Запрос на внешние инновации

|  |  |  |
| --- | --- | --- |
|  | Организация, ХК | АО «Концерн «Автоматика» |
|  | Наименование ЗВИ,Обобщенное краткое наименование задачи | Построение алгоритмов и программ для многопроцессорного вычислителя для решения больших разреженных систем над конечным полем – важного этапа решения задач дискретного логарифмирования и целой факторизации.Решение задачи вскрытия криптопротоколов на основе задачи дискретного логарифмирования и факторизации для небольших параметров, использовавшихся более 20 лет назад.  |
| 1. 2
 | Описание ситуации: ЦЕЛЬ, НАДСИСТЕМА,Проблема верхнего уровня, для решения которой ставится настоящая задача *(может быть несколько уровней иерархии целей)* | Необходимо построить программный комплекс для работы на суперкомпьютере, 1. Задача использования многопроцессорной техники включена в перечень перспективных направлений развития науки РФ. 2. Трудность состоит в том, что для эффективного использования кластеров, построенных во многом за рубежом, требуются глубокие знания по внедренным в них технологиям вычислений.3. Получены свидетельства о государственной регистрации прав на ПО, реализующие новые алгоритмы, полученные членами трудового коллектива.4. Эта работа позволит приблизить практическую криптографию к современным эффективным средствам вычислений. |
|  | Постановка задачи, кто, что и над чем должен сделать(Субъект – действие – объект) | Разработки алгоритмов вскрытия криптографических протоколов на основе дискретного логарифмирования и факторизации при помощи решения больших разреженных систем линейных уравнений над конечными полями. |
|  | Объект (устройства, система, техпроцесс) | Зашифрованные при помощи задачи дискретного логарифмирования и задачи факторизации сообщения противника. |
|  | Его функция | позволяют вскрывать сообщения, зашифрованные на старых ключах и создавать новые параметры безопасности |
|  | Значения ключевых характеристик, которые требуется достичьДля проблемной ситуации укажите какова ее первопричина и в чем состоит «неразрешимый конфликт (противоречие) в требованиях.Допускается ли компромисс (оптимизация) | Поставить мировой рекорд целой факторизации. |
|  | Уровень ключевых характеристик мирового лидера | В 2018 году французами разложено на множители число RSA из 250 десятичных знаков. |
|  |  |  |