# Облікова картка ДіР

## I. Загальні відомості

**Державний обліковий номер:** 0222U000150

**Державний реєстраційний номер:** 0121U113832

**Особливі позначки:** відкрита

**Дата реєстрації:** 03-01-2022

## II. Етап виконання ДіР

**Номер етапу:** 1

**Назва етапу:** Розроблення математичного та алгоритмічного забезпечення стеку протоколів квантового розподілення ключів; аналіз атак на квантові системи розподілення ключів по оптичному волокну.

**Початок етапу:** 11.2021

**Закінчення етапу:** 12.2021

**Вид звітного документа:** Остаточний звіт

## III. Відомості про виконавця ДіР

**Повне найменування юридичної особи (або ПІБ фізичної особи):** Державний університет інтелектуальних технологій і зв'язку

**Код за ЄДРПОУ:** 43997335

**Місцезнаходження:** вул. Кузнечна, буд. 1, м. Одеса, Одеська обл., 65029, Україна

**Форма власності:**

**Сфера управління:** Міністерство освіти і науки України

**Ідентифікатор ROR:** Не застосовується

**Розмір організації:**

**Телефон:** 380487050431, 380487050333

## IV. Відомості про співвиконавців ДіР

## V. Відомості про замовника ДіР

**Повне найменування юридичної особи (або ПІБ фізичної особи):** Міністерство освіти і науки України

**Код за ЄДРПОУ:** 38621185

**Місцезнаходження:** проспект Перемоги, буд. 10, м. Київ, 01135, Україна

**Форма власності:**

**Сфера управління:** Кабінет Міністрів України

**Ідентифікатор ROR:** Не застосовується

**Розмір організації:**

**Телефон:** 380444813221

## VI. Джерела, напрями та обсяги фінансування ДіР

**Підстава для проведення ДіР:** 34 - договір (замовлення) з центральним органом виконавчої влади, академією наук (головними розпорядниками бюджетних коштів на проведення НДДКР)

**Напрям фінансування:** 2.5 - програми і проекти у сфері міжнародного науково-технічного співробітництва

### Джерела фінансування

**7713 - кошти держбюджету**

**Код програмної класифікації видатків і кредитування (КПКВК):** 2201380

| |
|---|
| **Фактичний обсяг фінансування (тис. грн.):** 160.000 |

## VII. Відомості про ДіР

### Назва роботи українською:

Система передавання секретного ключа на основі протоколів квантової криптографії

### Назва роботи англійською:

Secret key transmission system based on quantum cryptography protocols

### Реферат українською:

Об'єктом дослідження є безпечна система квантового розподілення ключів по оптичному волокну. Метою проекту є створення експериментального зразка системи передавання секретного ключа на основі протоколів квантової криптографії. Розглянуто основні способи знімання інформації з оптичного волокна, які можуть бути використані для пасивних атак на системи квантового розподілення ключів. Встановлено, що найбільш небезпечним є компенсаційний спосіб внаслідок складності його виявлення. Проаналізовані різні види атак на системи квантової криптографії. Розглянуто один з ефективних методів протидії атаці розділення числа фотонів – використання станів приманки. Розглянуто математичне обґрунтування та проаналізовані відповідні алгоритми для трьох етапів стеку протоколів квантового розподілення ключів. Проаналізовано алгоритм оцінювання рівня шуму в просіяних ключах легітимних користувачів. Розглянуто питання вибору розміру підмножини бітів, які використовують легітимні користувачі для їх відкритого порівняння при оцінювання рівня шуму. З цією метою виконано обчислювальний експеримент та представлені відповідні рекомендовані розміри підмножин бітів. Розглянуто два алгоритми пошуку та виправлення помилок в просіяних ключах. Детально досліджено питання вибору розміру блоку для алгоритму пошуку та виправлення помилок у залежності від рівня шуму. На підставі виконаних розрахунків рекомендовані відповідні розміри блоків. Проаналізовано математичне обґрунтування процедури підсилення секретності. Розраховано інформацію порушника в залежності від довжини фінального секретного ключа при різних значеннях додаткового параметра безпеки та встановлено, що для виконання процедури підвищення секретності достатньо вибирати цей параметр порядку 0,1 при довжині фінального ключа, більшої ніж 40–50 бітів.

### Реферат англійською:

The object of research is a secure system of quantum key distribution on optical fiber. The objective of the project is to develop an experimental model of a secret key transmission system based on quantum cryptography protocols. The main methods of extracting information from optical fiber, which can be used for passive attacks on quantum key distribution systems, are considered. It is cleared up that the most dangerous is the compensatory method due to the complexity of its detection. Different types of attacks on quantum cryptography systems are analyzed. One of the effective methods of counteracting the photon number splitting attack is the use of decoy states. The mathematical background is considered and the corresponding algorithms for three stages of the stack of quantum key distribution protocols are analyzed. The algorithm for estimating the noise level in the sifted keys of legitimate users is analyzed. The question of choosing the size of a subset of bits used by legitimate users for their open comparison when estimating the noise level is considered. For this purpose, a computer simulation was performed and the corresponding recommended sizes of bit subsets were presented. Two algorithms for finding and correcting errors in sifted keys are considered. The issue of choosing the block size for the search and error correction algorithm depending on the noise level is studied in detail. Based on the performed calculations, the appropriate block sizes are recommended. The mathematical background of the privacy amplification procedure is analyzed. The eavesdropper's information was calculated depending on the length of the final secret key at different values of the additional security parameter. It was found that to perform the privacy amplification procedure it is enough to choose this parameter of 0.1 for the final key length greater than 40-50 bits.

**Індекс УДК:** 65.012.8; 003.26; 004.56.5, 531:530.145

**Коди тематичних рубрик:**20.53.37, 29.05.15

**Керівники роботи**

**Власне Прізвище Ім'я По-батькові:** Василіу Євген Вікторович

**Науковий ступінь:** д.т.н.

**Вчене звання:** професор

**Ідентифікатор ORCID ID:**

**Додаткова інформація:**

## VIII. Наукова (науково-технічна) продукція (НТП)

## IX. Бібліографічний опис

Vasiliu Ye., Okhrimenko T., Fesenko A., Dorozhynskyy S. Passive Eavesdropping Attack of Several Intruders on Deterministic Protocol with Pairs of Entangled Qubits. The 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications. 22-25 September, 2021, Cracow, Poland. – V. 1. – P. 1068–1072.

## X. Заключні відомості

**Керівник юридичної особи** Назаренко Олександр Аскольдович
к. ф.-м. н., 01.04.01

**Перелік осіб-виконавців**

Гончар Дмитро Ігорович

Лімарь Ігор Валерійович
(к. т. н.)

Рябуха Олександр Миколайович
(к. т. н., 05.12.13)

Склярук Анастасія Вадимівна

Стайкуца Сергій Володимирович
(к.філос.н., 09.00.10)

Сідень Сергій Віталійович
(к. т. н., 05.12.07)

**Відповідальний за підготовку облікових документів** Кутузакі Ірина Георгіївна

**Телефон** +38 (048) 705-03-54

**Реєстратор**

**Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності**