

**РЕФЕРАТ**

Отчет 35 с., 22 источ., 2 прил.

УНИТРЕУГОЛДЫ МАТРИЦАЛАР ГРУППАСЫ, БҰРАЛЫМСЫЗ НИЛЬПОТЕНТТІ ГРУППАЛАР, СИГМА–ИНТЕРПРЕТАЦИЯЛАНУ, ГОЛОГРАФИКАЛЫҚ ҚҰРЫЛЫМДАР, ЙОРДАН АЛГЕБРАСЫ, МОЗАЙКАЛЫҚ ҚҰРЫЛЫМДАР, ТЕОРИЯ, ТЕОРИЯЛАР ҮЙІРІ, ПСЕВДОАҚЫРЛЫ ТЕОРИЯЛАР, РАНГ, ДӘРЕЖЕ, ТҰЙЫҚТАЛУ

Жоба алгебралық құрылымдардың модельдік-теориялық және алгоритмдік қасиеттерін зерттеуге бағытталған. Бұл қасиеттерге тұрақтылық, псевдоақырлылық, есептелімділік, тұрақтылық, төмендетілгіштік, шешімділік, сонымен қатар теориялардың үйірлері, оның ішінде спектрлер, дәрежелер және басқа инварианттар күрделілігінің өлшемдері жатады. Бұл қасиеттер алгебралық құрылымдар арасындағы маңызды байланыстарды бақылауға, олардың жіктелуін жүзеге асыруға мүмкіндік береді.

Жобаның мақсаты - негізгі алгебралық құрылымдардың, оның ішінде голографиялық, сызықтық-минималды және съюрективтік құрылымдардың теориялық-модельдік және алгоритмдік қасиеттерін зерттеу, сонымен қатар теориялардың табиғи үйірлерінің теориялық-модельдік қасиеттерін сипаттау.

Жобаның қойылған мақсатына жету үшін группалар теориясы, сақиналар, есептеу теориясының әдістері ұсынылады; модельдердің жалпы теориясының классикалық және жаңа тұжырымдамаларын қолдануға негізделген модельдер теориясы, мысалы, аксиоматизация, толықтық, модель толықтығы, стабильділік, тотальді трансценденттілік; тікелей көбейтінділер, ультракөбейтінділер, қарапайым кеңейтулер сияқты әр түрлі модельдік-теориялық құрылымдар; жалпы топология әдістері.

Осы жобаның есепті кезеңінде келесі нәтижелер алынды:

* топтық теорияның зерттелген алгоритмдік мәселелері; толықтай ыдырайтын абель тобы табылды;
* есептелетін жиынтықтағы предикаттардың ақырлы отбасыларында төмендеудің екі түрі қарастырылды: ∆ -қысқартушылық және ∃-редукция; параметрлері бар экзистенциалды формулалар арқылы предикаттардың және олардың бір отбасының екіншісінің көмегімен толықтыруларының анықталуы және отбасылардың изоморфизм типтері бойынша бірдей анықтамасы;
* біртұтас предикаттардың отбасыларында пайда болатын реттелген дәрежелік құрылымдар сипатталған;
* ∆-қалпына келтірілетін және ∃-қалпына келтірілетін минималды нөлдік минимумдар континуумының болуы дәлелденді.

Нәтижелердің жаңашылдығы: Барлық нәтижелер алгебралық құрылымдардың алгоритмдік қасиеттері мен құрылымы туралы, алгебралық құрылымдардың әр түрлі кластарының аксиоматизациясы туралы жаңа және жаңа фактілер әкелді.

Ұлттық және халықаралық масштабтағы практикалық маңызы жоғары, өйткені зерттеу тақырыбы өзекті болып табылады және математикалық логиканың, алгоритмдер теориясының, есептелу теориясының, модельдер теориясының, тор теориясы мен әмбебап алгебраның қалыптасуына үлкен теориялық және практикалық үлес қосады.

Ғылыми қызығушылықтары отандық ғалымдар жұмысының бағытында болатын шетелдік ғалымдардың жарияланған жобасына бірлесіп қатысу зерттеулерді барынша толық және толық түрде жүргізуге мүмкіндік береді.

Қолданылуы - әмбебап алгебра, алгоритмдер теориясы, модельдер теориясы.

**РЕФЕРАТ**

Отчет 35 с., 22 источ., 2 прил.

ГРУППА УНИТРЕУГОЛЬНЫХ МАТРИЦ, НИЛЬПОТЕНТНЫЕ ГРУППЫ БЕЗ КРУЧЕНИЯ, СИГМА–ИНТЕРПРЕТИРУЕМОСТЬ, ГОЛОГРАФИЧНЫЕ СТРУКТУРЫ, ЙОРДАНОВА АЛГЕБРА, МОЗАИЧНЫЕ СТРУКТУРЫ, ТЕОРИЯ, СЕМЕЙСТВО ТЕОРИЙ, ПСЕВДОКОНЕЧНАЯ ТЕОРИЯ, РАНГ, СТЕПЕНЬ, ЗАМЫКАНИЕ

Проект направлен на исследования теоретико-модельных и алгоритмических свойств алгебраических структур. К этим свойствам относятся стабильность, псевдоконечность, вычислимость, автоустойчивость, сводимость, разрешимость, а также меры сложности семейств теорий, включая спектры, ранги, другие инварианты теорий. Эти свойства позволяют отслеживать существенные связи между алгебраическими структурами, проводить их классификацию.

Целью проекта является исследование теоретико-модельных и алгоритмических свойств основных алгебраических структур, в том числе голографические, линейно-минимальные и съюрективные структуры, а также описание теоретико-модельных свойств естественных семейтсв теорий.

Для достижения поставленной цели проекта предлагаются методы теории групп, колец, теории вычислимости; методы теории моделей, основанные на использовании классических и новых понятий общей теории моделей, таких как аксиоматизируемость, полнота, модельная полнота, стабильность, тотально трансцендентность; различные теоретико-модельные конструкции, такие как прямые произведения, ультрапроизведения, элементарные расширения; методы общей топологий.

За отчетный период выполнения данного проекта были получены следующие результаты:

* исследованы алгоритмические проблемы теории групп; найден вычислимая вполне разложимая абелева группа, которая не эффективно вполне разложима;
* рассмотрены два вида сводимости на конечных семействах предикатов на счетном множестве: -сводимость и -сводимость; определимость предикатов и их дополнений из одного семейства через другой посредством экзистенциальных формул с параметрами и такая же определимость на типах изоморфизма семейств;
* описаны возникающие при этом упорядоченные структуры степеней, порождаемые семействами одноместных предикатов;
* доказано существование континуума минимальных ненулевых степеней для -сводимости и -сводимости.

Новизна результатов: Все результаты являются новыми и принесли новые факты по алгоритмическим свойствам и строению алгебраических структур, по аксиоматизируемости различных классов алгебраических структур.

Практическая значимость в национальном и международном масштабе высока, поскольку тематика исследования актуальна и вносит большой теоретический и практический вклад в становление математической логики, теории алгоритмов, теории вычислимости, теории моделей, теории решеток и универсальной алгебры.

Совместное участие в заявленном Проекте зарубежных ученых, чьи научные интересы лежат в плоскости работ отечественных ученых позволят проводить исследования в наиболее полной и завершенной форме.

Область применения – универсальная алгебра, теория алгоритмов, теория моделей.

СОДЕРЖАНИЕ

[ВВЕДЕНИЕ 7](#_Toc57647765)

[ОСНОВНАЯ ЧАСТЬ ОТЧЕТА О НИР 9](#_Toc57647766)

[1 Алгоритмические проблемы теории групп 9](#_Toc57647767)

[1.1 Основные сведения 9](#_Toc57647768)

[1.2 Вычислимые вполне разложимые абелевы группы 11](#_Toc57647769)

[2 Исследование решёточных свойств сводимости по Сигма – интерпретируемости 12](#_Toc57647770)

[2.1 Изучение структур экзистенциальной определимости 12](#_Toc57647771)

[3 Изучение голографичных и слабо голографичных структур 14](#_Toc57647772)

[4 Изучение линейно минимальных и сюръективных алгебр 15](#_Toc57647773)

[4.1 Заметки о трехэтапном протоколе 15](#_Toc57647774)

[4.2 Трехэтапный протокол в общем виде 15](#_Toc57647775)

[4.3 Протоколы на ассоциативных структурах 17](#_Toc57647776)

[5 Теоретико-модельные свойства семейств теорий 19](#_Toc57647777)

[5.1 Основные сведения 19](#_Toc57647778)

[5.2 О замыканиях семейств теорий 20](#_Toc57647779)

[ЗАКЛЮЧЕНИЕ 22](#_Toc57647780)

[СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 23](#_Toc57647781)

[ПРИЛОЖЕНИЕ A](#_Toc57647782) - [Календарный план 24](#_Toc57647783)

[ПРИЛОЖЕНИЕ Б](#_Toc57647784) - [Освещение актуальных проблем информационной поддержки научных исследований в открытой печати 35](#_Toc57647785)

**ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ**

В настоящем отчете о НИР применяют следующие термины с соответствующими определениями:

|  |  |
| --- | --- |
| T- конечно аксиоматизируемой или конечно-аксиоматизируемой | * Для семейства T теория T является T -конечно аксиоматизируемой или конечно-аксиоматизируемой относительно T или конечно-аксиоматизируемой по T, если для некоторого (T) -предложений . |
| Δ-определимость предиката | * Будем говорить, что предикат R Δ-определим через предикаты P1,...,Pk (или Δ- определим над P1,...,Pk), если R и его дополнение определимы с параметрами через P1,...,Pk с помощью экзистенциальных формул первого порядка сигнатуры P1,...,Pk. |
| Δ-определимость семейства | * Пусть S0 и S1 - два конечных семейства предикатов на счётном множестве. Будем говорить, что семейство S0 Δ-определимо в S1, если все предикаты из S0 Δ-определимы вS1. |
| T-полным | * Для семейства Tязыка  предложение  языка  называется T-полным, если  изолирует единственную теорию в T, т.е. является одноэлементным. |
| Ранг | * Рангом семейства одноместных предикатов P0,...,Pk-1 назовём число бесконечных атомов в булевой алгебре, порождаемыми. |
| -ранжирующим | * Пусть T - семейство теорий,  - множество предложений,  - ординал RS(T) или 1. Множество  называется -ранжирующим для T, если . Предложение  называется -ранжирующим для T, если . * Множество  (предложение ) называется ранжирующим для T, если оно является -ранжирующим для T с некоторым . |
| Δ-сводимость | * Будем говорить, что тип изоморфизма семейства предикатов S0 Δ-сводится к типу изоморфизма семейства предикатов S1, если существует конечное семейство предикатов S'0 такое, что S'0 Δ-сводится к S1, и семейства S'0 такое, что S0 сопряжены при помощи некоторой перестановки. |
| экзистенциально замкнутость | * Подгруппа экзистенциально замкнута в группе , если любая конечная система уравнений и неравенств с константами из , имеющая решение в , имеет решение в . |

# ВВЕДЕНИЕ

В связи с уточнением поянтия алгоритма было дано точное понятие вычислимости данной алгебраической системы. В связи с этим в математике актуальной стала проблема описания, т.е. нахождение необходимых и достаточных условий вычислимости данной алгебраической системы. В теории групп и приложениях этой теории нильпотентные и разрешимые группы играют центральную роль. Поэтому исследования проблем вычислимости этого класса групп являлется актуальной.

