Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0407U004568

Особливі позначки: відкрита

Дата реєстрації: 19-11-2007

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Кінах Ярослав Ігорович
2. Kinakh Iaroslav Igorovych

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: кандидат наук

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 05.13.13

Назва наукової спеціальності: Обчислювальні машини, системи та мережі

Галузь / галузі знань: Не застосовується

Освітньо-наукова програма зі спеціальності: Не застосовується

Дата захисту: 25-10-2007

Спеціальність за освітою: 7.080101

Місце роботи здобувача: Тернопільський національний економічний університет

Код за ЄДРПОУ: 33680120

Місцезнаходження: 46020, м. Тернопіль, вул. Львівська, 11

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): К 58.082.02

Повне найменування юридичної особи: Чортківський коледж економіки та підприємництва Тернопільського національного економічного університету

Код за ЄДРПОУ: 37417766

Місцезнаходження: вул. Степана Бандери 46, м. Чортків, Чортківський р-н., Тернопільська обл., 46009, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

IV. Відомості про підприємство, установу, організацію, в якій було виконано дисертацію

Повне найменування юридичної особи: Тернопільський національний економічний університет

Код за ЄДРПОУ: 33680120

Місцезнаходження: 46020, м. Тернопіль, вул. Львівська, 11

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 50.39.19

Тема дисертації:

1. Методи паралельних обчислень та обґрунтування рівня криптографічного захисту інформації в комп'ютерних мережах

2. Methods of parallel calculations and ground of level of cryptographic defence of information are in computer networks

Реферат/анотація:

1. Об'єкт дослідження - комп'ютерні мережі для криптоаналізу асиметричних систем шифрування інформації на основі використання алгоритму Загального решета числового поля (ЗРЧП); мета дослідження - підвищення захисту комп'ютерних мереж на основі обґрунтування рівня криптографічного захисту та удосконалення методів паралельних обчислень у комп'ютерних мережах шляхом криптоаналізу на основі розподілених обчислень; методи та апаратура - аналітичні, експериментальні; теоретичні та практичні результати - розроблено методи та засоби, які забезпечують підвищення ефективності процесу криптоаналізу асиметричних алгоритмів за рахунок зменшення часу на пошук закритих ключів; новизна - вперше отримав подальший розвиток паралельний метод криптоаналізу системи шифрування інформації

RSA, за рахунок вибору спеціального поліному алгоритму ЗРЧП, що дозволяє зменшити загальну кількість групових операцій на етапах просіювання та обробки розрідженої матриці великої розмірності; удосконалено математичну модель роботи паралельного алгоритму криптоаналізу, завдяки чому точніше визначається стійкість асиметричних систем шифрування інформації в комп'ютерних мережах, а також сформульовано правила оптимізації для розподілених обчислень, що дозволяє підвищити рівень продуктивності запропонованої обчислювальної системи. Результати роботи впроваджено в ВАТ Тернопільський радіозавод "Оріон". Рекомендується використання результатів у сфері захисту інформації комп'ютерних мереж.

2. A research object is the computer networks are for cryptoanalysis of the asymmetric systems of enciphering of information on the basis of the use of algorithm of Number field sieve (NFS) method; the aim investigation - the increase of defence of computer networks on the basis of base level of cryptographic defence and improvement of methods of parallel calculations in computer networks by kryptoanaysis on the basis of the distributed calculations; methods and equipments are analytical, experimental; results theoretical and practical - methods and tools which assure the increase of efficiency of testing process of the computer systems and their constituents due to reduction of time on the finding of the secret keys; novelty - first the parallel method of kryptoanalysis of the system of enciphering of information of RSA got subsequent development, due to the choice of the special a polynomial algorithm of the NFS method, that allows lowed common amount of operations of groups on the stages of sifting and treatment of matrix of largeness. Results used at Ternopil radiofactory "Orion". Drawing on results is recommended in the field of defence of information of computer networks.

Державний реєстраційний номер ДіР:

Пріоритетний напрям розвитку науки і техніки:

Стратегічний пріоритетний напрям інноваційної діяльності:

Підсумки дослідження:

Публікації:

Наукова (науково-технічна) продукція:

Соціально-економічна спрямованість:

Охоронні документи на ОПІВ:

Впровадження результатів дисертації:

Зв'язок з науковими темами:

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Карпінський Микола Петрович

2. Karpinsky Mykola Petrovych

Кваліфікація: д.т.н., 05.11.05

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Петров Олександр Степанович
2. Петров Олександр Степанович

Кваліфікація: д.т.н., 05.22.07

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Власне Прізвище Ім'я По-батькові:

1. Петришин Любомир Богданович
2. Петришин Любомир Богданович

Кваліфікація: д.т.н., 05.13.08

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Рецензенти

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради	Саченко Анатолій Олексійович
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Саченко Анатолій Олексійович
Відповідальний за підготовку облікових документів	
Реєстратор	
Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності	Юрченко Т.А.