Облікова картка НДДКР

Державний обліковий номер: 0224U033279

Державний реєстраційний номер: 0121U113068

Відкрита

Дата реєстрації: 23-12-2024

1. Етапи виконання

Номер етапу: 4

Назва етапу: На виконання завдань перспективного плану розвитку наукового напряму «Технічні науки» Харківського національного університету імені В.Н.Каразіна на 2024 рік

Початок етапу: 01-2024

Закінчення етапу: 12-2024

Вид звітного документа: Проміжний звіт

2. Виконавець

Назва організації: Харківський національний університет імені В. Н. Каразіна

Код ЄДРПОУ/ІПН: 02071205

Підпорядкованість: Міністерство освіти і науки України

Адреса: майдан Свободи, буд. 4, м. Харків, Харківський р-н., Харківська обл., 61022, Україна

Телефон: 380577051247

E-mail: rector@karazin.ua

E-mail: univer@karazin.ua

WWW: http://www.univer.kharkov.ua/

3. Власник результатів НДДКР (продукції)

Назва організації: Харківський національний університет імені В. Н. Каразіна

Код ЄДРПОУ/ІПН: 02071205

Адреса: майдан Свободи, буд. 4, м. Харків, Харківський р-н., Харківська обл., 61022, Україна

Підпорядкованість: Міністерство освіти і науки України

Телефон: 380577051247

E-mail: rector@karazin.ua

E-mail: univer@karazin.ua

WWW: http://www.univer.kharkov.ua/

4. Джерела та напрями фінансування

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

КПКВК: 2201390

Напрям фінансування: 2.2 - прикладні дослідження і розробки

Джерела фінансування

Джерело фінансування: 7713 - кошти держбюджету

Фактичний обсяг фінансування за звітний етап: 486.132 тис. грн.

5. Науково-технічна робота

Назва роботи (укр)

На виконання завдань перспективного плану розвитку наукового напряму «Технічні науки» Харківського національного університету імені В.Н.Каразіна

Назва роботи (англ)

To fulfill the tasks of the long-term development plan of the scientific direction "Technical Sciences" of V. N. Karazin Kharkiv National University

Реферат (укр)

Предметом дослідження є методи і моделі забезпечення перешкодостійкості цифрових засобів. Метою НДР є виконання завдань відповідно до пріоритетних тематичних напрямів, зазначених на 2024 рік у розділі 2 Перспективного плану розвитку Харківського національного університету імені В. Н. Каразіна за науковим напрямом «Технічні науки» за період з 2021 по 2025 роки (далі – Перспективний план) зі змінами, внесеними Додатковою угодою № БФ/3-2024 від 01. 04. 2024 р, Додаток до Договору № БФ/33-2021 від 04.08.2021 р., а саме у 2024 році науковою школою «Прикладна криптологія» в рамках реалізації пріоритетного тематичного напряму «Розробка протоколів і механізмів криптографічних перетворень для перехідного та пост квантового періоду» буде виконуватися прикладне дослідження: «Розроблення цифрових перешкодостійких засобів передачі даних з метою приведення у відповідність можливостей існуючих каналів». В основу проведених у роботі досліджень були покладені принципи системного аналізу, теорія чисел, теорія обчислювальних процесів та систем, а також теорія кодування і прикладна криптологія. Результатами досліджень є розвиток теорії і практики розроблення та впровадження цифрових перешкодостійких засобів передачі даних. Розроблені математичні алгоритми та програмні імплементації методів оцінки рівня безпеки децентралізованих протоколів консенсусу із спеціальними властивостями, а також допоміжних криптографічних протоколів із відповідним рівнем гарантій безпеки. Розроблені математичні моделі визначення пріоритетності обробки кібератак/ кіберінцидентів з використанням методів інтелектуального аналізу. Для проведення експериментальних досліджень і ефективного моделювання процесу визначення пріоритетності обробки кібератак/ кіберінцидентів створено спеціальне програмне забезпечення.

