## *ФОРМА 2 ПРЕДЛОЖЕНИЕ ОБ УСЛОВИЯХ ИСПОЛНЕНИЯ ГОСУДАРСТВЕННОГО КОНТРАКТА НА ВЫПОЛНЕНИЕ ПОИСКОВЫХ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИХ РАБО**Т (Предложение о выполнении работ)*

«ФГАОУ ВПО «ЮЖНЫЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

*(наименование Участника размещения заказа)*

Документ должен быть составлен по нижеприведенной Форме в соответствии с требованиями, установленными в Разделе VIII «Заказ на выполнение поисковых научно-исследовательских работ» настоящей Конкурсной документации.

|  |  |  |  |
| --- | --- | --- | --- |
| **Раздел 1. Номер открытого конкурса, наименование поисковых научно-исследовательских работ, наименование проблемы исследований, код по ОКДП** | | | |
| **Номер открытого конкурса** | **Наименование поисковой научно-исследовательской работы** | **Наименование проблемы исследований** | **Код по Общероссийскому классификатору видов экономической деятельности, продукции и услуг (ОКДП) ОК 004-93** |
| **1** | **2** | **3** | **4** |
| НК -623П | Проведение поисковых научно-исследовательских работ по направлению «Обработка, хранение, передача и защита информации» в рамках мероприятия 1.2.2 Программы | Разработка и исследование схем специального широковещательного шифрования и методов защиты информации от технической утечки на основе теоретико-кодовых, алгебро-геометрических и теоретико-операторных подходов | 7310020 |

