# Облікова картка НДДКР

**Державний обліковий номер:** 0219U004677

**Державний реєстраційний номер:** 0119U002864

**Відкрита**

**Дата реєстрації:** 30-09-2019

## 1. Етапи виконання

**Номер етапу:** 1

**Назва етапу:** Програмний модуль псевдонедетермінованих криптографічних перетворень для технологій розподіленого реєстру

**Початок етапу:** 05-2019

**Закінчення етапу:** 08-2019

**Вид звітного документа:** Остаточний звіт

## 2. Виконавець

**Назва організації:** Вінницький національний технічний університет

**Код ЄДРПОУ/ІПН:** 02070693

**Підпорядкованість:** Міністерство освіти і науки України

**Адреса:** 21021 м. Вінниця, вул. Хмельницьке шосе, 95

**Телефон:** (0432) 51-15-81

**Телефон:** (0432) 51-15-81

**E-mail:** vntu@vntu.edu.ua

**Інше:** vntu.edu.ua

## 3. Власник результатів НДДКР (продукції)

**Назва організації:** "Інтернешнл Рісорсіз Груп" США

**Код ЄДРПОУ/ІПН:** US000000

**Адреса:** 01004, м. Київ, вул. Толстого 9а,1й поверх

**Підпорядкованість:** Міністерство освіти і науки України

**Телефон:** (202) 289-0100

**E-mail:** ggoldstain@irgltd.com

## 4. Джерела та напрями фінансування

**Підстава для проведення робіт:** 09 - договір із закордонним замовником

**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)

Програмний модуль псевдонедетермінованих криптографічних перетворень для технологій розподіленого реєстру

### Назва роботи (англ)

Software module of pseudonondeterministic cryptographic transformations implementation for distributed ledger technologies

### Реферат (укр)

Об'єктом дослідження є процес криптографічних перетворень для технологій розподіленого реєстру. Предметом дослідження є методи псевдонедетермінованих криптографічних перетворень для технологій розподіленого реєстру. Метою досліджень є покращення захисту даних, що зберігаються в розподіленому реєстрі, шляхом створення програмного модуля. Виконано аналіз загальновідомих підходів, які використовуються під час забезпечення захищеного процесу зберігання даних в розподіленому та виявлені їх основні недоліки. Запропоновано формалізований опис концепції та методів псевдонедетермінованих криптографічних перетворень, що забезпечуватимуть виконання протоколів консенсусу шляхом пришвидшення процесу шифрування за рахунок зменшення кількості раундів та використанні операцій, які найбільш просто та швидко реалізуються в сучасних мікропроцесорах. При цьому, можливість створення великої кількості модифікацій алгоритму шифрування теоретично робить неможливим попередні статистичні дослідження, які є базовими для найпотужніших сучасних методів криптографічного аналізу, що, в свою чергу дозволяє досягти заданих показників стійкості. Розроблено прототип програмного модуля для захисту персональних даних, який дозволяє забезпечити захищеність персональних даних під час їх зберігання в розподіленому реєстрі. Результати науково-дослідної роботи (НДР) упроваджені в процес захищеного зберігання персональних даних в розподіленому реєстрі BlockSoftLab Inc. Отримані результати НДР відносяться до галузі криптографічного захисту інформації і можуть бути використані у інформаційних системах, що використовують технології розподіленого реєстру.

### Реферат (англ)

The object of the study is the process of cryptographic overlap for technological distribution of the registry. Investigation of methods of pseudo-deterministic cryptographic overlaps for registry distributed technologies is proposed. The technique is to improve the various data stored in a split registry by creating a software module. Performed analysis is widely used during use, which is used during the secure process of storing data in distributed secrecy, which makes them the main disadvantages. A formalized description of the concept and methods of pseudo-deterministic cryptographic transformations is proposed, which will ensure consensus protocols are implemented by accelerating the encryption process by reducing the number of rounds and using the operations that are most easily and quickly implemented in modern microprocessors. At the same time, the possibility of creating a large number of modifications of the encryption algorithm theoretically makes it impossible to make preliminary statistical studies, which are the basis for the most powerful modern methods of cryptographic analysis, which in turn allows to achieve the specified stability indicators. A prototype of a software module for the protection of personal data has been developed, which allows to secure the personal data during its storage in a distributed registry. The results of the research work (GDR) are implemented in the process of secure storage of personal data in the distributed registry of BlockSoftLab Inc. The GDR results are related to the field of cryptographic information security and can be used in information systems using distributed registry technologies. A prototype of a software module for the protection of personal data has been developed, which allows to secure the personal data during its storage in a distributed registry. The results of the research work (GDR) are implemented in the process of secure storage of personal data in the distributed registry of BlockSoftLab Inc. The GDR results are related to the field of cryptographic information security and can be used in information systems using distributed registry technologies.

**Індекс УДК:** 004.7, 004.056+004.67

**Коди тематичних рубрик НТІ:** 50.37.23

## 6. Науково-технічна продукція (НТП)

### НТП 1

**Назва продукції (укр):** Програмний модуль псевдонедетермінованих криптографічних перетворень для технологій розподіленого реєстру

**Назва продукції (англ):** Software module of pseudonondeterministic cryptographic transformations implementation for distributed ledger technologies

**Очікувані результати:** Поліпшення якості продукції

**Галузь застосування:** 62.01 - Комп'ютерне програмування

**Опис продукції (укр):** Розроблено програмний модуль, який дозволяє забезпечити захист інформації під час її зберігання в розподіленому реєстрі, що дало змогу підвищити рівень інформаційної безпеки цілісності, конфіденційності та автентичності даних смарт-контрактів Ethereum

**Соціально-економічна спрямованість НТП:**

**Стадія завершеності НТП:** Звіт по НДДКР

**Впровадження НТП:** Впроваджено

**Строки впровадження:** 2019 р .

**Виробник продукції:** Вінницький національний технічний університет

**Споживачі продукції:** BlockSoftLab Inc

**Перспективні ринки:** Галузь криптографічного захисту інформації; технології розподіленого реєстру

**Права інтелектуальної власності:** За договорами

**Форми та умови передачі продукції:** Результати НДР передані Замовнику

## 7. Бібліографічний опис

## 8. Звітна документація

**Кількість сторінок в звіті:** 51

**Мова звіту:** Українська

**Умови поширення в Україні:** Не заборонено

**Умови передачі іншим країнам:** Не заборонено

**Кількість файлів у звіті:** 1

## 9. Заключні відомості

### Перелік осіб-виконавців

Баришев Юрій Володимирович

Караван В.Р.

Остапенко-Боженова А.В.

**Керівник організації:**

Павлов Сергій Володимирович (д. т. н., професор)

**Керівники роботи:**

Баришев Юрій Володимирович

**Керівник відділу реєстрації наукової діяльності УкрІНТЕІ**


Юрченко Т.А.