# Облікова картка дисертації

## I. Загальні відомості

**Державний обліковий номер:** 0412U005039

**Особливі позначки:** відкрита

**Дата реєстрації:** 25-06-2012

**Статус:** Захищена

**Реквізити наказу МОН / наказу закладу:**

## II. Відомості про здобувача

**Власне Прізвище Ім'я По-батькові:**

1. Мамедов Рахман Салман огли
2. Mammadov Rahman

**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:** 01-06-2012

**Спеціальність за освітою:** 7.07010601

**Місце роботи здобувача:**

**Код за ЄДРПОУ:**

**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 41.816.01

**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., 65029, 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:** 65029, м.Одеса, вул.Кузнечна,1

**Форма власності:**

**Сфера управління:** Державний комітет зв"язку та інформатизації України

**Ідентифікатор ROR:** Не застосовується

## V. Відомості про дисертацію

**Мова дисертації:**

**Коди тематичних рубрик:** 50.37.23

**Тема дисертації:**

1. Аналіз стійкості до атак протоколів квантової криптографії

2. The security analysis against attacks of protocols of quantum cryptography

**Реферат:**

1. Об'єкт - процеси передавання інформації квантовими каналами зв'язку й процеси перехоплення інформації у квантовому каналі. Предмет - протоколи квантового розподілення секретних ключів і квантового прямого безпечного зв'язку. Мета - вдосконалення квантових методів захисту інформації шляхом розробки нових протоколів квантового прямого безпечного зв'язку з підвищеною інформаційною місткістю, аналізу їх стійкості до атак, визначення найкращих протоколів за критеріями стійкості та інформаційної місткості в групах подібних протоколів квантової криптографії. Методи дослідження: математичні методи квантової механіки, квантової та класичної теорії інформації, методи процедурного програмування, чисельного експерименту та інтерпретації результатів експерименту. Теоретичні та практичні результати: 1. Вперше розроблено методи квантового кодування інформації та методи контролю підслуховування для трьох нових пінг-понг протоколів між двома користувачами й трьох нових протоколів виду "двоє до одного" з переплутаними чотирикубітними "омега"-, W- і "хі"-станами. 2. Вперше побудовано математичні моделі атаки пасивного перехоплення з використанням допоміжних квантових систем на розроблені пінг-понг

протоколи. Отримано вирази для кількості інформації, що може перехопити зловмисник, у залежності від параметрів протоколів та ймовірності виявити атаку при однократному контролі підслуховування. 3. Проаналізовано атаку "перехоплення - повторної посилки" кубітів на розроблені пінг-понг протоколи. Показано, що така атака можлива тільки на протокол з чотирикубітними W-станами й не можлива на протоколи з чотирикубітними "омега"- і "хі"-станами. 4. Виконано порівняльний аналіз стійкості, інформаційної місткості й завадостійкості різних пінг-понг протоколів, як розроблених у дисертаційній роботі, так і запропонованих іншими авторами. Показано, що за цими критеріями найкращими серед пінг-понг протоколів з чотирикубітними переплутаними станами є протоколи з "омега"- і "хі"-станами. 5. Удосконалено методи аналізу стійкості до різних некогерентних атак трьох класів квантових протоколів розподілення ключів з багатовимірними квантовими системами - кудитами. Двома взаємодоповнюючими методами проведене порівняльне дослідження стійкості до некогерентних атак, а також інформаційної місткості цих трьох класів протоколів. Показано, що за критеріями стійкості до некогерентних атак та інформаційної місткості найкращими є протоколи типу "приготування - вимірювання" з використанням двох взаємно незміщених базисів. Результати роботи впроваджуються в навчальний процес Навчального центру Міністерства зв'язку та інформаційних технологій Азербайджанської Республіки.

2. The object is information transfer processes by quantum communication channels and processes of interception of the information in the quantum channel. The subject is protocols of quantum keys distribution and protocols of quantum secure direct communication. The purpose is development of new protocols of quantum secure direct communication with increased information capacity, the analysis of their security to attacks, and also finding of the best protocols by criteria of security and information capacity in groups of similar protocols of quantum cryptography. Research methods: mathematical methods of quantum mechanics, the quantum and classical theory of the information, procedural programming methods, numerical experiment. Theoretical and practical results: 1. For the first time methods of quantum coding of the information and methods of the eavesdropping control are developed for three new ping-pong protocols of quantum secure direct communication between two users and three new protocols of a kind "two to one" with entangled four-qubit "omega"-, W- and "chi"-states. 2. For the first time mathematical models of eavesdropping attacks with use of auxiliary quantum systems on the developed ping-pong protocols are constructed. Expressions for quantity of the information which the eavesdropper can intercept, depending on protocol parameters and probability to detect attack at unitary control of eavesdropping are obtained. 3. The "intercept-resend" attack on the developed ping-pong protocols is analysed. It is shown that such attack is possible only on the protocol with four-qubit W-states, also such attack is not possible on protocols with four-qubit "omega"- and "chi"-states. 4. The comparative analysis of security, information capacity and a noise immunity of various ping-pong protocols, both developed in thesis, and offered by other authors is made. It is shown, what on these criteria the best among ping-pong protocols with the four-qubit entangled states are protocols with "omega"- and "chi"-states. 5. Methods of the analysis of security to various non-coherent attacks of three classes of quantum key distribution protocols with multidimensional quantum systems (qudits) are improved. Two methods comparative analysis of the security to non-coherent attacks, and also information capacity of these three classes of protocols is made. It is shown that under criteria of the security to non-coherent attacks and information capacity the best are the protocols of "preparation - measurement" kind using two mutually unbiased bases. Results of work are introducing into educational process of the educational centre of the Ministry of Communications and Information Technologies of the Republic Azerbaijan.

**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:** к.ф.-м.н., 01.04.02

**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. Рудницький Володимир Миколайович

2. Рудницький Володимир Миколайович

**Кваліфікація:** д.т.н., 05.13.06

**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. Корченко Олександр Григорович
2. Корченко Олександр Григорович

**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

**Рецензенти**

## VIII. Заключні відомості

| | |
|---|---|
| **Власне Прізвище Ім'я По-батькові голови ради** | Воробієнко Петро Петрович |
| **Власне Прізвище Ім'я По-батькові головуючого на засіданні** | Воробієнко Петро Петрович |
| **Відповідальний за підготовку облікових документів** | |
| **Реєстратор** | |
| **Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності** | Юрченко Т.А. |