УТВЕРЖДАЮ

Генеральный директор

АО «НПО «Эшелон», к.т.н.

_____ Цирлов В.Л.

«10» 04 2026 г.

ОТЗЫВ ВЕДУЩЕЙ ОРГАНИЗАЦИИ

Акционерного общества «Научно-производственное объединение «Эшелон» на диссертационную работу Волков Марии Сабины Александровны «Исследование комбинаторных свойств и оценка вычислительной сложности задач рюкзачного типа», представленную на соискание ученой степени кандидата физико-математических наук по специальности 1.2.3. «Теоретическая информатика, кибернетика».

Актуальность темы диссертации

Диссертационная работа посвящена исследованию комбинаторных свойств и оценке вычислительной сложности задач рюкзачного типа — одного из фундаментальных классов задач дискретной оптимизации и теории алгоритмов. Указанные задачи занимают важное место в современной теоретической информатике, выступая в качестве канонических представителей NP-трудных задач и широко используясь при анализе алгоритмической сложности и разработке методов оптимизации.

Интерес к задачам рюкзачного типа обусловлен как их теоретической значимостью, так и широким спектром практических приложений. Они возникают при решении задач распределения ограниченных ресурсов, оптимального планирования, финансового анализа, управления запасами, а также в задачах, связанных с проектированием и анализом информационных и вычислительных систем. В связи с этим исследование их структурных свойств и вычислительной сложности представляет собой актуальную научную проблему, имеющую междисциплинарный характер.

Несмотря на значительное количество исследований, посвященных различным аспектам задач рюкзачного типа, многие вопросы остаются открытыми. В частности, сохраняется потребность в более глубоком понимании комбинаторной структуры множества допустимых решений, разработке и уточнении оценок вычислительной сложности, а также в выявлении факторов, определяющих эффективность алгоритмов для различных классов входных данных. Особую актуальность приобретает развитие методов, позволяющих проводить детальный анализ сложности с учетом специфики постановки задачи и ее параметров.

Современные направления развития теории алгоритмов и математического программирования, включая параметризованный анализ сложности, изучение псевдополиномиальных алгоритмов и исследование структурных свойств NP-трудных задач, непосредственно связаны с задачами рюкзачного типа. В этом контексте получаемые результаты способствуют уточнению существующих теоретических представлений о сложности их решения, а также расширяют инструментарий комбинаторного анализа дискретных задач.

Таким образом, тема диссертационного исследования является актуальной и соответствует современному уровню развития теоретической информатики, включая такие ее направления, как теория сложности алгоритмов, математическая теория исследования операций и дискретная оптимизация, а также обусловлена потребностями практики в эффективных методах решения задач оптимального распределения ресурсов.

Структура и основное содержание диссертации

Диссертация состоит из введения, трех глав, заключения и списка литературы.

Во введении обоснована актуальность темы исследования, сформулированы цели и задачи работы, определены объект и предмет исследования, а также изложены основные положения, выносимые на защиту.

Первая глава носит постановочный и обзорный характер. В ней систематически изложены основные положения теории задач рюкзачного типа как одного из базовых классов NP-полных задач. Автор корректно формализует рассматриваемую задачу, вводит необходимые определения и параметры, в частности понятие плотности рюкзачного вектора, и проводит анализ известных результатов, касающихся вычислительной сложности. Особое внимание уделено зависимости сложности решения от структурных характеристик экземпляров задачи. Глава завершается постановкой основной научной задачи.

Вторая глава является центральной в работе и содержит основные теоретические результаты диссертации. В ней последовательно развиваются методы анализа комбинаторной структуры множества решений задач рюкзачного типа. Автором получены аналитические соотношения, связывающие параметры задачи с характеристиками множества допустимых решений, что представляет самостоятельный научный интерес. Существенным результатом является введение и исследование класса сюръективных линейных форм, для которых установлены строгие критерии и доказана возможность эффективного нахождения всех решений. Также в главе исследуются линейные формы с разрывами области значений, выявлены закономерности их структуры и предложены конструктивные методы их построения. Представленные результаты отличаются новизной и глубиной проработки.

Третья глава посвящена анализу вычислительной сложности задач рюкзачного типа с учетом полученных ранее теоретических результатов, а также вопросам практического применения. В ней исследуется влияние параметров задачи на трудоемкость ее решения и предлагаются методы целенаправленного конструирования экземпляров с заданными характеристиками сложности. Особый интерес представляет использование модульных преобразований для получения труднорешаемых экземпляров при сохранении структуры множества решений. Кроме того, автор демонстрирует применимость разработанных подходов в криптографических задачах, предлагая модифицированную схему, основанную на рюкзачных структурах. Представленные вычислительные эксперименты подтверждают работоспособность и эффективность предложенных методов.

