Облікова картка ДіР

I. Загальні відомості

Державний обліковий номер: 0225U001981

Державний реєстраційний номер: 0123U101020

Особливі позначки: відкрита

Дата реєстрації: 13-02-2025

II. Етап виконання ДіР

Номер етапу: 1

Назва етапу: Розробка симетричної криптосистеми на основі використання згорткової штучної нейронної мережі

Початок етапу: 01.2023

Закінчення етапу: 01.2025

Вид звітного документа: Остаточний звіт

III. Відомості про виконавця ДіР

Повне найменування юридичної особи (або ПІБ фізичної особи): Національний технічний університет "Харківський політехнічний інститут"

Код за ЄДРПОУ: 02071180

Місцезнаходження: вул. Кирпичова, буд. 2, м. Харків, Харківський р-н., Харківська обл., 61002, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Розмір організації:

Телефон: 380577076634

IV. Відомості про співвиконавців ДіР

V. Відомості про замовника ДіР

Повне найменування юридичної особи (або ПІБ фізичної особи): Національний технічний університет "Харківський політехнічний інститут"

Код за ЄДРПОУ: 02071180

Місцезнаходження: вул. Кирпичова, буд. 2, м. Харків, Харківський р-н., Харківська обл., 61002, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Розмір організації:

Телефон: 380577076634

VI. Джерела, напрями та обсяги фінансування ДіР

Підстава для проведення ДіР: 43 - власна ініціатива (якщо робота виконується з власної ініціативи за кошти виконавця НДР або безкоштовно)

Напрям фінансування: 2.2 - прикладні дослідження і розробки

Джерела фінансування

7706 - безплатно (договір про науково-технічне співробітництво, тощо)

VII. Відомості про ДіР

Назва роботи українською:

Розробка симетричної криптосистеми на основі використання згорткової штучної нейронної мережі

Назва роботи англійською:

Development of a symmetric cryptosystem based on the use of a convolutional artificial neural network

Реферат українською:

Об'єкт дослідження – системи захисту інформаційних ресурсів у кіберфізичних системах, зокрема банківських інформаційних ресурсів, соціальних інтернет-сервісів та каналів зв'язку в постквантовий період. Мета роботи – підвищення ефективності побудови та використання симетричних криптосистем в результаті застосування нейрокриптологічних моделей та алгоритмів на основі штучних нейронних мереж. Методи досліджень: Теоретичний аналіз криптографічних алгоритмів та кодів корекції помилок. Моделювання та аналіз властивостей гібридних крипто-кодових конструкцій. Експериментальні дослідження ефективності криптосистем у різних умовах загроз. Проведено дослідження властивостей несиметричних крипто-кодових систем, зокрема систем Мак-Еліса та Нідеррайтера, на модифікованих алгеброгеометричних кодах. Досліджено гібридні крипто-кодові конструкції з використанням збиткових кодів та LDPC-кодів для забезпечення конфіденційності, цілісності та автентичності інформації. Одержано математичні моделі гібридних крипто-кодових конструкцій, які демонструють високу стійкість до квантових атак і ефективне виправлення помилок у бездротових каналах зв'язку. Розроблено вдосконалений протокол SSL/TLS, що забезпечує захист від сучасних атак, таких як 0-RTT-атаки. Виявлено, що запропоновані методи дозволяють значно підвищити рівень захисту інформаційних ресурсів при зменшені енергоспоживання та забезпечити довготривалу надійність даних у критичних інфраструктурах. Проведено аналіз сучасних загроз і недоліків існуючих протоколів двофакторної автентифікації та запропоновано новий метод автентифікації на основі гібридних крипто-кодових конструкцій, який підвищує стійкість до атак у відкритих каналах зв'язку.

Реферат англійською:

The object of the research is information resource protection systems in cyber-physical systems, in particular banking information resources, social Internet services and communication channels in the post-quantum period. The purpose of the work is to improving the efficiency of building and using symmetric cryptosystems due to the use of neurocryptological models and algorithms based on artificial neural networks. Research methods: Theoretical analysis of cryptographic algorithms and error correction codes. Modeling and analysis of properties of hybrid crypto-code structures. Experimental studies of the effectiveness of cryptosystems under various threat conditions. The properties of asymmetric crypto-code systems, in particular the McAleese and Niederreiter systems, were studied using modified algebrogeometric codes. Hybrid crypto-code structures using lossy codes and LDPC codes were studied to ensure confidentiality, integrity and authenticity of information. Mathematical models of hybrid crypto-code structures were obtained, which demonstrate high resistance to quantum attacks and effective error correction in wireless communication channels. An improved SSL/TLS protocol has been developed that provides protection against modern attacks, such as 0-RTT attacks. It has been found that the proposed methods allow to significantly increase the level of protection of information resources while reducing energy consumption and ensuring long-term reliability of data in critical infrastructures. An analysis of modern threats and shortcomings of existing two-factor authentication protocols has been conducted and a new authentication method based on hybrid crypto-code constructions has been proposed, which increases resistance to attacks in open communication channels.

Індекс УДК: 004.8.032.26, 654.1; 654.14; 654.15; 654.16; 654.17; 654.19; 656.8, 002:651.928(083.73)

Коди тематичних рубрик: 28.23.37, 49.33.35

Керівники роботи

Власне Прізвище Ім'я По-батькові: Євсеєв Сергій Петрович

Науковий ступінь: д. т. н.

Вчене звання: професор

Ідентифікатор ORCID ID:

Додаткова інформація:

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

Назва НТП українською: Симетрична криптосистема на основі використання згорткової штучної нейронної мережі

Назва НТП англійською: A symmetric cryptosystem based on the use of a convolutional artificial neural network

НТП, яку передбачалося створити:

Причини, через які НТП не було створено:

Отримані результати: Методи, теорії

Галузь застосування: Кібербезпека

Реєстраційний номер картки технології:

Опис НТП: Одержано математичні моделі гібридних крипто-кодових конструкцій, які демонструють високу стійкість до квантових атак і ефективне виправлення помилок у бездротових каналах зв'язку. Розроблено вдосконалений протокол SSL/TLS, що забезпечує захист від сучасних атак, таких як 0-RTT-атаки.

Соціально-економічна спрямованість НТП: Розробка моделей симетричних та несиметричних криптосистем

Вплив НТП на довкілля:

Впровадження НТП: Не впроваджено

Практична реалізація НТП

Початок етапу: 01.2023

Закінчення етапу: 01.2025

Споживачі продукції: Державні установи, наукові заклади, бізнес-компанії та оборонний сектор.

Перспективні ринки: Перспективними ринками є IT, енергетика, транспорт, медицина, оборона та фінансовий сектор.

Характер співробітництва з інвестором

Потрібний обсяг інвестицій, тис. грн.:

Права, що надаються інвестору після завершення роботи:

Наявність бізнес-плану:

Техніко-економічне обгрунтування:

Потенціальний обсяг продажу, тис. грн.:

Очікуваний термін окупності (років):

Додаткова інформація:

IX. Бібліографічний опис

1. Yevseiev, S., Havrylova, A., Milevskyi, S., Sinitsyn, I., Chalapko, V., Dukin, H., Hrebeniuk, V., Diedov, M., Bekirova, L., & Shpak, O. (2023). Development of an improved SSL/TLS protocol using post-quantum algorithms. Eastern-

European Journal of Enterprise Technologies, 3(9 (123), 33–48. https://doi.org/10.15587/1729-4061.2023.281795

2. Yevseiev, S., Dzheniuk, N., Tolkachov, M., Milov, O., Voitko, T., Prygara, M., Shpak, O., Voropay, N., Volkov, A., & Lezik, O. (2023). Development of a multi-loop security system of information interactions in socio-cyberphysical systems. Eastern-European Journal of Enterprise Technologies, 5(9 (125), 53–74. https://doi.org/10.15587/1729-4061.2023.289467

3. Dzheniuk , N. ., Yevseiev , S. ., Lazurenko, B. ., Serkov , O. ., & Kasilov , O. . (2023). A METHOD OF PROTECTING INFORMATION IN CYBER-PHYSICAL SPACE . Advanced Information Systems, 7(4), 80–85. https://doi.org/10.20998/2522-9052.2023.4.11

4. S. Herasimov, A. Tkachov, V. Soroka, S. Yevseiev, T. Milevska and S. Dunaiev, "Method for Assessing Meter Error Characteristics of Random Signals," 2023 7th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), Ankara, Turkiye, 2023, pp. 1-5, doi: 10.1109/ISMSIT58785.2023.10304988.

5. S. Herasymov, V. Soroka, S. Yevseiev, S. Milevskyi and S. Pohasii, "Phase-Modulated Signals Synthesis Method to Control Information Transmission Channels," 2023 IEEE 4th KhPI Week on Advanced Technology (KhPIWeek), Kharkiv, Ukraine, 2023, pp. 1-5, doi: 10.1109/KhPIWeek61412.2023.10312859.