Изучение классических алгебраических систем относительно свойств формульных подмножеств порождают много интересных структурных свойств. Поля и кольца, удовлетворяющие различным условиям минимальности или конечности, до сих пор остаются в поле зрения специалистов по теории моделей.

В Казахстане и в мире не исследованы проблемы вычислимости для класса разрешимых групп. В настоящее время наиболее полно исследованы проблемы вычислимости для абелевых групп, т.е. разрешимых групп ступени 1, и для нильпотентных групп конечных размерностей. Поэтому исследование проблем вычислимости нильпотентных и разрешимых групп является актуальной задачей. Как сказано ранее, в мире более и менее исследована проблема вычислимости абелевых и некоторого класса нильпотентных групп. Проблема существования вычислимой нумерации для данной нильпотентной или разрешимой группы является главной задачей для этого для данного проекта.

Актуальность тематики обосновывается важностью развития теории классификаций с целью поиска, описания и характеризации новых объектов как для получения дальнейших алгебро-логических и алгоритмических результатов, так и их приложений в смежных областях.

Объектом исследований является алгоритмические свойства алгебр, аксиоматизируемость алгебраических структур, строение минимальных структур, теоретико-модельные свойства семейств теорий.

Предметом исследования является алгебры, алгебраические структуры, семейства теории, нильпотентные группы без кручения.

Основной целью данного проекта является: исследование алгоритмических проблем для различных классов алгебраических структур; проблемы конечной аксиоматизируемости теории; изучение решеточных свойств некоторых теорий и классов структур; строение минимальных структур; исследование свойств подалгебр общей алгебры полных теорий.

Задачи исследования:

Алгоритмические проблемы теории групп.

* нахождение необходимых и достаточных условий для вычислимости и автоустойчивости данной нильпотентной или разрешимой группы конечной ступени;
* использование найденных критериев и методов для нахождение необходимых и достаточных условий для вычислимости класса нильпотентных или разрешимых групп конечной ступени.

Исследование решёточных свойств сводимости по Сигма - интерпретируемости.

Изучение голографичных и слабо голографичных структур.

* построение новых примеров голографичных и слабо голографичных структур;
* изучение отношения между этими двумя свойствами структур.

Изучение линейно минимальных и сюръективных алгебр.

* получение критерия слабой тривиальности в структурных терминах в линейно минимальных квадратичных йордановых алгебрах характеристики 2; т.е. завершение полной классификации таких алгебр;
* построение локально конечной лиевой алгебры в виде объединения башни конечных подалгебр и выявления новых свойств минимальных лиевых алгебр;
* продолжить изучение сюръективных алгебр: построение новых примеров и доказательство новых теорем.

Теоретико-модельные свойства семейств теорий.

* описание рангов, степеней и е-спектров семейств теорий как в общем виде, так и для унаров, отношений эквивалентности, графов;
* нахождение наименьших порождающих множеств семейств теорий как в общем виде, так и для унаров, отношений эквивалентности, графов;
* описание теоретико-модельных свойств семейств теорий как в общем виде, так и для унаров, отношений эквивалентности, графов.

Разработанные алгоритмы и методы данного проекта могут быть применены в компьютерных науках. Вопросы трансляции абстрактных типов данных, логическое программирование и языки спецификаций являются актуальными и имеют применение в разработках трансляторов вычислительных устройств, языков программирования.

# ОСНОВНАЯ ЧАСТЬ ОТЧЕТА О НИР

# 1 Алгоритмические проблемы теории групп

## 1.1 Основные сведения

Проведено исследование алгоритмической проблемы вычисления дискретного логарифма в конечно порожденной нильпотентной группе. При этом было использовано два различных подхода к решению этой проблемы. Рассматривалось два случая: случай конечной нильпотентной группы, сводящийся к рассмотрению конечных p-групп, так как любая конечная нильпотентная группа является прямым произведением таких групп, и случай конечно порожденной нильпотентной группы без кручения. Результаты для общего случая произвольной конечно порожденной нильпотентной группы следовали из теоремы автора о вложении такой группы в прямое произведение конечной нильпотентной группы (прямого произведения конечныхp-групп) и конечно порожденной нильпотентной группы без кручения. Один из подходов использует точную представимость конечно порожденных нильпотентных групп матрицами. Конечная группа представима унитреугольными матрицами подходящего размера n над простым конечным полем характеристики . Конечно порожденная нильпотентная группа без кручения представима унитреугольными матрицами над кольцом целых чисел , то есть изоморфно вложима в группу унитреугольных матриц Затем были представлены эффективные алгоритмы вычисления дискретного логарифма в указанных матричных группах, комбинация которых дает эффективный алгоритм вычисления дискретного логарифма в произвольной конечно порожденной нильпотентной группе. Определена вычислительная сложность построенного алгоритма.

Второй подход основан на построении в конечной -группе конечного нормального ряда, факторы которого являются элементарными абелевыми -группами, а также на построении в конечно порожденной нильпотентной группе без кручения конечного нормального ряда, факторы которого – свободные абелевы группы конечного ранга. Далее представлены алгоритмы вычисления дискретного логарифма на основе построенных нормальных рядов и определена их вычислительная сложность. Переход к общему случаю осуществляется, как при первом подходе. Второй подход не использует представления матрицами. Он может быть применен в случаях, когда размер матриц для такого представления оказывается слишком громоздким, что затрудняет вычисления. Необходимость второго подхода вызвана тем обстоятельством, что авторы криптографических схем, незащищенность которых была установлена первым подходом, стали предлагать в качестве платформ шифрования нильпотентные группы, не допускающие вложений в матричные группы малых размерностей.

Также в работе по проекту было продолжено изучение универсальных элементов конечно порожденных нильпотентных групп. Так как универсальные элементы в таких группах существуют не всегда, было введено более общее понятие универсальной системы элементов, близкое к классическому понятию вербальной ширины. Такие множества существуют в любой конечно порожденной нильпотентной группе. Их размер является важной числовой характеристикой коммутанта группы, отвечающей за сложность коммутанта. Получен ряд структурных и вычислительных результатов в данном направлении. Основные результаты получены для свободных нильпотентных групп конечных рангов и групп конечных рангов свободных в нильпотентных многообразиях групп. Именно: вычислены ранги универсальности этих групп и установлена связь с элементарной теорией этих групп в теоретико-групповом языке с константами. Получены предварительные результаты по универсальным элементам свободных метабелевых групп.

Изучаются алгебраически и вербально замкнутые подгруппы и ретракты конечно порожденных нильпотентных групп. Особое внимание уделено свободным нильпотентным группам и группам  унитреугольных матриц над кольцом целых чисел для произвольного n. Замечено, что множества ретрактов конечно порожденных нильпотентных групп совпадают с множествами их алгебраически замкнутых подгрупп. Приведен пример, показывающий, что вербально замкнутая подгруппа конечно порожденной нильпотентной группы может не быть ретрактом (в рассматриваемом случае равносильно: алгебраически замкнутой подгруппой). Другой пример показывает, что пересечение ретрактов (алгебраически замкнутых подгрупп) свободной нильпотентной группы может не быть ретрактом (алгебраически замкнутой подгруппой) этой группы. Установлены необходимые условия, выполненные на ретрактах произвольных конечно порожденных нильпотентных групп. Получены достаточные условия для свойства “быть ретрактом” конечно порожденной нильпотентной группы. Представлен алгоритм, определяющий свойство “быть ретрактом” для подгруппы свободной нильпотентной группы конечного ранга (решение проблемы Мясникова). Также получен общий результат об экзистенциально замкнутых подгруппах конечно порожденных нильпотентных групп без кручения с циклическим центром, из которого следует, в частности, что при любом n группа  не содержит собственных экзистенциально замкнутых подгрупп.

Ретрактом группы называется такая подгруппа для которой существует эндоморфизм , тождественный на . Легко доказать, что подгруппа является ретрактом группы тогда и только тогда, когда существует нормальная подгруппа группы такая, что выполнены следующие условия:

(1.1.1)

Любой элемент группы однозначно записывается в виде где Ретракцией называется эндоморфизм определенный как . Нормальная подгруппа совпадает с ядром эндоморфизма и называется ядром ретракции

Очевидно, что прямые и свободные множители в группах являются их ретрактами. В абелевых группах прямые множители исчерпывают все множество ретрактов. В общем случае проблема описания всех ретрактов гораздо сложнее. В [2] доказано, что уже в классе конечно порожденных нильпотентных групп ступени нильпотентности два проблема определения, является ли подгруппа ретрактом, алгоритмически неразрешима. Тем самым решена проблема Мясникова N9(a) из [3]. В разд. 5 данной работы показано, что эта проблема для свободных нильпотентных групп решается положительно. А именно, существует алгоритм, определяющий, является ли подгруппа свободной нильпотентной группы конечного ранга ретрактом. Это решает проблему Мясникова N9(b) из [3].

В [4] доказано, что для любого n пересечение конечного множества ретрактов группы снова является ретрактом. В то же время остался открытым вопрос 17.19 из [5], он же вопрос из [3]: если — подгруппа свободной группы , — ретракт группы , то будет ли пересечение ретрактом группы ? В разд. 6 данной работы приведен пример двух ретрактов свободной нильпотентной группы, пересечение которых не является ретрактом ни во всей группе, ни в пересекаемых подгруппах.

Ретракты связаны с вербально и алгебраически замкнутыми подгруппами групп.

Пусть — группа. Подгруппа называется вербально замкнутой в группе , если для любого группового слова от независимых переменных без констант и любого элемента уравнение

(1.1.2)

разрешимо в группе тогда и только тогда, когда оно разрешимо в группе . Уравнение вида (2) называется расщепимым, более точно, расщепимым над подгруппой .

В [6] доказано, что множество вербально замкнутых подгрупп группы совпадает с множеством ретрактов и множеством алгебраически замкнутых подгрупп группы .

Напомним, что подгруппа группы называется алгебраически замкнутой в G тогда и только тогда, когда для любого набора групповых слов , с константами из H от независимых переменных система уравнений

(1.1.3)

имеет решение в группе тогда и только тогда, когда она имеет решение в H.

Очевидно, что любой ретракт произвольной группы является алгебраически замкнутой подгруппой, тем более вербально замкнутой подгруппой этой группы. В [6] доказана следующая теорема, в частности, показывающая, что в классе конечно определенных групп любая конечно порожденная алгебраически замкнутая подгруппа является ретрактом.

Теорема 1 [6]. 1) Пусть — конечно определенная группа. Тогда любая конечно порожденная подгруппа алгебраически замкнута в тогда и только тогда, когда — ретракт группы .

