Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0824U003031

Особливі позначки: відкрита

Дата реєстрації: 04-09-2024

Статус: Запланована

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Проскурін Дмитро Петрович
2. Dmytro Proskurin

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: доктор філософії

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 122

Назва наукової спеціальності: Комп'ютерні науки

Галузь / галузі знань: інформаційні технології

Освітньо-наукова програма зі спеціальності: Комп'ютерні науки

Дата захисту: 30-08-2024

Спеціальність за освітою: 122 Комп'ютерні науки та інформаційні технології

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 №6641

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: 28.23, 28.23.25, 28.23.37

Тема дисертації:

1. Інформаційна технологія оцінювання якості генераторів послідовностей псевдовипадкових чисел на основі машинного навчання

2. Information technology of quality assessment generators of sequences of pseudo-random numbers based on machine learning

Реферат:

1. Запропонована в дисертації інформаційна технологія базується на використанні сучасних методів машинного навчання, зокрема гібридних та згорткових нейронних мереж, що дозволяє суттєво підвищити точність і швидкість оцінювання якості генераторів ПВЧ навіть за умов обмеженої кількості вхідних даних. Використання гібридних моделей дозволяє поєднувати переваги різних типів нейронних мереж, що забезпечує більш ефективне виявлення патернів у даних і покращує якість передбачення. Зокрема, використання згорткових нейронних мереж дозволяє аналізувати локальні патерни в послідовностях, тоді як рекурентні нейронні мережі ефективні для аналізу послідовностей з довготривалими залежностями. Удосконалено модель передбачення наступної послідовності ПВЧ, яка за рахунок використання гібридної нейронної мережі та обмеженої кількості вхідних даних для навчання дозволяє передбачати чергові

послідовності для неякісних генераторів ПВЧ. Отримав подальшого розвитку метод оцінювання якості послідовностей ПВЧ, який, використовуючи одновимірну рекурентну нейронну мережу та датасети, сформовані різними генераторами ПВЧ, дозволяє швидше оцінювати якість генераторів для криптографічних та інших застосувань у галузі комп'ютерних наук. Практичне значення дисертації полягає у можливості застосування отриманих результатів у реальних умовах, де доступ до великої кількості даних обмежений, а вимоги до надійності та безпеки є надзвичайно високими. Наприклад, розроблені моделі та технології можуть бути використані у сфері мобільних комунікацій, зокрема для забезпечення безпеки мереж LTE/5G/6G, а також у сфері захисту критичної інфраструктури, де інформаційна безпека є питанням національної важливості. Окрім цього, результати дослідження можуть знайти застосування у багатьох інших галузях, включаючи фінансовий сектор, державне управління та військову справу, де якість та випадковість генераторів ПВЧ має вирішальне значення. Результати дослідження були впроваджені в освітній процес на кафедрі комп'ютерних інформаційних технологій Національного авіаційного університету, а також у науково-дослідну роботу, що проводиться в рамках Науково-дослідної лабораторії протидії кіберзагрозам в авіаційній галузі. Крім того, практичні результати були впроваджені в діяльність Головного управління розвідки Міністерства оборони України, що підкреслює значущість дослідження для національної безпеки.

2. The information technology proposed in the dissertation is based on the use of modern methods of machine learning, in particular hybrid and convolutional neural networks, which allows to significantly increase the accuracy and speed of assessing the quality of PVC generators even under the conditions of a limited amount of input data. The use of hybrid models allows combining the advantages of different types of neural networks, which provides more effective detection of patterns in data and improves the quality of predictions. In particular, the use of convolutional neural networks allows the analysis of local patterns in sequences, while recurrent neural networks are effective for analyzing sequences with long-term dependencies. The model for predicting the next PVC sequence has been improved, which, due to the use of a hybrid neural network and a limited amount of input data for training, allows predicting next sequences for low-quality PVC generators. The method for evaluating the quality of PVC sequences has received further development, which, using a one-dimensional recurrent neural network and datasets formed by various generators of PVC, allows to quickly evaluate the quality of generators for cryptographic and other applications in the field of computer science. The practical significance of the dissertation lies in the possibility of applying the obtained results in real conditions, where access to a large amount of data is limited, and the requirements for reliability and security are extremely high. For example, the developed models and technologies can be used in the field of mobile communications, in particular to ensure the security of LTE/5G/6G networks, as well as in the field of critical infrastructure protection, where information security is a matter of national importance. In addition, the research findings may find applications in many other industries, including the financial sector, public administration, and the military, where the quality and randomness of PVC generators are critical. The results of the study were implemented in the educational process at the Department of Computer Information Technologies of the National Aviation University, as well as in the research work carried out within the Scientific Research Laboratory for Combating Cyber Threats in the Aviation Industry. In addition, the practical results were implemented in the activities of the Main Directorate of Intelligence of the Ministry of Defense of Ukraine, which emphasizes the significance of the research for national security.

