Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0401U000239

Особливі позначки: відкрита

Дата реєстрації: 24-01-2001

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Яремчук Юрій Євгенович
2. Yaremchuk Yurij Yevgenovych

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: кандидат наук

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 05.13.21

Назва наукової спеціальності: Системи захисту інформації

Галузь / галузі знань: Не застосовується

Освітньо-наукова програма зі спеціальності: Не застосовується

Дата захисту: 28-12-2000

Спеціальність за освітою: 8.0804

Місце роботи здобувача: Вінницький державний технічний університет

Код за ЄДРПОУ: 02070693

Місцезнаходження: 21021, м. Вінниця, вул. Хмельницьке шосе, 95

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): Д 26.185.01

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

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

Повне найменування юридичної особи: Вінницький державний технічний університет

Код за ЄДРПОУ: 02070693

Місцезнаходження: 21021, м. Вінниця, вул. Хмельницьке шосе, 95

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 50.37.23

Тема дисертації:

1. Методи та засоби шифрування інформації на основі рекурентних послідовностей

2. Information encryption methods and tools on the recurrent sequences basis

Реферат:

1. Об'єкт дослідження: криптографічний захист інформації від несанкціонованого користувача. Мета дослідження: прискорення шифрування інформації на основі рекурентних послідовностей з використанням програмно-апаратних засобів. Методи дослідження і апаратура: теоретичні, аналітичні, комп'ютерне моделювання, ПЕОМ. Теоретичні і практичні результати: запропоновано нові рекурентні послідовності (Vk - та Uk - послідовності) та встановлено їх властивості. Запропоновано методи шифрування інформації на основі Vk - та Uk -послідовностей, які є модифікаціями відомих методів Ель-Гамаля та Шаміра і забезпечують при певних умовах меншу складність обчислень, ніж ці методи. Запропоновано принципи побудови спеціалізованих процесорів для шифрування інформації за модифікованими методами, розроблено алгоритми для обчислення елементів Vk - послідовностей, які дозволяють прискорити обчислення для великих значень індексу елементів, розроблено алгоритми шифрування інформації за модифікованими методами, які прискорюють шифрування інформації в порівнянні з відомими методами. Розроблено пакет програм та структури спеціалізованих процесорів для шифрування інформації за

модифікованими методами. Новітність нововпроваджуваного: підтверджується пріоритетними публікаціями. Новітність результатів встановлена експертами та доведена шляхом порівняння з відповідними аналогами. Ступінь впровадження: у межах підприємств, які займаються серійним випуском програмних та апаратних засобів захисту інформації. Сфера використання: телекомунікації, зокрема біржові та банківські.

2. Object of research - cryptographic protection of information from illegal users; purpose of research - speeding up of information encryption on the basis of recurrent sequences with the use of soft and hardware; methods of research and devices - theoretical and analytical methods, computer simulation, personal computers; theoretical and practical outcomes - there have been suggested new recurrent sequences (Vk- and Uk-sequences) and determined their features; there has been suggested the methods of information encryption on Vk- Uk-sequences basis; these sequences are the modifications of well-known El-Gamal and Shamir methods; at the certain conditions they provide less computational complexity than the above methods; the principles of construction of the processors for information encryption by modified methods have been presented; there has been developed the Vk-sequence elements computation algorithms which allow to speed up the computation for large values of the element indexes; the has been devel oped the algorithms for information encryption in according with modified methods which allow to speed up the information encryption in comparison with known methods; there has been developed the software and the specific processors structures for information encryption in according with modified methods; novelty of the invention is confirmed by priority publications, novelty of the outcomes is established by the experts and proved by means of comparison with analogues; extent of introduction - within the enterprises producing hardware and software of information encryption; field of application - telecommunications, in particular stock-exchange and banking telecommunications

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. Лужецький Володимир Андрійович

2. Лужецький Володимир Андрійович

Кваліфікація: к.т.н., 05.13.05

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. Тарасенко Володимир Петрович
2. Тарасенко Володимир Петрович

Кваліфікація: д.т.н., 05.13.05

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. Корченко Олександр Григорович
2. Корченко Олександр Григорович

Кваліфікація: к.т.н., 05.13.13

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	Євдокимов Віктор Федорович
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Євдокимов Віктор Федорович
Відповідальний за підготовку облікових документів	
Реєстратор	
Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності	Юрченко Т.А.