|  |  |
| --- | --- |
| **Раздел 2. Общие требования к качеству выполняемых поисковых научно-исследовательских работ** | |
| **№ п/п** | **Содержание общих требований** |
| 1 | Алг геом коды  Разл метрики  Спис дек  Свертки, Ольшевский  ССШШ(+ Кобатянский с вод знак)  Тех утеч част  Тех утеч полная (МЭ на разных кодах, протоколы Кос, Чек разл метрики Габ и модификации Берн, )  Спис дек как метод для ССШШ  Свертки (… ВМС)  Пел ВМС, декодер для ДвАГ(РС) ?? и применение к МЭ ??  Бибов АГ(Див), спис , ССШШ  В процессе обработки, хранения и передачи информации важной и актуальной проблемой является ее защита, как от действий нелегитимных субъектов, так и от воздействия помех. В рамках решения этой фундаментальной проблемы особый теоретический и практический интерес представляют такие значимые направления, как борьба с полной и частичной технической утечкой в зашумленных каналах передачи данных, так и разработка новых эффективных методов и средств защиты информации от несанкционированного доступа, несанкционированного копирования и распространения (тиражирования). Научными исследованиями в этих направлениях занимаются многие ученые отечественных и зарубежных научных центров. В частности, вопросами защиты информации от частичной и полной технической утечки с помощью помехоустойчивых кодов занимаются такие крупные ученые, как Э.М.Габидулин, В.И.Коржик, В.А.Яковлев, В.М.Сидельников, Е.А.Крук, Дж. ван Тилбург, Дж.Берштейн, Дж.Гибсон, А.Х.Аль-Джабри, Р.Овербек. Проблемой защиты информации от несанкционированного доступа, копирования и тиражирования, также используя современную теорию помехоустойчивых кодов, занимаются Г.Кабатянский, А.Сильверберг, Дж.Стэддон, Дж.Уолкер. Из работ этих ученых можно сделать вывод об актуальности исследования сформулированных проблем защиты информации в процессе ее обработки, хранения и передачи с помощью методов и результатов теории неклассических кодовых метрик, теории кодового зашумления, теории списочного декодирования. В последние годы получены новые мощные результаты, как в области теории неклассических кодовых метрик (Э.М.Габидулин), так и в области циклических и алгебро-геометрических кодов (Й.Юстесен, Т.Хёхольдт, Х.Штихтенот, М.А.Цфасман, С.Г.Влэдуц, А.Н.Скоробогатов) и методов их списочного декодирования (М.Судан, В.Гурусвами, Р.Рот, Г.Рукенштейн, М.Кудряшов). Анализ научно-исследовательских работ показывает, что некоторыми основными инструментами построения эффективных методов декодирования новых современных кодов являются методы быстрой факторизации многочленов нескольких переменных и быстрого решения операторных сверточных уравнений (С.Саката, Р.Рот, Г.Рукенштейн, К.Ву, П.Зигель, И.Ц.Гохберг, Д.Ольшевский). В связи с этим актуальным представляется разработка и применение новых методов математической теории помехоустойчивого кодирования для модификации и построения новых комплексных систем защиты информации.  Предусмотренное проектом исследование направлено на получение новых результатов в решении задач противодействия полной и частичной технической утечке в незашумленных и зашумленных каналах передачи данных и защиты информации от несанкционированного доступа, несанкционированного копирования и тиражирования на основе применения современных алгебро-геометрических и теоретико-операторных подходов в теории и практике помехоустойчивого кодирования.  Исследование должно быть направлено на решение актуальной, значимой проблемы и получение новых результатов. |
| 2 | В процессе выполнения данной поисковой научно-исследовательской работы предусматривается: обеспечение безопасности для жизни и здоровья людей и охраны окружающей среды, совместимости и взаимозаменяемости путем соблюдения действующих нормативных документов Российской Федерации; стандартизация и унификация используемых и разрабатываемых технических и программных средств путем использования требований ГОСТов и руководящих документов в этой области; соблюдение метрологических требований при выполнении работ; использование типовой номенклатуры программных и технических средств; направленность на экономичное и рациональное использование вычислительных средств и ресурсов в ходе проведения исследования. При выполнении ПНИР также предполагается обеспечение конкурентоспособности разрабатываемой научно-исследовательской продукции на основе анализа мировой литературы в предметной области и достижение при выполнении работ уровня результатов, сравнимого с мировым. |
| 3 | Процесс выполнения поисковой научно-исследовательской работы состоит из следующих этапов:  1. Проведение аналитического обзора существующих современных решений задачи защиты информации от несанкционированного доступа, несанкционированного копирования и распространения (тиражирования), полной или частичной технической утечки, сравнительная оценка вариантов возможных решений с учетом результатов прогнозных исследований специалистов в данной предметной области, проведение патентных исследований на предмет патентной чистоты рассматриваемых и используемых в исследовании методов и средств.  2. Проведение теоретических исследований в области применения современных теоретико-кодовых, алгебро-геометрических и теоретико-операторных подходов к созданию новых и модификации существующих схем специального широковещательного шифрования, криптографических систем типа Мак-Элиса, Нидерайтера, Габидулина и Сидельникова, протоколов симметричного и асимметричного шифрования для противодействия полной и (или) частичной технической утечки. Построение и программная реализация новых моделей защиты информации на основе проведенных исследований. Экспериментальное исследование эффективности и границ применимости разработанных моделей. Программная реализация наиболее эффективных способов защиты информации, разработанных в рамках данного исследования. Публикация полученных результатов.  3. Обобщение и оценка результатов проведенных исследований, выпуск отчетной научно-технической документации по работе в целом, оценка эффективности полученных результатов в сравнении с современным научно-техническим уровнем, оценка конкурентоспособности полученной научно-технической продукции.  4. Предъявление результатов работ к приемке. |
| 4 | Предполагаемое содержание аналитического обзора:  1. Систематизация сведений о ключевых задачах, известных положениях, классификациях, терминах и определениях в проблеме защиты информации.  2. Обзор существующих современных (1990 – 2009 гг.) методов решения проблемы защиты информации от несанкционированного доступа, несанкционированного копирования и распространения (тиражирования), полной или частичной технической утечки, основанный на статьях в российских и зарубежных научных журналах (открытая печать), монографиях ведущих специалистов, патентах. Выводы о приоритетных направлениях исследований и круга перспективных методов решения проблемы защиты информации на основе рассмотренных в обзоре источников.  3. Детализированное описание наиболее актуальных подходов к решению основной задачи, в частности, описание существующих современных теоретико-кодовых, алгебро-геометрических и теоретико-операторных подходов. Описание методов выполнения работы в целом.  4. Проведение сравнительной оценки вариантов возможных решений исследуемой проблемы с учетом результатов прогнозных исследований, проводившихся по аналогичной тематике. |
| 5 | Для получения новых результатов в рассмотренных выше задачах противодействия технической утечки в различных каналах передачи данных и защиты информации от несанкционированного доступа, копирования и тиражирования на основе применения современных алгебро-геометрических и теоретико-операторных подходов представляется оптимальным следующий вариант направления исследований:  1. Объекты исследований  1.1 Защищенность информационного обмена от технической утечки в каналах передачи данных.  1.2 Защищенность информационного обмена от несанкционированного доступа, копирования и тиражирования в информационно-телекоммуникационных системах обмена, обработки и хранения данных.  1.1 Модели защиты информации от несанкционированного копирования, распространения и тиражирования с использованием схем специального широковещательного шифрования, основанные на циклических и алгебро-геометрических помехоустойчивых кодах и методах их списочного декодирования.  1.2. Модели защиты информации от полной технической утечки на основе кодовых криптосистем Мак-Элиса, Нидерайтера, Габидулина, Сидельникова и протоколов симметричной и асимметричной криптографии.  1.3. Модели защиты информации от частичной технической утечки путем применения факторных защитных кодов, построенных на основе слабоплотных кодов и кодов Габидулина.  1.4. Конструкция, сложность, оптимальная реализация алгоритмов классического и списочного декодирования циклических и алгебро-геометрических помехоустойчивых кодов.  1.5 Разрешимость операторных сверточных уравнений.  2. Методы исследований  2.1. Математическое моделирование схем защиты информации.  2.2 Теоретическое обоснование моделей схем защиты информации и экспериментальное исследование их программных реализаций.  2.3 Модификация и разработка теоретико-кодовых методов защиты информации на основе новых результатов в декодировании семейств алгебро-геометрических помехоустойчивых кодов.  2.4 Развитие существующих теоретико-кодовых методов защиты информации на основе применения новых результатов в области исследования разрешимости операторных сверточных уравнений.  3. Оборудование.  3.1. Персональные компьютеры.  3.2 Кластер  4. Ожидаемые научные результаты  4.1 Новая модель защиты информации от несанкционированного копирования, распространения и тиражирования.  4.1.1 Общая математическая модель эффективной защиты тиражируемых цифровых данных от несанкционированного копирования, основанная на методе наборных ключей, циклических и алгебро-геометрических кодах, списочных декодерах, с противодействием коалиционным атакам на ключи, и ее программная реализация для систем электронной коммерции.  4.1.2 Классификация различных видов угроз пользователю модели защиты.  4.1.3 Методики экспериментального исследования модели.  4.1.4 Границы применимости модели, основанные на теоретических и экспериментальных исследованиях.  4.2 Новые модели защиты информации от полной технической утечки на основе кодовых криптосистем Мак-Элиса, Нидерайтера, Габидулина, Сидельникова и модификаций протоколов симметричной и асимметричной криптографии.  4.2.1 Усовершенствованный для кодов Габидулина симметричный протокол Стройка-Тилбурга и новая схема защиты информации от полной утечки.  4.2.2 Модель защиты информации от полной утечки на основе криптосистем Габидулина с ранговыми метриками и F-метриками.  4.2.3 Модель защиты информации от полной утечки на основе криптосистем Мак-Элиса, Нидерайтера и Сидельникова с использованием асимметричного протокола Бернштейна и списочного декодирования кодов Гоппы.  4.3 Новые модели защиты информации от частичной технической утечки в бесшумных и зашумленных каналах путем применения факторных защитных кодов, построенных на основе слабоплотных кодов и кодов Габидулина.  4.3.1 Анализ существующих схем защиты информации от технической утечки. Обоснование выбора схем защиты от технической утечки, основанных на применении помехоустойчивых кодов.  4.3.2 Математическая модель защиты информации в бесшумном канале с перехватом, свойство (λ,δ)-защищенности линейных кодов, теорема о достаточных условиях (λ,δ)-защищенности.  4.3.3 Теоретическая и экспериментальная оценки иерархии весов слабоплотных кодов класса LDPC(2,r).  4.3.4 Математическая модель защиты информации в зашумленном канале с перехватом, оценки уровня понимания перехваченной информации для произвольных и МДР-кодов, программная реализация модели на основе применения слабоплотных кодов и кодов Габидулина.  4.3.5 Универсальный способ защиты информации от полной и частичной технической утечки в зашумленном канале передачи данных.  4.3.6 Границы применимости модели защиты на основе кодового зашумления, основанные на теоретических и экспериментальных исследованиях.  4.4 Новые алгоритмы декодирования семейств алгебро-геометрических кодов.  4.4.1 Алгоритмы списочного декодирования алгебро-геометрических кодов типа кодов Рида-Соломона на плоских проективных кривых, вычислительная сложность алгоритмов, вычислительно эффективная программная реализация алгоритмов.  4.4.2 Алгоритм факторизации вычисления функциональных корней многочленов нескольких переменных над произвольной областью целостности и его модификация для алгоритмов списочного декодирования.  4.4.3 Вычислительно эффективная программная реализация алгоритмов списочного декодирования алгебро-геометрических кодов дивизорного типа.  4.4.4 Вычислительно эффективная программная реализация алгоритмов однозначного декодирования алгебро-геометрических кодов типа кодов Рида-Соломона с использованием схемы Берлекэмпа-Месси-Сакаты.  4.4.5 Библиотека алгоритмов декодирования семейств алгебро-геометрических кодов, допускающая высокоуровневое распараллеливание вычислений.  4.5 Условия разрешимости и применимости методов решения операторных сверточных уравнений.  4.5.1 Схема решения семейств операторов дискретной свертки над полями Галуа, основанная на методе Берлекэмпа-Месси-Сакаты.  4.5.2 Условия фредгольмовости и обратимости операторов свертки на группе Z с несуммируемыми ядрами и схема применения проекционных методов решения сверточных уравнений.  4.5.3 Условия фредгольмовости и индекс операторов свертки на произвольной коммутативной локально компактной группе в терминах операторной К-теории.  4.5.4 Схема применения сдвиговых методов Гохберга-Кайласа-Ольшевского и Финка-Рост к решению систем линейных уравнений с составными матрицами типа Теплица, Вандермонда, Коши.  Обоснование оптимального варианта направления исследований должно включать систематизированный перечень того, что необходимо исследовать, предполагаемые методы и экспериментальное оборудование, и ожидаемые научные результаты. |
| 6 | План проведения теоретических и (или) прогнозных исследований должен позволять получить достаточные теоретические и (или) достоверные экспериментальные результаты для решения поставленных научно-исследовательских задач и предусматривать (включать):  - наименование работ и виды работ (экспериментальные / теоретические);  - планируемые научные результаты (указываются в соответствии официальным перечнем результатов научно-технической деятельности, установленным постановлением Правительства Российской Федерации от 4 мая 2005 г. N 284 "О государственном учете результатов научно-исследовательских, опытно-конструкторских и технологических работ гражданского назначения") и не должны подпадать под перечни сведений, подлежащих засекречиванию органов государственной власти и организаций, руководители которых наделены полномочиями по отнесению сведений к государственной тайне по Распоряжению Президента Российской федерации №151-РП от 16.04.2005 г. (с изменениями и дополнениями);  - сроки проведения работ;  - форма представления результатов работ (статьи, монографии, доклады, патенты, полезные модели и др.)  План проведения исследований должен быть рассмотрен на ученом (научно-техническом) совете. |
| 7 | Материалы, описывающие проведение теоретических и (или) экспериментальных исследований могут включать:  - лабораторные технологические инструкции;  - акты изготовления экспериментальных образцов;  - методики и протоколы измерений характеристик экспериментальных образцов;  - акты готовности испытательных стендов (установок) (при необходимости разработки испытательного стенда);  - протоколы испытаний (исследований) экспериментальных образцов;  - результаты оптимизации параметров;  - описание применяемых для решения поставленных научно-исследовательских задач моделей, алгоритмов, методик (и) или закономерностей;  - результаты систематизации и предварительной оценки полученных результатов и др. |
| 8 | Результаты теоретических и экспериментальных исследований будут рассмотрены на Ученом совете Южного федерального университета (факультета математики, механики и компьютерных наук Южного федерального университета)  Результаты теоретических и (или) экспериментальных исследований должны быть рассмотрены на ученом (научно-техническом) совете. |
| 9 | В данной поисковой научно-исследовательской работе предполагается построение новых математических моделей защиты информации от технической утечки и нелегального доступа, копирования и тиражирования, а также теоретическое и экспериментальное исследование их применимости. Особенностью разрабатываемых моделей является применение для их построения теории помехоустойчивого кодирования, в частности, использование новых разработанных результатов в области декодирования семейств алгебро-геометрических кодов и решения операторных сверточных уравнений. В мировом сообществе это было, однако, применение новых результатов позволит построить вычислительно эффективные и более криптографически стойкие схемы защиты информации по сравнению с существующими.  Результаты, приведенные в пункте 5 настоящего раздела, предполагается получить полностью, что позволит достигнуть поставленных целей. На основе анализа мировой литературы в предметной области можно заключить, что планируемые теоретические и экспериментальные исследования обеспечивают конкурентоспособность разрабатываемой научно-исследовательской продукции и при их выполнении результаты достигнут уровня, сравнимого с мировым. Обоснованный в пункте 5 настоящего раздела оптимальный вариант исследований дает основание сделать вывод о том, что развитие алгебро-геометрического и теоретико-операторного подходов позволит получить вычислительно эффективные и криптографически стойкие решения задач модификации и построения систем защиты информации от технической утечки, несанкционированного доступа, копирования и тиражирования информации. Результаты поисковой научно-исследовательской работы могут быть использованы для построения программно-аппаратных систем защиты информации в системах обмена, обработки и хранения информации, например, системах цифровой связи, электронных платежей, электронного документооборота, распространения и продажи лицензионной продукции и т.п. Кроме того, эти результаты могут быть использованы при подготовке бакалавров и магистров по специальностям группы защиты информации и информационных технологий.  Обобщение и оценка результатов исследований должны включать:  - оценку полноты решения задач и достижения поставленных целей;  - сопоставление и обобщение результатов анализа научно-информационных источников и теоретических (экспериментальных) исследований;  - оценку эффективности полученных результатов в сравнении с современным научно-техническим уровнем;  - разработку рекомендаций по возможности использования результатов поисковой научно-исследовательской работы в реальном секторе экономики;  - разработку рекомендаций по использованию результатов поисковой научно-исследовательской работы при создании научно-образовательных курсов.  Должен быть обоснован выбор (подход к разработке) моделей, методов, программ и (или) алгоритмов, позволяющие увеличить объем знаний для более глубокого понимания и путей применения новых явлений, механизмов или закономерностей. |
| 10 | Рекомендации по возможности использования результатов проведенной поисковой научно-исследовательской работы в реальном секторе экономики должны быть оценены и согласованы с предприятием (организацией) отрасли промышленности |
| 11 | Рекомендации по использованию результатов поисковой научно-исследовательской работы при разработке научно-образовательных курсов должны быть рассмотрены на ученом (научно-техническом) совете. |
| 12 | Перед публикацией результатов должно быть получено заключение экспертной комиссии по открытому опубликованию. |

