

Облікова картка ДіР



I. Загальні відомості

Державний обліковий номер: 0221U105824

Державний реєстраційний номер: 0121U112489

Особливі позначки: відкрита

Дата реєстрації: 02-09-2021

II. Етап виконання ДіР

Номер етапу: 1

Назва етапу: Отримання нового науково обґрунтованого знання з аналізу безпеки моніторингових систем, що використовують однорангові мережі, а також моделей, методів та алгоритмів взаємодії, зберігання та обробки даних, стійких до його можливого застосування. Розробка та дослідження криптографічних примітивів та протоколів взаємодії для побудови безпечних моніторингових систем запобігання поширенню інфекційних захворювань, що функціонують в умовах децентралізованої взаємодії.

Початок етапу: 05.2021

Закінчення етапу: 08.2021

Вид звітнього документа: Проміжний звіт

III. Відомості про виконавця ДіР

Повне найменування юридичної особи (або ПІБ фізичної особи): Харківський національний університет імені В. Н. Каразіна

Код за ЄДРПОУ: 02071205

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

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Розмір організації:

Телефон: 380577051247

IV. Відомості про співвиконавців ДіР

V. Відомості про замовника ДіР

Повне найменування юридичної особи (або ПІБ фізичної особи): Національний фонд досліджень України

Код за ЄДРПОУ: 42734019

Місцезнаходження: вул. Бориса Грінченка, 1, м. Київ, 01001, Україна

Форма власності:

Сфера управління: Кабінет Міністрів України

Ідентифікатор ROR: Не застосовується

Розмір організації:

Телефон: 380442981622, 380442981622

VI. Джерела, напрями та обсяги фінансування ДіР

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

Напрямок фінансування: 2.1 - фундаментальні дослідження

Джерела фінансування

7713 - кошти держбюджету

Код програмної класифікації видатків і кредитування (КПКВК): 2201300

Фактичний обсяг фінансування (тис. грн.): 3247.942

VII. Відомості про ДіР

Назва роботи українською:

Аналіз, дослідження, розробка та впровадження сучасних технологій інформаційної безпеки для глобального моніторингу кібернетичного простору України в умовах кризових та надзвичайних ситуацій

Назва роботи англійською:

Analysis, research, development and implementation of modern information security technologies for global monitoring of the cyberspace of Ukraine in crisis and emergency situations

Реферат українською:

Об'єкт дослідження – процеси забезпечення інформаційної та кібербезпеки, моделі, методи та механізми моніторингу кібернетичного простору України в умовах кризових та надзвичайних ситуацій. Предмет досліджень – технології інформаційної безпеки для глобального моніторингу кібернетичного простору України в умовах кризових та надзвичайних ситуацій. Метою НДР є аналіз та дослідження сучасних вимог та загроз національної безпеки в інформаційній сфері, обґрунтування, розробка та впровадження ефективних технологій захисту інформації для глобального моніторингу кібернетичного простору України в умовах кризових та надзвичайних ситуацій. Методи дослідження: методи теорії захисту інформації, криптології, сучасних протоколів та технологій комп'ютерних мереж та систем, теорії систем та системного аналізу, комп'ютерного та імітаційного моделювання тощо. В проміжному звіті наводяться результати з: аналізу безпеки моніторингових систем, що використовують однорангові мережі, а також моделей, методів та алгоритмів взаємодії, зберігання та обробки даних, стійких до його можливого застосування; розробки та дослідження криптографічних примітивів та протоколів взаємодії для побудови безпечних моніторингових систем запобігання поширенню інфекційних захворювань, що функціонують в умовах децентралізованої взаємодії.

Реферат англійською:

The object of research is the processes of providing information security and cybersecurity, models, methods and mechanisms for monitoring Ukraine cyberspace in crisis and emergency situations. The subject of research is information security technologies for global monitoring of Ukraine cyberspace in the crisis and emergency situations. The purpose of the work is to analyze and study modern requirements and threats to national security in the information sector, substantiation, development and implementation of effective information protection technologies for global monitoring of Ukraine cyberspace in crisis and emergency situations. Research methods are methods of information security theory, cryptology, modern protocols and technologies of computer networks and systems, systems theory and systems analysis, simulation, etc. The interim report presents the results of security analysis of monitoring systems using peer-to-peer networks, as well as models, methods and algorithms for interaction, storage and processing of data resistant to its possible application; development and research of cryptographic primitives and interaction protocols for the construction of secure monitoring systems that operate in the decentralized interaction to prevent the spread of infectious diseases.

