.

2. Проблема тождества для групп.

3. Проблема сопряженности для групп.

4. Проблема изоморфизма для групп.

5. Массовые (алгоритмические) проблемы, их положительное и отрицательное решение.

6. Общая проблема о распознавании групповых свойств по заданию группы.

7. Понятие о фундаментальных результатах П.С. Новикова и С.И. Адяна.

Тема 4. Свободные группы.

1. Определение свободных групп, различные способы задания их элементов: классы эквивалентности и несократимые слова.

2. Решение проблемы тождества для свободных групп. Решение проблемы сопряженности для свободных групп.

3. Подгруппы свободных групп. Убывающие цепочки подгрупп свободных групп и теоремы об их пересечении.

4. Хопфовость свободных групп. Финитная аппроксимируемость свободных групп.

Тема 5. Преобразования Тице.

1. Преобразования Тице T1, T2, T3 и T4. Изоморфность групп, задания которых получаются друг из друга преобразованиями Тице.

2. Теорема, о возможности перейти с помощью преобразований Тице от одного задания группы к любому другому ее заданию.

3. Построение инвариантов групп.

Тема 6. Граф Кэли группы.

1. Построение графа Кэли по заданию группы образующими и определяющими соотношениями.

2. Граф Кэли свободной группы, некоторых симметрических групп. Связь между группами и графами.

Тема 7. Фундаментальные группы топологических пространств.

1. Определение топологического пространства, примеры. Непрерывные отображения топологических пространств.

2. Непрерывные пути и петли в топологическом пространстве. Умножение путей.

3. Гомотопическая эквивалентность путей. Фундаментальная группа топологического пространства.

4. Группы узлов. Группы кос. Связь между непрерывными отображениями топологических пространств и гомоморфизмами их фундаментальных групп. 5.

5. Гомеоморфизмы топологических пространств и изоморфизмы фундаментальных групп.

Тема 8. Задание факторгрупп и подгрупп.

1. Нахождение задания факторгруппы по заданию исходной группы и ее нормальной подгруппы.

2. Вербальные подгруппы и приведенные свободные группы. Тождества в группах, многообразия групп.

3. Абелевы, нильпотентные и разрешимые тождества и многообразия.

4. Метод Рейдемейстера - Шрейера для нахождения задания подгруппы по заданию исходной группы. Система представителей правых смежных классов группы по подгруппе.

5. Переписывающий процесс Рейдемейстера - Шрейера. Шрейеровская система представителей правых смежных классов группы по подгруппе.

Тема 9. Факторгруппы по коммутанту.

1. Специальные системы образующих для конечно порожденных подгрупп свободных абелевых групп конечного ранга.

2. Прямое произведение групп. Теорема о строении конечно порожденных абелевых групп.

3. Тест для изоморфизма групп. Факторгруппы групп узлов.

Тема 10. Свободное дифференциальное исчисление.

1. Групповое кольцо.

2. Свободное дифференциальное исчисление Фокса. Частные производные Фокса в свободной группе. Основная формула свободного дифференциального исчисления.

3. Матрица Александера. Элементарные идеалы, их цепочки. Полиномы узлов.

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

1. Определение свободного произведения групп. Каноническая форма элементов свободного произведения групп.

2. Подгруппы свободного произведения групп, понятие о теореме А.Г. Куроша.

3. Решение алгоритмических проблем для свободного произведения групп.

4.Определение свободного произведения групп с объединенной подгруппой, каноническая форма элементов.

5. Понятие о теореме Зейферта - ван Кампена**.**

6. HNN-расширение группы, каноническая форма элементов, лемма Британа.

Тема 12. Группы с условием малого сокращения.

1. Условие малого налегая определяющих слов, классы групп C'(1/k) и C(k).

2. 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.

1. Протокол Anschel-Anschel-Goldfeld: начальная установка, выработка материалов для создания общего секретного ключа, выработка общего секретного ключа.

2. Протокол Wang-Cao-Okamoto-Shao: начальная установка, выработка материалов для создания общего секретного ключа, выработка общего секретного ключа.

3. Протокол Сидельников В.М.-Черепнев М.А.-Ященко В.Ю.: начальная установка, выработка материалов для создания общего секретного ключа, выработка общего секретного ключа.

4. Протокол Stickel: начальная установка, выработка материалов для создания общего секретного ключа, выработка общего секретного ключа.

5. Протоколы базируются на групповых автоморфизмах и эндоморфизмах. Протокол Mahalanobis: начальная установка, выработка материалов для создания общего секретного ключа, выработка общего секретного ключа.

6. Протокол Mahalanobis: начальная установка, выработка материалов для создания общего секретного ключа, выработка общего секретного ключа.

7. Протокол Habeeb-Kahrobaei-Koupparis-Shpilrain: начальная установка, выработка материалов для создания общего секретного ключа, выработка общего секретного ключа.

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

9. Протокол Романькова-Григорьева-Шпильрайна: начальная установка, выбор "Системой" ("Доказывающим") открытого ключа, выбор "Доказывающим" "Секретного" ключа, раунд аутентификации.

10. Протокол Шпильрайна-Ушакова на базе проблемы скрученной сопряженности для групп.
Начальная установка, "Секретный"' ключ "Доказывающего" и "Открытый" ключ, раунд аутентификации.

11. Протокол Мегрелишвили-Джинджихадзе: начальная установка, выработка материалов для создания общего секретного ключа, выработка общего секретного ключа.

12. Система Росошека: начальная установка, открытый ключ, зашифрование, расшифрование.

Приложение № 2 к рабочей программе дисциплины
«Методы комбинаторной теории групп в криптографии»

Методические указания для аспирантов по освоению дисциплины

Для успешного освоения дисциплины важно самостоятельное изучение теоретического материала, решение достаточно большого набора задач, прежде всего, самостоятельно в качестве домашних заданий, так "Учебный план" из аудиторных занятий включает лишь 8 часов лекций. Примеры решения задач разбираются на лекциях, при необходимости по наиболее трудным темам проводятся дополнительные консультации. Основная цель решения задач – помочь усвоить фундаментальные понятия, методы и теоремы комбинаторной теории групп, научиться применять их в криптографии. Для решения задач необходимо не только знать, но и понимать теоретический материал. Поэтому в процессе изучения дисциплины рекомендуется регулярная работа с рекомендованной литературой.

Для проверки и контроля усвоения теоретического материала, приобретенных практических навыков работы с основными понятиями в течение обучения проводятся мероприятия текущей аттестации в виде устного опроса на занятиях и консультациях и разбору некоторых заданий для самостоятельной работы.

Аспиранты сдают зачет в четвертом семестре. Зачет проводится на основании выполнения домашних заданий и собеседования на основании списка вопросов к зачету, который охватывает полностью всю программу дисциплины.

Учебно-методическое обеспечение самостоятельной работы аспирантов по дисциплине

В качестве учебно-методического обеспечения рекомендуется использовать литературу, указанную в разделе № 7 данной рабочей программы.