2) Пусть — н¨етерова по уравнениям подгруппа группы , причем конечно порождена относительно . При этих условиях алгебраически замкнута в тогда и только тогда, когда является ретрактом в .

## 1.2 Вычислимые вполне разложимые абелевы группы

В [7] введено понятие эффективно вполне разложимой абелевой группы. Счетная абелева группа А вполне разложима, если А=⊕{Аi|i∈ω}, где Аi- подгруппа аддитивной группы Q всех рациональных чисел. Если существует такая конструктивная нумерация ν группы А, что в (А,ν) найдется вычислимо перечислимая последовательность элементов аi∈Аi, то группу А назовем эффективно вполне разложимой. Рассмотрим следующий класс вполне разложимых групп.

Пусть р0, р1, … некоторая последовательность простых чисел, Q(рi) – аддитивная группа рациональных чисел, знаменатели которых являются степенями рi и

А=⊕{Q(рi)|i∈ω} (1.2.1)

Характеристикой χ(А) группы А назовем множество

χ(А)={<р,к>|∃i1…∃ik (pi1=…=pik=p)} (1.2.2)

В [7] доказана следующая

Теорема 1.2.1 Абелева группа А=⊕{Q(рi)|i∈ω} эффективно вполне разложима тогда и только тогда, когда ее характеристика χ(А), принадлежит классу Σ2(0) арифметической иерархии.

В данном сообщении доказана

Теорема 1.2.2 Абелева группа А, определенная равенством (1) вычислима тогда и только тогда, когда ее характеристика, определенная равенством (2), принадлежит классу Σ3(0) арифметической иерархии.

Из теорем 1, 2 вытекает

Следствие. Существует вычислимая вполне разложимая абелева группа, которая не эффективно вполне разложима.

# 2 Исследование решёточных свойств сводимости по Сигма – интерпретируемости

## 2.1 Изучение структур экзистенциальной определимости

Кратко работу по этому напрравлению можно охарактеризовать так: рассмотрены два вида сводимостей на конечных семействах предикатов на счётном множестве: определимость предикатов и их дополнений из одного семейства через другой посредством экзистенциальных формул с параметрами и такая же определимость на типах изоморфизма семейств. Описаны возникающие при этом упорядоченные структуры степеней, порождаемые семействами одноместных предикатов. Для обеих сводимостей доказано существование континуума минимальных ненулевых степеней.

Далее приводится более детальное изложение результатов.

В математической логике сводимость между объектами, такими, как множества, функции, структуры и т.п. всегда можно рассматривать как определимость (возможность определить один объект через другой) с использованием средств (определений) из некоторого заранее фиксированного класса, который собственно и определяет данную сводимость. Идеологически, постановка задачи и введённая терминология близки к используемым в теории степеней неразрешимости.

Определение 2.1.1 Будем говорить, что предикат R Δ-определим через предикаты P1,...,Pk (или Δ- определим над P1,...,Pk), если R и его дополнение определимы с параметрами через P1,...,Pk с помощью экзистенциальных формул первого порядка сигнатуры P1,...,Pk.

Определение 2.1.2Пусть S0 и S1 - два конечных семейства предикатов на счётном множестве. Будем говорить, что семейство S0 Δ-определимо в S1, если все предикаты из S0 Δ-определимы в S1.

Легко проверяется, что Δ-определимость является предпорядком на множестве конечных семейств предикатов. Далее естественным образом определяется эквивалентность, порождаемая этой определимостью: два семейства эквивалентны, если они Δ-определимы друг в друге. Назовём её эквивалентностью по Δ- определимости. Фактор-отношение предпорядка этой определимости по данной эквивалентности образует верхнюю полурешётку, причём точной верхней гранью для классов эквивалентности, определяемых семействами S0 и S1, будет класс, определяемый их объединением. Обозначим эту полурешётку через D0 . Её элементы назовём степенямиΔ-определимости.

Δ/

Теперь мы определим понятие Δ-сводимости уже на типах изоморфизма семейств предикатов.

Определение 2.1.3 Будем говорить, что тип изоморфизма семейства предикатов S0Δ-сводится к типу изоморфизма семейства предикатов S1, если существует конечное семейство предикатов S'0 такое, что S'0 Δ-сводится к S1, и семейства S'0 такое, что S0 сопряжены при помощи некоторой перестановки.

Теперь как обычно определяются сводимости и степени типов изоморфизма. Получившееся в результате частично упорядоченное множество степеней мы обозначим через DΔ.

Сначала была получена серия результатов о том, что каждая степень может быть представлена предикатами с некоторыми специфическими свойствами, облегчающие дальнейшую работу со степенями, которые здесь не приводятся, но стоит отметить, что есть уверенность, что разработанный при этом инструментарий будет полезен в дальнейшем при решении задач, связанных с определимостью.

В ходе исследования были полностью описаны структуры степеней, для семейств одноместных предикатов.

Определение 2.1.4Рангом семейства одноместных предикатов P0,...,Pk-1 назовём число бесконечных атомов в булевой алгебре, порождаемыми.

Это описание даётся следующей теоремой:

Теорема 2.1.5 Пусть P и Q - семейства одноместных предикатов рангов p и q соответственно. Тогда следующие условия эквивалентны:

* тип изоморфизма P Δ-сводится к типу Q
* p не превосходит q.

Следствие 2.1.6Множество элементов из DΔ, определяемых семействами одноместных предикатов, замкнуто вниз и упорядочено отношением Δ-определимости по типу натуральных чисел, т.е. образует идеал в этой структуре.

Следуя традиционной терминологии из теории степеней неразрешимости, будем называть степень минимальной, если она не наменьшая, но между ней и наименьшей уже не содержится других степеней.

Главным результатом в данном разделе здесь является следующая:

Теорема 2.1.7Каждая из структур степеней по Δ-определимости и по Δ-определимости на типах изоморфизма содержит континуум минимальных элементов.

Кроме того, был доказан следующий результат:

Теорема 2.1.8Структура Δ-определимости на типах изоморфизма не является верхней полурешёткой.

По результатам исследования была подготовлена, сдана в печать в журнал Алгебра и логика работа, которая уже принята к печати.

А.С. Морозов, Д.А. Тусупов Минимальные предикаты относительно Δ- определимости

# 3 Изучение голографичных и слабо голографичных структур

Изучалось следующее обобщение понятия голографической структуры. Здесь для произвольной конечной предикатной сигнатуры σ через ||σ|| обозначается максимальная арность её символов.

Определение. Алгебраическая структура A конечной предикатной сигнатуры σ называется слабо голографичной, если существует конечное подмножество S в A, называемое множеством прототипов, такое, что для любого подмножества M в A, мощность которого не превосходит ||σ||, существует изоморфное вложение φ из A в A такое, что φ(M) является подмножеством в S.

Первоначально изучавшееся понятие голографичности формулировалось аналогичным образом, но предполагало наличие автоморфизма φ, а не изоморфного вложения, с заданным свойством.

За отчётный период показано, что всякая счётная несуператомная булева алгебра слабо голографична.

Ранее авторами было получено полное описание не более чем счётных голографичных булевых алгебр, а именно, было показано, что произвольная не более, чем счётная булева алгебра голографична тогда и только тогда, когда она содержит конечное число атомов. Для булевых алгебр это условие совпадает со счётной категоричностью.

Полученный нами результат показывает, что понятие слабой голографичности отличается от обычной голографичности и обосновывает интерес к изучению слабой голографичности.

# 4 Изучение линейно минимальных и сюръективных алгебр

## 4.1 Заметки о трехэтапном протоколе

Трехэтапный протокол является популярным и привлекательным способом передачи секретных данных, благодаря простоте лежащей в его основе теории [10].

Мы опишем сначала этот протокол в несколько упрощенном по сравнению с [10] виде. Имеется множество кодов, которого мы обозначим через . Две стороны — отправитель (Алиса) и получатель (Боб) — хотят осуществить передачу некоторого секретного кода по открытому каналу. Для этого у имеется множество перестановок , а у — множество такие, что

для любых , , где обозначает группу перестановок множества . На языке теории групп это означает, что является подмножеством централизатора множеств , и наоборот.

В этом случае протокол, которого мы назовем примарным (т.е. простейшим), для отправки Алисой кода Бобу состоит из следующих трех этапов:

1. Алиса выбирает случайно элемент , применяет ее к и результат отправляет Бобу;
2. Боб выбирает случайно элемент , применяет ее кполученному и возвращает Алисе;
3. Алиса применяет к полученному и возвращает результат Бобу.

Использование канала связи на этом завершается. Для восстановления сообщения Бобу достаточно применить к последнему полученному сообщению обратную перестановку . Важно отметить, что применяемые здесь функции и должны быть быстро-вычислимыми.

Тройка , которая может быть названа платформой вышеописанной схемы, считается известной всем, в том числе персонам, обозревающим канал связи. Выберем одну такую персону и назовем его Оскаром. Если задача восстановления кода из тройки , элементы которой обозреваются Оскаром, является алгоритмически сложной задачей, то в принципе схема считается «рабочей», так как обеспечивает секретность передаваемого кода относительно пассивных наблюдателей.

## 4.2 Трехэтапный протокол в общем виде

Если примарная схема, описанная во введении может быть представлена как цепь перестановок одного множества

то трехэтапный протокол в общем виде представляется как цепь отображений

где — множество сообщений, а , , — вспомогательные множества. Здесь пара быстро-вычислимых отображений , выбирается Алисой, а пара , с аналогичным свойством— Бобом, причем эти выборы осуществляются независимо и случайно из некоторых фиксированных семейств пар отображений. Эти семействаподобраны так, что при любых выборах Алисы и Боба выполняется тождество (некоторая форма коммутативности):

(4.2.1)

В отличие от [10], мы здесь сознательно избегаем использование терминов «текст», «шифротекст», «шифрование», «дешифрование» и т.п., чтобы не отвлекать читателя от основной темы. По этой же причине не вводим обозначений для семейств пар отображений, т.е. не пытаемся строго очертить платформу для схемы в общем виде.

Некоторые простые свойства отображений и все же стоит отметить. Они должны быть локально инъективными: должно быть инъективным, ограничение на должно быть инъективными т.д. Как следствие, каждое содержит, по крайней мере, элементов. Если хотя бы одно содержит больше элементов, то глобальной инъективности не будет.

С другой стороны, если каждое содержит ровно элементов, то каждое из отображений , , и должно быть биективным. Тогда из условия коммутативности (C) вытекает, что между множествами и имеется взаимно-однозначное соответствие, быстро-вычислимое в обе стороны, что позволяет (вычислимо) отождествить каждое из множеств с множеством , аотображения , , и считать элементами . Таким образом, в этом случае представление трехэтапного протокола упрощается:

(4.2.2)

и почти сводится к примарному варианту. Трехэтапный протокол с цепочкой перестановок как в (P) назовем простым.

