Облікова картка НДДКР

Державний обліковий номер: 0220U101910

Державний реєстраційний номер: 0119U100071

Відкрита

Дата реєстрації: 27-02-2020

1. Етапи виконання

Номер етапу: 1

Назва етапу: Виконання НДР

Початок етапу: 12-2018

Закінчення етапу: 12-2019

Вид звітного документа: Остаточний звіт

2. Виконавець

Назва організації: Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського "

Код ЄДРПОУ/ІПН: 34979237

Підпорядкованість: Адміністрація державної служби спеціального зв'язку та захисту інформації

Адреса: вул. Верхньоключова, 4, 27 корпус, м. Київ, Київська обл., 03056, Україна

Телефон: 380442049151

E-mail: iszzi@iszzi.kpi.ua

WWW: http://iszzi.kpi.ua

3. Власник результатів НДДКР (продукції)

Назва організації: Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського "

Код ЄДРПОУ/ІПН: 34979237

Адреса: вул. Верхньоключова, 4, 27 корпус, м. Київ, Київська обл., 03056, Україна

Підпорядкованість: Адміністрація державної служби спеціального зв'язку та захисту інформації

Телефон: 380442049151

E-mail: iszzi@iszzi.kpi.ua

WWW: http://iszzi.kpi.ua

4. Джерела та напрями фінансування

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

КПКВК:

Напрям фінансування: 2.2 - прикладні дослідження і розробки

Джерела фінансування

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

Фактичний обсяг фінансування за звітний етап: 0 тис. грн.

5. Науково-технічна робота

Назва роботи (укр)

Дослідження варіантів реалізації криптографічних алгоритмів ДСТУ 7624 та ДСТУ 7564 в середовищі різних операційних систем

Назва роботи (англ)

Research of variants of realization of cryptographic algorithms SSU 7624 and SSU 7564 using environment of different operating systems

Реферат (укр)

Звіт про НДР: 56 с., 14 табл., 27 джерел. КРИПТОГРАФІЧНА СИСТЕМА, КРИПТОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ, БЛОКОВИЙ ШИФР, ПРОГРАМНА РЕАЛІЗАЦІЯ Об'єкт дослідження – проведення експертизи криптографічних алгоритмів, що використовуються в спеціальних системах зв'язку України. Мета роботи – дослідження існуючих та створення нових реалізацій стандартів шифрування з точки зору їх використання для проведення експертизи, застосування отриманих результатів при вивченні навчальних дисциплін спеціальної кафедри № 1. Методи дослідження – аналіз відомих реалізацій криптографічних алгоритмів, визначених державними стандартами ДСТУ 7624 та ДСТУ 7564 та розроблення власної реалізації зазначених криптографічних алгоритмів. Робота спрямована на вирішення наукового завдання, суть якого полягає в розробці методів для покращення експертизи криптографічних засобів в Україні, що включає в себе: розробку та аналіз власної реалізації криптографічного алгоритму, визначеного національним стандартом ДСТУ 7624:2014 розробку та аналіз власної реалізації криптографічного алгоритму, визначеного національним стандартом ДСТУ 7564:2014 Отримані в науково-дослідній роботі результати можуть бути використані в освітньому процесі спеціальної кафедри № 1 під час проведення лекцій та практичних занять з навчальних дисциплін "Основи криптографії", "Математичні методи побудови та аналізу симетричних криптосистем", "Математичні методи побудови та аналізу асиметричних криптосистем", "Криптографічні протоколи".

Реферат (англ)

SRW Report: 56 pp., 14 tables, 27 sources. CRYPTOGRAPHIC SYSTEM, CRYPTOGRAPHIC INFORMATION SECURITY, BLOCK CODE, SOFTWARE REALIZATION The object of the study is to conduct an examination of the cryptographic algorithms used in special communication systems of Ukraine. The purpose of the work is to study the existing and create new implementations of the encryption standards in terms of their usage for examination, application of the obtained results in the study of disciplines of the special department № 1. Research methods - analysis of known implementations of cryptographic algorithms defined by state standards DSTU 7624 and DSTU 7564 and development of own implementation of these cryptographic algorithms. The work is aimed at solving a scientific problem, the essence of which is to develop methods for improving the expertise of cryptographic tools in Ukraine, which includes: development and analysis of own implementation of cryptographic algorithm defined by national standard DSTU 7624: 2014 development and analysis of own implementation of cryptographic algorithm defined by national standard DSTU 7564: 2014 The results obtained in the research work can be used in the educational process of the special department # 1 during lectures and practical training in the disciplines "Fundamentals of cryptography", "Mathematical methods for constructing and analyzing symmetric cryptosystems", "Mathematical methods for constructing and analyzing asymmetric cryptosystems" "," Cryptographic Protocols ".

Індекс УДК:

Коди тематичних рубрик НТІ: 20.56.01

6. Науково-технічна продукція (НТП)

НТП 1

Назва продукції (укр): ДОСЛІДЖЕННЯ ВАРІАНТІВ РЕАЛІЗАЦІЇ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ ДСТУ 7624 ТА ДСТУ 7564 В СЕРЕДОВИЩІ РІЗНИХ ОПЕРАЦІЙНИХ СИСТЕМ

Назва продукції (англ):

Очікувані результати: Програмні продукти

Галузь застосування: Криптографічний захист інформації

Опис продукції (укр): Аналіз відомих реалізацій криптографічних алгоритмів, визначених державними стандартами ДСТУ 7624 та ДСТУ 7564 та розроблення власної реалізації зазначених криптографічних алгоритмів.

Соціально-економічна спрямованість НТП: Робота спрямована на вирішення наукового завдання, суть якого полягає в розробці методів для покращення експертизи криптографічних засобів в Україні, що включає в себе: розробку та аналіз власної реал

Стадія завершеності НТП: Звіт по НДДКР

Впровадження НТП: Не впроваджено

Строки впровадження:

Виробник продукції: ІСЗЗІ КПІ ім. Ігоря Сікорського

Споживачі продукції:

Перспективні ринки:

Права інтелектуальної власності: У відкритому доступі

Форми та умови передачі продукції: У відкритому доступі

7. Бібліографічний опис

8. Звітна документація

Кількість сторінок в звіті: 56

Мова звіту: Українська

Умови поширення в Україні: Не заборонено

Умови передачі іншим країнам: Не заборонено

Кількість файлів у звіті: 1

9. Заключні відомості

Керівник організації:

Пучков Олександр Олександрович (к. філос. н., професор)

Керівники роботи:

Конюшок Сергій Миколайович (к. т. н., доц.)

Керівник відділу реєстрації наукової діяльності УкрІНТЕІ

Юрченко Т.А.