В заключении сформулированы основные результаты диссертации, которые логически вытекают из содержания работы и отражают достигнутые автором научные результаты.

Структура диссертации является последовательной, изложение материала — логически связанным, а содержание глав соответствует поставленным задачам исследования.

Основные результаты и их новизна

В диссертационной работе получен ряд новых научных результатов, имеющих значение для развития теории сложности вычислений и комбинаторного анализа задач рюкзачного типа.

К числу основных результатов относятся:

1. Получены новые аналитические формулы, описывающие комбинаторную структуру множества допустимых решений задач рюкзачного типа. В частности, выведены соотношения для среднего числа решений и среднего значения целевой функции, позволяющие связать параметры задачи с характеристиками пространства решений.
2. Введен и исследован класс сюръективных линейных форм. Установлены необходимые и достаточные условия их сюръективности, а также выявлены свойства, определяющие вычислительную сложность соответствующих задач. Для данного класса разработан алгоритм нахождения всех допустимых решений, обладающий линейной сложностью по числу переменных и количеству решений.
3. Разработаны методы построения линейных форм с контролируемыми комбинаторными характеристиками, позволяющие управлять структурой множества решений и, тем самым, сложностью решения соответствующих задач.
4. Исследованы линейные формы с разрывами в области значений, установлены зависимости между значениями коэффициентов и структурой множества достижимых значений, а также предложены алгоритмы построения форм с заданным числом разрывов.
5. Предложены методы преобразования экземпляров задач рюкзачного типа, обеспечивающие переход от легкорешаемых к труднорешаемым случаям при сохранении структуры множества решений, что представляет интерес как с теоретической, так и с прикладной точки зрения.

Полученные результаты характеризуются научной новизной, внутренней согласованностью и представляют собой вклад в развитие методов анализа NP-полных задач.

Достоверность полученных результатов

Достоверность и обоснованность результатов, представленных в диссертации, обеспечиваются использованием строгого математического аппарата и опорой на фундаментальные положения теории алгоритмов, дискретной оптимизации и теории сложности вычислений.

Все основные утверждения и выводы диссертации сопровождаются корректными математическими доказательствами. Полученные теоретические результаты согласуются с известными ранее результатами в данной области и логически развивают их.

Корректность предложенных методов также подтверждается результатами вычислительных экспериментов. Проведенные эксперименты иллюстрируют применимость предложенных подходов и подтверждают сделанные в работе выводы.

Основные результаты диссертации прошли апробацию на научных конференциях и опубликованы в рецензируемых научных изданиях.

Значимость полученных результатов

Теоретическая значимость диссертационной работы заключается в развитии методов анализа комбинаторных свойств задач рюкзачного типа и углублении представлений о взаимосвязи структуры множества решений и вычислительной сложности. Полученные в работе аналитические формулы и установленные зависимости между параметрами задачи

и характеристиками пространства решений расширяют существующий аппарат исследования NP-полных задач и позволяют проводить более детализированную классификацию их экземпляров.

Важным теоретическим результатом является введение и исследование класса сюръективных линейных форм, а также анализ линейных форм с разрывами области значений. Эти результаты формируют основу для дальнейших исследований в области комбинаторного анализа дискретных задач и позволяют описывать механизмы перехода от легкоразрешимых к труднорешаемым случаям. Предложенные методы параметрических преобразований экземпляров задач представляют самостоятельный интерес для теории сложности вычислений и дискретной оптимизации.

Практическая значимость работы определяется разработкой алгоритмических методов, позволяющих управлять структурой экземпляров задач рюкзачного типа. В частности, предложенные алгоритмы генерации задач с заданными характеристиками могут быть использованы при тестировании и сравнительном анализе алгоритмов решения задач дискретной оптимизации.

Особый интерес представляют результаты, связанные с возможностью преобразования легкорешаемых экземпляров в труднорешаемые при сохранении структуры множества решений, что открывает перспективы их применения в задачах защиты информации. Предложенные подходы могут быть использованы при разработке криптографических схем, основанных на рюкзачных конструкциях, а также при анализе их устойчивости к известным методам криптоанализа.

