

# Облікова картка дисертації

## I. Загальні відомості

Державний обліковий номер: 0498U001238

Особливі позначки: відкрита

Дата реєстрації: 25-06-1998

Статус: Захищена

Реквізити наказу МОН / наказу закладу:



## II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Холоша Александр Александрович

2. Холоша Александр Александрович

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: dashboard/okd.okd\_type\_names.0

Аспірантура/Докторантура: ні

Шифр наукової спеціальності: 01.05.03

Назва наукової спеціальності: Математичне та програмне забезпечення обчислювальних машин і систем

Галузь / галузі знань: Не застосовується

Освітньо-наукова програма зі спеціальності: Не застосовується

Дата захисту: 04-06-1998

Спеціальність за освітою: 0102

Місце роботи здобувача: в/ч Е-6642

Код за ЄДРПОУ: 200001941

Місцезнаходження:

Форма власності:

Сфера управління:

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:** Інститут проблем моделювання в енергетиці НАН України

**Код за ЄДРПОУ:** 05516949

**Місцезнаходження:** 252680, г. Київ-164, ул. Ген. Наумова, 15

**Форма власності:**

**Сфера управління:** НАН України

**Ідентифікатор ROR:** Не застосовується

### **V. Відомості про дисертацію**

**Мова дисертації:**

**Коди тематичних рубрик:** 27.47.15

**Тема дисертації:**

1. Методи и средства анализа качества некоторых алгоритмов криптографической защиты
- 2.

**Реферат:**

1. Объект исследования: Криптографические алгоритмы. Цель исследования: Развитие теории и методов анализа качества криптографических алгоритмов; разработка универсальных узлов для генераторов псевдослучайных чисел. Методы исследования и аппаратура: Методы алгебры логики, теории булевых функций, теории чисел и математической статистики; линейная алгебра и теория вероятностей. Теоретические результаты и новизна: Предложен метод анализа качества блока подстановки битовых векторов; исследован отдельный класс линейных регистров сдвига с неравномерным движением. Практические результаты и новизна: Разработан алгоритм и программный комплекс генерации долговременных ключей для алгоритма ГОСТ 28147-89. Предмет и степень внедрения: Комплекс внедрен в Национальном банке Украины. Эффективность внедрения: Метод дает возможность генерировать стойкие долговременные ключи для алгоритма ГОСТ 28147-89. Сфера (область) использования: Информационные технологии, системы защиты информации.

2.

**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. Евдокимов В.Ф.

2. Евдокимов В.Ф.

**Кваліфікація:** д.т.н., 01.05.02, 1

**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. Коростиль Ю.М.

2. Коростиль Ю.М.

**Кваліфікація:** д.т.н., 05.13.13, 1

**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 А.Г.

2. Корченко А.Г.

**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**

Евдокимов В.Ф.

**Власне Прізвище Ім'я По-батькові  
головуючого на засіданні**

Евдокимов В.Ф.

**Відповідальний за підготовку  
облікових документів**

**Реєстратор**

**Керівник відділу УкрІНТЕІ, що є  
відповідальним за реєстрацію наукової  
діяльності**



Юрченко Т.А.