|  |  |  |
| --- | --- | --- |
| **Раздел 3. Требования, предъявляемые к поисковым научно-исследовательским работам (этапам), cрок (период) выполнения поисковых научно-исследовательских работ (этапов)** | | |
| **Номер этапа** | **Требования, предъявляемые к поисковым научно-исследовательским работам (этапам) (Параметры, определяющие качество заказываемых поисковых научно-исследовательских работ (этапов)) Параметры, определяющие количественные (и/или объемные, структурные и иные) характеристики поисковых научно-исследовательских работ (этапов)** | **Дата окончания выполнения работ (этапов)[[1]](#footnote-1)\*** |
| **1** | **2** | **3** |
| **I** | Должны быть проведены экспериментальные и (или) теоретические исследования и при необходимости патентные исследования, в том числе:   * + - * аналитический обзор;       * выбор и обоснование оптимального варианта направления исследований;       * план проведения экспериментальных и (или) теоретических исследований;       * экспериментальные и (или) теоретические исследования I этапа.   Материалы, описывающие проведение теоретических и (или) экспериментальных исследований должны включать все необходимые сведения для обеспечения возможности воспроизведения результатов проведенных исследований. | 6 сентября  2010 г. |
| **II** | Должны быть проведены экспериментальные и (или) теоретические исследования в соответствии с разработанным планом проведения исследований II этапа.  Материалы, описывающие проведение теоретических и (или) экспериментальных исследований должны включать все необходимые сведения для обеспечения возможности воспроизведения результатов проведенных исследований.  Результаты научных исследований должны быть опубликованы в трудах (тезисах докладов) международной или всероссийской конференции с обязательной ссылкой на проведение поисковой научно-исследовательской работы в рамках реализации ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009 – 2013 годы (не менее 1-ой публикации). | 26 ноября  2010 г. |
| **III** | Должны быть проведены экспериментальные и (или) теоретические исследования в соответствии с разработанным планом проведения исследований III этапа.  Материалы, описывающие проведение теоретических и (или) экспериментальных исследований должны включать все необходимые сведения для обеспечения возможности воспроизведения результатов проведенных исследований. | 6 сентября  2011 г. |
| **IV** | Должны быть проведены экспериментальные и (или) теоретические исследования в соответствии с разработанным планом проведения исследований IV этапа.  Материалы, описывающие проведение теоретических и (или) экспериментальных исследований должны включать все необходимые сведения для обеспечения возможности воспроизведения результатов проведенных исследований.  Результаты теоретических и (или) экспериментальных исследований должны быть опубликованы в зарубежных журналах или в рекомендованных Президиумом Высшей аттестационной комиссией ведущих рецензируемых научных журналах и (или) изданиях, в которых должны быть опубликованы основные научные результаты диссертации на соискание ученой степени доктора и кандидата наук (далее – Журналы ВАК), с обязательной ссылкой на проведение поисковой научно-исследовательской работы в рамках реализации ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009 – 2013 годы (не менее 1-ой публикации). | 25 ноября  2011 г. |
| **V** | Должны быть проведены экспериментальные и (или) теоретические исследования в соответствии с разработанным планом проведения исследований V этапа.  Материалы, описывающие проведение теоретических и (или) экспериментальных исследований должны включать все необходимые сведения для обеспечения возможности воспроизведения результатов проведенных исследований. | 6 сентября  2012 г. |
| **VI** | Должны быть проведены обобщение и оценка результатов исследований.  Должны быть выработаны рекомендации по возможности использования результатов проведенной поисковой научно-исследовательской работы в реальном секторе экономики.  Должны быть разработаны рекомендации по использованию результатов поисковой научно-исследовательской работы при разработке научно-образовательных курсов.  Основные результаты поисковой научно-исследовательской работы должны быть опубликованы в зарубежных журналах или в журналах ВАК, с обязательной ссылкой на проведение поисковой научно-исследовательской работы в рамках реализации ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009 – 2013 годы (не менее 1-ой публикации). | 26 ноября  2012 г. |

