Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0418U001073

Особливі позначки: відкрита

Дата реєстрації: 05-02-2018

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Захаріудакіс Лефтеріс ---

2. Zacharioudakis Eleftherios

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: кандидат наук

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 05.13.05

Назва наукової спеціальності: Комп'ютерні системи та компоненти

Галузь / галузі знань: Не застосовується

Освітньо-наукова програма зі спеціальності: Не застосовується

Дата захисту: 29-01-2018

Спеціальність за освітою: Комп'ютерні системи та мережі

Місце роботи здобувача: Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

Код за ЄДРПОУ: 02070921

Місцезнаходження: пр. Перемоги, 37, корп. 1, м. Київ, Київська обл., 03056, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): Д 26.002.02

Повне найменування юридичної особи: Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

Код за ЄДРПОУ: 02070921

Місцезнаходження: пр. Перемоги, 37, корп. 1, м. Київ, Київська обл., 03056, 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: Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

Код за ЄДРПОУ: 02070921

Місцезнаходження: пр. Перемоги, 37, корп. 1, м. Київ, Київська обл., 03056, 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. Методи та засоби підвищення ефективності ідентифікації користувачів розподілених систем

2. Methods and tools for increasing the efficiency of distributed systems users identifications

Реферат/анотація:

1. Дисертація присвячена проблемі підвищення ефективності ідентифікації користувачів розподілених систем за рахунок зниження ризику несанкціонованого доступу до її ресурсів та прискорення ідентифікації. В роботі проведено аналіз факторів. що впливають на ефективність ідентифікації віддалених користувачів інтегрованих систем. Основну увагу приділено підвищенню продуктивності ідентифікації. З теоретичної точки зору найбільший рівень протидії незаконному доступу до ресурсів системи забезпечується при використанні строгої ідентифікації, в основі якої лежить модель “нульових знань” і яка передбачає використання математичних незворотних перетворень. В дисертаційній роботі пропонується для прискорення строгої ідентифікації використовувати незворотні перетворення булевої алгебри та алгебри полів Галуа. Для строгої ідентифікації на основі незворотних булевих перетворень пропонується три методи. Перший із них передбачає використання спеціально побудованого перетворення, яке формує однакових

вихідний код для групи різних вхідних кодів. Інший розроблений метод реалізації строгої ідентифікації з використанням булевих перетвореннях базується на застосуванні стандартизованих хеш-алгоритмів таких як SHA чи Ripemd-160. Третій метод для прискореної строгої ідентифікації на булевих перетвореннях передбачає використання стандартизованих шифроблоків типу AES.

2. Thesis is dedicated to a problem of increasing of efficiency of distributed systems users identifications by impairsing the risk of illegal access to system resources and by speed up identification. In this work the analysis the factors which affect on efficiency of identification of remote user of integrate systems have been workwed out. The main attention is concentrated to identification performance increase. From the theoretical point of view the best for high degree of safety again illegal access to system resources is zero-knowledge or strikt identification, based on utilization of nonreversable mathematical transformation. In dissertation work proposed for speed up strikt identification to use nonreversable transformation of boolean algebra and Galoise fields algebra. For strikt identification based on nonreversable boolean transformation the three method have been proposed. Fist of them provision utilization special building transformation which formed one output code for groop different input code. Another diveloped method strikt identification implementation by nonrever¬sable boolean transformation are based on using standard hash-algorithms lile SHA or Ripemd-160. Third proposed method for strict identification by using boolean transformation is based on using of standard block ciphers such as AES.

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. Стіренко Сергій Григорович
2. Stirenko Sergij Grygorovych

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

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Додонов Олександр Георгійович

2. Dodonov Oleksandr Georgijovych

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

Власне Прізвище Ім'я По-батькові:

1. Чемерис Олександр Анатолійович

2. Chemerys Oleksandr Anatolijovych

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

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради	Луцький Георгій Михайлович
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Луцький Георгій Михайлович
Відповідальний за підготовку облікових документів	
Реєстратор	
Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності	Юрченко Т.А.