6. Yevseiev, S., Milevskyi, S., Sokol, V., Yemanov, V., Volobuiev, A., Dakova, L., Brailovskyi, M., Rahimova, I., Kravchenko, V., & Cherniavskiy, O. (2024). Development of functionality principles for the automated data transmission system through wireless communication channels to ensure information protection . Eastern-European Journal of Enterprise Technologies, 4(9 (130), 18–33. https://doi.org/10.15587/1729-4061.2024.310547

7. Tolkachov, M., Dzheniuk, N., Yevseiev, S., Lysetskyi, Y., Shulha, V., Grod, I., Faraon, S., Ivanchenko, I., Pasko, I., & Balagura, D. (2024). Development of a method for protecting information resources in a corporate network by segmenting traffic . Eastern-European Journal of Enterprise Technologies, 5(9 (131), 63–78. https://doi.org/10.15587/1729-4061.2024.313158

8. R. Korolov, S. Milevskyi, L. Shcherbyna, Y. Lutsenko, S. Dunaiev and V. Stetsenko, "Authentication and Authorization Method Based on McEliece Crypto-Code Construction," 2024 8th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), Ankara, Turkiye, 2024, pp. 1-5, doi: 10.1109/ISMSIT63511.2024.10757296

9. O. Kushnerov, P. Murr, S. Herasymov, S. Milevskyi, M. Melnyk and S. Golovashych, "Application of Neural Networks for Network Traffic Monitoring and Analysis," 2024 8th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), Ankara, Turkiye, 2024, pp. 1-8, doi: 10.1109/ISMSIT63511.2024.10757251.

10. S. Herasymov, V. Soroka, S. Milevskyi, O. Korol, I. Aksonova and V. Stetsenko, "Method for Reducing the Frequency Spectrum Overlaying Error in Digital Narrow-Band Filtration," 2024 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), Istanbul, Turkiye, 2024, pp. 1-5, doi: 10.1109/HORA61326.2024.10550889.

11. S. Pohasii, S. Holdobin, N. Brynza, O. Vilkhivska, O. Bilotserkivskyi and B. Samorodov, "Management Models for Wireless Communication Channel Interference Monitoring," 2024 8th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), Ankara, Turkiye, 2024, pp. 1-7, doi: 10.1109/ISMSIT63511.2024.10757190.

12. Y. Parzhin, S. Galkyn and M. Sobol, "Method For Binary Contour Images Vectorization Of Handwritten Characters For Recognition By Detector Neural Networks," 2022 IEEE 3rd KhPI Week on Advanced Technology (KhPIWeek), Kharkiv, Ukraine, 2022, pp. 1-6, doi: 10.1109/KhPIWeek57572.2022.9916331.

13. S. Pohasii, M. Mashchenko, O. Serhiienko, O. Klimenko, T. Andriushchenko and T. Milevska, "Assessing the Economic and Technical Effectiveness of Intercepting UAVs Using Alternative Methods," 2023 7th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), Ankara, Turkiye, 2023, pp. 1-5, doi:

10.1109/ISMSIT58785.2023.10304959.

14. S. Pohasii, S. Milevskyi, O. Bilotserkivskyi, V. Baranova, I. Ippolitova and I. Pyvavar, "Cost-Effective Software and Hardware Complex to Ensure Security Against Unauthorized Use of Enemy Commercial Uavs on the Combat Territory," 2023 IEEE 4th KhPI Week on Advanced Technology (KhPIWeek), Kharkiv, Ukraine, 2023, pp. 1-6, doi: 10.1109/KhPIWeek61412.2023.10312972.

15. Yevseiev, S., Khokhlachova, Yu., Ostapov, S., Laptiev, O., Korol, O., Milevskyi, S. et. al.; Yevseiev, S., Khokhlachova, Yu., Ostapov, S., Laptiev, O. (Eds.) (2023). Models of socio-cyber-physical systems security. Kharkiv: PC TECHNOLOGY CENTER, 184. doi: http://doi.org/10.15587/978-617-7319-72-5

X. Заключні відомості

Керівник юридичної особи Марченко Андрій Петрович
д. т. н., 05.05.03

Перелік осіб-виконавців

Голдобін Сергій Миколаевич

Дунаєв Сергій Владиславович

Кушнерьов Олександр Сергійович
(д.філософ, 051)

Меленті Євген Олександрович
(к.т.н., 05.12.17)

Мілевський Станіслав Валерійович
(к. е. н., 08.03.02)

Паржин Юрій Володимирович
(д.т.н., 05.13.05)

Погасій Сергій Сергійович
(к. е. н., 08.00.03)

Сокол Владислав Євгенович
(к.т.н., 05.13.06)

Стеценко Вадим Олегович

Відповідальний за підготовку облікових документів Гуренко Ю.І.

Телефон +38 (050) 609-83-92

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності