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:

- 1. Proskurin D., Gnatyuk S., Okhrimenko T., Iavich M. ML-Based Cryptographic Keys Quality Assessment for 5G / 6G Networks Privacy and Security, Proceedings of the IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS. 2023. С. 1025-1030.
- 2. Gnatyuk S., Okhrimenko A., Navrotskyi D., Proskurin D., Horbakha B. Dataset of Cryptographic Algorithms for UAV Image Encryption based on Artificial Neural Networks, CEUR Workshop Proceedings. 2023. Ed. 3504. С. 63-71.
- 3. Hu Z., Ryabyy M., Prystavka P., Janisz K., Proskurin D. Advanced Method for Compressing Digital Images as a Part of Video Stream to Pre-processing of UAV Data Before Encryption, Lecture Notes on Data Engineering and Communications Technologies. 2023. Ed. 181. С. 371-381.
- 4. Proskurin D., Gnatyuk S., Okhrimenko T. Predicting Pseudo-Random and Quantum Random Number Sequences using Hybrid Deep Learning Models, CEUR Workshop Proceedings. 2023. Ed. 3426. С. 77-88.
- 5. Proskurin D., Gnatyuk S., Bauyrzhan M. Distributive Training Can Improve Neural Network Performance based on RL-CNN Architecture, CEUR Workshop Proceedings. 2021. Вип. 3187. С. 48-57.
- 6. Рябий М., Кінзерявий О., Проскурін Д., Сорокопуд В. An advanced method of compressing digital images as part of a video stream to pre-process the data before encrypting, Проблеми інформатизації та управління. 2023. Т. 1, № 73. С. 128-137.
- 7. Гнатюк С.О., Поліщук Ю.Я., Кінзерявий В.М., Горбаха Б.М., Проскурін Д.П. Формування датасету криптоалгоритмів для забезпечення конфіденційності даних, які передаються з розвідувально-пошукового БПЛА, Кібербезпека: освіта, наука, техніка. 2023. № 4 (20). С. 205–219.
- 8. Проскурін Д.П., Явіч М.П., Гнатюк С.О. Модель ідентифікації джерела послідовностей псевдовипадкових чисел на основі гібридної нейронної мережі, Проблеми інформатизації та управління. 2024. Т. 1, № 73. С. 54-62.
- 9. Proskurin D. P. Assessing Randomness in Number Sequences in Cryptography: A Comparative Study of the Chi-Squared Test and Neural Network-Based Approaches, EEML 2023: Eastern European Machine Learning Conference, June 2023.

Наукова (науково-технічна) продукція: технології; програмні продукти, програмно-технологічна документація

Соціально-економічна спрямованість: створення принципово нової продукції (матеріалів, технологій тощо) для забезпечення експортного потенціалу та заміщенню імпорту

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. Гнатюк Сергій Олександрович

2. Serhii Gnatyuk

Кваліфікація: д. 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:

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Чевардін Владислав Євгенійович
2. Vladyslav Chevardin

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

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Військовий інститут телекомунікацій та інформатизації імені Героїв Крут

Код за ЄДРПОУ: 24978555

Місцезнаходження: вул. Московська, буд. 45/1, Київ, 01011, Україна

Форма власності: Державна

Сфера управління: Міністерство оборони України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Опірський Іван Романович
2. Ivan Opirskyi

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

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Національний університет "Львівська політехніка"

Код за ЄДРПОУ: 02071010

Місцезнаходження: вул. Степана Бандери, буд. 12, Львів, 79013, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Фауре Еміль Віталійович

2. Emil Faure

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

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Черкаський державний технологічний університет

Код за ЄДРПОУ: 05390336

Місцезнаходження: бульвар Шевченка, буд. 460, Черкаси, Черкаський р-н., 18006, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Фесенко Андрій Олександрович

2. Andrii Fesenko

Кваліфікація: д. 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	Нечипорук Олена Петрівна
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Нечипорук Олена Петрівна
Відповідальний за підготовку облікових документів	Довженко Олена Андріївна
Реєстратор	УкрІНТЕІ

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності

Юрченко Тетяна Анатоліївна