

Облікова картка ДіР



I. Загальні відомості

Державний обліковий номер: 0213U002641

Державний реєстраційний номер: 0112U004169

Особливі позначки: відкрита

Дата реєстрації: 01-02-2013

II. Етап виконання ДіР

Номер етапу: 1

Назва етапу: Розробка математичного та програмного ґрид-орієнтованого забезпечення для моделювання та прикладних досліджень в галузях механіки, ідентифікації нанопористих матеріалів, біометрії та криптоаналізу

Початок етапу: 03.2012

Закінчення етапу: 12.2012

Вид звітнього документа: Остаточний звіт

III. Відомості про виконавця ДіР

Повне найменування юридичної особи (або ПІБ фізичної особи): Інститут кібернетики ім. В. М. Глушкова НАНУ

Код за ЄДРПОУ: 05417176

Місцезнаходження:

Форма власності:

Сфера управління: Національна академія наук України

Ідентифікатор ROR: Не застосовується

Розмір організації:

Телефон: (044) 526-20-08 , (044) 526-74-18

IV. Відомості про співвиконавців ДіР

Повне найменування юридичної особи (або ПІБ фізичної особи): Тернопільський національний технічний університет імені Івана Пулюя

Код за ЄДРПОУ: 05408102

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Розмір організації:

Телефон:

Внесок співвиконавця у звітний етап:

V. Відомості про замовника ДіР

Повне найменування юридичної особи (або ПІБ фізичної особи): Національна академія наук України

Код за ЄДРПОУ: 00019270

Місцезнаходження: вул. Володимирська, 54, м. Київ, Київська обл., 01030, Україна

Форма власності:

Сфера управління: Національна академія наук України

Ідентифікатор ROR: Не застосовується

Розмір організації:

Телефон: 380442396594

VI. Джерела, напрями та обсяги фінансування ДіР

Підстава для проведення ДіР: 34 - договір (замовлення) з центральним органом виконавчої влади, академією наук (головними розпорядниками бюджетних коштів на проведення НДДКР)

Напрямок фінансування: 2.3 - виконання робіт за державними цільовими програмами

Джерела фінансування

7713 - кошти держбюджету

Код програмної класифікації видатків і кредитування (КПКВК): 6541030

Фактичний обсяг фінансування (тис. грн.): 84

VII. Відомості про ДіР

Назва роботи українською:

Розробка математичного та програмного ґрид-орієнтованого забезпечення для моделювання та прикладних досліджень в галузях механіки, ідентифікації нанопористих матеріалів, біометрії та криптоаналізу

Назва роботи англійською:

Development of grid-oriented software for simulation and applied research in fields of mechanic, identification of nanoporous materials, biometry and cryptoanalysis

Реферат українською:

Розроблено та програмно реалізовано програмне забезпечення багатоваріантного моделювання процесів теплопровідності, орієнтоване на розподілені обчислення (архітектура програмного комплексу, формати файлів вхідних та вихідних даних; схема зберігання даних розв'язуваної задачі в оперативній пам'яті). Розроблено ґрид-орієнтоване математичне та програмне забезпечення, що реалізує метод "сендвіч-атаки" на алгоритм Kasumi, алгебраїчний криптоаналіз та метод повного перебору. Розроблено спеціалізований лабораторний практикум по застосуванню ґрид-технологій в межах курсів "Паралельні та розподілені обчислення" та "Системне програмне забезпечення" для студентів напряму 6.050102 – Комп'ютерна інженерія, а також для магістрів спеціальності 8.05010201– Комп'ютерні системи та мережі в межах курсу "Інформаційні системи паралельної та розподіленої обробки даних" ТНТУ. Підготовано до друку навчальний посібник з курсу "Паралельні та розподілені обчислення".

Реферат англійською:

The distributed computing oriented software for multivariant simulation of heat-transfer processes (architecture of software, formats of input and output files, scheme of storage of processing problem data in RAM) was developed and implemented. A grid-oriented software that implements the method of "sandwich attack" on algorithm Kasumi, algebraic cryptanalysis method and exhaustive search are designed and implemented. A specialized laboratory workshop on application of Grid technology for courses "Parallel and distributed computing" and "System software" for students in 6.050102 – Computer Engineering, as well as masters in 8.05010201–Computer systems and networks within the course "Information systems in parallel and distributed computing" in TNTU was developed. A handbook devoted to "Parallel and distributed computing" was prepared for publishing.

Індекс УДК: 519.713;519.711:53, 519.713; 519.711:53; 53.072; 53:004;

Коди тематичних рубрик: 28.17.23

Керівники роботи

Власне Прізвище Ім'я По-батькові: Дейнека Василь Степанович

Науковий ступінь:

Вчене звання:

Ідентифікатор ORCID ID:

Додаткова інформація:

VIII. Наукова (науково-технічна) продукція (НТП)

Назва НТП українською: Математичне та програмне грід-орієнтоване забезпечення для моделювання та прикладних досліджень в галузях теплофізики та криптоаналізу.

Назва НТП англійською: The grid-oriented software for simulation and applied investigations in fields of thermal physics and cryptanalysis.

