# Облікова картка дисертації

## I. Загальні відомості

**Державний обліковий номер:** 0821U102987

**Особливі позначки:** відкрита

**Дата реєстрації:** 28-12-2021

**Статус:** Захищена

**Реквізити наказу МОН / наказу закладу:**

## II. Відомості про здобувача

**Власне Прізвище Ім'я По-батькові:**

1. Циганенко Олексій Сергійович
2. Tsyhanenko Oleksii S

**Кваліфікація:**

**Ідентифікатор ORCHID ID:** Не застосовується

**Вид дисертації:** доктор філософії

**Шифр наукової спеціальності:** 122

**Назва наукової спеціальності:** Комп'ютерні науки

**Галузь / галузі знань:**

**Освітньо-наукова програма зі спеціальності:** Не застосовується

**Дата захисту:** 16-12-2021

**Спеціальність за освітою:** Інформаційні управляючі системи та технології

**Місце роботи здобувача:** Харківський національний економічний університет імені Семена Кузнеця

**Код за ЄДРПОУ:** 02071211

**Місцезнаходження:** проспект Науки, буд. 9-а, м. Харків, Харківський р-н., Харківська обл., 61166, Україна

**Форма власності:**

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

**Ідентифікатор ROR:** Не застосовується

**Сектор науки:** Не застосовується

## III. Відомості про дисертацію

**Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради):** ДФ 41.090.007

**Повне найменування юридичної особи:** Одеський державний екологічний університет

**Код за ЄДРПОУ:** 26134086

**Місцезнаходження:** вул. Львівська, буд. 15, м. Одеса, Одеська обл., 65016, Україна

**Форма власності:**

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

**Ідентифікатор ROR:** Не застосовується

**Сектор науки:** Не застосовується

## IV. Відомості про підприємство, установу, організацію, в якій було виконано дисертацію

**Повне найменування юридичної особи:** Харківський національний економічний університет імені Семена Кузнеця

**Код за ЄДРПОУ:** 02071211

**Місцезнаходження:** проспект Науки, буд. 9-а, м. Харків, Харківський р-н., Харківська обл., 61166, Україна

**Форма власності:**

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

**Ідентифікатор ROR:** Не застосовується

**Сектор науки:** Не застосовується

## V. Відомості про дисертацію

**Мова дисертації:**

**Коди тематичних рубрик:** 50.37.23

**Тема дисертації:**

1. Моделі та методи підвищення якості обслуговування інформаційних систем
2. Models and methods of improving the quality of information systems service

**Реферат:**

1. Дисертаційне дослідження присвячене актуальним питанням розроблення нових та удосконалення існуючих моделей і методів забезпечення конфіденційності та достовірності для підвищення ефективності використання протоколу TLS в умовах постквантового періоду. У дисертаційній роботі проведено аналіз існуючих підходів щодо забезпечення основних послуг якості обслуговування (QoS) – надійності та безпеки, визначені основні загрози в умовах значного росту обчислювальних ресурсів, появи повномасштабного квантового комп'ютера та можливості його застосування зловмисниками. Запропоновані інтегровані механізми, які дозволяють одночасно забезпечити вимоги щодо надійності (достовірності доставлення інформаційних повідомлень/інформаційних потоків), безпеки (забезпечення послуг цілісності та

