Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0418U002918

Особливі позначки: відкрита

Дата реєстрації: 19-07-2018

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Лімарь Ігор Валерійович

2. Limar Igor Valerievich

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: кандидат наук

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 05.13.21

Назва наукової спеціальності: Системи захисту інформації

Галузь / галузі знань: Не застосовується

Освітньо-наукова програма зі спеціальності: Не застосовується

Дата захисту: 04-07-2018

Спеціальність за освітою: інженер-механік

Місце роботи здобувача: Інженерно-технологічний інститут "Біотехніка" Національної академії аграрних наук України

Код за ЄДРПОУ: 00495929

Місцезнаходження: Маяцька дорога, 26, смт. Хліободарське, Біляївський р-н., Одеська обл., 67667, Україна

Форма власності:

Сфера управління: Національна академія аграрних наук України

Ідентифікатор ROR: Не застосовується

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): Д 41.816.02

Повне найменування юридичної особи: Одеська національна академія зв'язку ім. О.С. Попова

Код за ЄДРПОУ: 01180116

Місцезнаходження: Кузнечна вулиця, 1, м. Одеса, Одеська обл., 65000, 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: Одеська національна академія зв'язку ім. О.С. Попова

Код за ЄДРПОУ: 01180116

Місцезнаходження: Кузнечна вулиця, 1, м. Одеса, Одеська обл., 65000, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 50.37.23

Тема дисертації:

1. Криптографічний захист системи електронного голосування з використанням протоколів квантової криптографії

2. The cryptographic protection of the electronic voting system with using of quantum cryptography protocols

Реферат/анотація:

1. Об’єкт дослідження - процес захисту інформації у системі електронного голосування засобами квантової криптографії. Предмет дослідження - методи та способи підвищення безпечності криптографічного захисту систем електронного голосування з використанням засобів квантової криптографії.Методи дослідження. Дослідження проводилися з використанням математичних методів нерелятивістської квантової механіки, квантової теорії інформації, квантової криптографії, математичних методів: методи лінійної алгебри та інші, методів класичної криптографії: гамування, оборотні перетворювання. Теоритичні та практичні результати: вперше розроблено новий протокол квантового розділення секрету з використанням кубітів, який може бути реалізований на сучасній технологічній базі; на відміну від раніш створених аналогів протокол не потребує використання великих обсягів квантової пам’яті; вперше розроблено новий протокол квантового розділення секрету з використанням кутритів, який забезпечує підвищену інформаційну місткість у порівнянні зі схемами на основі кубітів; цей протокол орієнтований на перспективну технологічну базу; на відміну від

раніш відомих також не потребує використання великих обсягів квантової пам'яті; вперше розроблено протокол криптографічного захисту системи електронного голосування із спільним використанням протоколів квантового бітового зобов'язання та квантового розділення секрету, який відрізняється від відомих схем захисту систем електронного голосування використанням примітиву квантового бітового зобов'язання, що забезпечує приховування інформації до закінчення голосування без можливості зміни її виборцем та стійкість протоколу до атак із застосуванням квантових алгоритмів; удосконалено класифікацію атак на квантові криптосистеми, яка на відміну від раніш створених враховує деякі відносно нові види атак, головним чином ті, що відносяться до квантового хакінгу; отримав подальшій розвиток метод захисту від витоку конфіденційних даних протоколів квантової криптографії, що ґрунтується на множенні блоків даних на трійкові випадкові оборотні матриці і відрізняється від відомих відсутністю необхідності використання ключів шифрування, використанням трійкових матриць замість двійкових та виразом для розрахунку довжини блоку; отримав подальшій розвиток метод захисту від витоку конфіденційних даних протоколів квантової криптографії, що ґрунтується на трійковому гамуванні блоків даних і відрізняється від відомих відсутністю необхідності використання ключів шифрування, використанням трійкових гам замість двійкових та виразом для розрахунку довжини блоку.

2. The object of research is the process of information security in the electronic voting system by means of quantum cryptography. Subject of research - methods and ways of increasing the safety of cryptographic protection of electronic voting systems using quantum cryptography techniques. Methods of research. The research was carried out using mathematical methods of non-relativistic quantum mechanics, quantum information theory, quantum cryptography, mathematical methods: methods of linear algebra and others, methods of classical cryptography: gamma, reversible transformations. Theoretical and practical results: for the first time a new protocol of quantum secret sharing using qubits was developed, which can be implemented on a modern technological basis; Unlike earlier analogues, the protocol does not require the use of large volumes of quantum memory; For the first time a new protocol of quantum secret sharing using qutrits was developed, which provides increased information capacity compared to schemes based on qubits; this protocol is oriented on a promising technological base; unlike the earlier known also does not require the use of large volumes of quantum memory; the protocol for cryptographic protection of the electronic voting system was developed for the first time with the common use of quantum bit commitment protocol and quantum secret sharing protocol, which differs from known circuits for protecting electronic voting systems using of a quantum bit commitment primitive, which ensures that information is concealed till the end of voting without the possibility of changing it by voter and stability protocol for attacks using quantum algorithms; the classification of attacks on a quantum cryptosystem is improved, which, unlike the earlier ones, takes into account some relatively new types of attacks, mainly those relating to quantum hacking; received a further development of a method of protection against the leakage of confidential data of quantum cryptography protocols based on the multiplication of data blocks on triple random inverse matrices and differs from the known absence of the need to use encryption keys, using triple matrices instead of binary and expressions for calculating the length of a block; received a further development of a method of protection against the leakage of confidential data of quantum cryptography protocols based on triple gamma data blocks and differs from the known lack of need to use encryption keys, using triple gamut instead of binary and expression to calculate block length.

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. Василіу Євген Вікторович

2. Vasiliu Yevhen Viktorovich

Кваліфікація: д. т. н., 05.13.21

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. Гнатюк Сергій Олександрович

2. Gnatyuk Sergiy

Кваліфікація: д. т. н., 05.13.21

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. Горбенко Іван Дмитрович

2. Gorbenko Ivan Dmytrovych

Кваліфікація: д. т. н., 20.02.12

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 Захарченко Микола Васильович

Власне Прізвище Ім'я По-батькові головуючого на засіданні Захарченко Микола Васильович

Відповідальний за підготовку облікових документів

Реєстратор

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