Індекс УДК: 004.056.5

Коди тематичних рубрик: 20.56

Керівники роботи

Власне Прізвище Ім'я По-батькові: Олійников Роман Васильович

Науковий ступінь: д.т.н.

Вчене звання: професор

Ідентифікатор ORCID ID:

Додаткова інформація:

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

Назва НТП українською: Комплекс криптографічних протоколів для побудови децентралізованої приватної бази даних.

Назва НТП англійською: Complex of cryptographic protocols for creating decentralized private data base.

НТП, яку передбачалося створити:

Причини, через які НТП не було створено:

Отримані результати: Методи, теорії

Галузь застосування: Дослідження та розробки у галузі природничих та технічних наук

Реєстраційний номер картки технології:

Опис НТП: Комплекс криптографічних протоколів для побудови децентралізованої приватної бази даних орієнтований на моделі, методи та алгоритми КЗІ, що є необхідними для роботи додатків з відстеження контактів у моніторингових системах; запропоновані рішення враховують специфіку моніторингових систем, їх використання дозволить забезпечити достатній рівень анонімності.

Соціально-економічна спрямованість НТП: Поліпшення якості життя та здоров'я населення, ефективності діагностики та лікування хворих

Вплив НТП на довкілля:

Впровадження НТП: Впроваджено

Практична реалізація НТП

Початок етапу: 05.2021

Закінчення етапу: 08.2021

Споживачі продукції: Національний фонд України, Приватне акціонерне товариство "Інститут інформаційних технологій"

Перспективні ринки:

Характер співробітництва з інвестором

Потрібний обсяг інвестицій, тис. грн.:

Права, що надаються інвестору після завершення роботи:

Наявність бізнес-плану:

Техніко-економічне обґрунтування:

Потенціальний обсяг продажу, тис. грн.:

Очікуваний термін окупності (років):

Додаткова інформація:

Назва НТП українською: Результати критичного порівняння та аналізу існуючих протоколів консенсусу

Назва НТП англійською: Results of critical comparison and analysis of existing consensus protocols

НТП, яку передбачалося створити:

Причини, через які НТП не було створено:

Отримані результати: Методи, теорії

Галузь застосування: Дослідження та розробки у природничих та технічних наук

Реєстраційний номер картки технології:

Опис НТП: Результати критичного порівняння та аналізу існуючих протоколів консенсусу показують, що децентралізовані системи, побудовані у вигляді блокчейну, мають додаткові переваги, а крім того, за рахунок певних надбудов, можуть бути удосконалені за такими напрямками: підвищення надійності та стабільності зберігання, обробки та передачі інформації; підвищення швидкості зберігання, обробки та передачі інформації; підвищення ефективності пошуку інформації, розміщеної у багатьох незалежних, автономних однорангових системах.

Соціально-економічна спрямованість НТП: Поліпшення якості життя та здоров'я населення, ефективності діагностики та лікування хворих

Вплив НТП на довкілля:

Впровадження НТП: Впроваджено

Практична реалізація НТП

Початок етапу: 05.2021

Закінчення етапу: 08.2021

Споживачі продукції: Національний фонд досліджень України

Перспективні ринки:

Характер співробітництва з інвестором

Потрібний обсяг інвестицій, тис. грн.:

Права, що надаються інвестору після завершення роботи:

Наявність бізнес-плану:

Техніко-економічне обґрунтування:

Потенціальний обсяг продажу, тис. грн.:

Очікуваний термін окупності (років):

Додаткова інформація:

Назва НТП українською: Вимоги та умови практичного застосування криптографічних примітивів та протоколів взаємодії для побудови системи запобігання поширенню інфекційних захворювань. Механізми економічного стимулювання підключення до системи й активної взаємодії.

Назва НТП англійською: Requirements and conditions for practical application of cryptographic approaches and interaction protocols for developing a system to prevent the spread of infectious diseases. Mechanisms of economic stimulation of connection to the system and active interaction.

НТП, яку передбачалося створити:

Причини, через які НТП не було створено:

Отримані результати: Методи, теорії

Галузь застосування: Дослідження та розробки у природничих та технічних наук

Реєстраційний номер картки технології:

Опис НТП:Вимоги та умови практичного застосування криптографічних примітивів та протоколів взаємодії для побудови системи запобігання поширенню інфекційних захворювань, механізми економічного стимулювання підключення до системи й активної взаємодії носять комплексний характер та враховують не тільки вимоги на параметри окремих алгоритмів та протоколів, а і повний комплект організаційних та технічних заходів; є повністю математично обґрунтованими та оновленими відповідно до сьогоденних вимог до криптографічної стійкості; для кожного криптографічного примітиву рівень стійкості визначався індивідуально, що дає можливість гарантувати загальну стійкість комплексу всіх криптографічних примітивів, що плануються до використання.