Реферат (англ)

The subject of research is the methods and models of ensuring the immunity of digital devices. The goal of the NDR is to fulfill tasks in accordance with the priority thematic areas specified for 2024 in section 2 of the Perspective Development Plan of Kharkiv National University named after V. N. Karazina in the scientific direction "Technical sciences" for the period from 2021 to 2025 (hereinafter referred to as the Prospective Plan) as amended by Additional Agreement No. BF/3-2024 dated April 1, 2024, Annex to Agreement No. BF/33-2021 from 04.08.2021, namely, in 2024, the scientific school "Applied Cryptology" as part of the implementation of the priority thematic direction "Development of protocols and mechanisms of cryptographic transformations for the transitional and post-quantum period" will carry out applied research: "Development of digital interference-resistant means of data transmission in order to bring the capabilities of existing channels". The principles of system analysis, number theory, theory of computing processes and systems, as well as coding theory and applied cryptology were the basis of the research carried out in the work. The research results are the development of the theory and practice of development and implementation of digital interference-resistant means of data transmission. Mathematical algorithms and software implementations of methods for assessing the security level of decentralized consensus protocols with special properties, as well as auxiliary cryptographic protocols with the appropriate level of security guarantees, have been developed. Developed mathematical models for determining the priority of processing cyberattacks/cyberincidents using methods of intellectual analysis. Special software has been created to conduct experimental research and effectively model the process of prioritizing

the processing of cyberattacks/cyberincidents.

Індекс УДК: , 621.391

Коди тематичних рубрик НТІ: 28.31.02

6. Науково-технічна продукція (НТП)

НТП 1

Назва продукції (укр): Аналіз протоколів та механізмів криптографічних перетворень для перехідного та постквантового періоду з урахуванням вимог стандартів та існуючих загроз.

Назва продукції (англ): Analysis of protocols and mechanisms of cryptographic transformations for the transitional and post-quantum period, taking into account the requirements of standards and existing threats.

Очікувані результати: Методи, теорії, Програмні продукти, Аналітичні матеріали

Галузь застосування: Технічні науки

Опис продукції (укр): Представлені аналітичні матеріали огляду алгоритмів постквантової криптографії, які можуть забезпечити надійний захист інформації в умовах використання квантових комп'ютерів. Доведено, що розробка та впровадження алгоритмів постквантової криптографії дозволять Україні убезпечити не лише інформацію, але й об'єкти критичної інфраструктури в умовах інформаційної війни та для потреб реальних бойових дій.

Соціально-економічна спрямованість НТП: Створення принципово нової продукції (матеріалів, технологій тощо) для забезпечення експортного потенціалу та заміщенню імпорту, Підвищення автоматизації виробничих процесів, Забезпечення промисловості чи населення новим видом інформаційно-комунікаційних послуг

Стадія завершеності НТП: Звіт по НДДКР

Впровадження НТП: Не впроваджено

Строки впровадження:

Виробник продукції: ХНУ імені В.Н.Каразіна

Споживачі продукції:

Перспективні ринки:

Права інтелектуальної власності: За договорами

Форми та умови передачі продукції: Спільні НДДКР

НТП 2

Назва продукції (укр): Математичні алгоритми та програмні імплементації методів оцінки рівня безпеки децентралізованих протоколів консенсусу із спеціальними властивостями, а також допоміжних криптографічних протоколів із відповідним рівнем гарантій безпеки.

Назва продукції (англ): Mathematical algorithms and software implementations of methods for assessing the security level of decentralized consensus protocols with special properties, as well as auxiliary cryptographic protocols with the appropriate level of security guarantees.