Пример 1. Следующий пример объясняет, почему мы говорим «почти». Рассмотрим простую схему, которая является модификацией примарного трехэтапного протокола на платформе , где — подмножество некоторой абелевой подгруппы в ; все известные доселе трехэтапные протоколы — схемы Шамира, Мэсси-Омуры— являются примарными и таковыми, т.е. у них (см. [10], [11], [12]). Сначала Алиса и Боб договариваются и выбирают (фиксируют) некоторый элемент , который известен и Оскару. Снова здесь важно, чтобы функции , были быстро-вычислимыми. Далее, для отправки сообщения Алиса случайно выбирает и создает пару , а Боб создает случайную пару , где .

Можно показать, что схема из Примера 1 криптографически эквивалентна примарному трехэтапному протоколу , на базе которого она строится. Действительно, если у Оскара имеется алгоритм, который получив на входе , на выходе дает , то он может быть использован для получения кода из тройки , что обозревается Оскаром при передаче кода по простой схеме из Примера 1: Оскар к последней компоненте тройки применяет и в остальном полагается на алгоритм. Аналогично, существование алгоритма взлома простой схемы из Примера 1 влечет существование такового для примарной, лежащей в ее основе.

Вопрос.Можно ли доказать, что каждый простой трехэтапный протокол криптографически эквивалентен некоторому примарному?

Пример 2. Простой трехэтапный протокол не применимв чистом виде на практике, поскольку неустойчива против атаки посредника [13]. Фольклорная идея обретения стойкости к подобным атакам заключается в сочетании (примарного) трехэтапного протокола на платформе с некоторой схемой подписи кодов из множества . И каждый раз сторона не просто отправляет код, а еще его подписывает. Протокол продолжает работу до тех пор, пока процедуры верификации будут подтверждать подлинность подписей. Для наглядности скажем, что разницу простого и комбинированного протоколов Оскар почувствует так: если раньше информацию о передаче кода он получал в виде тройки

то теперь в его распоряжении будет тройка , где — функция подписи. Функция подписи многих схем, в том числе и стандартных, вовлекает случайный параметр, и как следствие, один и тот же человек при подписании одного и того же сообщения может получить разные (электронные) подписи. Поэтому в комбинированных схемах мы, вообще говоря, имеем , . Комбинированная со схемой подписи трехэтапный протокол протокол надежно противостоит атаке посреднике [13] и, кроме того, обеспечивает целостность сообщения, если канал связи подвержен различным помехам, искажающим передаваемые сообщения.

Касательно непримарных протоколов, в этой статье мы ограничимся приведенными выше двумя примерами. В дальнейшем все рассматриваемые протоколы будут примарными.

## 4.3 Протоколы на ассоциативных структурах

Конечная структура с бинарной ассоциативной операцией и единицей очень естественно предоставляет платформу для примарного трехэтапного протокола вида с и , где —подмножество перестановок из , индуцированных умножением слева (справа) на элемент из . Из конечности начальной ассоциативной структуры вытекает, что множества и замкнуты относительно обращения [легко проследить следующую цепь импликаций: элемент обратим слева или справаоператор умножения на слева или оператор умножения на справа является перестановкой множества некоторая степень этого оператора равна тождественному отображению соответствующая степень элемента равна элемент обратим и слева, и справа]. Важно заметить, что обратимые элементы образуют подструктуру (т.е. есть замкнутость относительно умножения), которая является группой. Предполагается, что операция обращения, равно как и основная бинарная операция , являются быстро-вычислимыми.Отметим, что в данном случае, тройка кодов, обозреваемая Оскаром, имеет вид для некоторых (по традиции мы опускаем скобки и знаки бинарной операции). Если обратим, то через обозначим обратный к нему элемент.

Изложение дальнейшего материала требует рассмотрения простейших атак на трехэтапный протокол, к чему мы и приступаем. Заметим, что если Оскар сможет вычислить из обозреваемой с канала связи тройки перестановку , то он вычислит и код , аналогичным образом, если у него есть алгоритм, который из тройки вычисляет , то такой протокол для передачи секретных сообщений не годится. Это наблюдение выдвигает первое требование к стойкости протокола:

(1) Задача вычисления или из обозреваемой тройки должна быть алгоритмически сложной задачей (с вероятностью, близкой к 1).

Здесь мы вынуждены говорить о вероятности и признать, что нельзя надеяться на абсолютную стойкость трехэтапного протокола: Оскар может «ткнуть пальцем в небо» и найти случайно решение задачи (1). Это обстоятельство сильно ограничивает область применения данного протокола: его не рекомендуется применять, где цена информации высока.

Смысл требования (1) для протоколов с платформой вида , упомянутого в начале параграфа, неформально звучит так: обратимых элементов в должно быть не слишком много.Действительно, если, например, в тройке компонента окажется обратимой, то может быть вычислен как ; по этой причине любая группа для платформы вида не годится. С другой стороны, обратимых элементов в должно быть не слишком мало, иначе задача (1) может быть решена простым перебором. Возникает вопрос: что делать, если обратимых элементов, например, примерно половина? Понятно, что применение протокола на такой платформе весьма рискованно.

Алгоритмические характеристики структуры могут быть настолько хорошими, что тяжело от нее отказаться. Ясно, чтобы ее «спасти», нужно внести изменения в платформу .

Если в необратимых элементов достаточное количество, то следующая модификация позволяет избежать «прямых провалов», описанных в предыдущем абзаце. Обозначим через множество необратимых элементов из . Платформа получается из всего лишь заменой множества (кодов) на , то есть , где и . Поскольку инвариантно относительно операторов умножения (т.е. и для любого ), действительно может служить платформой для трехэтапного протокола.

Теперь перейдем к более сильному требованию к платформе примарного трехэтапного протокола общего вида:

(2) Задача нахождения решения уравнения в централизаторе множества вместе с или решения уравнения в централизаторе множества вместе с из обозреваемой тройки должна быть алгоритмически сложной задачей (с вероятностью, близкой к 1).

Действительно, допустим Оскару удалось найти такой элемент централизатора множества , что выполняется . Тогда имеем . Поэтому он получит искомый код как .

Требование (2) индуцирует определенные требования к ассоциативной структуре , применяемой для трехэтапного протокола на платформе (или модифицированной платформе типа ). Например:

(А) Нахождение решения уравнения с вычислимым должна быть алгоритмически сложной задачей почти для всех кодов , , .

В отдельной статье мы покажем, что популярный среди поклонников этого жанра трехэтапный протокол [14] не удовлетворяет требованию (2).

# 5 Теоретико-модельные свойства семейств теорий

## 5.1 Основные сведения

Понятие ранга для семейств теорий, аналогичное рангу Морли для фиксированных теорий, служит мерой сложности для данных семейств. Возникает естественная проблема описания иерархии ранга для ряда семейств теорий. Ранг для семейств теорий, аналогичный рангу Морли [16] и определенный в работе [18], можно рассматривать как меру сложности или богатства этих семейств. Таким образом, повышая ранг за счет расширения семейства, мы получаем более богатые семейства, включая семейство с бесконечным рангом, который можно считать «достаточно богатым».

Следуя [18], мы определим ранг RS(\*) для семейств теорий, аналогичный рангу Морли [16], и иерархию по этим рангам следующим образом.

RS()=-1, если семейство пусто;

RS(\mathcal{T})=0, если семейство конечно и непусто;

RS() 1, если семейство бесконечно.

Для семейства и ординала положим RS(), если имеются попарно несовместные-предложения , , такие, что RS(), .

Если – предельный ординал, то RS(), если RS() для любого .

Положим RS(), если RS() и RS() +1.

Если RS() для любого , положим RS(.

Семейство называется e-тотально трансцендентным или тотально трансцендентным, если RS() является ординалом.

Предложение 5.1.1 [18] Если бесконечное семейство не имеет e-минимальных подсемейств , то не является e-тотально трансцендентным.

Если семейство является e-тотально трансцендентным и RS() 0, определим степень ds () для как максимальное число попарно несовместных предложений таких, что RS(=.

Предложение 5.1.2 [22] Любое семейство теорий можно расширить до семейства с наименьшим порождающим множеством.

Определение 5.1.3 [18] Семейство с бесконечным числом точек накопления называется a-минимальным, если для любого предложения , или имеет конечное число точек накопления.

Пусть --- ординал. Семейство ранга называется -минимальным, если для любого предложения (T), RS ( или RS (.

Предложение 5.1.4 [18] (1) Семейство является 0-минимальным тогда и только тогда, когда является одноэлементным.

(2) Семейство – 1-минимально тогда и только тогда, когда – e-минимально.

(3) Семейство --- 2-минимально тогда и только тогда, когда --- a-минимально.

(4) Для любого ординала непустое семейство --- -минимально тогда и только тогда, когда RS() и ds () =1.

Теорема 5.1.5 [18] Для любого семейства , RS()=2 и ds () = n, если и только если представляется в виде непересекающегося объединения подсемейств , для некоторых попарно несовместных предложений , таких, что каждое является a-минимальным.

Предложение 5.1.6 [18] Для любого семейства , RS()= и ds () = n, если и только если представлен в виде непересекающегося объединения подсемейств , для некоторых попарно несовместных предложений , таких, что каждое является - минимальным.

Определение 5.1.7 Пусть -семейство теорий, а T - теория, T. Теория T называется -аппроксимируемой или аппроксимируемой по или псевдо- -теорией, если для любой формулы T существует T' такая, что T'.

Если теория T является -аппроксимируемой, то T называется аппроксимирующим семейством для T, теории T' являются аппроксимациями для T, а T является точкой накопления для . Положим ={T |T}. Множество будем называть-окрестностью или просто окрестностью для семейства .

Аппроксимирующее семейство называется e-минимальным, если для любого предложения, конечно или конечно.

В [21] показано, что любое e-минимальное семейство имеет единственную точку накопления T относительно окрестностей и также называется e-минимальным.

Предложение 5.1.8 [19] Теория T является -аппроксимируемой тогда и только тогда, когда T ClE ().

Определение 5.1.9 [17] Бесконечная структура называется псевдоконечной, если каждое истинное предложение в имеет конечную модель.

Если T = Th () для псевдоконечного , то теория T также называется псевдоконечной.

Обозначаем через класс всех полных элементарных теорий, через fin подкласс , состоящий из всех теорий с конечными моделями.

Предложение 5.1.10 [19] Для любой теории T следующие условия эквивалентны:

(1) T псевдоконечна;

(2) T является fin -аппроксимируемой;

(3) T ClE (fin) \fin

## 5.2 О замыканиях семейств теорий

Мы определяем и изучаем естественные обобщения E-замыканий [21, 22] семейств T полных теорий для произвольных семейств теорий, возможно, неполных.

Следуя [21, 22] для семейства T теорий и предложения , обозначим через семейство {TT|T}.

Определение 5.2.1 Мы говорим, что теория T принадлежит замыканию (соответственно ), если TT или T аксиоматизируется максимальным набором предложений  (соответственно ) такое, что (соответственно ) непусто (где ).

Заметим, что семейства для образуются предложениями в T, тогда как семейства для расширяются булевыми комбинациями предложений в T. Более того, теории T в T преобразуются в теории с путем добавления -разделяющих предложений: если T,T'T с TT', то существует предложение с или с . Таким образом, семейство T получает в соответствующее семейство , состоящее из теорий для теорий TT, которые -разделены. Оператор внутри называется хаусдорфизацией семейства T.

Операторы и рефлексивны, транзитивны, но могут не работать в условиях монотонности относительно расширений семейств: существуют семейства T такие, что , и .

Определение 5.2.2 Для семейства теорий T языка  и теории T положим , если TT, или T непусто и для некоторых T'T. Если T' фиксировано, то мы говорим, что T принадлежит -замыканию T относительно T', и T является точкой накопления T относительно T'.

Теорема 5.2.3 Для любого семейства T полных теорий не более чем счетного языка , .

Свойство теоремы, а также транзитивность могут не выполняться для языков  несчетной мощности.

# ЗАКЛЮЧЕНИЕ

В период выполнения данного проекта были получены следующие результаты:

* исследованы алгоритмические проблемы теории групп;
* рассмотрены два вида сводимости на конечных семействах предикатов на счетном множестве: -сводимость и -сводимость; определимость предикатов и их дополнений из одного семейства через другой посредством экзистенциальных формул с параметрами и такая же определимость на типах изоморфизма семейств;
* описаны возникающие при этом упорядоченные структуры степеней, порождаемые семействами одноместных предикатов;
* доказано существование континуума минимальных ненулевых степеней для -сводимости и -сводимости;

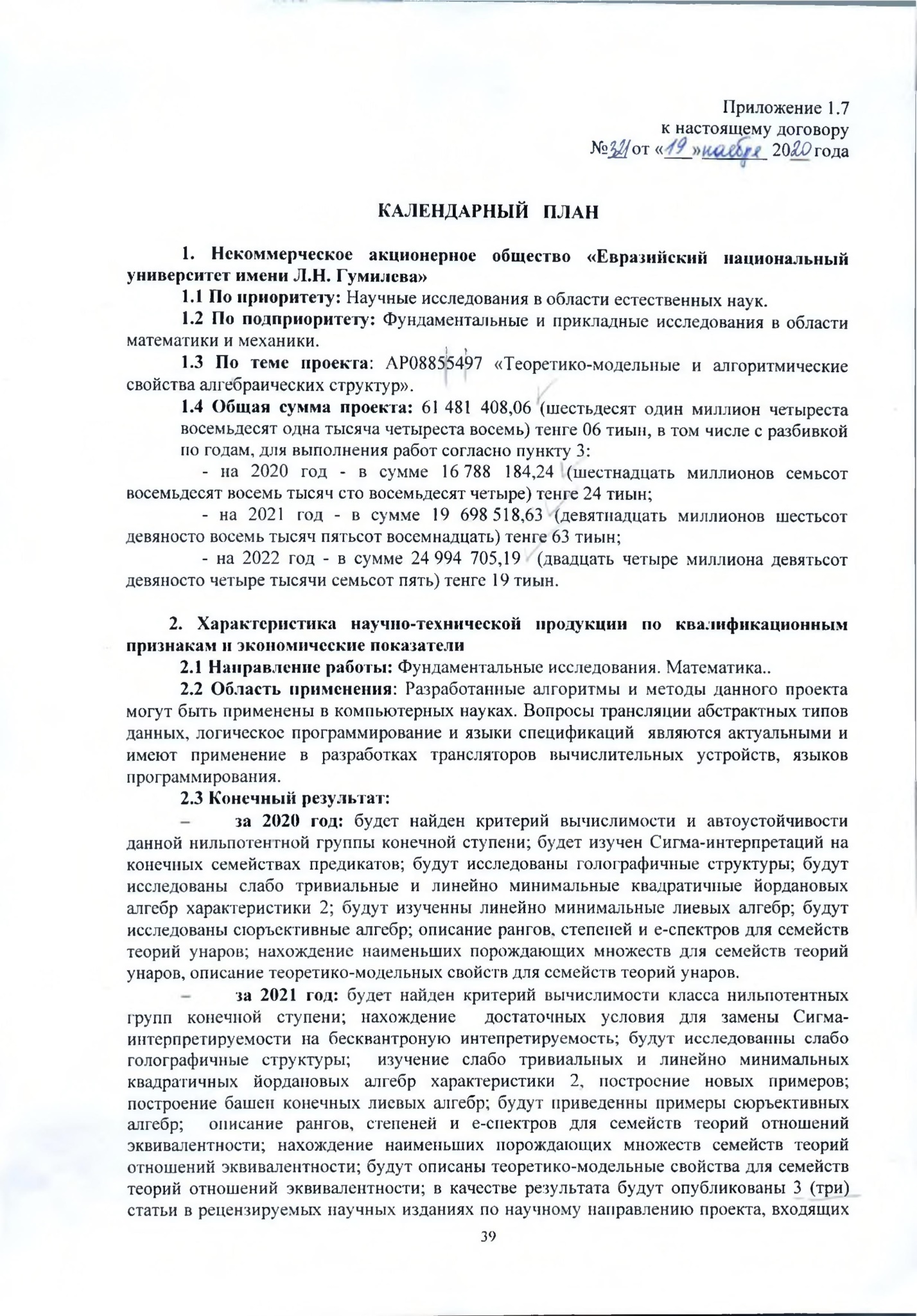
По результатам исследования опубликованы 2 публикации в трудах международных конференций.

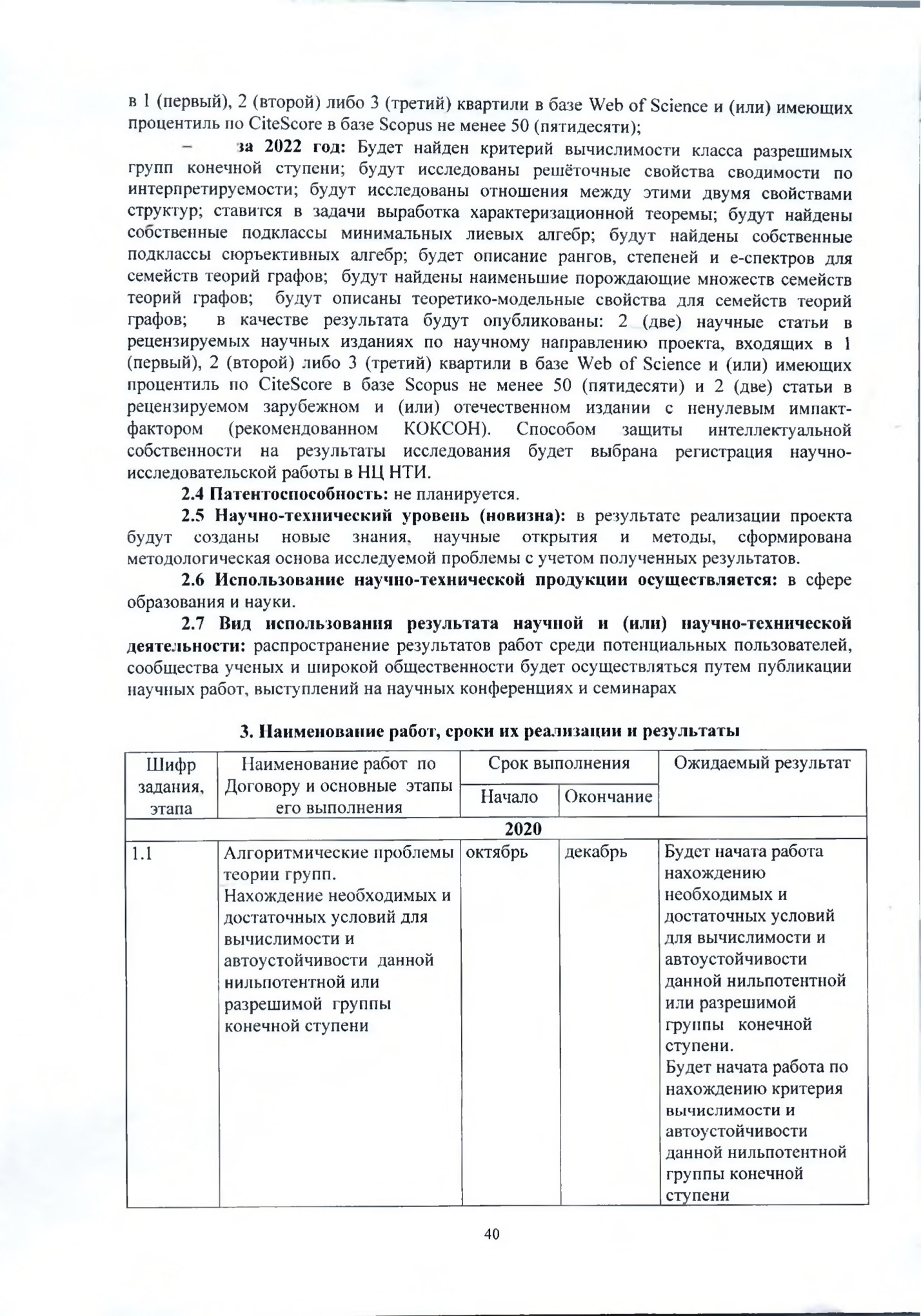
# СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

