Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0821U102081

Особливі позначки: відкрита

Дата реєстрації: 08-07-2021

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Гальченко Андрій Віталійович
2. Halchenko Andrii V.

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: доктор філософії

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 122

Назва наукової спеціальності: Комп'ютерні науки

Галузь / галузі знань:

Освітньо-наукова програма зі спеціальності: Не застосовується

Дата захисту: 24-06-2021

Спеціальність за освітою: Системи технічного захисту інформації, автоматизація її обробки

Місце роботи здобувача:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): ДФ 17.051.035

Повне найменування юридичної особи: Запорізький національний університет

Код за ЄДРПОУ: 02125243

Місцезнаходження: вул. Жуковського, буд. 66, м. Запоріжжя, Запорізький р-н., Запорізька обл., 69600, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

IV. Відомості про підприємство, установу, організацію, в якій було виконано дисертацію

Повне найменування юридичної особи: Запорізький національний університет

Код за ЄДРПОУ: 02125243

Місцезнаходження: вул. Жуковського, буд. 66, м. Запоріжжя, Запорізький р-н., Запорізька обл., 69600, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 50.37.23

Тема дисертації:

1. Інструментальні засоби криптографічних систем на базі заперечуваного шифрування

2. Cryptography systems' tools based on the deniable encryption

Реферат:

1. У вступі обґрунтовано актуальність теми дисертаційної роботи, зазначено зв'язок роботи з науково-технічними проектами, сформульовано мету і завдання дослідження, визначено об'єкт, предмет та методи дослідження, показано наукову новизну та практичне значення отриманих результатів, наведено інформацію про практичне використання доробку, особистий внесок здобувача, апробацію результатів дослідження та їх висвітлення у наукових публікаціях. У розділі 1 виконано аналіз відкритих джерел і встановлено, що захист електронної інформації – це одна з актуальних проблем в галузі інформаційної безпеки, яка тісно пов'язана зі станом розвитку та впровадженням засобів машинної обробки даних та фактично залежить від нього. Визначено, що для захисту електронної інформації використовують різноманітні пристрої та методи, зокрема програмні. Зазначено, що поява атак, які ґрунтуються на застосуванні примусу до користувачів інформаційних систем, призводить до зменшення рівня захисту механізмів класичної криптографії та

стеганографії, оскільки надійність їх захисту ґрунтується лише на обчислювальній стійкості алгоритмів перетворення даних. Тому розвиток перспективних напрямів програмного захисту даних, зокрема криптографії, позбавлених вказаних недоліків є актуальною проблемою в теперішній час. Аналіз існуючих алгоритмів перетворення даних дозволив виділити найбільш перспективні напрями розвитку криптографії. У розділі 2 наведено опис розробленої блокової моделі перетворення даних, використання якої дозволяє досягти швидкості необхідної для виконання криптографічних перетворень, покладених в основу алгоритмів заперечуваного шифрування. Зазначено, що вказана модель стала фундаментом для розробок у подальших розділах. В її основі лежить комбінація елементів симетричної криптографії та криптографічних перетворень з відкритим ключем. Результатом застосування даного підходу стали збільшення розміру вихідних даних і зростання швидкості криптографічних перетворень. У порівнянні з існуючими рішеннями, використання запропонованої моделі дозволило збільшити швидкість перетворень та виключити необхідність внесення змін у вихідні алгоритми заперечуваного шифрування. Також у контексті вивчення елементів симетричної криптографії розглянуто можливість використання режимів шифрування. Для цього були розроблені адаптивні схеми режимів перетворення даних призначені для застосування в алгоритмах заперечуваного шифрування. Однак аналіз їх структури дозволив встановити, що для вихідних алгоритмів заперечуваного шифрування на практиці доцільною є імплементація саме режимів ECB і CBC, оскільки їх механізми дозволяють захисти саме дані. Окрім того, експериментами встановлено, що показники сумарної швидкодії вихідної моделі в значній мірі залежать від апаратного забезпечення кінцевих пристроїв. У розділі 3 виконано подальший аналіз структури алгоритмів заперечуваного шифрування, результати якого продемонстрували, що перетворення вказаних алгоритмів ґрунтуються на вирішенні великої кількості складних задач за одиницю машинного часу. При цьому вирішення власне складних задач за рахунок розпаралелення обчислень ускладнене через лінійність обчислювальних алгоритмів (зокрема алгоритму Тоннелі-Шенкса та подібних до нього). Для вирішення цієї проблеми удосконалено вихідну модель перетворення даних за допомогою паралельних обчислень. Для отримання більш високого показника прискорення розроблено механізм попередньої обробки вихідних даних, який ґрунтується на використанні принципу «розділяй та володарюй». У розділі 4 зазначено, що швидкість криптографічних перетворень в алгоритмах заперечуваного шифрування залежить від розміру вихідних даних, розміру та кількості блоків з даними. Управління вказаними характеристиками у попередньому розділі дозволило позитивно вплинути на кінцеву продуктивність моделі. В зв'язку з цим розроблено адаптивний механізм кодування даних, який ґрунтується на: прогнозуванні коефіцієнту компресії файлів з даними; управлінні рівнем компресії даних; компресії/декомпресії даних за допомогою алгоритмів кодування LZMA2 і Deflate. У розділі 5 зазначено, що можливість збільшення швидкості криптографічних перетворень на кінцевих пристроях обмежена обчислювальними потужностями локальних пристроїв. Акцентовано увагу на тому, що не усі кінцеві пристрої мають однаково високі обчислювальні потужності, у зв'язку з чим сумарна швидкість перетворення даних для кожного кінцевого пристрою буде відрізнятися. Для отримання більш стабільних показників швидкодії та можливості перетворення файлів з даними більшого розміру розроблено розподілену модель заперечуваного перетворення даних, в основу якої покладено метод статичного балансування навантаження.

