Авторська довідка

(кваліфікаційної роботи бакалавра)

Назва кваліфікаційної роботи бакалавра *Дослідження сучасних методів блочного симетричного шифрування інформації в автоматизованих банківських системах*
назви записувати нижнім регістром (як у реченні)

Назва (англ.): *Study of modern methods of information block symmetrical encryption in automated bank systems*
переклад англійською

Освітній ступінь : бакалавр

Шифр та назва спеціальності: 125 «Кібербезпека»
напр.:151 Автоматизація та комп'ютерно-інтегровані технології

Екзаменаційна комісія: Екзаменаційна комісія № 37
напр.: Екзаменаційна комісія №1

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

Дата захисту: 17 червня 2021 року **Місто:** Тернопіль

Сторінки:
Кількість сторінок роботи: 101

УДК: 004.056

Автор роботи
Прізвище, ім'я, по батькові (укр.): Коробка Назар Петрович
розкривати ініціали

Прізвище, ім'я (англ.): Korobka Nazar Petrovych
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.): Стадник Марія Андріївна
повністю

Прізвище, ім'я (англ.): Stadnyk Mariia Andriivna
використовувати паспортну транслітерацію (КМУ 2010)

Місце праці (установа, підрозділ, місто, країна): ТНТУ ім. І. Пулюя, Україна

Вчене звання, науковий ступінь, посада: кандидат технічних наук, старший викладач кафедри кібербезпеки

Рецензент
Прізвище, ім'я, по батькові (укр.): Скоренький Юрій Любомирович
повністю

Прізвище, ім'я (англ.): Skorenkyi Yurii Liubomyrovych
використовувати паспортну транслітерацію (КМУ 2010)

Місце праці (установа, підрозділ, місто, країна): ТНТУ ім. І. Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра фізики, м.Тернопіль, Україна
Вчене звання, науковий ступінь, посада: доцент, кандидат фізико-математичних наук, зав. кафедри ФЗ

Ключові слова
українською конфіденційність, внутрішньо-платіжна банківська система, загрози, атаки, криптопримітиви, методи блочного симетричного шифрування, математична модель
до 10 слів

англійською confidentiality, the inner-payment banking system, threats, attacks, kriptoprimitivi, methods of sectional symmetric enciphering, the mathematical model *до 10 слів*

Анотація

українською:

Кваліфікаційна робота присвячена аналізу методів блочного симетричного шифрування в автоматизованих банківських системах і підвищення криптографічної стійкості алгоритмів блочного симетричного перетворення інформації на підґрунті динамічно керованих криптографічних примітивів

Розроблено динамічно керованих блоків нелінійних замін, дослідження їх криптографічних властивостей виконані з використанням математичного апарату булевих функцій, методів кореляційного і спектрального аналізу. Розроблено алгоритму блочного симетричного криптографічного перетворення інформації з динамічно керованими примітивами і дослідження криптографічної стійкості проведені з використанням методів теорії захисту інформації. Досліджено криптостійкість алгоритму проведено з використанням теорії імовірності та математичної статистики, теорії захисту інформації.

англійською:

The qualification thesis is devoted to analysis of methods of the block symmetric enciphering in computer-aided bank systems and an increase of cryptographic firmness of algorithms of sectional symmetric transformation of information on the basis of the dynamically guided cryptographic primitives.

Development of the dynamically guided blocks of nonlinear replacements, research of their cryptographic properties executed with the use of mathematical vehicle of boolean functions, methods of cross-correlation and spectral analysis is conducted. Development of algorithm of block symmetric cryptographic transformation of information with the dynamically guided primitives and research of cryptographic firmness is conducted with the use of the methods of the theory of information security. Criptofirmness of algorithm is researched with the use of probability theory and mathematical statistics, the theory of information security.