|  |  |
| --- | --- |
| **Раздел 4. Права на объекты интеллектуальной собственности (ОИС), создаваемые в результате выполнения поисковых научно-исследовательских работ (этапов)** | |
| **№ п/п** | **Формулировки требований (наименование ОИС, виды и объемы прав на использование ОИС)** |
| **1** | **2** |
| 1 | В случае создания объекта(ов) интеллектуальной собственности предусмотренного(ых) частью четвертой Гражданского кодекса Российской Федерации в рамках выполнения поисковой научно-исследовательской работы неисключительные имущественные права, а именно: право на воспроизведение; право на распространение; право на импорт; право на публичный показ; право на перевод; право на переработку передаются Заказчику сроком на 5 лет. |
| 2 | Исполнитель обязан передать Заказчику результаты поисковой научно-исследовательской работы, в т.ч. результаты интеллектуальной деятельности, свободные от прав третьих лиц. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Раздел 5. Результат поисковых научно исследовательских работ (этапов). Состав, формы и требования, предъявляемые к отчетной документации, срок предоставления отчетной документации** | | | | |
| **Номер этапа** | **Результат поисковых научно-исследовательских работ (этапов)** | **Состав отчетной документации, предоставляемой Государственному заказчику** | **Общие требования к составу, форме и иные требования к отчетной документации, предоставляемой Государственному заказчику** | **Срок предоставления отчетной документации (не позднее указанной даты)[[2]](#footnote-2)\*** |
| **1** | **2** | **3** | **4** | **5** |
| **I** | Аналитический обзор существующих методов и средств защиты цифровой продукции от несанкционированного копирования, лежащих в их основе принципов и существующих теоретических и экспериментальных результатов. Обоснованный вариант и план проведения экспериментальных и теоретических исследований по построению общей математической модели эффективной защиты тиражируемых цифровых данных от несанкционированного копирования, основанной на методе наборных ключей, циклических кодах и списочных декодерах для циклических кодов, с противодействием коалиционным атакам на ключи.  Анализ существующих схем защиты информации от технической утечки, теоретических и экспериментальных результатов. Обоснование варианта выбора схем защиты от технической утечки, основанных на применении помехоустойчивых кодов, и план проведения экспериментальных и теоретических исследований схем защиты информации от технической утечки.  Анализ существующих методов и теоретических результатов декодирования циклических и алгебро-геометрических кодов, подходов к их программым реализациям. Обоснованный вариант и план проведения экспериментальных и теоретических исследований циклических и алгебро-геометрических кодеков.  Анализ существующих методов и теоретических результатов исследования разрешимости операторных сверточных уравнений и приближенных методов решений операторных уравнений. Обоснованный вариант и план проведения экспериментальных и теоретических исследований методов разрешимости операторных сверточных уравнений и приближенных методов их решений.  Материалы теоретических и (или) экспериментальных исследований (объем не менее 2,0 п.л.), раскрывающие содержание работ по решению поставленных научно-исследовательских задач и обеспечивающие возможность воспроизведения результатов проведенных исследований, включая:  - аналитический обзор;  - обоснованный вариант направления исследований;  - план проведения экспериментальных и (или) теоретических исследований;  - результаты экспериментальных и (или) теоретических исследований и при необходимости патентных исследований. | Научно-технический отчет | Научно-технический отчет о выполнении I этапа Государственного контракта представляется на бумажном носителе формата А4 (2 экз.) и на электронном носителе (CD с файлом в формате Microsoft Word).  В состав отчета входит презентация результатов поисковой научно-исследовательской работы в формате Microsoft PowerPoint.  Отчет содержит результаты поисковой научно-исследовательской работы I этапа Государственного контракта. К отчету прилагается аннотация объемом 3-5 страниц. Отчет оформляется в соответствии с требованиями ГОСТ 7.32-2001.  В состав отчетной документации входит выписка из протокола заседания ученого совета факультета математики, механики и компьютерных наук Южного федерального университета о рассмотрении результатов поисковой научно-исследовательской работы по I этапу. В состав отчетной документации входит отчет о выполнении целевых индикаторов и показателей Программы.  Отчетная документация представляется в Управление научных исследований и инновационных программ Федерального агентства по образованию (г. Москва, ул. Люсиновская, д. 51). | 6 августа  2010 г. |
| **II** | Материалы теоретических исследований, раскрывающие содержание работ по построению классификации различных видов угроз пользователю модели защиты тиражируемых цифровых данных от несанкционированного копирования, основанной на методе наборных ключей, циклических кодах и списочных декодерах циклических кодов, а также по построению методики экспериментального исследования модели защиты.  Усовершенствованный для кодов Габидулина симметричный протокол Стройка-Тилбурга и новая схема защиты информации от полной технической утечки. Модель защиты информации от полной утечки на основе криптосистем Габидулина с ранговыми и F-метриками.  Алгоритм декодирования с ограниченным расстоянием алгебро-геометрических кодов типа кодов Рида-Соломона.  Теоремы о разрешимости парных уравнений дискретной свертки с несуммируемыми ядрами, теоремы о применимости проекционных методов решения парных уравнений дискретной свертки. Развитие локального метода исследования разрешимости сверточных уравнений в парах пространств. Способ использования алгоритма Берлекэмпа-Месси-Сакаты к решению последовательности сверточных уравнений.  Не менее трех статей с изложением полученных результатов в трудах (тезисах докладов) международных или всероссийских конференциях с обязательной ссылкой на проведение поисковой научно-исследовательской работы в рамках реализации ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009 – 2013 годы. Заключение экспертной комиссии по открытому опубликованию.  Материалы теоретических и (или) экспериментальных исследований, раскрывающие содержание работ по решению поставленных научно-исследовательских задач и обеспечивающие возможность воспроизведения результатов проведенных исследований, включая аналитический отчет о проведении теоретических и (или) экспериментальных исследований (объем не менее 2,0 п.л.).  Заключение экспертной комиссии по открытому опубликованию.  Копии не менее 1 статьи, опубликованной в трудах (тезисах докладов) международной или всероссийской конференции с обязательной ссылкой на проведение поисковой научно-исследовательской работы в рамках реализации ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009 – 2013 годы. | Научно-технический отчет | Научно-технический отчет о выполнении II этапа Государственного контракта представляется на бумажном носителе формата А4 (2 экз.) и на электронном носителе (CD с файлом в формате Microsoft Word).  В состав отчета входит презентация результатов поисковой научно-исследовательской работы в формате Microsoft PowerPoint.  Отчет содержит результаты поисковой научно-исследовательской работы II этапа Государственного контракта. К отчету прилагается аннотация объемом 3-5 страниц. Отчет оформляется в соответствии с требованиями ГОСТ 7.32-2001.  В состав отчетной документации входит выписка из протокола заседания ученого совета факультета математики, механики и компьютерных наук Южного федерального университета о рассмотрении результатов поисковой научно-исследовательской работы по II этапу. В состав отчетной документации входит отчет о выполнении целевых индикаторов и показателей Программы.  Отчетная документация представляется в Управление научных исследований и инновационных программ Федерального агентства по образованию (г. Москва, ул. Люсиновская, д. 51). | 26 октября 2010 г. |
| **III** | Материалы теоретических исследований, раскрывающие содержание работ по построению общей математической модели эффективной защиты тиражируемых цифровых данных от несанкционированного копирования, основанной на методе наборных ключей, алгебро-геометрических кодах и списочных декодерах для алгебро-геометрических кодов, с противодействием коалиционным атакам на ключи.  Математическая модель защиты информации в бесшумном канале с перехватом, свойство (λ,δ)-защищенности линейных кодов, результаты о достаточных условиях (λ,δ)-защищенности. Теоретическая и экспериментальная оценки иерархии весов слабоплотных кодов. Модель защиты информации от полной утечки на основе модификации Берштейна классической криптосистемы Мак-Элиса.  Алгоритм списочного декодирования алгебро-геометрических кодов типа кодов Рида-Соломона. Программная модель декодера алгебро-геометрических кодов типа кодов Рида-Соломона с использованием алгоритма Берлекэмпа-Месси-Сакаты.  Теоремы о разрешимости операторов из алгебр, порожденных дискретными свертками. Алгоритмы обращения операторов Теплица, операторов свертки, составных операторов типа Вандермонда, Коши.  Аналитический отчет о проведении теоретических и экспериментальных исследований.  Материалы теоретических и (или) экспериментальных исследований, раскрывающие содержание работ по решению поставленных научно-исследовательских задач и обеспечивающие возможность воспроизведения результатов проведенных исследований, включая аналитический отчет о проведении теоретических и (или) экспериментальных исследований (объем не менее 2,0 п.л.). | Научно-технический отчет | Научно-технический отчет о выполнении III этапа Государственного контракта представляется на бумажном носителе формата А4 (2 экз.) и на электронном носителе (CD с файлом в формате Microsoft Word).  В состав отчета входит презентация результатов поисковой научно-исследовательской работы в формате Microsoft PowerPoint.  Отчет содержит результаты поисковой научно-исследовательской работы III этапа Государственного контракта. К отчету прилагается аннотация объемом 3-5 страниц. Отчет оформляется в соответствии с требованиями ГОСТ 7.32-2001.  В состав отчетной документации входит выписка из протокола заседания ученого совета факультета математики, механики и компьютерных наук Южного федерального университета о рассмотрении результатов поисковой научно-исследовательской работы по III этапу. В состав отчетной документации входит отчет о выполнении целевых индикаторов и показателей Программы.  Отчетная документация представляется в Управление научных исследований и инновационных программ Федерального агентства по образованию (г. Москва, ул. Люсиновская, д. 51) | 5 августа  2011 г. |
| **IV** | Материалы теоретических исследований, раскрывающие содержание работ по построению классификации различных видов угроз пользователю модели защиты тиражируемых цифровых данных от несанкционированного копирования, основанной на методе наборных ключей, алгебро-геометрических кодах и списочных декодерах для алгебро-геометрических кодов и по построению методики экспериментального исследования модели защиты и обеспечивающие возможность воспроизведения результатов проведенных исследований.  Модель защиты информации от полной утечки на основе криптосистем Габидулина с ранговыми и F-метриками. Математическая модель защиты информации в зашумленном канале с перехватом, оценки уровня понимания перехваченной информации для произвольных и МДР-кодов, программная реализация модели на основе применения слабоплотных кодов и кодов Габидулина.  Теоретическое исследование применимости алгоритма списочного декодирования алгебро-геометрических кодов типа кодов Рида-Соломона к построению схем специального широковещательного шифрования, схем защиты от полной технической утечки. Программная модель декодера алгебро-геометрических кодов типа кодов Рида-Соломона с использованием алгоритма Берлекэмпа-Месси-Сакаты.  Теоремы о применении К-теории и топологических методов к исследованию разрешимости алгебр операторов свертки на общих абелевых группах. Экспериментальное исследование алгоритмов обращения операторов Теплица, операторов свертки, составных операторов типа Вандермонда, Коши.  Аналитический отчет о проведении теоретических и экспериментальных исследований.  Не менее трех статей с изложением полученных результатов в журналах ВАК или зарубежных журналах с обязательной ссылкой на проведение поисковой научно-исследовательской работы в рамках реализации ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009 – 2013 годы. Заключение экспертной комиссии по открытому опубликованию.  Материалы теоретических и (или) экспериментальных исследований, раскрывающие содержание работ по решению поставленных научно-исследовательских задач и обеспечивающие возможность воспроизведения результатов проведенных исследований, включая аналитический отчет о проведении теоретических и (или) экспериментальных исследований (объем не менее 2,0 п.л.).  Заключение экспертной комиссии по открытому опубликованию.  Копии не менее 1 статьи, опубликованной в журнале ВАК или зарубежном журнале с обязательной ссылкой на проведение поисковой научно-исследовательской работы в рамках реализации ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009 – 2013 годы. | Научно-технический отчет | Научно-технический отчет о выполнении IV этапа Государственного контракта представляется на бумажном носителе формата А4 (2 экз.) и на электронном носителе (CD с файлом в формате Microsoft Word).  В состав отчета входит презентация результатов поисковой научно-исследовательской работы в формате Microsoft PowerPoint.  Отчет содержит результаты поисковой научно-исследовательской работы IV этапа Государственного контракта. К отчету прилагается аннотация объемом 3-5 страниц. Отчет оформляется в соответствии с требованиями ГОСТ 7.32-2001.  В состав отчетной документации входит выписка из протокола заседания ученого совета факультета математики, механики и компьютерных наук Южного федерального университета о рассмотрении результатов поисковой научно-исследовательской работы по IV этапу. В состав отчетной документации входит отчет о выполнении целевых индикаторов и показателей Программы.  Отчетная документация представляется в Управление научных исследований и инновационных программ Федерального агентства по образованию (г. Москва, ул. Люсиновская, д. 51). | 25 октября 2011 г. |
| **V** | Материалы экспериментальных исследований, раскрывающие содержание работ по исследованию модели эффективной защиты тиражируемых цифровых данных от несанкционированного копирования, основанной на методе наборных ключей, циклических кодах и списочных декодерах для циклических кодов, и по проведению экспериментального исследования модели эффективной защиты тиражируемых цифровых данных от несанкционированного копирования, основанной на методе наборных ключей, алгебро-геометрических кодах и списочных декодерах для алгебро-геометрических кодов, а также результаты теоретических исследований по построению границ применимости модели защиты.  Модель защиты информации от полной утечки на основе криптосистем Мак-Элиса, Нидеррайтера и Сидельникова с использованием асимметричного протокола Бернштейна и списочного декодирования кодов Гоппы.  Универсальный способ защиты информации от полной и частичной технической утечки в зашумленном канале передачи данных. Границы применимости модели защиты на основе кодового зашумления и кодовых криптосистем, основанные на теоретических и экспериментальных исследованиях  Программная модель декодера дивизорных алгебро-геометрических кодов. Экспериментальное исследование применимости программной модели к построению эффективных схем специального широковещательного шифрования и схемы защиты от полной технической утечки.  Формулы для инвариантов пространств фредгольмовых и обратимых операторов и формулы индекса для дискретных операторов свертки и операторов на общих абелевых группах. Схема применения и экспериментальное исследование сдвиговых методов Гохберга-Кайласа-Ольшевского и Финка-Рост к решению систем линейных уравнений с составными матрицами типа Теплица, Вандермонда, Коши.  Аналитический отчет о проведении теоретических и экспериментальных исследований.  Материалы теоретических и (или) экспериментальных исследований, раскрывающие содержание работ по решению поставленных научно-исследовательских задач и обеспечивающие возможность воспроизведения результатов проведенных исследований, включая аналитический отчет о проведении теоретических и (или) экспериментальных исследований (объем не менее 2,0 п.л.). | Научно-технический отчет | Научно-технический отчет о выполнении V этапа Государственного контракта представляется на бумажном носителе формата А4 (2 экз.) и на электронном носителе (CD с файлом в формате Microsoft Word).  В состав отчета входит презентация результатов поисковой научно-исследовательской работы в формате Microsoft PowerPoint.  Отчет содержит результаты поисковой научно-исследовательской работы V этапа Государственного контракта. К отчету прилагается аннотация объемом 3-5 страниц. Отчет оформляется в соответствии с требованиями ГОСТ 7.32-2001.  В состав отчетной документации входит выписка из протокола заседания ученого совета факультета математики, механики и компьютерных наук Южного федерального университета о рассмотрении результатов поисковой научно-исследовательской работы по V этапу. В состав отчетной документации входит отчет о выполнении целевых индикаторов и показателей Программы.  Отчетная документация представляется в Управление научных исследований и инновационных программ Федерального агентства по образованию (г. Москва, ул. Люсиновская, д. 51). | 6 августа  2012 г. |
| **VI** | Материалы теоретических и экспериментальных исследований, раскрывающие содержание работ по решению поставленных в проекте в целом научно-исследовательских задач и обеспечивающие возможность воспроизведения результатов проведенных исследований, включая:  - отчет по обобщению и оценке результатов исследований разработанной в ходе проекта общей математической модели эффективной защиты тиражируемых цифровых данных от несанкционированного копирования, основанной на методе наборных ключей, циклических и алгебро-геометрических кодах дивизорного типа и типа кодов Рида-Соломона, новых разработанных списочных декодерах, с противодействием коалиционным атакам на ключи, и ее программной реализации на основе разработанной библиотеки алгоритмов декодирования, допускающих высокоуровневое распараллеливание вычислений;  - отчет по обобщению и оценке результатов исследований разработанной в ходе проекта модели защиты информации от полной технической утечки на основе новых модифицированных кодовых криптосистем Мак-Элиса, Нидерайтера, Габидулина, Сидельникова и новых модификаций протоколов симметричной и асимметричной криптографии;  - отчет по обобщению и оценке результатов исследований разработанной в ходе проекта модели защиты информации от частичной технической утечки в бесшумных и зашумленных каналах путем применения факторных защитных кодов, построенных на основе слабоплотных кодов и кодов Габидулина;  - новые модели, методы, алгоритмы и программы, позволяющие увеличить объем знаний для более глубокого понимания проблем защиты информации во время ее обработки, хранения и передачи, а также пути применения новых явлений, механизмов и закономерностей;  - рекомендации по применению построенных моделей и оценки возможности использования в реальном секторе экономике (программно-аппартные системы защиты информации, вычислительные сети, системы электронного документооборота, электронной коммерции, цифровой связи);  - рекомендации по использованию результатов поисковой научно-исследовательской работы при подготовке специалистов в области защиты информации, компьютерной безопасности, информационных технологий, прикладной математики.  Не менее трех статей с изложением полученных результатов в журналах ВАК или зарубежных журналах с обязательной ссылкой на проведение поисковой научно-исследовательской работы в рамках реализации ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009 – 2013 годы. Заключение экспертной комиссии по открытому опубликованию.  Материалы теоретических и (или) экспериментальных исследований (объем не менее 2,5 п.л.), раскрывающие содержание работ по решению поставленных научно-исследовательских задач и обеспечивающие возможность воспроизведения результатов проведенных исследований, включая:  - отчет по обобщению и оценке результатов исследований;  - модели, методы, программы и (или) алгоритмы, позволяющие увеличить объем знаний для более глубокого понимания изучаемого предмета исследования и пути применения новых явлений, механизмов или закономерностей;  - рекомендации по возможности использования результатов поисковой научно-исследовательской работы в реальном секторе экономики;  - рекомендации по использованию результатов поисковой научно-исследовательской работы при разработке научно-образовательных курсов.  Заключение экспертной комиссии по открытому опубликованию.  Копии не менее 1 статьи, опубликованной в журнале ВАК или зарубежном журнале с обязательной ссылкой на проведение поисковой научно-исследовательской работы в рамках реализации ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009 – 2013 годы. | Научно-технический отчет | Итоговый научно-технический отчет о выполнении Государственного контракта представляется на бумажном носителе формата А4 (2 экз.) и на электронном носителе (CD с файлом в формате Microsoft Word).  В состав отчета входит презентация результатов поисковой научно-исследовательской работы в формате Microsoft PowerPoint.  Отчет содержит обобщенные результаты поисковой научно-исследовательской работы, полученные на I - V этапах. К отчету прилагается аннотация объемом 3-5 страниц. Отчет оформляется в соответствии с требованиями ГОСТ 7.32-2001.  В состав отчетной документации входит выписка из протокола заседания ученого совета факультета математики, механики и компьютерных наук Южного федерального университета о рассмотрении результатов поисковой научно-исследовательской работы по проекту. В состав отчетной документации входит отчет о выполнении целевых индикаторов и показателей Программы.  Отчетная документация представляется в Управление научных исследований и инновационных программ Федерального агентства по образованию (г. Москва, ул. Люсиновская, д. 51). | 26 октября 2012 г. |

|  |  |
| --- | --- |
| **Раздел 6. Порядок приемки выполненных поисковых научно-исследовательских работ (этапов):** | |
| **Номер этапа** | **Требования к порядку приемки и утверждения выполненных поисковых научно исследовательских работ (этапов)** |
| **1** | **2** |
| 1 | 1. Отчетные материалы по I этапу Государственного контракта принимаются в соответствии с требованиями Государственного контракта.  2. Приемочная комиссия Заказчика оценивает научно-технический уровень исследований, обоснованность предлагаемых решений по реализации и использованию результатов поисковой научно-исследовательской работы по I этапу Государственного контракта.  3. Выполненные работы принимаются Заказчиком по акту сдачи-приемки исполнения обязательств по I этапу Государственного контракта.  4. Заключенный Государственный контракт должен быть зарегистрирован в соответствии с законодательством Российской Федерации о выполнении научно-исследовательских работ. |
| 2 | 1. Отчетные материалы по II этапу Государственного контракта принимаются в соответствии с требованиями Государственного контракта.  2. Приемочная комиссия Заказчика оценивает научно-технический уровень исследований, обоснованность предлагаемых решений по реализации и использованию результатов поисковой научно-исследовательской работы по II этапу Государственного контракта.  3. Выполненные работы принимаются Заказчиком по акту сдачи-приемки исполнения обязательств по II этапу Государственного контракта. |
| 3 | 1. Отчетные материалы по III этапу Государственного контракта принимаются в соответствии с требованиями Государственного контракта.  2. Приемочная комиссия Заказчика оценивает научно-технический уровень исследований, обоснованность предлагаемых решений по реализации и использованию результатов поисковой научно-исследовательской работы по III этапу Государственного контракта.  3. Выполненные работы принимаются Заказчиком по акту сдачи-приемки исполнения обязательств по III этапу Государственного контракта. |
| 4 | 1. Отчетные материалы по IV этапу Государственного контракта принимаются в соответствии с требованиями Государственного контракта.  2. Приемочная комиссия Заказчика оценивает научно-технический уровень исследований, обоснованность предлагаемых решений по реализации и использованию результатов поисковой научно-исследовательской работы по IV этапу Государственного контракта.  3. Выполненные работы принимаются Заказчиком по акту сдачи-приемки исполнения обязательств по IV этапу Государственного контракта. |
| 5 | 1. Отчетные материалы по V этапу Государственного контракта принимаются в соответствии с требованиями Государственного контракта.  2. Приемочная комиссия Заказчика оценивает научно-технический уровень исследований, обоснованность предлагаемых решений по реализации и использованию результатов поисковой научно-исследовательской работы по V этапу Государственного контракта.  3. Выполненные работы принимаются Заказчиком по акту сдачи-приемки исполнения обязательств по V этапу Государственного контракта. |
| 6 | 1. Созданные в результате выполнения Государственного контракта объекты интеллектуальной собственности должны быть зарегистрированы в соответствии с законодательством Российской Федерации об интеллектуальной собственности.  2. Отчетные материалы по Государственному контракту принимаются в соответствии с требованиями Государственного контракта.  3. При приемке Приемочная комиссия Заказчика оценивает научно-технический уровень исследований, обоснованность предлагаемых решений по реализации и использованию результатов поисковой научно-исследовательской работы по Государственному контракту.  4. Выполненные работы принимаются Заказчиком по акту сдачи-приемки исполнения обязательств по Государственному контракту.  5. Результаты работ, полученные при выполнении Государственного контракта, должны быть зарегистрированы в соответствии с законодательством Российской Федерации о выполнении научно-исследовательских работ. |

|  |
| --- |
| **Участник размещения заказа** |
|  |
|  |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_) |