Очікувані результати: Методи, теорії, Програмні продукти, Аналітичні матеріали

Галузь застосування: Технічні науки

Опис продукції (укр): Оцінено стійкість хеш-функції Poseidon проти небінарного лінійного і диференціального криптоаналізу. Зауважимо, що для побудови таких оцінок використовуються серйозні алгебраїчні прийоми, зокрема деякі властивості сум характерів для адитивної групи скінченного поля та властивості сум таких характерів. Наведено загальні параметри для хеш-функції Poseidon, яка дозволяє використовувати цю хеш-функцію в рекурсивних SNARK-доказах на основі MNT-4 та MNT-6 триплетів. Показано, як вибрати S-блок для такої функції, щоб цей вибір був оптимальним з точки зору кількості констрейнтів і безпеки. Показано, скільки повних раундів буде достатньо, щоб гарантувати стійкість хеш-функції Poseidon від небінарних лінійних і диференціальних атак. Розраховано кількість констрейнтів на біт, що

досягається в запропонованій реалізації; було продемонстровано значний виграш у порівнянні з хеш-функцією Педерсена. Для всіх перерахованих результатів надаються формальні докази.

Соціально-економічна спрямованість НТП: Створення принципово нової продукції (матеріалів, технологій тощо) для забезпечення експортного потенціалу та заміщенню імпорту, Підвищення автоматизації виробничих процесів, Забезпечення промисловості чи населення новим видом інформаційно-комунікаційних послуг

Стадія завершеності НТП: Звіт по НДДКР

Впровадження НТП: Не впроваджено

Строки впровадження:

Виробник продукції: ХНУ імені В.Н.Каразіна

Споживачі продукції:

Перспективні ринки:

Права інтелектуальної власності: За договорами

Форми та умови передачі продукції: Спільні НДДКР

НТП 3

Назва продукції (укр): Математичні моделі визначення пріоритетності обробки кібератак/ кіберінцидентів з використанням методів інтелектуального аналізу

Назва продукції (англ): Mathematical models for determining the priority of processing cyber attacks or cyber incidents using methods of intellectual analysis

Очікувані результати: Методи, теорії, Програмні продукти, Аналітичні матеріали

Галузь застосування: Технічні науки

Опис продукції (укр): Запропонована модель ґрунтується на загальноприйнятих інструментах для визначення основних параметрів для пріоритизації, таких як Наказ Адміністрації Держспецзв'язку від 03.07.2023 № 570 «Про затвердження Методичних рекомендацій щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі» та Базових метрик Загальної системи оцінки вразливостей версії 3.1 (CVSS, Common Vulnerability Scoring System) американського Національного інституту стандартів та технологій (NIST, National Institute of Standards and Technology). Створено спеціальне програмне забезпечення для проведення експериментальних досліджень і ефективного моделювання процесу визначення пріоритетності обробки кібератак/ кіберінцидентів.

Соціально-економічна спрямованість НТП: Створення принципово нової продукції (матеріалів, технологій тощо) для забезпечення експортного потенціалу та заміщенню імпорту, Підвищення автоматизації виробничих процесів, Забезпечення промисловості чи населення новим видом інформаційно-комунікаційних послуг

Стадія завершеності НТП: Звіт по НДДКР

Впровадження НТП: Не впроваджено

Строки впровадження:

Виробник продукції: ХНУ імені В.Н.Каразіна

Споживачі продукції:

Перспективні ринки:

Права інтелектуальної власності: За договорами

Форми та умови передачі продукції: Спільні НДДКР

7. Бібліографічний опис

Rodinko, M., Oliynykov, R., Nastenko, A. (2024). Decentralized Proof-of-Burn auction for secure cryptocurrency upgrade. Blockchain: Research and Applications, 5(1), 100170. (Scopus).

Lyudmila Kovalchuk, Hanna Nelasa, Mariia Rodinko, and Oleksii Bespalov. A new extended strategy of processing of statistical

testing results. Proceedings of Information Technology and Implementation (IT&I-2024), November 20-21, 2024, Kyiv, Ukraine. (Scopus)

Lyudmila Kovalchuk, Mariia Rodinko, Roman Oliynykov, and Tatiana Klymenko. Using Chernoff bound to statistical tests independence checking. Proceedings of Information Technology and Implementation (IT&I-2024), November 20-21, 2024, Kyiv, Ukraine. (Scopus).

