

Облікова картка ДіР



I. Загальні відомості

Державний обліковий номер: 0220U103654

Державний реєстраційний номер: 0119U103662

Особливі позначки: відкрита

Дата реєстрації: 31-10-2020

II. Етап виконання ДіР

Номер етапу: 1

Назва етапу: Розробка методів генерування бінарних псевдовипадкових послідовностей з підвищеною криптографічною стійкістю на основі динамічного хаосу

Початок етапу: 09.2019

Закінчення етапу: 06.2020

Вид звітнього документа: Остаточний звіт

III. Відомості про виконавця ДіР

Повне найменування юридичної особи (або ПІБ фізичної особи): Одеська національна академія зв'язку ім. О.С. Попова

Код за ЄДРПОУ: 01180116

Місцезнаходження: Кузнечна вулиця, 1, м. Одеса, Одеська обл., 65029, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Розмір організації:

Телефон: 0487050411, 0487050454

IV. Відомості про співвиконавців ДіР

V. Відомості про замовника ДіР

Повне найменування юридичної особи (або ПІБ фізичної особи): Одеська національна академія зв'язку ім. О.С. Попова

Код за ЄДРПОУ: 01180116

Місцезнаходження: Кузнечна вулиця, 1, м. Одеса, Одеська обл., 65029, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Розмір організації:

Телефон: 0487050411

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)

Напрямок фінансування: 2.2 - прикладні дослідження і розробки

Джерела фінансування

7704 - власні кошти, кошти підприємств, установ, організацій, фізичної особи на виконання ініціативних робіт

Фактичний обсяг фінансування (тис. грн.): 10.22
--

VII. Відомості про ДіР

Назва роботи українською:

Розробка методів генерування бінарних псевдовипадкових послідовностей з підвищеною криптографічною стійкістю на основі динамічного хаосу

Назва роботи англійською:

Development of methods for generating binary pseudorandom sequences with enhanced cryptographic stability based on dynamic chaos

Реферат українською:

Розробка методів генерування бінарних псевдовипадкових послідовностей з підвищеною криптографічною стійкістю на основі динамічного хаосу. Дослідження якості генерування послідовностей за допомогою статистичних тестів NIST.

Реферат англійською:

Development of methods for generating binary pseudo-random sequences with increased cryptographic stability based on dynamic chaos. Investigation of the quality of sequence generation using NIST statistical tests.

Індекс УДК: 004.056:061.68; 004.3.75:061.68, 004.056

Коди тематичних рубрик: 50.37.21

Керівники роботи

Власне Прізвище Ім'я По-батькові: Захарченко Микола Васильович

Науковий ступінь: д. т. н.

Вчене звання: професор

Ідентифікатор ORCID ID:

Додаткова інформація:

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

Назва НТП українською: Розробка методів генерування бінарних псевдовипадкових послідовностей з підвищеною криптографічною стійкістю на основі динамічного хаосу

Назва НТП англійською: Development of methods for generating binary pseudo-random sequences with increased cryptographic stability based on dynamic chaos

НТП, яку передбачалося створити:

Причини, через які НТП не було створено:

Отримані результати: Методи, теорії

Галузь застосування: Кібербезпека, захист інформації

Реєстраційний номер картки технології:

Опис НТП: Розробка методів генерування бінарних псевдовипадкових послідовностей з підвищеною криптографічною стійкістю на основі динамічного хаосу. Дослідження якості генерування послідовностей за допомогою статистичних тестів NIST.

Соціально-економічна спрямованість НТП: Дослідження якості генерування псевдовипадкових послідовностей за допомогою відомих математичних виразів генераторів хаосу за допомогою тестів NIST

Вплив НТП на довкілля:

Впровадження НТП: Впроваджено

Практична реалізація НТП

Початок етапу: 09.2019

Закінчення етапу: 06.2020

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 обґрунтування:

Потенціальний обсяг продажу, тис. грн.:

Очікуваний термін окупності (років):

Додаткова інформація:

Назва НТП українською: Розробка методів генерування бінарних псевдовипадкових послідовностей з підвищеною криптографічною стійкістю на основі динамічного хаосу

Назва НТП англійською: Development of methods for generating binary pseudo-bad messages with advanced cryptographic style on the basis of dynamic chaos

НТП, яку передбачалося створити:

Причини, через які НТП не було створено:

Отримані результати: Методи, теорії

Галузь застосування: Кібербезпека та теорія захисту інформації

Реєстраційний номер картки технології:

Опис НТП: Розглянуто генератори і дана якісна оцінка по формуванню на їх основі бінарної псевдовипадкової послідовності. Виконано тестування генераторів псевдовипадкових чисел за допомогою системи NIST. Запропоновано методи поліпшення статистичних властивостей генераторів хаосу. Проведено порівняльний аналіз генераторів псевдовипадкових чисел на основі статистичних тестів NIST для визначення генератора з кращими статистичними властивостями. Розроблений метод генерування гами послідовностей дозволяє поліпшити статистичні характеристики бінарних послідовностей, які формуються на основі різних генераторів хаосу

Соціально-економічна спрямованість НТП: Підвищення криптографічної стійкості систем потокового шифрування.

Вплив НТП на довкілля:

Впровадження НТП: Впроваджено

Практична реалізація НТП

Початок етапу: 09.2019

Закінчення етапу: 06.2020

Споживачі продукції: ОНАЗ ім. О.С. Попова

Перспективні ринки: Україна

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

Korchynskiy V.V. Methods for generating noise-like timer signals based on pseudo-random tuning of the operating frequency / Korchynskiy V.V., Kildishev V.I., Berdnikov A.M., Bielova I.V. // Наукові праці ОНАЗ ім. О.С. Попова. – 2019, № 2. – С.

Korchynskiy V.V., The methods of forming noise-like timer signals based on The random rebuilding of the operating frequency / Korchynskiy V.V., Kildishev V.I., Berdnikov A.M., Bielova I.V. // Наукові праці ОНАЗ ім. О.С. Попова. – 2019, № 3. – С.

Korchynskiy Volodymyr The generating random sequences with the increased cryptographic strength / Volodymyr Korchynskiy, Vitalii Kildishev, Oleksandr Riabukha, Oleksandr Berdnikov // IAPGOS, 1/2020, 20–23 (Польща)

Х. Заключні відомості

Керівник юридичної особи

Воробієнко Петро Петрович

д. т. н., 05.12.13

Перелік осіб-виконавців

Бердніков Олександр Михайлович

Валигурський Юрій Петрович

Голев Денис Володимирович

Захарченко Микола Васильович

(д.т.н.)

Корчинський Володимир Вікторович

(д.т.н.)

Кільдішев Віталій Йосипович

Поліщук Кирил Вадимович

Відповідальний за підготовку

Грішина Олена Вікторівна

облікових документів

Телефон

+38 (048) 705-04-64

Реєстратор

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