конфіденційності інформаційних повідомлень) та оперативності на основі використання постквантових алгоритмів – крипто-кодових конструкцій Niederreiter (ССС) на алгеброгеометрічних (кодах, які використовують алгебраїчний апарат теорії завадостійкого кодування та параметри геометричних кривих, АГК). Таким чином, актуальним завданням є розробка інформаційної технології на основі ССС Niederreiter, що дозволяють забезпечити сучасні вимоги до якості обслуговування клієнтів в умовах переходу на NGN та постквантового періоду. У роботі запропоновано модель функціонування (криптосхема) несиметричних ССС Niederreiter на модифікованих (укорочених та подовжених) еліптичних кодах, впровадження якої, за рахунок методу формування та розкодування кодограми, дозволяє забезпечити рівень безпеки (безпечний час – ТБ> 200 р., стійкість до криптоаналізу РК <1025 групових операцій) та рівень надійності (достовірность передачі даних (Рпом <10-9) інформації, що циркулює в інформаційних системах, а також в умовах кібератак підвищити рівень якості обслуговування та живучість самих систем. У роботі запропоновано метод забезпечення конфіденційності та цілісності інформаційних ресурсів, який ґрунтується на модифікованих ССС Niederreiter (МССС) .з модифікованими (укороченими або подовженими) еліптичними кодами, що дозволяє підвищити рівень інформаційної прихованості та достовірності, зменшити у 5 разів час на формування кодограми за рахунок зменшення порядку GF (q). Розроблені моделі функціонування (криптосхема) гібридних ССС Niederreiter, впровадження якої за рахунок методу формування та разкодування кодограми дозволяє підвищити рівень якості обслуговування інформаційних систем та забезпечити рівень криптостійкості (РК<1035 групових операцій), рівень надійності (достовірность передачі даних (Рпом<10-12) інформації, що циркулює в інформаційних системах, а також в умовах постквантового періоду. Запропоновано метод забезпечення конфіденційності та цілісності інформаційних ресурсів, який ґрунтується на гібридних ССС Niederreiter зі збитковими кодами, що дозволяє підвищити рівень інформаційної прихованості та достовірності, зменшити енергетичні витрати на їх практичну реалізацію в 10 – 12 разів (шифрування, розшифрування) за рахунок зменшення порядку GF (q). Удосконалено метод оцінки якості обслуговування інформаційних систем на основі багатокритеріальної оцінки, що дозволило, на відміну від існуючих, виділити діапазони зміни параметрів критеріїв надійності та безпеки і визначити їх в умовних балах. Запропоновано методи двофакторної (строгої) автентифікації на основі використання ССС McEliece та Niederreiter, алгоритм цифрового підпису DSA (Digital Signature Algorithm), які дозволяють забезпечити послугу безпеки – автентичність. Виконано практичну реалізацію запропонованих методів і моделей у вигляді програмних застосунків, що дозволяє їх практичне використання в протоколах TLS, DSA та 2FA. Експериментально доведено, що використання запропонованих ССС Niederreiter на МЕС забезпечує зменшення енергетичної місткості без втрати рівня безпеки в 4,5 рази порівняно з класичною схемою Нідеррайтера на двійкових кодах, при використані збиткових кодів ще на 7%. Виконано впровадження результатів дисертаційної роботи у діяльність ТОВ “Сайфер” (м. Київ). Результати досліджень впроваджено у навчальний процес кафедри кібербезпеки та інформаційних технологій Харківського національного економічного університету імені Семена Кузнеця.

2. The dissertation research is devoted to topical issues of development of new and improvement of existing models and methods of ensuring confidentiality and reliability to increase the efficiency of using the TLS protocol in the post-quantum period. The dissertation analyzes the existing approaches to providing basic quality of service (QoS) – reliability and security, identifies the main threats in the context of significant growth of computing resources, the emergence of a full-scale quantum computer, and the possibility of its use by attackers. Integrated mechanisms are proposed, which allow to simultaneously provide requirements for reliability (probability of delivery of information messages / information flows), security (provision of information integrity and confidentiality services) and efficiency based on the use of post-quantum algorithms - crypto-code constructions of Niederreiter (CCC) codes that use the algebraic apparatus of noise-tolerant coding theory and parameters of geometric curves, AGC). Thus, the urgent task is to develop information technology based on crypto-code constructions of Niederreiter, which allow to provide modern requirements for the quality of customer service in the transition to NGN and the post-quantum period. Models of functioning (cryptoscheme) of asymmetric crypto-code constructions of Niederreiter on modified (shortened and extended) elliptical codes are developed in the