O. Kuznetsov, O. Peliukh, N. Poluyanenko, S. Bohucharskyi, and I. Kolovanova, “Comparative Analysis of Cryptographic Hash Functions in Blockchain Systems,” in Proceedings of the Cybersecurity Providing in Information and Telecommunication Systems II, V. Sokolov, T. Radivilova, V. Ustimenko, and M. Nazarkevych, Eds., in CEUR Workshop Proceedings, vol. 3550. Kyiv, Ukraine: CEUR, Oct. 2023, pp. 81–94. Accessed: Nov. 16, 2023. [Online]. Available: https://ceur-ws.org/Vol-3550/#paper7

Olena Tolstoluzka, Denys Telezhenko. Development and training of LSTM models for control of virtual distributed systems using TensorFlow and Keras, Radioelectronic and Computer Systems, 2024, (3(2024)), страницы 27–37 (Scopus).

Uzlov, D., Rukkas, K., Morozova, A., Kuznietcova, V., Chumachenko, D.OPTIMIZING INFORMATION SUPPORT TECHNOLOGY FOR NETWORK CONTROL: A PROBABILISTIC-TIME GRAPH APPROACH | ОПТИМІЗАЦІЯ ТЕХНОЛОГІЇ ІНФОРМАЦІЙНОЇ ПІДТРИМКИ УПРАВЛІННЯ МЕРЕЖЕЮ: ПІДХІД НА ОСНОВІ ЙМОВІРНІСНО-ЧАСОВИХ ГРАФІВ, Radioelectronic and Computer Systems, 2024, (2(110)), страницы 85–97 (Scopus).

Колованова, Є., Малахов, С., & Мелкозьорова, О. (2023). Поведінкові реакції HoneyNet на прикладах характерних мережевих атак. Збірник наукових праць □□ГО□, 145-152. URL: https://archive.logos-science.com/index.php/conference-proceedings/issue/view/14/14 Available at: https://doi.org/10.36074/logos-18.08.2023.040

Honcharov , M., Malakhov , S., & Kolovanova , I. (2023). Results of modeling different schemes of the spatial orientation and scanning series of base blocks of images to confront an unauthorized extraction of steganographic data. Computer Science and Cybersecurity, (2), 58-70. https://doi.org/10.26565/2519-2310-2023-2-06 (https://periodicals.karazin.ua/cscs/article/view/23122)

Малахов, С., Колованова, Є., & Гончаров, М. (2023). Особливості несанкціонованої екстракції стеганоконтенту при змінах просторового позиціювання опорних блоків контенту. Збірник наукових праць □□ГО□, 152-157. Available at: https://doi.org/10.36074/logos-26.05.2023.041

D. Uzlov, Ye. Havryliuk, I. Hushchyn, V. Strukov, S. Yakovlev. Handling outliers in swarm algorithms: a review // ProfIT AI 2024 4th International Workshop of IT-professionals on Artificial Intelligence 2024 Proceedings of the 4th International Workshop of IT-professionals on Artificial Intelligence (ProfIT AI 2024) 2024 Cambridge, MA, USA, September 25-27, 2024 (Scopus)

Lyudmila Kovalchuk, Roman Oliynykov, Mariia Rodinko. Probability of Double Spend Attack for PoS Consensus with Ouroboros Praos Slot Leader Election Procedure. Central European Conference on Cryptology 2024, Book of Abstracts, p. 46-49. (Scopus)

Колованова, Є., Мелкозьорова, О., & Малахов, С. Специфіка використання експлойтів та особливості протидії цій загрозі. Proceedings of the XXIX International Scientific and Practical Conference. Warsaw, Poland. 2023. Pp. 216-224. URL: https://isg-konf.com/wp-content/uploads/2023/07/Modern-scientific-trends-and-youth-development.pdf Available at: DOI 10.46299/ISG.2023.1.29