Соціально-економічна спрямованість НТП: Поліпшення якості життя та здоров'я населення, ефективності діагностики та лікування хворих

Вплив НТП на довкілля:

Впровадження НТП: Впроваджено

Практична реалізація НТП

Початок етапу: 05.2021

Закінчення етапу: 08.2021

Споживачі продукції: Національний фонд досліджень України

Перспективні ринки:

Характер співробітництва з інвестором

Потрібний обсяг інвестицій, тис. грн.:

Права, що надаються інвестору після завершення роботи:

Наявність бізнес-плану:

Техніко-економічне обґрунтування:

Потенціальний обсяг продажу, тис. грн.:

Очікуваний термін окупності (років):

Додаткова інформація:

Назва НТП українською: Протоколи взаємодії для побудови системи моніторингу.

Назва НТП англійською: Interaction protocols for building the monitoring system.

НТП, яку передбачалося створити:

Причини, через які НТП не було створено:

Отримані результати: Методи, теорії

Галузь застосування: Дослідження та розробки у природничих та технічних наук

Реєстраційний номер картки технології:

Опис НТП: Протоколи взаємодії для побудови системи моніторингу носять комплексний характер. Проактивність рішень (до компрометації елементів мережі) забезпечується використанням моделі моніторингу мережі з реалізацією принципів балансування навантаження за рахунок врахування параметрів завантаженості ресурсів мережі.

Соціально-економічна спрямованість НТП: Поліпшення якості життя та здоров'я населення, ефективності діагностики та лікування хворих

Вплив НТП на довкілля:

Впровадження НТП: Впроваджено

Практична реалізація НТП

Початок етапу: 05.2021

Закінчення етапу: 08.2021

Споживачі продукції: Національний фонд досліджень України

Перспективні ринки:

Характер співробітництва з інвестором

Потрібний обсяг інвестицій, тис. грн.:

Права, що надаються інвестору після завершення роботи:

Наявність бізнес-плану:

Техніко-економічне обґрунтування:

Потенціальний обсяг продажу, тис. грн.:

Очікуваний термін окупності (років):

Додаткова інформація:

Назва НТП українською: Результати оцінки безпеки протоколів та криптографічних перетворень, які можуть застосовуватися при відстеженні контактів. Пропозиції та рекомендації щодо створення дублюючої системи оповіщення населення про надзвичайні події у регіоні та небезпеки в зоні перебування людини

Назва НТП англійською: Results of security assessment of protocols and cryptographic conversions which can be used for contact detection. Proposals and recommendations on creation of a duplicate system of informing the population about extraordinary events in the region and hazards in the area of people's stay

НТП, яку передбачалося створити:

Причини, через які НТП не було створено:

Отримані результати: Методи, теорії

Галузь застосування: Дослідження та розробки у природничих та технічних наук

Реєстраційний номер картки технології:

Опис НТП: Результати оцінки безпеки протоколів та криптографічних перетворень комплексно враховують різні підходи до формалізованого опису моделей безпеки, а також моделей криптографічних примітивів та криптографічних систем. На підставі отриманих результатів з оцінки безпеки протоколів та криптографічних перетворень розроблено пропозиції та рекомендації щодо створення дублюючої системи оповіщення населення про надзвичайні події у регіоні та небезпеки в зоні перебування людини.

Соціально-економічна спрямованість НТП: Поліпшення якості життя та здоров'я населення, ефективності діагностики та лікування хворих

Вплив НТП на довкілля:

Впровадження НТП: Впроваджено

Практична реалізація НТП

Початок етапу: 05.2021

Закінчення етапу:08.2021

Споживачі продукції: Національний фонд досліджень України

Перспективні ринки:

Характер співробітництва з інвестором

Потрібний обсяг інвестицій, тис. грн.:

Права, що надаються інвестору після завершення роботи:

Наявність бізнес-плану:

Техніко-економічне обґрунтування:

Потенціальний обсяг продажу, тис. грн.:

Очікуваний термін окупності (років):

Додаткова інформація:

Назва НТП українською: Методи моніторингу та аналізу мультифрактальних та рекурентних характеристик мережного трафіка.

Назва НТП англійською: Methods for monitoring and analysis of multifractal and recurrent characteristics of the network traffic

НТП, яку передбачалося створити:

Причини, через які НТП не було створено:

Отримані результати: Методи, теорії

Галузь застосування: Дослідження та розробки у природничих та технічних наук

Реєстраційний номер картки технології:

Опис НТП: Методи моніторингу та аналізу мережного трафіка враховують мультифрактальні характеристики трафіка та ймовірність виявлення вторгнень

Соціально-економічна спрямованість НТП: Поліпшення якості життя та здоров'я населення, ефективності діагностики та лікування хворих

Вплив НТП на довкілля:

Впровадження НТП: Впроваджено

Практична реалізація НТП

Початок етапу: 05.2021

Закінчення етапу: 08.2021

Споживачі продукції: Національний фонд досліджень України

Перспективні ринки:

Характер співробітництва з інвестором

Потрібний обсяг інвестицій, тис. грн.:

Права, що надаються інвестору після завершення роботи:

Наявність бізнес-плану:

Техніко-економічне обґрунтування:

Потенціальний обсяг продажу, тис. грн.:

Очікуваний термін окупності (років):

Додаткова інформація:

Назва НТП українською: Методи виявлення вторгнень на підставі аналізу сигнатур та аномалій в поведінці (зміні стану) мережі.

Назва НТП англійською: Methods for detecting intrusions based on the analysis of signatures and anomalies in the behavior (status changes) of the network.

НТП, яку передбачалося створити:

Причини, через які НТП не було створено:

Отримані результати: Методи, теорії

Галузь застосування: Дослідження та розробки у природничих та технічних наук

Реєстраційний номер картки технології:

Опис НТП: Методи виявлення вторгнень на підставі аналізу сигнатур та аномалій в поведінці (зміні стану) мережі засновано на статистичних характеристиках трафіка та поведінкових характеристиках трафіка та системи, що забезпечує комплексний аналіз даних як трафіка, так зміни в поведінці системи.

Соціально-економічна спрямованість НТП: Поліпшення якості життя та здоров'я населення, ефективності діагностики та лікування хворих

Вплив НТП на довкілля:

Впровадження НТП: Впроваджено

Практична реалізація НТП

Початок етапу: 05.2021

Закінчення етапу: 08.2021

Споживачі продукції: Національний фонд досліджень України

Перспективні ринки:

Характер співробітництва з інвестором

Потрібний обсяг інвестицій, тис. грн.:

Права, що надаються інвестору після завершення роботи:

Наявність бізнес-плану:

Техніко-економічне обґрунтування:

Потенціальний обсяг продажу, тис. грн.:

Очікуваний термін окупності (років):

Додаткова інформація:

IX. Бібліографічний опис

Kuznetsov, A.A., Potii, O.V., Poluyanenko, N.A., Gorbenko, Y.I., Kryvinska, N.: Stream Ciphers in Modern Real-time IT Systems: Analysis, Design and Comparative Studies. Springer International Publishing (2022).

<https://doi.org/10.1007/978-3-030-79770-6>.

Lemeshko O., Yeremenko O., Yevdokymenko M., Radivilova T. (2021) Research of the QoE Fast ReRouting Processes with Differentiated R-Factor Maximization for VoIP-Flows Using the Tensor Model of the Corporate Telecommunication Network. In: Vorobiyenko P., Ilchenko M., Strelkovska I. (eds) Current Trends in Communication and Information Technologies. IPF 2020. Lecture Notes in Networks and Systems, vol 212. pp. 95–110. Springer, Cham. https://doi.org/10.1007/978-3-030-76343-5_6.

Kuznetsov, A., Poluyanenko, N., Kiian, A.: Fundamentals of Functioning of Global Contact Monitoring Systems in the Context of COVID-19 Spread Prevention. In: Vorobiyenko, P., Ilchenko, M., and Strelkovska, I. (eds.) Current Trends in Communication and Information Technologies. pp. 311–328. Springer International Publishing, Cham (2021). https://doi.org/10.1007/978-3-030-76343-5_16.