НТП, яку передбачалося створити:

Причини, через які НТП не було створено:

Отримані результати:

Галузь застосування: 74.20.1 Діяльність у сфері інжинірингу

Реєстраційний номер картки технології:

Опис НТП: Математичну основу створеного програмного забезпечення складають моделі усталеної теплопровідності, обчислювальні алгоритми їх дискретизації. Програмна реалізація розроблених алгоритмів виконана у вигляді спеціалізованих підсистем грід-орієнтованого програмного забезпечення багатоваріантного моделювання просторових процесів в багатокомпонентних середовищах. Створене криптоаналітичне грід-орієнтоване математичне та програмне забезпечення реалізує метод "сендвіч-атаки" на алгоритм Kasumi, алгебраїчний криптоаналіз та метод повного перебору.

Соціально-економічна спрямованість НТП:

Вплив НТП на довкілля:

Впровадження НТП: Не впроваджено

Практична реалізація НТП

Початок етапу: 2013-2015

Закінчення етапу:

Споживачі продукції: дослідницькі та проектні організації, користувачі Українського національного гріду

Перспективні ринки: Україна

Характер співробітництва з інвестором

Потрібний обсяг інвестицій, тис. грн.:

Права, що надаються інвестору після завершення роботи:

Наявність бізнес-плану:

Техніко-економічне обґрунтування:

Потенціальний обсяг продажу, тис. грн.:

Очікуваний термін окупності (років):

Додаткова інформація:

IX. Бібліографічний опис

Сергиенко И.В., Дейнека В.С. Оптимальное управление эллиптической системой и идентификация ее параметров при наблюдениях за производными решениями // Проблемы управления и информатики. - 2012. - №5. - С.80-101. Сергиенко И.В., Дейнека В.С. Численное решение некоторых обратных задач нестационарной теплопроводности с использованием псевдообратных матриц // Кибернетики и системный анализ. - 2012. - №5. - С.49-70. Дейнека В.С. Системний аналіз багатокomпонентних розподілених систем // Матеріали II-ї науково-технічної конференції "Обчислювальні методи і системи перетворення інформації", присвяченої пам'яті Б.О.Попова, Львів, 4-5 жовтня 2012. - Львів, 2012. - С.70-72. Дейнека В.С. Білоус М.В. Побудова моделі ґрунтового масиву чернігівського регіону в програмному комплексі НАДРА-3D // Матеріали II-ї науково-технічної конференції "Обчислювальні методи і системи перетворення інформації", присвяченої пам'яті Б.О.Попова, Львів, 4-5 жовтня 2012. - Львів, 2012. - С.70-72. Лупенко С. Підвищення ефективності криптоаналізу сучасних поточкових шифрів мереж передачі даних / О. Кравець, С. Лупенко, А. Луцків // Матеріали I-ї міжнародної науково-технічної конференції "Захист інформації і безпека інформаційних систем", Львів, 31 травня-01 червня 2012. - Львів, 2012. - С.132-133. Лупенко С. Криптоаналітична віртуальна лабораторія у грид-середовищі / С. Лупенко, А. Луцків // Праці міжнародної конференції "Кластерні обчислення", Київ, 12 червня-14 червня 2012. - Київ, 2012. - С.40-43. Луцків А. Особливості викладання спеціалізованих курсів з інформаційної безпеки / А.Луцків // Матеріали I-ї науково-методичної конференції ТНТУ імені Івана Пулюя "Актуальні питання організації навчання іноземних громадян у технічних вищих навчальних закладах України", Тернопіль, 26-28 квітня 2012. - Тернопіль : ТНТУ, 2012. - [Електронний ресурс]. - Режим доступу: URL: http://www.nalabs.te.ua/publications/conf/lutskev_thesis_inoz_stud_2012.pdf - Назва з екрану. Висоцький В. Криптографічний захист смарт-карт / В.Висоцький, С.Лупенко, А.Луцків // Системний аналіз. Інформатика. Управління (САІУ-2012): матеріали III Міжнародної науково-практичної конференції (м. Запоріжжя, 14-16 березня 2012 року) / Міністерство освіти і науки України, Запорізька обласна державна адміністрація, Академія наук вищої школи України, Класичний приватний університет. - Запоріжжя: КПУ, 2012. - С.51-53. Луцків А.М. Дослідження криптостійкості алгоритму UEA1 мереж передачі даних стандарту UMTS / Ю. Кондрацький, А.Луцків // Матеріали другої науково-технічної конференції "Інформаційні моделі, системи та технології", Тернопіль, 25 квітня 2012. - Тернопіль : ТНТУ, 2012. - С. 33. Луцків А. Підвищення якості викладання спеціалізованих курсів технологій векторних, паралельних та розподілених обчислень / А.Луцків // Міжнародна науково-практична конференція "Актуальні питання теорії та практики неперервної ступеневої підготовки фахівців в системі вищої освіти", Тернопіль, 13-14 листопада 2012. - Тернопіль : ТНТУ, 2012. - С.247-249. Поліщук Г.В. Програмно-апаратні засоби високопродуктивних обчислювальних систем для задач біометрії / Г.В. Поліщук, С.А. Лупенко, А.М. Луцків // Науковий вісник національного лісотехнічного університету України : збірник науково-технічних праць. - Львів : РВВ НЛТУ України. - 2012. - Вип. 22.9. - С.352-359.

