Облікова картка ДіР

Image not found or type unknow

I. Загальні відомості

Державний обліковий номер: 0221U105298

Державний реєстраційний номер: 0121U107879

Особливі позначки: відкрита

Дата реєстрації: 25-06-2021

II. Етап виконання ДіР

Номер етапу: 1

Назва етапу: Подальший розвиток теорії побудови системи забезпечення інформаційної безпеки, підвищення рівня інформаційної безпеки за рахунок розроблення та впровадження відповідної методології в умовах постквантової криптографії

Початок етапу: 09.2020

Закінчення етапу: 06.2021

Вид звітного документа: Проміжний звіт

III. Відомості про виконавця ДіР

Повне найменування юридичної особи (або ПІБ фізичної особи): Харківський національний економічний університет імені Семена Кузнеця

Код за ЄДРПОУ: 02071211

Місцезнаходження: проспект Науки, буд. 9-а, м. Харків, Харківський р-н., Харківська обл., 61166, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Розмір організації:

Телефон: 380577020304, 380577020717

IV. Відомості про співвиконавців ДіР

V. Відомості про замовника ДіР

Повне найменування юридичної особи (або ПІБ фізичної особи): Харківський національний економічний університет імені Семена Кузнеця

Код за ЄДРПОУ: 02071211

Місцезнаходження: проспект Науки, буд. 9-а, м. Харків, Харківський р-н., Харківська обл., 61166, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Розмір організації:

Телефон: 380577020304

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:

Методологічні основи побудов систем захисту інформації в умовах постквантової криптографії

Назва роботи англійською:

Methodological foundations of building information security systems in post-quantum cryptography

Реферат українською:

Об’єкт роботи – розвиток технологій та практичних методик побудови систем захисту інформації. Предмет дослідження – системи захисту інформації. Метою дослідження є формування методологічних основ побудов систем захисту інформації в умовах постквантової криптографії. У роботі наведено шляхи формування методологічних основ побудов систем захисту інформації в умовах постквантової криптографії, враховано системи критичної інфраструктури, застосування стандарту блочно-симетричного шифрування (БСШ) ГОСТ 28147-89 в режимі OFB, виконано аналіз мереж Wi-Fi та математичні властивості обробки даних відповідно до застосування радіохвильового обладнання.

Реферат англійською:

The object of work is the development of technologies and practical methods of building information security systems. The subject of research – information security systems. The aim of the research is to form the methodological bases of constructing information security systems in the conditions of post-quantum cryptography. The paper presents ways of forming methodological bases of constructing information security systems in post-quantum cryptography, considers critical infrastructure systems, application of standard block-symmetric encryption (BSE) GOST 28147-89 in OFB mode, analyzes of Wi-Fi networks and mathematical properties of data processing respectively before the use of radio wave equipment.

Індекс УДК: 65.012.8; 003.26; 004.56.5

Коди тематичних рубрик: 20.53.37

Керівники роботи

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

Науковий ступінь: д.пед.н.

Вчене звання: професор

Ідентифікатор ORCID ID:

Додаткова інформація:

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

Назва НТП українською: Методологічні основи побудов систем захисту інформації в умовах постквантової криптографії

Назва НТП англійською: НТП англійською Methodological bases of constructions of information protection systems in the conditions of postquantum cryptography

НТП, яку передбачалося створити:

Причини, через які НТП не було створено:

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

Галузь застосування: Подальший розвиток теорії побудови системи забезпечення інформаційної безпеки, підвищення рівня інформаційної безпеки за рахунок розроблення та впровадження відповідної методології в умовах постквантової криптографії

Реєстраційний номер картки технології:

Опис НТП: На основі запропонованих моделей значно скорочуються вимоги до обчислювальних ресурсів для отримання поточного стану інформаційної безпеки (ІБ), з урахуванням вимог міжнародних регуляторів і національних нормативних актів. Запропонований підхід дозволить проводити самооцінку стану ІБ, формувати превентивні заходи і системи захисту інформації на основі аналізу критичних точок в елементах інфраструктури, з урахуванням відповідних взаємозв'язків. Пропонується модифікація відомого алгоритму ГОСТ28147-89, який забезпечує "усунення" можливих кріптозакладок і підвищення криптостійко-сті в умовах постквантового періоду (поява повномасштабного квантового комп'ютера, який дозволяє зламати на основі алгоритмів Гровера і Шора сучасні симетричні і несиметричні криптосистеми). Проведено динамічний аналіз стану кібербезпеки галузей, які найчастіше піддаються кібератакам. Класифіковано основні рекомендації спеціалістів щодо заходів з кібербезпеки. Розглянуто особливості відомих методів шифрування в безпроводовій мережі Wi-Fi. Проаналізовано їх відмінності з точки зору криптостійкості, вразливостей і наслідків проведених атак. Зроблено висновок про можливість використання алгоритму шифрування WPA3 різними групами користувачів безпроводових мереж. Визначено роль рішень конкурсу NIST щодо ступеню значущості його впливу на розвиток методів синтезу і аналізу нових квантово-стійких криптографічних схем. Обґрунтовано необхідність оцінювання ступеня зниження точності вимірювання інформативних параметрів радіолокаційного сигналу в реальних умовах його поширення та відбиття. Результати оцінювання дозволять ви-значити вимоги для оптимізації такого вимірювання для забезпечення необхідної ефективності.

Соціально-економічна спрямованість НТП: Покращення існуючих систем захисту інформації.

Вплив НТП на довкілля:

Впровадження НТП: Впроваджено

Практична реалізація НТП

Початок етапу:

Закінчення етапу:

Споживачі продукції:

Перспективні ринки:

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

X. Заключні відомості

Керівник юридичної особи Пономаренко Володимир Степанович
д. е. н.

Перелік осіб-виконавців

Євсеєв Сергій Петрович
(д.т.н., 13.00.04)

Алексієв Володимир Олегович
(д.т.н., 05.22.01)

Гаврилова Алла Андріївна

Король Ольга Григорієвна
(к.т.н.)

Корольов Роман Володимирович
(к.т.н.)

Мілов Олександр Володимирович
(д.т.н., 05.09.12)

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

Ткачов Андрій Михайлович
(к.т.н.)

Хвостенко Владислав Сергійович
(к. е. н.)

Відповідальний за підготовку облікових документів Шелкунова Наталія Леонідівна

Телефон +38 (057) 702-06-70

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності

