Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0413U005956

Особливі позначки: відкрита

Дата реєстрації: 07-11-2013

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Білецький Олександр Анатолійович
2. Biletskyi Oleksandr

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: кандидат наук

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 21.05.01

Назва наукової спеціальності: Інформаційна безпека держави

Галузь / галузі знань: Не застосовується

Освітньо-наукова програма зі спеціальності: Не застосовується

Дата захисту: 24-10-2013

Спеціальність за освітою: 7.160103

Місце роботи здобувача: Національний авіаційний університет

Код за ЄДРПОУ: 01132330

Місцезнаходження: 03058,Україна,м.Київ,Просп.Космонавта Комарова,1

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 26.062.17

Повне найменування юридичної особи: Національний авіаційний університет

Код за ЄДРПОУ: 01132330

Місцезнаходження: пр. Космонавта Комарова 1, м. Київ, Київська обл., 03058, 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: Національний авіаційний університет

Код за ЄДРПОУ: 01132330

Місцезнаходження: 03058,Україна,м.Київ,Просп.Космонавта Комарова,1

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 81.14.11.05

Тема дисертації:

1. Методи побудови симетричних алгоритмів криптографічного захисту інформації з динамічно керованими примітивами

2. Methods of symmetric information security cryptographic algorithms creation with dynamic controlled primitives

Реферат/анотація:

1. У дисертаційній роботі розв'язано актуальне наукове завдання щодо розробки методів побудови симетричних криптографічних алгоритмів з параметрами шифрування, які динамічно змінюються, та матричного протоколу розподілу ключів для підвищення ефективності захисту інформаційних ресурсів. В роботі запропоновано новий клас симетричних блочних алгоритмів шифрування, названий сімейством RSB (Round-Step-Block) алгоритмів. Відмінна риса RSB алгоритмів шифрування полягає в тому, що в них використовується новий криптографічний примітив типу "ковзного кодування", який забезпечує не лише глибоке перемішування відкритого тексту, але й бере участь у формуванні блочних раундових ключів для чергових блоків, що шифруються. Отже, всі перетворення, які виконуються алгоритмом, стають залежними не лише від секретного ключа, але і від даних, що шифруються, і, тим самим, набувають властивість керованих криптоперетворень. Основу побудови примітивів "ковзного кодування" складає сукупність

класичних (лівосторонніх) і правосторонніх кодів Грея "навпаки". Перетворення "навпаки" означає, що пряме "ковзне кодування" є не що інше, як відповідне зворотне перетворення Грея, тоді як зворотне "ковзне кодування" являє собою пряме перетворення Грея. Завдяки примітиву "ковзного кодування" шифр RSB забезпечує приємне відбілювання вхідного тексту за два раунди криптографічного перетворення, коли в той же час відомі шифри, наприклад, AES, ГОСТ та ін. - за чотири і більше раундів, що надає можливість зменшити в RSB шифрах загальну кількість раундів шифрування і, тим самим, збільшити швідкість криптографічних перетворень. Удосконалено метод шифрування в класичних SP-мережах за рахунок використання примітиву стохастичного циклічного зсуву даних, що призвело до побудови нових поточних SPS шифраторів. Крім того, на основі узагальнених матриць Галуа і Фібоначчі, а також їх сполучених варіантів, розроблено протокол формування секретних ключів шифрування абонентами мережі з відкритими каналами зв'язку, який в порівнянні з відомими протоколами Діффі-Хеллмана, Ероша-Скуратова та ін. захищений від атаки "людина посередині".

2. This dissertation work has solved actual scientific problem of development symmetrical cryptographic algorithms with dynamic parameters and matrix based protocol of key distribution. In this work we've proposed a new class of symmetrical block algorithm named RSB (Round, Step, Block). The distinctive feature of RSB is so called "sliding coding" operation, which brings great permutation of open text as well as participates in round key generation algorithm. Because of that, all cryptographic operations parameters became dependent not only on secret key but on content of open text. "Sliding coding" operation is based on common Grey's transformations, in so called "otherwise" form. The "othewise" form means that forward "slide coding" is backward Grey's coding and otherwise. Through primitive of "slide coding" the RSB gives good statistical charectistics of cryto text already with 2 rounds of cryptographic transformations, in the same time known algorithms AES, GOST gives same result for 4 and more rounds. We have improved classical SP-transformation with operation of stochastic shift, which gives ability to create new types of SPS generators. Besides of that, based on Galois and Fibonachi generic matricies, we've developed algorithms of session keys generators. Despite of know algorithms Diffie-Hellman and Erosha-Skuratova, proposed algorithm is protected from "man in the middle" attack.

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. Бойко Іван Федорович

2. Boiko Ivan

Кваліфікація: д.т.н., 05.13.14

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. Лужецький Володимир Андрійович
2. Лужецький Володимир Андрійович

Кваліфікація: д.т.н., 01.05.02, 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. Рудницький Володимир Миколайович
2. Рудницький Володимир Миколайович

Кваліфікація: д.т.н., 05.13.06

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