Колованова, Є., Малахов, С., & Чорна, Т. Передумови та основні складові з протидії доксінгу персональних даних.. Proceedings of the XXVII International Scientific and Practical Conference. Edmonton, Canada. 2023. Pp. 194-201. URL: https://isg-konf.com/wp-content/uploads/2023/07/trends-of-young-scientists-regarding-the-development-of-science.pdf DOI – 10.46299/ISG.2023.1.27

O.Pichugina, S.Yakovlev, D. Uzlov, O.Matsiy. Drone Swarm Monitoring: Novel Modeling Approaches//The 14th International Conference on Dependable Systems, Services and Technologies, DESSERT'2024, 11-13 October, 2024, Athens, Greece (Scopus)

Малахов, С., Мелкозьорова, О., & Колованова, Є. Результати спроб несанкціонованої екстракції відеоданих в умовах просторового перетворення опорних блоків стеганоконтенту. Proceedings of the XXVI International Scientific and Practical Conference. La Rochelle, France. 2023. Pp. 263-267. URL: https://isg-konf.com/scientific-trends-and-ways-of-solving-modern-problems/ DOI – 10.46299/ISG.2023.1.26

Мелкозьорова, О., Колованова, Є & Малахов, С. Імплементація рішення СЛАР з використанням QR-розподілу у MathCad

Prime. Proceedings of the XXVIII International Scientific and Practical Conference. Melbourne, Australia. 2023. Pp. 210-213 URL: https://isg-konf.com/wp-content/uploads/2023/07/SCIENCE-AND-DEVELOPMENT-OF-METHODS-FOR-SOLVING-MODERN-PROBLEMS.pdf DOI – 10.46299/ISG.2023.1.28

Чепель, Д., Малахов, С. & Колованова, Є. (2024). Огляд можливостей фільтрації DNS, як інструмента безпеки сучасних інформаційних систем. Grail of Science, (42), 395–398. https://doi.org/10.36074/grail-of-science.02.08.2024 (INTERNATIONAL SCIENTIFIC JOURNAL GRAIL OF SCIENCE № 42 (August, 2024) with the proceedings of the: III Correspondence International Scientific and Practical Conference SCIENCE IN MOTION: CLASSIC AND MODERN TOOLS AND METHODS IN SCIENTIFIC INVESTIGATIONS held on August 2nd

Толстолузька О. Г. та ін. Корисна модель. Канал вимірювання радіальної швидкості літальних апаратів з кибернетичним захистом отриманої інформації для мобільної одно-пунктної інформаційно-вимірювальної системи. Патент України на корисну модель № 152307, 11.01.2023, бюл. № 2

Толстолузька О. Г. та ін. Корисна модель. Канал вимірювання похилої дальності до літальних апаратів з кибернетичним захистом отриманої інформації для мобільної однопунктної інформаційно-вимірювальної системи. Патент України на корисну модель № 152306, 11.01.2023, бюл. № 2

Толстолузька О. Г. та ін. Корисна модель. Канал автоматичного суповодження літальних апаратів за напрямком з кибернетичним захистом отриманої інформації для мобільної однопунктної інформаційно-вимірювальної системи. Патент України на корисну модель № 152305, 11.01.2023, бюл. № 2

8. Звітна документація

Кількість сторінок в звіті: 20

Мова звіту: Українська

Кількість файлів у звіті: 1

9. Заключні відомості

Перелік осіб-виконавців

Артюх Олексій Анатолійович

Колованова Євгенія Павлівна (к. т. н.)

Олійников Роман Васильович (д. т. н., доцент)

Родінко Марія Юріївна (к. т. н.)

Скриннік Володимир Андрійович (н.с)

Узлов Дмитро Юрійович (к. т. н.)

Керівник організації:

Катрич Віктор Олександрович (д. ф.-м. н., пров.н.с.)

Керівники роботи:

Толстолузька Олена Геннадіївна (д. т. н., проф.)

Керівник відділу реєстрації наукової діяльності УкрІНТЕІ

Юрченко Т.А.