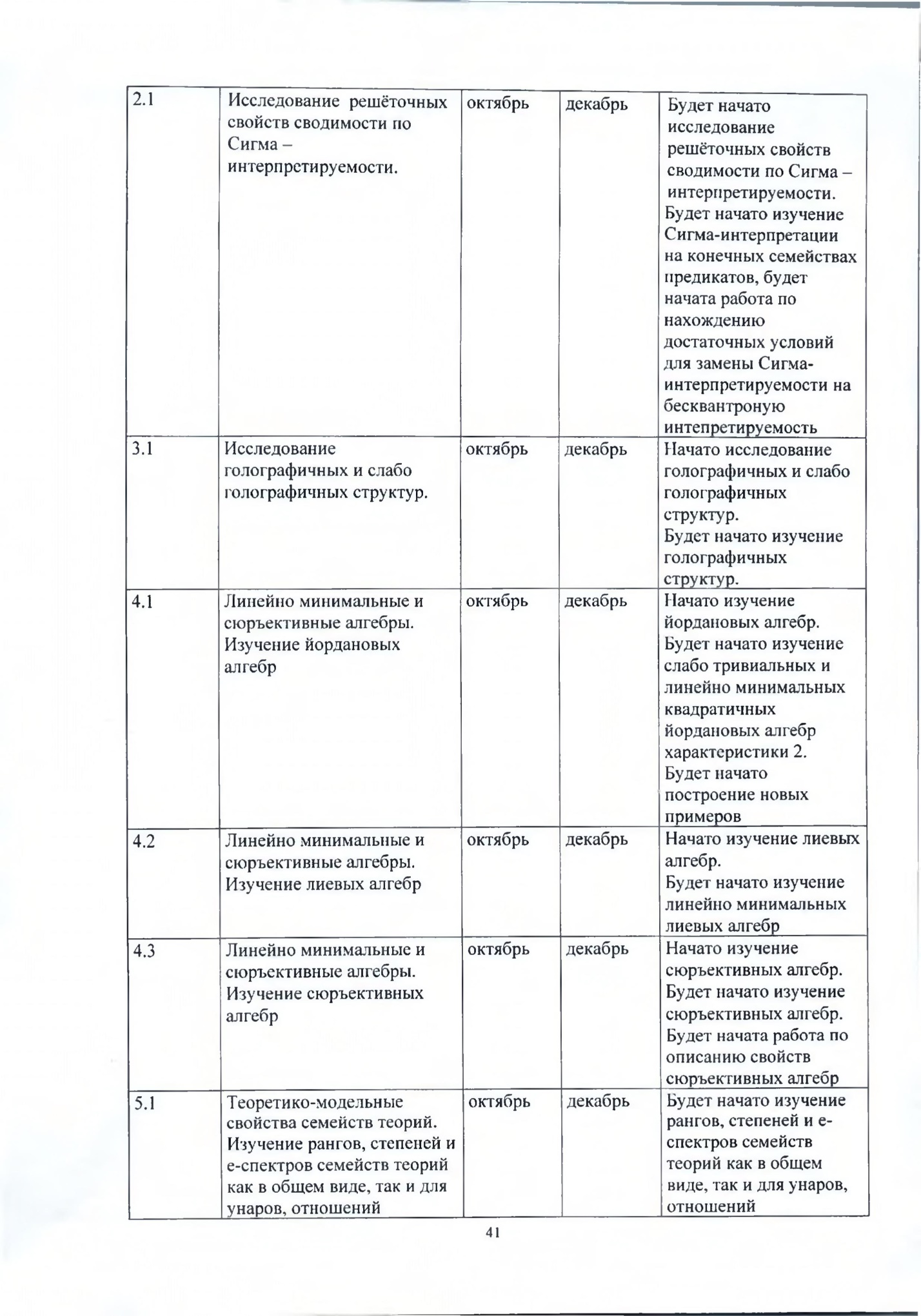
1. M.I.Kargapolov, Yu.I.Merzlyakov, Foundations of groups theory / Moscow: “Nauka”- 1982 – 240 p.
2. Bier, The width of verbal subgroups in the group of unitriangular matrices over a field // Int. J. Alg. Comput – 2012 – V.22:3 – P. 21-41.
3. N.S. Bahta, On the representability of the commutator of group UT(n, K) by the set of values of one variable // Herald of Omsk University – 2012 – V.2 – P.44–46.
4. N.S. Bahta, On representability of members of the low central series of the group UT(n, K) by values of one-variable function // Herald of Omsk University – 2013 – V.4 – P.13-15.
5. A.V. Men’shov, V.A. Roman’kov, On p-solvability of some regular equations over a Heisenberg p-group // Herald of Omsk University – 2014 – V.3 – P.11-14.
6. V.A. Roman’kov, Equations over groups // Groups Complexity Cryptology – 2012 – V. 2:4 – P.191–240.
7. С.С.Гончаров, Ю.Л.Ершов Конструктивные модели: Научная книга / Новосибирск – 1999 – 345c.
8. Н.Г.Хисамиев, А.А. Крыкпаева Эффективно вполне разложимые абелевы группы // Сибирский математический журнал – 1997 - T.38, №6 - C.1410-1412.
9. А.С. Морозов, Дж.А. Тусупов Минимальные предикаты относительно Δ-определимости // Алгебра и логика– 2020 – N 4 - *принята в печать*
10. Википедия – URL: [https://ru.wikipedia.org/wiki/Трёхэтапный\_протокол](https://ru.wikipedia.org/wiki/Трёхэтапный_протокол%20) (дата обращения 05.11.2020)
11. Menezes, P. van Oorschot, S. Vanstone. Handbook of Applied Cryptography. — 5th printing // CRC Press – 1996 — 816p.
12. U.S. Patent 4567600 (U.S. patent on the Massey–Omura cryptosystem)
13. Википедия – URL: <https://ru.wikipedia.org/wiki/Атака_посредника> (дата обращения 05.11.2020)
14. T. Hurley, CRYPTOGRAPHIC SCHEMES, KEY EXCHANGE, PUBLIC KEY // International Journal of Pure and Applied Mathematics – 2014 – T.93,N 6 – C.897-927.
15. В.А. Романьков. Алгебраическая криптография. / Издательство ОГУ им. Ф.М. Достоевского, Омск - 2013 — 136c.
16. Morley M., Categoricity in Power // Transactions of the American Mathematical Society - 1965 – V. 114:2 – P.514–538
17. Rosen E. Some Aspects of Model Theory and Finite Structures // The Bulletin of Symbolic Logic – 2002 V. 8:3 – P. 380–403
18. Sudoplatov S. V., Ranks for families of theories and their spectra - 2019, arXiv: 1901.08464v1 [math.LO]
19. Sudoplatov S. V., Approximations of theories - 2019, arXiv: 1901.08961v1 [math.LO]
20. Markhabatov N. D., Sudoplatov S. V., Ranks for families of all theories of given languages - 2019, arXiv: 1901.09903v1 [math.LO]
21. Sudoplatov S. V. Closures and generating sets related to combinations of structures // The Bulletin of Irkutsk State University, Series “Mathematics” – 2016 - V.16. - P.131–144.
22. Sudoplatov S. V. Combinations of structures and of their theories (an informative survey) // Algebra and model theory 12. Collection of papers - Novosibirsk: NSTU – 2019 - P.86–127.