Рекомендации по использованию результатов

– В научных исследованиях в области теории сложности вычислений и дискретной оптимизации для дальнейшего изучения структурных свойств NP-полных задач и разработки новых методов их анализа;

– В области криптографии и защиты информации при построении и анализе криптосистем, основанных на задачах рюкзачного типа, а также при исследовании их устойчивости к атакам, основанным на методах редукции решеток;

– В области разработки программного обеспечения и тестирования для генерации тестовых наборов с контролируемой вычислительной сложностью, что дает возможность проводить стресс-тестирование алгоритмов и выявлять их поведение в предельных и наихудших случаях;

– В высоконагруженных вычислительных системах и центрах обработки данных при моделировании и анализе задач распределения вычислительных ресурсов, где предложенные подходы позволяют учитывать сложность возникающих комбинаторных конфигураций и выбирать более эффективные стратегии управления;

– В области телекоммуникации при анализе устойчивости алгоритмов и протоколов к атакам, основанным на решении сложных комбинаторных задач, а также при моделировании сценариев, требующих учета предельной вычислительной сложности;

– В системах кодирования и передачи данных для построения помехоустойчивых и избыточных схем кодирования, а также для анализа устойчивости алгоритмов декодирования при наличии множественных решений.

Замечания

1. Экспериментальные исследования проведены для ограниченного набора параметров (в частности, фиксированной размерности $n = 200$). Представляется целесообразным расширить их на более широкий диапазон размерностей и

плотностей, а также провести сравнение с альтернативными методами решения задач рюкзачного типа.

2. В анализе криптостойкости основное внимание уделено алгоритму LLL, тогда как современные методы включают более мощные схемы редукции, такие как BKZ. Отсутствие анализа устойчивости относительно BKZ, в том числе с учетом параметра блока, несколько ограничивает полноту оценки криптографической стойкости.
3. Вопросы масштабируемости методов генерации экземпляров задач с заданными характеристиками освещены ограниченно. Было бы полезно проанализировать их вычислительную эффективность при росте размерности.
4. В тексте работы приведено ограниченное количество сведений о деталях программной реализации предложенных алгоритмов. Между тем именно эти факторы во многом определяют эффективность применения алгоритмов на практике.
5. Представляется, что практическая значимость работы могла бы быть дополнительно усилена за счет более подробного анализа сценариев внедрения предложенных методов в прикладные системы, в том числе с оценкой выигрыша по сравнению с существующими подходами в реальных вычислительных средах.
6. В автореферате упоминается использование усеченного хэш-преобразования SHA-256 для формирования контрольной суммы с длиной $l = 16$ бит. Не поясняется, почему выбрано именно такое значение и проводился ли анализ вероятности коллизий с учетом конкретной структуры множества решений сюръективных форм, которая может отличаться от равномерного распределения.

Отмеченные замечания носят преимущественно рекомендательный характер и не снижают общей положительной оценки диссертационной работы.

Заключительная оценка

Диссертационная работа представляет собой завершенное научное исследование, выполненное на высоком теоретическом уровне и посвященное актуальной проблеме анализа комбинаторных свойств и вычислительной сложности задач рюкзачного типа.

Полученные автором результаты обладают научной новизной, теоретической и практической значимостью, являются обоснованными и достоверными. Они вносят вклад в развитие теории сложности вычислений, дискретной оптимизации и методов анализа NP-полных задач.

Основные результаты опубликованы в 9 работах, в том числе в 5 статьях из списка изданий, рекомендованных ВАК, прошли апробацию на научных конференциях и получили достаточное освещение в автореферате, который корректно отражает содержание работы.

Диссертационная работа соответствует требованиям, предъявляемым «Положением о присуждении ученых степеней» к кандидатским диссертациям по специальности 1.2.3 «Теоретическая информатика, кибернетика», а ее автор, Волков Мария Сабина Александровна заслуживает присуждения ученой степени кандидата физико-математических наук по указанной специальности.

Диссертация, автореферат и отзыв рассмотрены и одобрены на заседании секции Научно-технического совета АО «НПО «Эшелон».

Протокол № 26/4 от «10» апреля 2026 г.

Президент АО «НПО «Эшелон»
доктор технических наук, старший научный сотрудник

Алексей Сергеевич Марков

Директор департамента тестирования и сертификации
кандидат технических наук

Виталий Викторович Варенница

«10» 04 2026 г.

Контактная информация:
107023, г. Москва, ул. Электрозаводская, д. 24; тел./факс: +7 (495) 223-23-92,
эл.почта: mail@npo-echelon.ru