## *ФОРМА 3 ДЕТАЛИЗИРОВАННОЕ ПРЕДЛОЖЕНИЕ О КАЧЕСТВЕ ПОИСКОВЫХ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИХ РАБОТ (Сведения о планируемых работах)*

|  |  |  |  |
| --- | --- | --- | --- |
| **Детализированное Предложение о качестве поисковых научно-исследовательских работ** | | | |
| **Номер этапа** | **Действия Исполнителя при выполнении отдельных поисковых научно-исследовательских работ** | **«Инструментарий, методы, оборудование»** | **Научные результаты** |
| **1** | **2** | **3** | **4** |
| **I** | 1. Изучение существующих методов, теоретических и практических результатов в области построения систем защиты информации от несанкционированного копирования, тиражирования и распространения по реферативным журналам, научной журнальной и монографической литературе, материалам Всероссийских и Международных конференций. Выбор и обоснование оптимального варианта исследований, разработка плана проведения теоретических и экспериментальных исследований. | 1. Реферативные журналы, научные журналы и монографии в библиотеках ЮФУ (г.Ростов, г.Таганрог), МГУ (г.Москва), КГУ (г.Краснодар), материалы Всероссийских и Международных конференций в библиотеках и Интернете. Персональные компьютеры. | Анализ существующих методов и средств защиты цифровой продукции от несанкционированного копирования, лежащих в их основе принципов, построение аналитического обзора, выбор и обоснование оптимального варианта направления исследований, построение плана проведения экспериментальных и теоретических исследований проблемы защиты цифровой продукции от несанкционированного копирования.  Анализ существующих схем защиты информации от технической утечки. Обоснование выбора схем защиты от технической утечки, основанных на применении помехоустойчивых кодов.  Анализ существующих методов и теоретических результатов декодирования циклических и алгебро-геометрических кодов, подходов к их программым реализациям. Обоснованный вариант и план проведения экспериментальных и теоретических исследований циклических и алгебро-геометрических кодеков.  Анализ существующих методов и теоретических результатов исследования разрешимости операторных сверточных уравнений и приближенных методов решений операторных уравнений. Обоснованный вариант и план проведения экспериментальных и теоретических исследований методов разрешимости операторных сверточных уравнений и приближенных методов их решений. |
| 2. Изучение существующих методов, теоретических и практических результатов в области построения систем защиты информации от полной и частичной технической утечки по реферативным журналам, научной журнальной и монографической литературе, материалам Всероссийских и Международных конференций. Выбор и обоснование множества критериев и показателей эффективности методов и средств защиты информации от технической утечки. Сравнение схем защиты на помехоустойчивых кодах с существующими схемами по выбранному множеству показателей. Проведение теоретического и экспериментального исследования эффективности методов защиты информации от технической утечки, основанных на применении помехоустойчивых кодов. Выбор и обоснование оптимального варианта исследований, разработка плана проведения теоретических и экспериментальных исследований. | 2. Реферативные журналы, научные журналы и монографии в библиотеках ЮФУ (г.Ростов, г.Таганрог), МГУ (г.Москва), КГУ (г.Краснодар), материалы Всероссийских и Международных конференций в библиотеках и Интернете. Персональные компьютеры. |
| 3. Изучение существующих методов, теоретических и практических результатов в области современного помехоустойчивого кодирования по реферативным журналам, научной журнальной и монографической литературе, материалам Всероссийских и Международных конференций. Выбор и обоснование оптимального варианта исследований, разработка плана проведения теоретических и экспериментальных исследований. | 3. Реферативные журналы, научные журналы и монографии в библиотеках ЮФУ (г.Ростов, г.Таганрог), МГУ (г.Москва), НМУ (г.Москва), ИППИ РАН (г.Москва), ЯрГУ (г.Ярославль), материалы Всероссийских и Международных конференций в библиотеках и Интернете. Персональные компьютеры. |
| 4. Изучение существующих методов и теоретических результатов исследования разрешимости операторных сверточных уравнений и приближенных методов решений операторных уравнений по реферативным журналам РЖМатематика (Россия), Mathematical Reviews (USA), Zentralblatt MATH (EMS), журнальной и монографической литературе, материалам Всероссийских и Международных конференций. . Выбор и обоснование оптимального варианта исследований, разработка плана проведения теоретических и экспериментальных исследований. | 4. Реферативные журналы РЖМатематика (Россия), Mathematical Reviews (USA), Zentralblatt MATH (EMS) и их электронные версии в Интернете. Журналы и монографии в библиотеках ЮФУ (г.Ростов), МГУ (г.Москва), ВГУ (г.Владимир) и электронные версии журналов и монографий в Интернете. Материалы Всероссийских и Международных конференций в библиотеках и Интернете, участие в конференциях ВЗМШ-10 (г.Воронеж), Международной конференции в г.Суздале. Персональные компьютеры. |
| **II** | 1. Построение классификации различных видов угроз пользователю модели защиты тиражируемых цифровых данных от несанкционированного копирования, основанной на методе наборных ключей, циклических кодах и списочных декодерах циклических кодов, математическая формулировка классификации различных видов угроз пользователю модели защиты, выделение областей компрометаций невиновных. Построение общей математической модели эффективной защиты тиражируемых цифровых данных от несанкционированного копирования, основанной на методе наборных ключей, циклических кодах и списочных декодерах для циклических кодов, с противодействием коалиционным атакам на ключи: построение математической модели распространения данных, включая разработку алгоритмов действий распространителя данных и пользователя, построение математической модели коалиционной атаки, выделение условий на помехоустойчивые коды и декодеры для последующего применения в ССШШ, построение математической модели противодействия коалиционным атакам, включая разработку алгоритма действий контролера, проведение анализа производительности алгоритма противодействия коалиционным атакам. Разработка методики экспериментального исследования модели защиты. | 1. Методы теории помехоустойчивого кодирования, теории вероятности, криптографии, комбинаторики, математическое моделирование схем защиты информации, теоретическое обоснование моделей схем защиты информации. | Математическая модель эффективной защиты тиражируемых цифровых данных от несанкционированного копирования, основанная на методе наборных ключей, циклических кодах и списочных декодерах, с противодействием коалиционным атакам на ключи, включающая математическую модель распространения данных, алгоритмы действий распространителя данных и пользователя, математическую модель коалиционной атаки, математическую модель противодействия коалиционным атакам. Леммы обоснования корректности. Анализ производительности алгоритма противодействия коалиционным атакам. Классификация различных видов угроз пользователю модели защиты. Математическое описание областей компрометаций невиновных пользователей модели защиты. Методика экспериментального исследования модели защиты тиражируемых цифровых данных от несанкционированного копирования, основанной на методе наборных ключей, циклических кодах и списочных декодерах.  Усовершенствованный для кодов Габидулина симметричный протокол Стройка-Тилбурга и новая схема защиты информации от полной технической утечки. Модель защиты информации от полной утечки на основе криптосистем Габидулина с ранговыми и F-метриками.  Алгоритм декодирования с ограниченным расстоянием класса алгебро-геометрических кодов типа кодов Рида-Соломона.  Теоремы о разрешимости парных уравнений дискретной свертки с несуммируемыми ядрами, теоремы о применимости проекционных методов решения парных уравнений дискретной свертки. Развитие локального метода исследования разрешимости сверточных уравнений в парах пространств. Способ использования алгоритма Берлекэмпа-Месси-Сакаты к решению последовательности сверточных уравнений. |
| 2. Изучение эффективности методов криптоанализа симметричных криптосистем на помехоустойчивых кодах. Построение модификации симметричного протокола Стройка-Тилбурга на ранговых кодах Габидулина для защиты информации от полной технической утечки. Исследование стойкости построенного протокола. Построение схем защиты информации на основе модифицированного протокола Стройка-Тилбурга. Построение модификации симметричного протокола Стройка-Тилбурга на кодах Рида-Соломона в F-метрике. | 2. Методы дискретной математики, алгебры и математической статистики, теории криптографических протоколов. |
| 3. Разработка алгоритма декодирования с ограниченным расстоянием класса алгебро-геометрических кодов типа кодов Рида-Соломона, аналогичного алгоритму декодирования Берлекэмпа-Велча класса кодов Рида-Соломона. | 3. Методы теории алгебраических кривых, теории полиномиальных колец, конечных полей, помехоустойчивого кодирования. |
| 4. Построение символического исчисления для парных операторов дискретной свертки с несуммируемыми ядрами и получение условий фредгольмовости, формулы индекса и условий применимости проекционных методов для парных операторов дискретной свертки с несуммируемыми ядрами в терминах построенного символического исчисления. Построение общих моделей локальной теории для операторов в парах пространств, распространение основных результатов локального подхода И.Б.Симоненко на этот случай. Анализ возможности переноса одномерного алгоритма Берлекэмпа-Месси и многомерного алгоритма Берлекэмпа-Месси-Сакаты к решению последовательности сверточных уравнений. Анализ применимости алгоритма Берлекэмпа-Месси-Сакаты к модификации алгоритма декодирования Питерсона-Горенстейна-Цирлера класса алгебро-геометрических кодов типа кодов Рида-Соломона. | 4. Техника преобразования Фурье, техника теплицевых матриц, общий подход Гохберга-Фельдмана. Локальный метод И.Б.Симоненко. Метод Сакаты построения базиса Гребнера. |
| **III** | 1. Построение общей математической модели эффективной защиты тиражируемых цифровых данных от несанкционированного копирования, основанной на методе наборных ключей, алгебро-геометрических кодах и списочных декодерах для алгебро-геометрических кодов, с противодействием коалиционным атакам на ключи: построение математической модели распространения данных, включая разработку алгоритмов действий распространителя данных и пользователя, построение математической модели коалиционной атаки, выделение условий на помехоустойчивые коды и декодеры для последующего применения в ССШШ, построение математической модели противодействия коалиционным атакам, включая разработку алгоритма действий контролера, проведение анализа производительности алгоритма противодействия коалиционным атакам. | 1. Методы теории помехоустойчивого кодирования, криптографии, комбинаторики, математическое моделирование схем защиты информации, теоретическое обоснование моделей схем защиты информации. | Математическая модель эффективной защиты тиражируемых цифровых данных от несанкционированного копирования, основанной на методе наборных ключей, алгебро-геометрических кодах и списочных декодерах для алгебро-геометрических кодов, с противодействием коалиционным атакам на ключи, включающая математическую модель распространения данных, алгоритмы действий распространителя данных и пользователя, математическую модель коалиционной атаки, математическую модель противодействия коалиционным атакам. Леммы обоснования корректности. Анализ производительности алгоритма противодействия коалиционным атакам.  Математическая модель защиты информации в бесшумном канале с перехватом, свойство (λ,δ)-защищенности линейных кодов, Теорема о достаточных условиях (λ,δ)-защищенности. Теоретическая и экспериментальная оценки иерархии весов слабоплотных кодов класса LDPC(2,r); экспериментальная оценка случайных слабоплотных кодов и случайных кодов.  Алгоритмы списочного декодирования алгебро-геометрических кодов типа кодов Рида-Соломона. Программная модель декодера алгебро-геометрических кодов типа кодов Рида-Соломона с использованием алгоритма Берлекэмпа-Месси-Сакаты.  Теоремы о разрешимости операторов из алгебр, порожденных дискретными свертками. Алгоритмы обращения операторов Теплица, операторов свертки, составных операторов типа Вандермонда, Коши. |
| 2. Распространение математической модели защиты информации от технической утечки в бесшумном канале с перехватом второго типа на случай q-ичных каналов. Нахождение достаточных условий (λ,δ)-защищенности. Вычисление (λ,δ)-защищенности для используемых на практике линейных кодов. Теоретическое и экспериментальное оценивание весовой иерархии одного класса слабоплотных кодов класса LDPC(2,r). Экспериментальное оценивание весовой иерархии случайных слабоплотных кодов, общих случайных кодов. | 2. Методы алгебраической теории кодирования, математической статистики и теории информации, методы теории графов. Персональные компьютеры. |