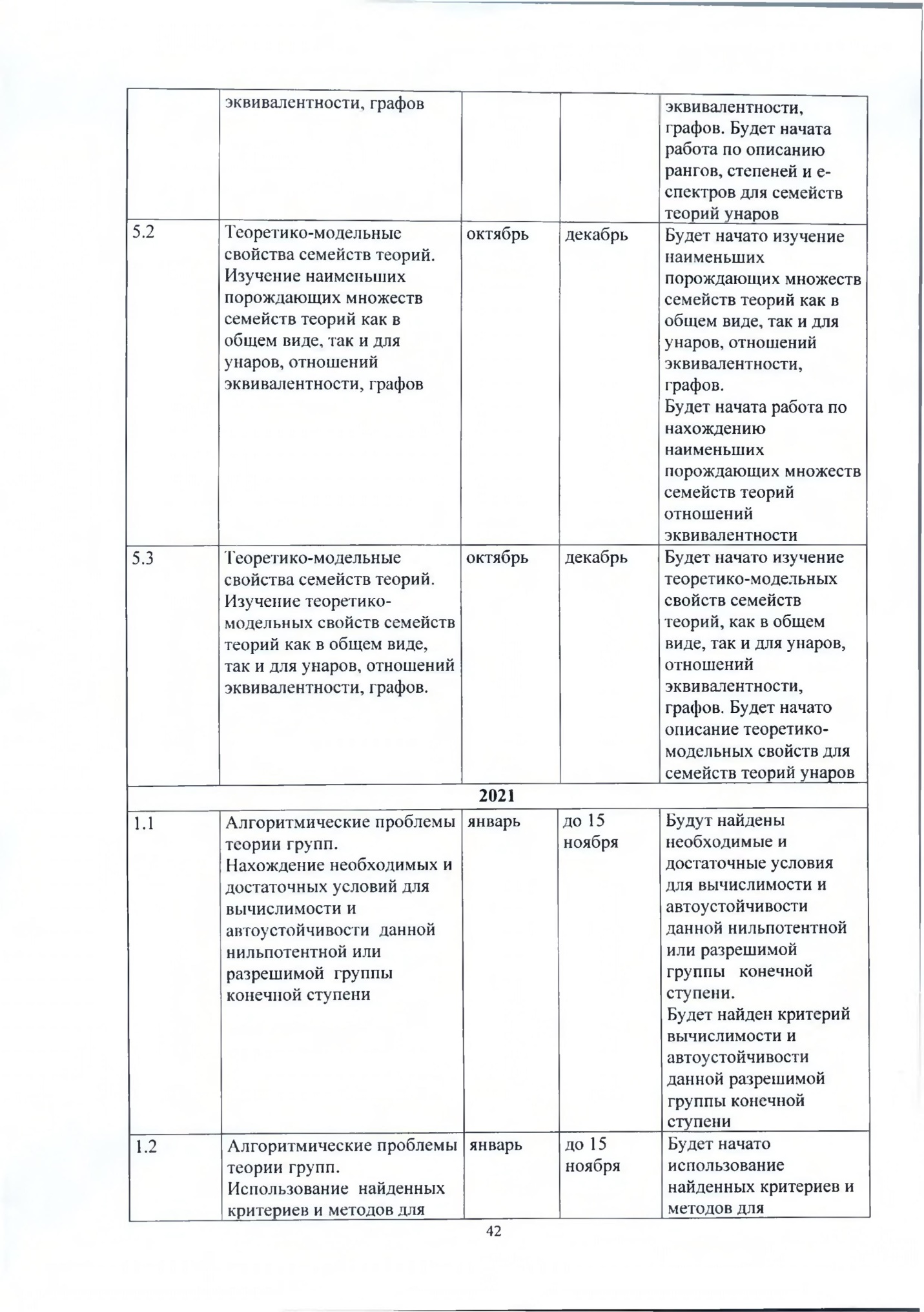
# ПРИЛОЖЕНИЕ A

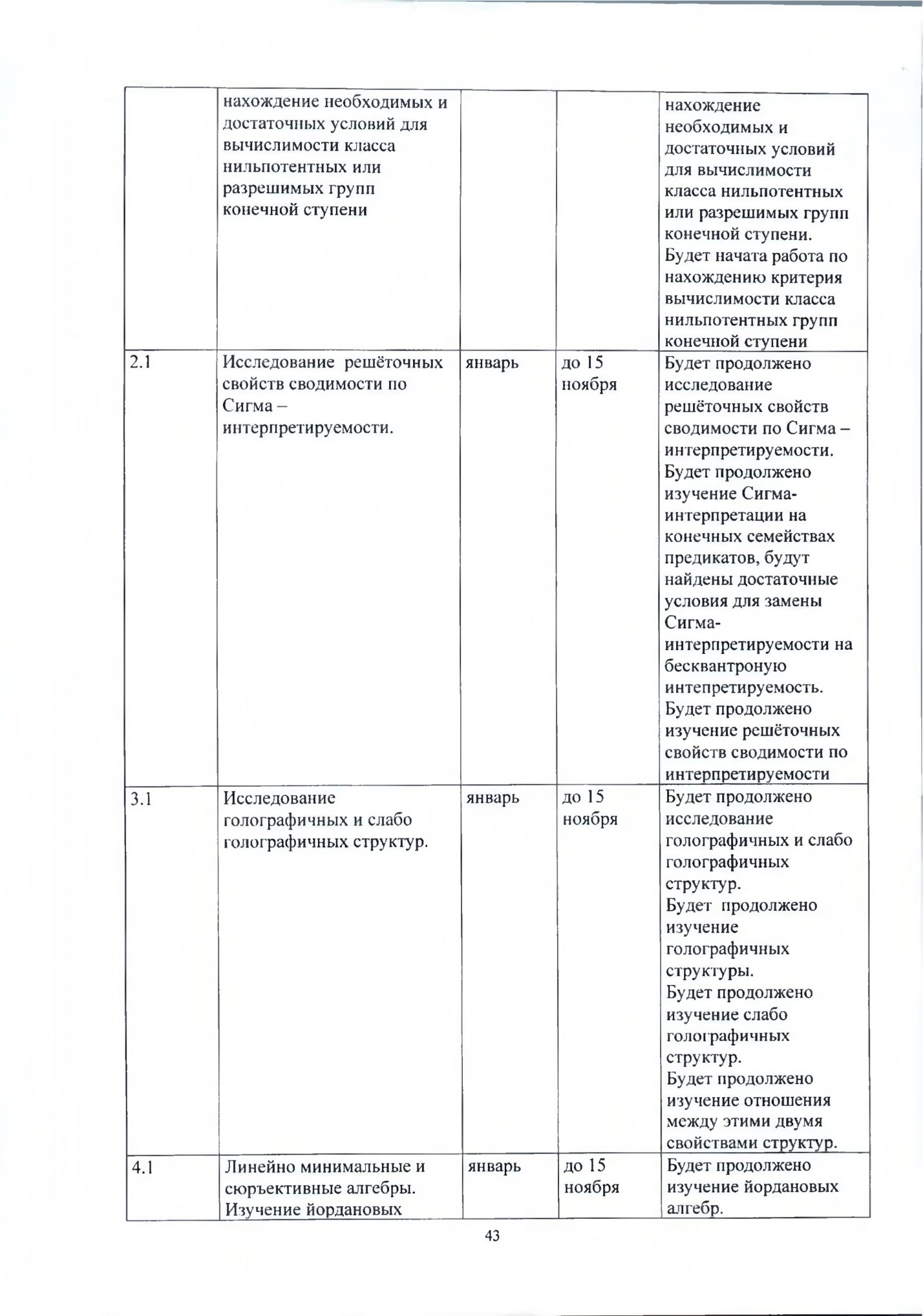
# Календарный план

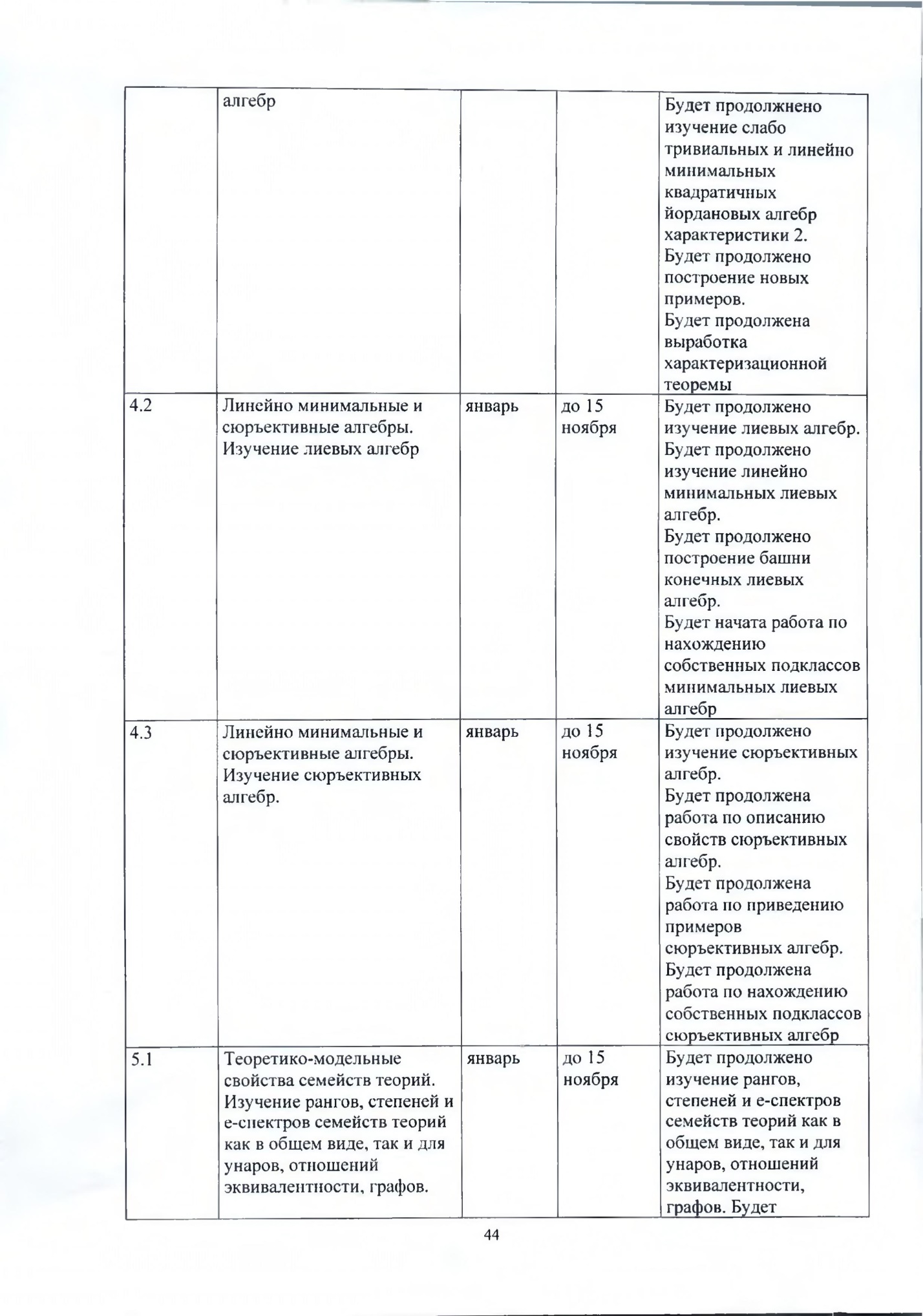


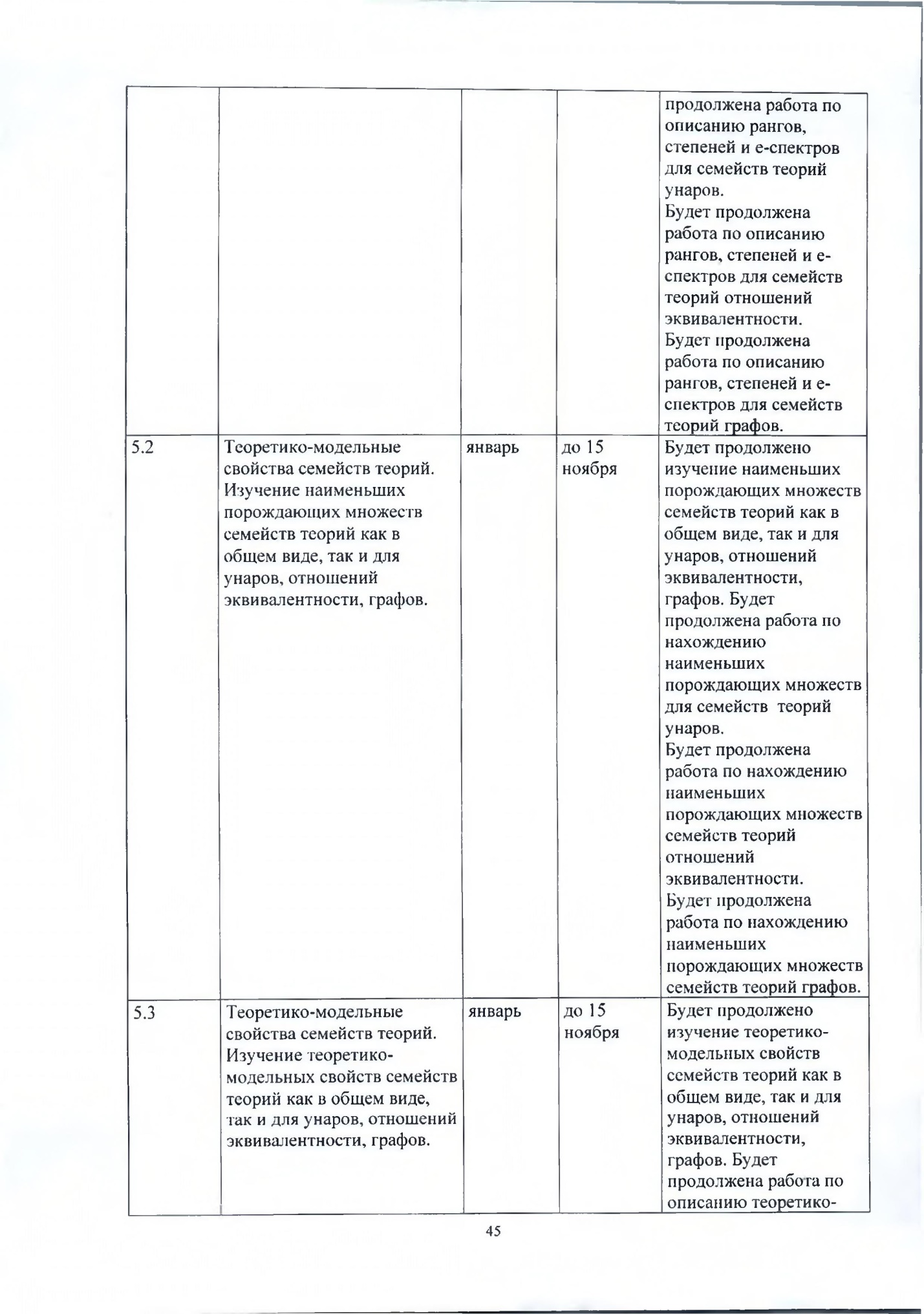


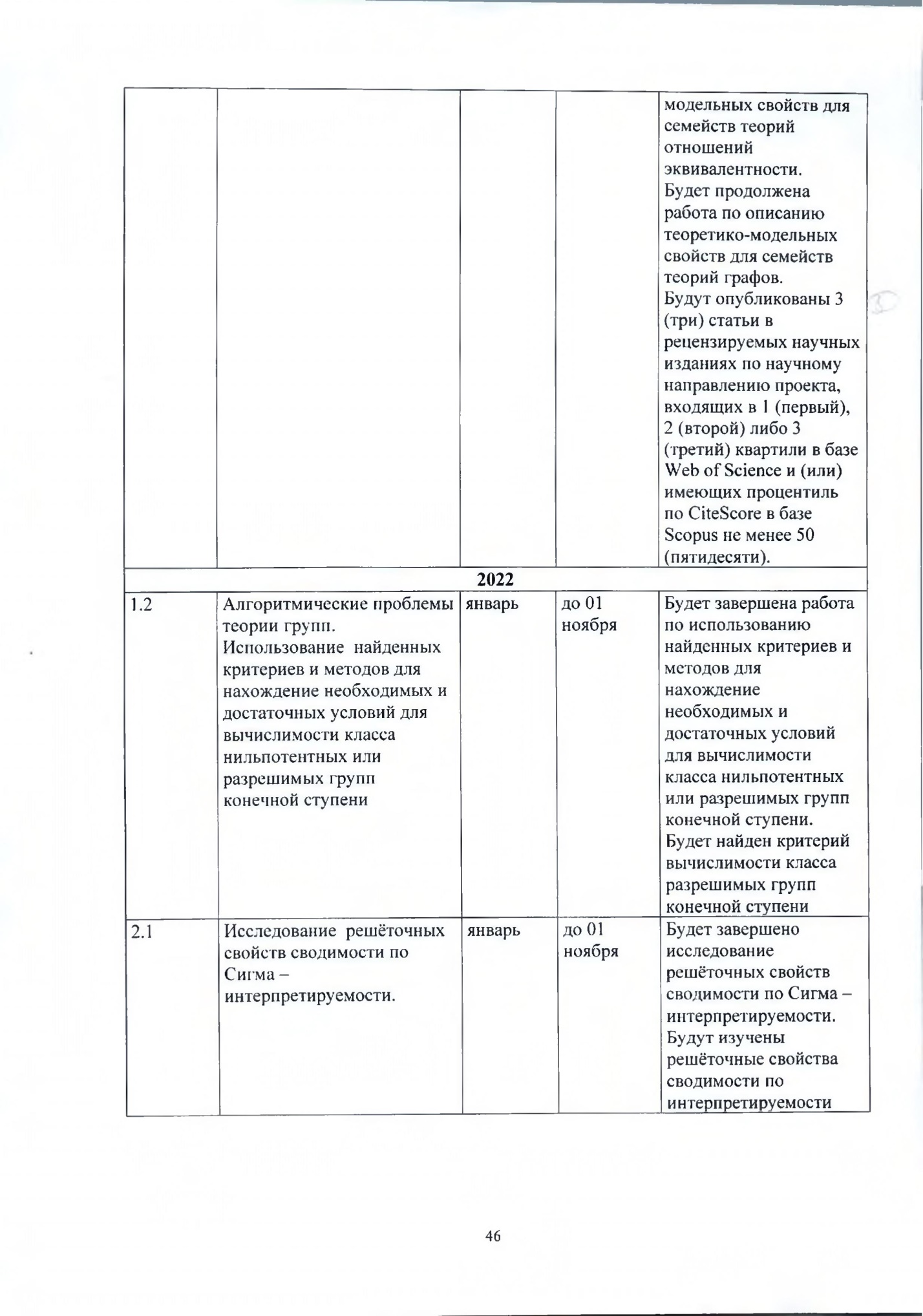


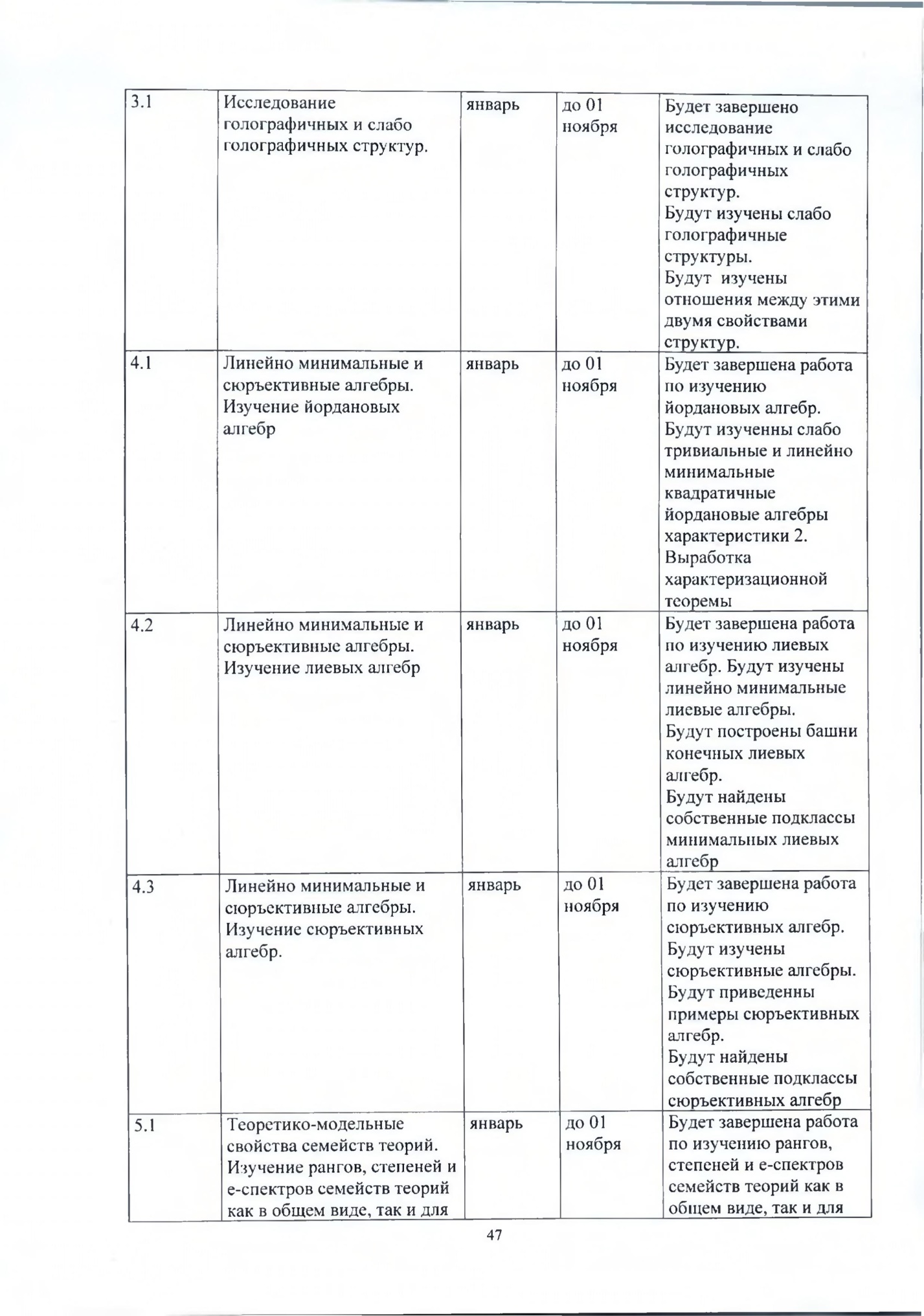


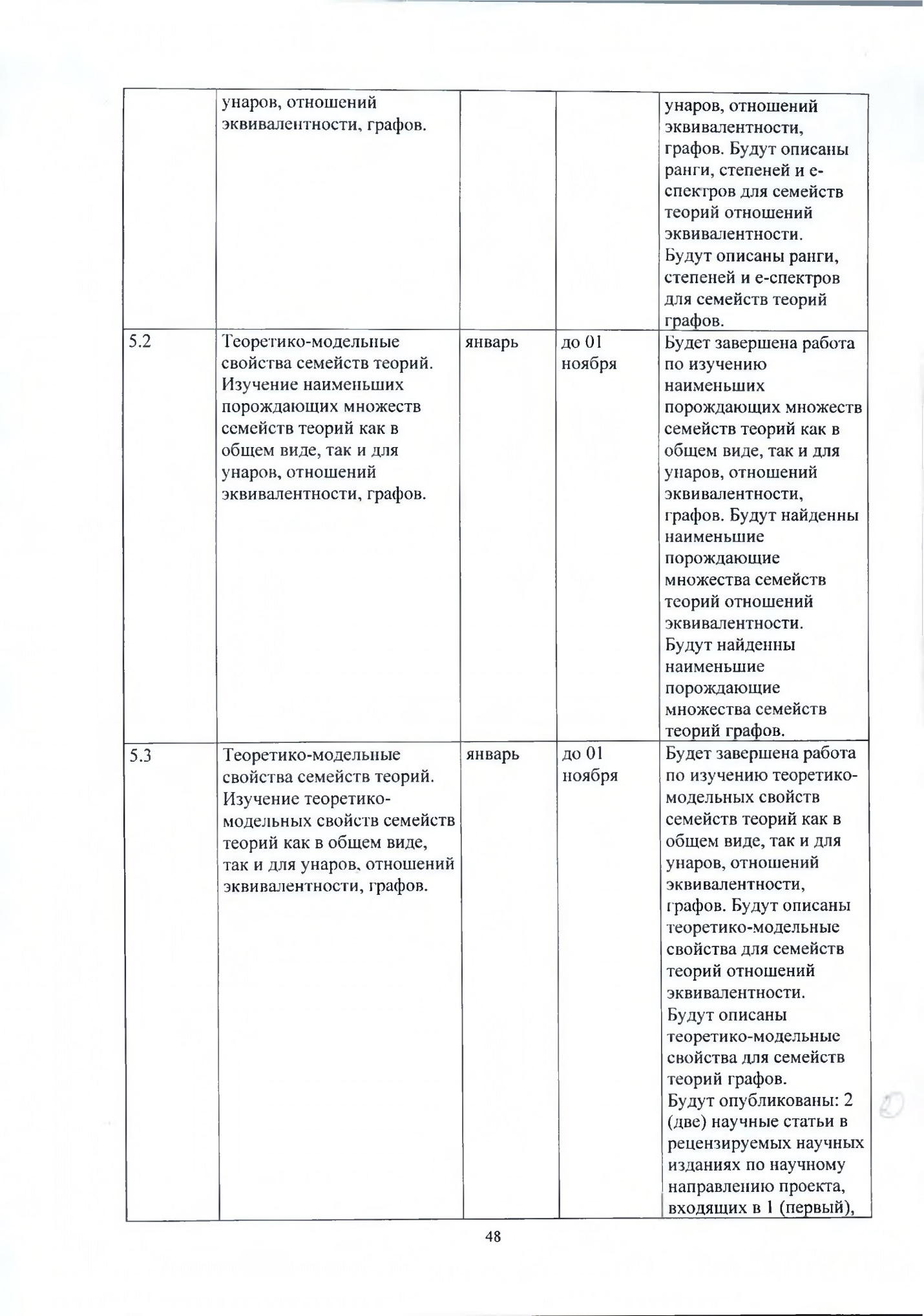














# ПРИЛОЖЕНИЕ Б

# Освещение актуальных проблем информационной поддержки научных исследований в открытой печати

Ведется активная работа по освещению актуальных проблем информационной поддержки научных исследований в открытой печати.

По результатам исследования опубликованы 2 публикации в трудах международных конференций:

1. N. D. Markhabatov, S. V. Sudoplatov On closures for families of theories // Международная конференция «Мальцевская чтения-2020» -2020 - C.243
2. N. D. Markhabatov On approximations of acyclic graphs// Международная конференция «Мальцевская чтения-2020»-2020 - C.244