Kirichenko L., Zinchenko P., Radivilova T. (2021) Classification of Time Realizations Using Machine Learning Recognition of Recurrence Plots. In: Babichev S., Lytvynenko V., Wójcik W., Vyshemyrskaya S. (eds) Lecture Notes in Computational Intelligence and Decision Making. ISDMCI 2020. Advances in Intelligent Systems and Computing, vol 1246. Springer, Cham. https://doi.org/10.1007/978-3-030-54215-3_44

Poluyanenko, N., Kuznetsov, A., Lisickiy, K., Datsenko, S., Nakisko, O., Rudenko, S.: The Problem of Double Costs in Blockchain Systems. In: Hu, Z., Petoukhov, S., Dychka, I., and He, M. (eds.) Advances in Computer Science for Engineering and Education III. pp. 640–652. Springer International Publishing, Cham (2021). https://doi.org/10.1007/978-3-030-55506-1_57

Krasnobayev, V., Kuznetsov, A., Yanko, A., Akhmetov, B., Kuznetsova, T., 2021. Processing of the Residuals of Numbers in Real and Complex Numerical Domains, in: Radivilova, T., Ageyev, D., Kryvinska, N. (Eds.), Data-Centric Business and Applications, Lecture Notes on Data Engineering and Communications Technologies. Springer International Publishing, Cham, pp. 529–555. https://doi.org/10.1007/978-3-030-43070-2_24

Технології інформаційної безпеки в децентралізованих розподілених мережах : монографія / Л. Ковальчук, Р. Олійников, Ю. Беспалов та ін.; за загальною редакцією Р. Олійникова, О. Кузнецова та О. Лемешка. – Харків: Видавництво «Форт», 2021. – 308 с.

О. О. Кузнецов, М. О. Полуяненко, В. А. Краснобаєв, С. О. Кошман. Довідник термінів і визначень технології блокчейн / уклад. О. О. Кузнецов, М. О. Полуяненко, В. А. Краснобаєв, С. О. Кошман. Харків: ХНУ імені В. Н. Каразіна, 2020. 48 с.

В. А. Краснобаєв, С. О. Кошман, О. О. Кузнецов, М. О. Полуяненко. Непозиційна система числення в залишкових класах: довідник термінів і визначень / уклад. В. А. Краснобаєв, С. О. Кошман, О. О. Кузнецов, М. О. Полуяненко. – Харків : ХНУ ім. В. Н. Каразіна, 2020. – 36 с.

Kovalchuk L., Oliynykov R., Rodinko M. Security of the Poseidon Hash Function Against Non-Binary Differential and Linear Attacks // Cybernetics and Systems Analysis. – 2021. – Т. 57. – №. 2. – С. 268–278.

Radivilova T., Kirichenko L., Lemeshko O., Ageyev D., Tawalbeh M., Ilkov A. "Analysis of Approaches of Monitoring, Intrusion Detection and Identification of Network Attacks," 2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T), 2020, pp. 819–822, doi: 10.1109/PICST51311.2020.9467973.

Lyudmila Kovalchuk, Mariia Rodinko, and Roman Oliynykov. 2020. Upper Bound Probability of Double Spend Attack on SPECTRE. In CryBlock '20:3rd Workshop on Cryptocurrencies and Blockchains for Distributed Systems, September 25th, 2020, Virtual (online) Conference.ACM, New York, NY, USA.

Kuznetsov, A., Kryvinska, N., Kiian, A., Smirnov, O., Kuznetsova, K.: Full Non-Binary Constant-Weight Codes. SN COMPUT. SCI. 2, 337 (2021). <https://doi.org/10.1007/s42979-021-00739-w>.

Х. Заключні відомості

Керівник юридичної особи

Катрич Віктор Олександрович

д. ф.-м. н.

Перелік осіб-виконавців

Іваненко Дмитро Вікторович

(к. т. н.)

Агеев Дмитро Володимирович

(д.т.н., 05.12.02)

Беспалов Юрій Миколайович

(к. т. н.)

Горбенко Юрій Іванович

(к. т. н.)

Ковальчук Людмила Василівна

(д. т. н.)

Кошман Сергій Олександрович

(д. т. н.)

Краснобаєв Віктор Анатолійкович

(д. т. н.)

Кузнецов Олександр Олександрович

(д. т. н.)

Кузнецова Тетяна Юріївна

Кіян Анастасія Сергіївна

Лемешко Олександр Віталійович

(д. т. н., 05.12.02)

Полуяненко Микола Олександрович

(к. т. н.)

Радівілова Тамара Анатоліївна

(к. т. н.)

Родінко Марія Юріївна

Відповідальний за підготовку облікових документів

Майстренко Людмила Олексіївна

Телефон

+38 (057) 707-55-23

Реєстратор

**Керівник відділу УкрІНТЕІ, що є
відповідальним за реєстрацію наукової
діяльності**

