Додаток 1
Форма відомостей про авторів матеріалу та описова інформація для видань ТНТУ

Авторська довідка

(реферату дипломної роботи магістра)

Назва дипломної роботи магістра: Методи формування псевдовипадкових чисел в криптографічних засобах захисту банківських інформаційних систем
назви записувати нижнім регістром (як у реченні)

Назва (англ.): Methods of Pseudorandom Numbers Generation in Cryptographic Security Means of Bank Information Systems
переклад англійською

Освітній ступінь : магістр

Шифр та назва спеціальності: 125 «Кіберберпека»

Екзаменаційна комісія: Екзаменаційна комісія №38
напр.: Екзаменаційна комісія №1

Установа захисту: Тернопільський національний технічний університет імені Івана Пулюя
напр.: Тернопільський національний технічний університет імені Івана Пулюя

Дата захисту: 23 грудня 2021 року **Місто:** Тернопіль

Сторінки:
Кількість сторінок дипломної роботи: 109 Кількість сторінок реферату: 1

УДК: УДК 004.421.5

Автор дипломної роботи
Прізвище, ім'я, по батькові (укр.): Баняс Богдан Миронович
розкривати ініціали

Прізвище, ім'я (англ.): Bohdan Banias
використовувати паспортну транслітерацію (КМУ 2010)

Місце навчання (установа, факультет, місто, країна): ТНТУ ім. І. Пулюя, Факультет комп'ютерно-інформаційних систем і програмної інженерії, Кафедра кібербезпеки, м.Тернопіль, Україна

Керівник
Прізвище, ім'я, по батькові (укр.): Александер Марек Богуслав Антонович
повністю

Прізвище, ім'я (англ.): Aleksander Marek Bohuslav Antonovych
використовувати паспортну транслітерацію (КМУ 2010)

Місце праці (установа, підрозділ, місто, країна): ТНТУ ім. І. Пулюя, Факультет комп'ютерно-інформаційних систем і програмної інженерії, Кафедра кібербезпеки, м.Тернопіль, Україна

Вчене звання, науковий ступінь, посада: доктор технічних наук, професор кафедри КБ

Рецензент
Прізвище, ім'я, по батькові (укр.): Дуда Олексій Михайлович
повністю

Прізвище, ім'я (англ.): Duda Oleksiy
використовувати паспортну транслітерацію (КМУ 2010)

Місце праці (установа, підрозділ, місто, країна): ТНТУ, Факультет комп'ютерно-інформаційних систем і програмної інженерії, Кафедра комп'ютерних наук м.Тернопіль, Україна

Вчене звання, науковий ступінь, посада: кандидат технічних наук, доцент кафедри КН

Ключові слова

українською: ГЕНЕРАТОР ПСЕВДОВИПАДКОВИХ ЧИСЕЛ, НАДЛИШКОВІ КОДИ,ДЕКОДУВАННЯ ВИПАДКОВОГО КОДУ, СТАТИСТИЧНА БЕЗПЕКА

до 10 слів

англійською: PSEUDORANDOM NUMBER GENERATOR, SURPLUSES CODES, DECODING INCIDENTAL CODE, STATISTICAL SECURITY

до 10 слів

Анотація

українською:

Об'єктом дослідження є процес формування псевдовипадкових чисел в криптографічних засобах захисту банківських інформаційних систем.

Предметом дослідження є метод формування псевдовипадкових чисел на основі надлишкових блокових кодів в криптографічних засобах захисту банківських інформаційних систем.

Метою роботи є підвищення стійкості криптографічних засобів захисту банківських інформаційних систем на основі використання методів формування псевдовипадкових чисел.

Методами розробки обрано: при аналізі методів і алгоритмів генерації псевдовипадкових чисел використані методи теорії захисту інформації. При дослідженні статистичної безпеки та оцінці швидкодії генерації псевдовипадкових чисел на основі надлишкових блокових кодів використані методи математичної статистики.

В результаті роботи проведено аналіз сучасних методів формування псевдовипадкових чисел, розглянуто вдосконалений метод формування псевдовипадкових чисел на основі на основі надлишкових блокових кодів, проведено дослідження статистичної безпеки розглянутого генератора та приведені можливі варіанти його практичного використання

англійською:

The object of the research is the process of generating random numbers of cryptographic protection of bank information systems.

The research object is the method of generating random numbers based on block codes in excess of cryptographic protection of bank information systems.

The purpose of work is to improve the stability of cryptographic protection of bank information systems through the use of methods of generating random numbers.

As the development method were chosen: the analysis methods and algorithms to generate random numbers used methods of the theory of information security. A study of statistical assessment of safety and performance generation of random numbers based on redundant block codes used methods of mathematical statistics.

The result of work are the analysis of modern methods of generating random numbers, is considered an improved method of forming the basis of random numbers based on redundant block codes, a study of statistical safety reporting generator and given options for its practical use.

Бібліографічний опис:

1. Баняс Б. Методи формування псевдовипадкових чисел в криптографічних засобах захисту банківських інформаційних систем [Текст] / Баняс Б. Матеріали IX науково-технічної конференції Тернопільського національного технічного університету імені Івана Пулюя «Інформаційні моделі, системи та технології» – Тернопіль (8 – 9 грудня 2021 р.), ТНТУ, 2021. – с.25