Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0515U000364

Особливі позначки: відкрита

Дата реєстрації: 21-05-2015

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Скобелєв Володимир Володимирович
2. Skobelev Volodimir Volodimirovich

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: доктор наук

Аспірантура/Докторантура: ні

Шифр наукової спеціальності: 01.05.01

Назва наукової спеціальності: Теоретичні основи інформатики та кібернетики

Галузь / галузі знань: Не застосовується

Освітньо-наукова програма зі спеціальності: Не застосовується

Дата захисту: 14-05-2015

Спеціальність за освітою: 8.04020101

Місце роботи здобувача: Інститут кібернетики ім. В.М.Глушкова НАН України

Код за ЄДРПОУ: 05417176

Місцезнаходження: 03680,МСП,м.Київ-187,пр.Академіка Глушкова, 40

Форма власності:

Сфера управління: Національна академія наук України

Ідентифікатор ROR: Не застосовується

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): Д 26.001.09

Повне найменування юридичної особи: Київський національний університет імені Тараса Шевченка

Код за ЄДРПОУ: 02070944

Місцезнаходження: вул. Володимирська, 60, м. Київ, Київська обл., 01033, 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: Київський національний університет імені Тараса Шевченка

Код за ЄДРПОУ: 02070944

Місцезнаходження: 01033, м. Київ, вул. Володимирська, 64

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 27.17.33

Тема дисертації:

1. Розробка і дослідження методів аналізу автоматних моделей, визначених на алгебраїчних структурах.

2. Elaboration and investigation of methods of analysis of automata models defined on algebraic structures.

Реферат/анотація:

1. Метою дисертаційної роботи є розробка математичного апарату для дескриптивного, алгоритмічного та метричного аналізу сімей автоматів, які представлено системами рекурентних співвідношень на алгебраїчних структурах над скінченним кільцем з позиції їх потенційного використання у процесі розв'язання задач захисту інформації. Розро-блено математичний апарат для дослідження систем рівнянь та нерівностей над скінченним кільцем, а саме: метод аналізу статистичної еквівалентності відображень від багатьох змінних скінченної множини у себе, схему представлення у неявному вигляді множини розв'язків системи алгебраїчних рівнянь з параметрами, схему вирішувача для перевірки виконуваності формул лінійної арифметики.

2. The thesis is devoted to elaboration of mathematical tools intended for de-scriptive, algorithmic and metric analysis of families of automata presented via systems of recurrent relations on algebraic structures over a finite

ring under supposition of their potential application for resolving problems of information protection. There are elaborated mathematical tools intended for investigation of systems of equations and disequalities over a finite ring, namely: the method for analysis of statistical equivalence of multy-variable mappings of a finite set into itself, the scheme for presentation of the set of solutions of algebraic equations with parameters in implicit form, the scheme of a solver for checking satisfya-bility of formulae of linear arithmetic. The problem of design of imitational model for a family of automata presented via systems of recurrent relations over a finite ring is resolved, and the class of asymptotically exact imitational models is extracted. It is investigated computational security of families of hash-functions, realized by strongly-connected automata without output function presented via systems of recurrent relations over a finite ring. It is investigated families of automata over a finite associative-commutative ring, which transition and output functions are algebraic sum of a function of the state of automaton and a function of an input symbol, under condition that the value of every component of transition function is some element of fixed ideals of the ring. It is investigated families of automata presented over a finite ring via systems of recurrent relations over varieties with algebra, as well as over parameterized varieties with some extracted set of trajectories. Families of automata presented via systems of recurrent relations on elliptic curve over a finite field are investigated. The results obtained in this thesis can be used in development of software intended for re-solving problems of transformation and protection of information.

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. Летичевський Олександр Адольфович
2. Letichevskiy Aleksandr Adol'fovich

Кваліфікація: д.ф.-м.н., 01.05.01

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. Глазунов Микола Михайлович
2. Глазунов Микола Михайлович

Кваліфікація: д.ф.-м.н., 01.05.01

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. Бедратюк Леонід Петрович
2. Бедратюк Леонід Петрович

Кваліфікація: д.ф.-м.н., 01.01.06

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. Савчук Михайло Миколайович
2. Савчук Михайло Миколайович

Кваліфікація: д.ф.-м.н., 01.05.01

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 Анісімов Анатолій Васильович

Власне Прізвище Ім'я По-батькові головуючого на засіданні Анісімов Анатолій Васильович

Відповідальний за підготовку облікових документів

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності Юрченко Т.А.