2. The Introduction substantiates the topicality of the thesis, outlines its relationship to scientific and technical research projects. It formulates the research goal and objectives, specifies the object, subject, and methods of research, and highlights the scientific novelty and practical value of the obtained results. It sketches out how the research results were used in practical cases. Further, it summarizes the personal contribution of the applicant, and presents how the approbation and publication of the contributed results were done. Chapter 1 reviews the top issue in the information security industry, which depends on the information technologies development. It determined that a plenty of methods applied to protect the electronic information (hardware, software, etc.). The special software applying is more widespread. Information security software and same tools improvement is one of the most important approaches for information technology and information security, both. It's also determined that data protection tools have become more widespread in various human activities. They are based on the cryptography and steganography methods. It allows hiding the data and its context, preventing data from

uncontrolled access and unauthorized changes, the third party abusing. It admits that the data context is the most valuable for users and offenders. Not only that, but it can be used to illegally enrich, harm the physical and mental condition of users, inflict reputational damages on legal entities, etc. It's highlighted that classical cryptography and steganography safety is based on the protection scheme's computational stability. Therefore, the specified software development with the progressive protection schemes is an urgent issue nowadays. It's found the most advanced cybersecurity approaches. In Chapter 2, we developed the new computational scheme. It's based on the symmetric and public key cryptography combination and used to improve the basic deniable encryption algorithms. This approach has become to the original data size and data processing speed increasing. The suggested model allowed increasing transformations speed and eliminate changes of the original deniable encryption algorithms comparing to the existed solutions. Symmetric cryptography modes have been investigated. As a result, the common encryption modes have been transformed and become specialized for the deniable encryption algorithms applying. However, their analysis appears that the ECB and CBC modes can be applied. These modes provide the data protection immediately. Besides, it's found that suggested computational model performance depends on the workstations' capacity. Chapter 3 focuses on the second deniable encryption algorithms investigation. It determined that the base model consists of plenty of complex tasks. It reduces the general capacity of the model. But these tasks cannot be calculated with parallel computing mechanisms (the Tunnel-Shanks algorithm, etc.). That's why the basic computing model has been improved. This approach provides a wrapper for the deniable encryption algorithms, which does not affect the computing model. The parallel computing model low performance is highlighted. However, the basic computing model has been advanced with the data pre-processor applying. This method is based on the "divide and conquer" concept. Chapter 4 establishes that both models' performance depends on the original data length and quantity of data blocks. These variables' management allows influences the summary model performance. An adaptive data encoding mechanism has been developed for this task. It's based on the files' compression ratio forecasting, data compression management, LZMA2 and Deflate encoding algorithms applying. In Chapter 5 found that some local computing technologies have been investigated and applied. It allowed to increase the deniable encryption algorithms performance on the end clients. But it's found that clients had the different capacity, because of hardware restrictions. The distributed encryption model with the static load balancing developed.

Державний реєстраційний номер ДіР:

Пріоритетний напрям розвитку науки і техніки:

Стратегічний пріоритетний напрям інноваційної діяльності:

Підсумки дослідження:

Публікації:

Наукова (науково-технічна) продукція:

Соціально-економічна спрямованість:

Охоронні документи на ОПІВ:

Впровадження результатів дисертації:

Зв'язок з науковими темами:

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Чопоров Сергій Вікторович

2. Choporov Serhii Viktorovych

Кваліфікація: д. т. н., 05.13.12

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Неласа Ганна Вікторівна
2. Nelasa Hanna Viktorivna

Кваліфікація: к. т. н., 05.13.21

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Власне Прізвище Ім'я По-батькові:

1. Халімов Геннадій Зайдулович
2. Khalimov Hennadii Zaidulovych

Кваліфікація: д. т. н., 05.13.05

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Козін Ігор Вікторович

2. Kozin Ihor Viktorovych

Кваліфікація: д. ф.-м. н., 01.05.02

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Власне Прізвище Ім'я По-батькові:

1. Кудін Олексій Володимирович

2. Kudin Oleksii Volodymyrovych

Кваліфікація: к. ф.-м. н., 01.02.04

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради

Гоменюк Сергій Іванович

Власне Прізвище Ім'я По-батькові головуючого на засіданні Гоменюк Сергій Іванович

Відповідальний за підготовку облікових документів

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності

Юрченко Т.А.