Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0823U101036

Особливі позначки: відкрита

Дата реєстрації: 30-10-2023

Статус: Запланована

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Гаврилова Алла Андріївна

2. Alla Havrylova

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: доктор філософії

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 125

Назва наукової спеціальності: Кібербезпека та захист інформації

Галузь / галузі знань: інформаційні технології

Освітньо-наукова програма зі спеціальності: Кібербезпека

Дата захисту: 09-11-2023

Спеціальність за освітою: 125 Кібербезпека

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): Разова спеціалізована вчена рада №2569

Повне найменування юридичної особи: Національний авіаційний університет

Код за ЄДРПОУ: 01132330

Місцезнаходження: проспект Любомира Гузара, буд. 1, Київ, 03058, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

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

Повне найменування юридичної особи: Національний авіаційний університет

Код за ЄДРПОУ: 01132330

Місцезнаходження: проспект Любомира Гузара, буд. 1, Київ, 03058, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

V. Відомості про дисертацію

Мова дисертації: Українська

Коди тематичних рубрик: 50.37.23, 81

Тема дисертації:

1. Моделі і методи контролю цілісності та автентичності на основі каскадного алгоритму UMAC

2. Models and methods of integrity and authenticity control based on the UMAC cascade algorithm

Реферат:

1. Дисертаційна робота присвячена актуальним питанням розроблення нових та удосконалення існуючих моделей і методів забезпечення цілісності та автентичності інформації, яка циркулює в кіберпросторі в умовах постквантового періоду. В умовах бурхливого зростання обчислювальних можливостей щодо зламу криптографічних алгоритмів, виникає необхідність у розробці та практичної реалізації алгоритмів щодо забезпечення послуг безпеки – цілісності та автентичності. Для забезпечення послуг безпеки (цілісності та автентичності) як правило використовуються алгоритми гешування та цифрового підпису, але проведений аналіз спеціалістами NIST у 2020 р. свідчать про те, що існуючі алгоритми в постквантовий криптоперіод не забезпечуть необхідний рівень безпеки та можуть бути зламані. Кіберзагрози можуть бути реалізовані через слабкості алгоритмів гешування. Існує низка підходів до створення геш-кодів для підвищення криптостійкості переданих повідомлень, але практичні дослідження дають змогу говорити про недосконаліть існуючих варіантів гешування з погляду швидкості їх формування та ступеня

криптостійкості. Для ліквідації цього недоліку запропоновано використовувати псевдовипадкову підкладку криптографічно стійкими алгоритмами. Але жоден з відомих алгоритмів не забезпечує стійкість до квантових комп'ютерів

2. The dissertation study is devoted to the topical issues of developing new and improving existing models and methods for ensuring the integrity and authenticity of information circulating in cyberspace in the post-quantum period. In the conditions of the rapid growth of computing capabilities for breaking cryptographic algorithms, there is a need for the development and practical implementation of algorithms for ensuring security services – integrity and authenticity. To ensure security services (integrity and authenticity), hashing and digital signature algorithms are usually used, but the analysis conducted by NIST specialists in 2020 indicates that the existing algorithms in the post-quantum cryptoperiod will not provide the required level of security and may be broken. Cyber threats can be implemented through weaknesses in hashing algorithms. There are a number of approaches to creating hash codes to increase the crypto-resistance of transmitted messages, but practical studies allow us to talk about the imperfection of existing hashing options in terms of the speed of their formation and the degree of crypto-resistance. To eliminate this shortcoming, it is proposed to use a pseudo-random layer with cryptographically stable algorithms. But none of the known algorithms provides stability to quantum computers

Державний реєстраційний номер ДіР:

Пріоритетний напрям розвитку науки і техніки: Інформаційні та комунікаційні технології

Стратегічний пріоритетний напрям інноваційної діяльності: Розвиток сучасних інформаційних, комунікаційних технологій, робототехніки

Підсумки дослідження: Нове вирішення актуального наукового завдання

Публікації:

- Havrylova Alla A., Korol Olha H., Milevskyi Stanyslav V., Bakirova Lala R. Mathematical model of authentication of a transmitted message based on a McEliece scheme on shorted and extended modified elliptic codes using UMAC modified algorithm. Кібербезпека: освіта, наука, техніка, 2019, № 1(5). P. 40-51.
- Gavrilova A., Volkov I., Kozhedub Yu. Development of a modified UMAC algorithm based on crypto-code constructions Eastern-European Journal of Enterprise Technologies. 2020, № 4/9 (106). P. 45-63.
- Гаврилова Алла, Хохлачова Юлія, Погорелов Володимир. Аналіз застосування гібридних крипто-кодових конструкцій для підвищення рівня стійкості геш-кодів до зламу. Безпека інформації, 2022, Том 28, № 2. С. 87-101.
- Yevseiev S., Havrylova A., Milevskyi S., Sinitsyn I. and others. Development of an improved SSL/TLS protocol using post-quantum algorithms. Eastern-European Journal of Enterprise Technologies. 2023, № 3/9 (123). P. 33-48.
- Havrylova A., Khokhlachova Y., Tkachov A., Voropay N., Khvostenko V. Justification of directions for improving authentication protocols in information and communication systems. Ukrainian Information Security Research Journal. 2023, Vol. 25, №. 1. P. 6-19.

Наукова (науково-технічна) продукція:

Соціально-економічна спрямованість:

Охоронні документи на ОПІВ:

Впровадження результатів дисертації: Впроваджено

Зв'язок з науковими темами:

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Хохлачова Юлія Євгеніївна

2. Yuliia Khokhlachova

Кваліфікація: к.т.н., доц., 05.13.21

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Національний авіаційний університет

Код за ЄДРПОУ: 01132330

Місцезнаходження: проспект Любомира Гузара, буд. 1, Київ, 03058, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Смірнов Олексій Анатолійович

2. Oleksii Smirnov

Кваліфікація: д.т.н., професор, 21.05.01

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Центральноукраїнський національний технічний університет

Код за ЄДРПОУ: 02070950

Місцезнаходження: просп. Університетський, буд. 8, Кропивницький, Кропівницький р-н., 25006, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Казакова Надія Феліксівна

2. Nadiia Kazakova

Кваліфікація: д.т.н., професор, 05.13.21

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Одеський державний екологічний університет

Код за ЄДРПОУ: 26134086

Місцезнаходження: вул. Львівська, буд. 15, Одеса, 65016, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Кінзерявий Василь Миколайович
2. Vasyl Kinzeriavyi

Кваліфікація: к. т. н., доц., 21.05.01

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Національний авіаційний університет

Код за ЄДРПОУ: 01132330

Місцезнаходження: проспект Любомира Гузара, буд. 1, Київ, 03058, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Іванченко Євгенія Вікторівна
2. Yevgeniia Ivanchenko

Кваліфікація: к. т. н., професор, 05.13.21

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Національний авіаційний університет

Код за ЄДРПОУ: 01132330

Місцезнаходження: проспект Любомира Гузара, буд. 1, Київ, 03058, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради	Корченко Олександр Григорович
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Корченко Олександр Григорович
Відповідальний за підготовку облікових документів	Довженко Олена Андріївна
Реєстратор	УкрІНТЕІ
Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності	Юрченко Тетяна Анатоліївна