work, the introduction of which due to the method of formation and decoding of the codegram allows to provide the level of security (secure time – Ts> 200 years, resistance to cryptanalysis RC <1025 group operations) and reliability level (probability of data transfer (Peror <10-9) of information circulating in information systems and in cyber-attacks to increase the level of service quality and survivability of the systems themselves. The paper proposes a method of ensuring the confidentiality and integrity of information resources, which is based on modified crypto-code constructions of Niederreiter with modified (shortened or extended) elliptical codes, which increases the level of information concealment and probability, reduces 5 times the time to form code order GF (q). Developed models of functioning (cryptoscheme) of hybrid crypto-code constructions of Niederreiter, the introduction of which due to the method of formation and decoding of the codegram allows to increase the level of service quality of information systems and to provide the level of cryptosecurity (Pcrypt<1035 group operations), reliability level (transmission probability (Perror<10-12) of information circulating in information systems in the post-quantum period. A method of ensuring the confidentiality and integrity of information resources, which is based on hybrid crypto-code constructions of Niederreiter with unprofitable codes, which allows to increase the level of information concealment and reliability, reduce energy costs for their practical implementation by 10 – 12 times (encryption, decryption) by reducing the order GF (q) is proposed. An improved method of assessing the quality of service information systems based on multi-criteria evaluation, which allowed, in contrast to the existing, to highlight ranges of change in the parameters of the criteria of reliability and security to determine them in conditional points. The method of two-factor (strict) authentication based on the use of crypto-code constructions (CCC) of McEliece and Niederreiter, DSA (Digital Signature Algorithm), which allow to provide a security service – authenticity, is proposed. The practical implementation of the proposed methods and models in the form of software applications, which allows their practical use in the protocols TLS, DSA and 2FA is performed. It has been experimentally proven that the use of the proposed crypto-code constructions of Niederreiter on MEC provides a 4.5 time reduction without loss of security compared to the classical scheme of Niederreiter on binary codes, with the use of loss codes by another 7%. The implementation of the results of the dissertation performed in the activities of LLC “Cypher” (Kyiv). The research results are implemented in the educational process of the Department of Cybersecurity and Information Technologies of Simon Kuznets Kharkiv National University of Economics.

**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. Євсеєв Сергій Петрович

2. Yevseiev Serhii P.

**Кваліфікація:** 21.05.01

**Ідентифікатор ORCHID ID:** Не застосовується

**Додаткова інформація:**

**Повне найменування юридичної особи:**

**Код за ЄДРПОУ:**

**Місцезнаходження:**

**Форма власності:**

**Сфера управління:**

**Ідентифікатор ROR:** Не застосовується

**Сектор науки:** Не застосовується

## VII. Відомості про офіційних опонентів та рецензентів

### Офіційні опоненти

**Власне Прізвище Ім'я По-батькові:**

1. Кучук Георгій Анатолійович
2. Kuchuk Heorhii A.

**Кваліфікація:** 05.13.06

**Ідентифікатор ORCHID ID:** Не застосовується

**Додаткова інформація:**

**Повне найменування юридичної особи:**

**Код за ЄДРПОУ:**

**Місцезнаходження:**

**Форма власності:**

**Сфера управління:**

**Ідентифікатор ROR:** Не застосовується

**Сектор науки:** Не застосовується

**Власне Прізвище Ім'я По-батькові:**

1. Андрощук Олександр Степанович
2. Androshchuk Oleksandr S.

**Кваліфікація:** 05.13.06

**Ідентифікатор ORCHID ID:** Не застосовується

**Додаткова інформація:**

**Повне найменування юридичної особи:**

**Код за ЄДРПОУ:**

**Місцезнаходження:**

**Форма власності:**

**Сфера управління:**

**Ідентифікатор ROR:** Не застосовується

**Сектор науки:** Не застосовується

**Рецензенти**

**Власне Прізвище Ім'я По-батькові:**

1. Казакова Надія Феліксівна

2. Kazakova Nadiia F.

**Кваліфікація:** 05.13.21

**Ідентифікатор ORCHID ID:** Не застосовується

**Додаткова інформація:**

**Повне найменування юридичної особи:**

**Код за ЄДРПОУ:**

**Місцезнаходження:**

**Форма власності:**

**Сфера управління:**

**Ідентифікатор ROR:** Не застосовується

**Сектор науки:** Не застосовується

**Власне Прізвище Ім'я По-батькові:**

1. Фразе-Фразенко Олексій Олексійович

2. Fraze-Frazenko Oleksiy

**Кваліфікація:** 05.13.21

**Ідентифікатор ORCHID ID:** Не застосовується

**Додаткова інформація:**

**Повне найменування юридичної особи:**

**Код за ЄДРПОУ:**

**Місцезнаходження:**

**Форма власності:**

**Сфера управління:**

**Ідентифікатор ROR:** Не застосовується

**Сектор науки:** Не застосовується

## VIII. Заключні відомості

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