| 3. Разработка алгоритмов списочного декодирования класса алгебро-геометрических кодов типа кодов Рида-Соломона на основе алгоритмов списочного декодирования Судана, Гурусвами-Судана класса кодов Рида-Соломона. Разработка программного пакета, реализующего модифицированный алгоритм Питерсона-Горенстейна-Цирлера декодирования класса алгебро-геометрических кодов типа кодов Рида-Соломона с использованием алгоритма Берлекэмпа-Месси-Сакаты. | 3. Методы теории алгебраических кривых, теории полиномиальных колец, конечных полей, помехоустойчивого кодирования, компьютерной алгебры. Персональные компьютеры |
| 4. Построение символического исчисления для алгебры операторов дискретной свертки с несуммируемыми ядрами и получение условий фредгольмовости, формулы индекса для операторов из алгебр, порожденных дискретными свертками в терминах построенного символического исчисления. Разработка и тестирование алгоритмов обращения операторов Теплица, операторов свертки, составных операторов типа Вандермонда, Коши. | 4. Техника преобразования Фурье, локальный метод И.Б.Симоненко. Метод Финка-Рост, перестановочный метод Гохберга-Кайласа-Ольшевского. |
| **IV** | 1. Построение классификации различных видов угроз пользователю модели защиты тиражируемых цифровых данных от несанкционированного копирования, основанной на методе наборных ключей, алгебро-геометрических кодах и списочных декодерах для алгебро-геометрических кодов, математическая формулировка классификации различных видов угроз пользователю модели защиты, выделение областей компрометаций невиновных пользователей для дальнейшего исследования соотношений различных видов угроз пользователю границ и границ областей компрометации. Разработка методики экспериментального исследования модели защиты. | 1. Методы теории вероятности, теории помехоустойчивого кодирования, комбинаторики. Экспериментальное моделирование на компьютерах с процессорами мощностью 2,5 ГГц и ОЗУ объемом 512 Мб в количестве сорока штук. | Классификация различных видов угроз пользователю модели защиты, математическое описание областей компрометаций невиновных пользователей модели защиты в случае использования алгебро-геометрических кодов. Эесперимечнтальные оценки применимости модели защиты тиражируемых цифровых данных от несанкционированного копирования, основанной на методе наборных ключей, алгебро-геометрических кодах и списочных декодерах.  Модель защиты информации от полной утечки на основе криптосистем Габидулина с ранговыми и F-метриками. Математическая модель защиты информации в зашумленном канале с перехватом, оценки уровня понимания перехваченной информации для произвольных и МДР-кодов. Имитационная программная модель на основе применения слабоплотных кодов и кодов Габидулина.  Теорема об обосновании возможности применения алгоритмов списочного декодирования алгебро-геометрических кодов типа кодов Рида-Соломона к построению схем специального широковещательного шифрования, схем защиты от полной технической утечки. Алгоритм вычисления корней специального вида многочленов нескольких переменных. Модифицированные алгоритмы декодирования класса алгебро-геометрических кодов типа кодов Рида-Соломона. Теорема об обосновании возможности применения метода Берлекэмпа-Месси-Сакаты в алгоритмах декодирования класса одноточечных алгебро-геометрических кодов с целью уменьшения их вычислительной сложности.  Теоремы о достаточных и необходимых условиях разрешимости операторов из сверточных алгебр на общих абелевых группах. Экспериментальное исследование алгоритмов обращения операторов Теплица, операторов свертки, составных операторов типа Вандермонда, Коши. |
| 2. Исследование стойкости модифицированного симметричного протокола Стройка-Тилбурга на кодах Рида-Соломона в F-метрике. Построение обобщенной модели защиты информации от полной технической утечки на основе кодовых симметричных криптосистем с использованием кодов в ранговой и F-метрике. Построение математической модели защиты информации от технической утечки в зашумленном канале с перехватом второго типа. Теоретическое оценивание уровня понимания информации в зашумленном канале перехвата второго типа при использовании метода кодового зашумления. Разработка программного средства, реализующего протокол кодового зашумления в зашумленном канале перехвата второго типа на слабоплотных кодах, кодах Габидулина, случайных кодах. | 2. Методы алгебраической теории кодирования, математической статистики и теории информации, методы теории графов, теории криптографических протоколов. Персональные компьютеры. |
| 3. Теоретическое исследование применимости алгоритма списочного декодирования алгебро-геометрических кодов типа кодов Рида-Соломона к построению схем специального широковещательного шифрования, схем защиты от полной технической утечки. Разработка вычислительно эффективных методов факторизации многочленов нескольких переменных с коэффициентами специального вида с целью повышения эффективности алгоритмов декодирования класса алгебро-геометрических кодов типа кодов Рида-Соломона. Теоретическое исследование применимости метода Берлекэмпа-Месси-Сакаты в алгоритмах декодирования класса одноточечных алгебро-геометрических кодов с целью уменьшения их вычислительной сложности. | 3. Методы теории алгебраических кривых, теории полиномиальных колец, конечных полей, помехоустойчивого кодирования, компьютерной алгебры. Метод Сакаты построения базиса Гребнера. |
| 4. Вычисление К-групп и гомотопических групп для пространств символов алгебр операторов свертки на общих абелевых группах, обоснование необходимых условий фредгольмовости и обратимости сверточных операторов в терминах К-групп и гомотопических групп. Программная реализация алгоритмов обращения операторов Теплица, операторов свертки, составных операторов типа Вандермонда, Коши. | 4. Методы операторной К-теории. Программные пакеты, персональный компьютер. |
| **V** | 1. Проведение экспериментального исследования модели эффективной защиты тиражируемых цифровых данных от несанкционированного копирования, основанной на методе наборных ключей, циклических кодах и списочных декодерах для циклических кодов, с противодействием коалиционным атакам на ключи. Проведение экспериментального исследования модели эффективной защиты тиражируемых цифровых данных от несанкционированного копирования, основанной на методе наборных ключей, алгебро-геометрических кодах и списочных декодерах для алгебро-геометрических кодов, с противодействием коалиционным атакам на ключи. | 1. Методы теории вероятности, комбинаторики, теории помехоустойчивого кодирования. Экспериментальное моделирование на компьютерах с процессорами мощностью 2,5 ГГц и ОЗУ объемом 512 Мб в количестве сорока штук. | Результаты экспериментов и рекомендации по практическому применению схем защиты, основанных на циклических и алгебро-геометрических кодах и списочных декодерах.  Модель защиты информации от полной утечки на основе асимметричных криптосистем Мак-Элиса, Нидеррайтера и Сидельникова с использованием асимметричного протокола Бернштейна и списочного декодирования кодов Гоппы.  Программный пакет декодирования декодирования с ограниченным расстоянием и списочного декодирования класса дивизорных алгебро-геометрических кодов, класса алгебро-геометрических кодов типа кодов Рида-Соломона.  Формулы для инвариантов пространств фредгольмовых и обратимых операторов и формулы индекса для дискретных операторов свертки и операторов на общих абелевых группах. Схема применения и экспериментальное исследование сдвиговых методов Гохберга-Кайласа-Ольшевского и Финка-Рост к решению систем линейных уравнений с составными матрицами типа Теплица, Вандермонда, Коши. |
| 2. Теоретическое исследование асимметричного протокола Бернштейна. Построение модели и схемы реализации модели защиты информации от полной утечки в каналах передачи данных на основе кодовых асимметричных криптосистем Мак-Элиса, Нидеррайтера и Сидельникова с использованием асимметричного протокола Бернштейна и списочного декодирования кодов Гоппы. | 2. Методы теории алгоритмов на решетках, теории криптографических протоколов. |
| 3. Разработка программного пакета, реализующего алгоритмы декодирования с ограниченным расстоянием и списочного декодирования класса дивизорных алгебро-геометрических кодов, класса алгебро-геометрических кодов типа кодов Рида-Соломона. | 3. Программные пакеты, персональный компьютер. |
| 4. Вычисление формул для инвариантов пространств фредгольмовых и обратимых операторов в терминах К-функтора, вычисление формулы индекса для дискретных операторов свертки, вычисление формулы индекса для операторов на общих абелевых группах. Исследование применимости сдвиговых методов Гохберга-Кайласа-Ольшевского и Финка-Рост к решению систем линейных уравнений с составными матрицами типа Теплица, Вандермонда, Коши; разработка алгоритмов и их программная реализация. | 4. Методы операторной К-теории. Программные пакеты, персональный компьютер. |
| **VI** | 1. Построение границ применимости модели эффективной защиты тиражируемых цифровых данных от несанкционированного копирования, основанной на методе наборных ключей, циклических и алгебро-геометрических кодах и списочных декодерах, с противодействием коалиционным атакам на ключи. Разработка отчета по обобщению и оценке результатов исследований модели защиты от несанкционированного тиражирования. | 1. Имитационное компьютерное моделирование. | Универсальный метод защиты информации от полной и частичной технической утечки в зашумленном канале передачи данных.  Границы применимости способа защиты на основе кодового зашумления и кодовых криптосистем, основанные на теоретических и экспериментальных исследованиях  Материалы теоретических и экспериментальных исследований, раскрывающие содержание работ по решению поставленных в проекте в целом научно-исследовательских задач и обеспечивающие возможность воспроизведения результатов проведенных исследований, включая:  - отчет по обобщению и оценке результатов исследований разработанной в ходе проекта общей математической модели эффективной защиты тиражируемых цифровых данных от несанкционированного копирования, основанной на методе наборных ключей, циклических и алгебро-геометрических кодах дивизорного типа и типа кодов Рида-Соломона, новых разработанных списочных декодерах, с противодействием коалиционным атакам на ключи, и ее программной реализации на основе разработанной библиотеки алгоритмов декодирования, допускающих высокоуровневое распараллеливание вычислений;  - отчет по обобщению и оценке результатов исследований разработанной в ходе проекта универсального способа защиты информации от полной и частичной технической утечки на основе новых модифицированных кодовых криптосистем Мак-Элиса, Нидерайтера, Габидулина, Сидельникова и новых модификаций протоколов симметричной и асимметричной криптографии;  - новые модели, методы, алгоритмы и программы, позволяющие увеличить объем знаний для более глубокого понимания проблем защиты информации во время ее обработки, хранения и передачи, а также пути применения новых явлений, механизмов и закономерностей;  - рекомендации по применению построенных моделей и оценки возможности использования в реальном секторе экономике (программно-аппартные системы защиты информации, вычислительные сети, системы электронного документооборота, электронной коммерции, цифровой связи);  - рекомендации по использованию результатов поисковой научно-исследовательской работы при подготовке специалистов в области защиты информации, компьютерной безопасности, информационных технологий, прикладной математики. |
| 2. Исследование стойкости метода кодового зашумления в случае получения перехватчиком ненулевой информации из части перехваченных данных. Определение границ применимости кодового зашумления и кодовых криптосистем в зависимости от параметров применяемых кодов. Разработка методики выбора схемы защиты на основе параметров линейных кодов, уровня перехвата и уровня помех. Разработка универсального способа защиты информации от полной и частичной технической утечки в зашумленном канале передачи данных, построение компьютерной модели и проведение экспериментальных исследований. | 2. Имитационное компьютерное моделирование. |
| 1. Построение схемы реализации метода защиты информации от полной и частичной технической утечки на основе применения кодового зашумления и кодовых симметричных и асимметричных криптосистем. | 1. Методы дискретной математики |
| 2. | 2. Методы дискретной математики, алгебры и математической статистики |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
| 1. | 1. |
| 2. | 2. |
| 3. | 3. |
| …. | …. |
|  |  |

Участник размещения заказа может представить в составе Заявки на участие в Конкурсе Приложение №1 к Форме №3, содержащее обоснование предложенного(-ых) «Инструментария, методов, оборудования»:

|  |  |  |
| --- | --- | --- |
| **Приложение №1 к Форме №3** | | |
| **Наименование каждого (-ых) предложенного(-ых) Участником размещения заказа «Инструментария, методов, оборудования»** | **Обоснование соответствия предложенного(-ых) «Инструментария, методов, оборудования» проблеме исследования и требованиям Конкурсной документации** | **Обоснование прогнозируемого повышения качества выполнения поисковых научно-исследовательских работ (этапов), предложенных Участником размещения заказа, в результате использования «Инструментария, методов, оборудования»** |
| *Должны быть перечислены все предложенные Участником размещения заказа «Инструментарии, методы, оборудование»* |  |  |

Участник размещения заказа может представить в составе Заявки на участие в Конкурсе Приложение №2 к Форме №3:

|  |  |
| --- | --- |
| **Приложение №2 к Форме №3** | |
| *Аннотация поисковых научно-исследовательских работ, включающая обоснование актуальности и научной значимости исследуемой проблемы ( не более 3-х страниц)* |  |
| *Коды по классификатору ГРНТИ* |  |
| *Ключевые слова (не более 15)* |  |

|  |
| --- |
| **Участник размещения заказа** |
|  |
|  |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_) |

## 

## *ФОРМА 4 ПРЕДЛОЖЕНИЕ О ЦЕНЕ ГОСУДАРСТВЕННОГО КОНТРАКТА*

«\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_»

*(наименование Участника размещения заказа)*

|  |  |  |  |
| --- | --- | --- | --- |
| **Предложение о цене Государственного контракта** | | | |
| **№ этапа** | **Наименование работ (этапа)** | | |
| **1** | **2** | | |
| **I** | Проведение I этапа исследований. | | |
| Итого стоимость (цена) поисковых научно-исследовательских работ по I этапу в 2010 году составляет: \_\_\_\_\_\_\_\_\_\_\_\_ рублей \_\_\_\_ коп. (сумма прописью), НДС не облагается на основании п.п. 16 п. 3 ст. 149 Налогового кодекса Российской Федерации. | | | |
| **II** | Проведение II этапа исследований. | | |
| Итого стоимость (цена) поисковых научно-исследовательских работ по II этапу в 2010 году составляет: \_\_\_\_\_\_\_\_\_\_\_\_ рублей \_\_\_\_ коп. (сумма прописью), НДС не облагается на основании п.п. 16 п. 3 ст. 149 Налогового кодекса Российской Федерации. | | | |
| **III** | | Проведение III этапа исследований. | |
| Итого стоимость (цена) поисковых научно-исследовательских работ по III этапу в 2011 году составляет: \_\_\_\_\_\_\_\_\_\_\_\_ рублей \_\_\_\_ коп. (сумма прописью), НДС не облагается на основании п.п. 16 п. 3 ст. 149 Налогового кодекса Российской Федерации. | | | |
| **IV** | | Проведение IV этапа исследований. | |
| Итого стоимость (цена) поисковых научно-исследовательских работ по IV этапу в 2011 году составляет: \_\_\_\_\_\_\_\_\_\_\_\_ рублей \_\_\_\_ коп. (сумма прописью), НДС не облагается на основании п.п. 16 п. 3 ст. 149 Налогового кодекса Российской Федерации. | | | |
| **V** | | Проведение V этапа исследований. | |
| Итого стоимость (цена) поисковых научно-исследовательских работ по V этапу в 2012 году составляет: \_\_\_\_\_\_\_\_\_\_\_\_ рублей \_\_\_\_ коп. (сумма прописью), НДС не облагается на основании п.п. 16 п. 3 ст. 149 Налогового кодекса Российской Федерации. | | | |
| **VI** | | | Проведение VI этапа исследований. |
| Итого стоимость (цена) поисковых научно-исследовательских работ по VI этапу в 2012 году составляет: \_\_\_\_\_\_\_\_\_\_\_\_ рублей \_\_\_\_ коп. (сумма прописью), НДС не облагается на основании п.п. 16 п. 3 ст. 149 Налогового кодекса Российской Федерации. | | | |

**Итого стоимость (цена) поисковых научно-исследовательских работ составляет: \_\_\_\_\_\_\_\_\_\_\_\_ рублей \_\_\_\_ коп. ( \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ рублей \_\_\_\_ коп.), НДС не облагается на основании п.п. 16 п. 3 ст. 149 Налогового кодекса Российской Федерации.**

|  |
| --- |
| **Участник размещения заказа** |
|  |
|  |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_) |

1. \* Под «Датой окончания этапа (этапов) выполнения работ (оказания услуг)» понимается дата регистрации Сторонами по Государственному контракту Акта сдачи-приемки исполнения обязательств по Государственному контракту (этапу государственного контракта) [↑](#footnote-ref-1)
2. \* Отчетная документация предоставляется Исполнителем не позднее, чем за 30 (тридцать) дней до окончания выполнения поисковых научно-исследовательских работ (этапа) по Государственному контракту. [↑](#footnote-ref-2)