Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0520U101659

Особливі позначки: відкрита

Дата реєстрації: 24-11-2020

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Защолкін Костянтин Вячеславович
2. Zascholkin Kostiantin Vyacheslavovich

Кваліфікація: к. т. н., 05.13.12

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: доктор наук

Аспірантура/Докторантура: ні

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: 19-11-2020

Спеціальність за освітою: Комп’ютерні системи та мережі

Місце роботи здобувача: Одеський національний політехнічний університет

Код за ЄДРПОУ: 02071045

Місцезнаходження: пр. Шевченка, 1, м. Одеса, Одеська обл., 65044, 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 41.052.01

Повне найменування юридичної особи: Одеський національний політехнічний університет

Код за ЄДРПОУ: 02071045

Місцезнаходження: пр. Шевченка, 1, м. Одеса, Одеська обл., 65044, 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: Одеський національний політехнічний університет

Код за ЄДРПОУ: 02071045

Місцезнаходження: пр. Шевченка, 1, м. Одеса, Одеська обл., 65044, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 50.41

Тема дисертації:

1. Стеганографічно-орієнтовані моделі, методи і засоби контролю цілісності та автентичності FPGA-базованих компонентів комп'ютерних систем

2. Steganography-oriented models, methods and means for the integrity and authenticity monitoring of the FPGA-based components of computer systems

Реферат:

1. Дисертація присвячена вирішенню актуальної науково-прикладної проблеми підвищення достовірності контролю цілісності та автентичності FPGA-базованих компонентів комп'ютерних систем шляхом розробки моделей, методів та засобів, основаних на стеганографічно-орієнтованому зберіганні, доступі й обробці контрольних даних. В роботі запропоновано стеганографічно-орієнтовані моделі для основних складових забезпечення контролю цілісності та автентичності програмного коду FPGA-базованих компонентів. На основі цих моделей розроблено метод вбудовування контрольного цифрового водяного знаку в простір програмного коду FPGA-базованих компонентів. Розроблено стеганографічно-орієнтований метод контролю цілісності FPGA-базованих компонентів, який характеризується зберіганням контрольних даних у складі цифрового водяного знаку, вбудованого в програмний код FPGA. Метод дозволяє підвищити достовірність контролю порівняно з відомими підходами, за рахунок зменшення тих складових помилок контролю, які

пов'язані з дією атак на контрольні дані. Запропоновано модель життєвого циклу цілісності FPGA-базованих компонентів та на її основі розроблено метод зниження обчислювальної складності етапу валідації таких компонентів перед запуском контролю цілісності. На основі отриманих теоретичних положень розроблено апаратно-програмний модуль та набір програмних інструментальних засобів, що в сукупності забезпечують процеси контролю цілісності та автентичності FPGA-базованих компонентів комп'ютерних систем відповідно до запропонованого стеганографічо-орієнтованого підходу.

2. The dissertation is devoted to the solution of the actual scientific and applied problem, which deals with increasing the reliability of integrity and authenticity monitoring of FPGA-based components of computer systems by developing the models, methods and means founded on steganography-oriented storing, access and processing of monitoring data. In the dissertation, the steganography-oriented models for principal constituents, which provide the integrity and authenticity monitoring for program code of FPGA-based components are proposed, namely: a model of a steganographic medium for extra data bits in the environment of FPGA-based components program code; a model of an embedding path of extra data in the program code space of FPGA LUT-units; a model of a steganographic LUT-container and the one of a steganographic key for stego-container of such type. The mentioned models are characterized by their taking into consideration the following: dual program code representation of elementary FPGA parts; the nature of links between FPGA units, and the restrictions, which are imposed by FPGA structure on the usage of LUT-units as elementary target parts of embedding; FPGA program code structure; the peculiarities of FPGA operation modes. The presence of dual program code representation of elementary FPGA parts has allowed to reveal the functional redundancy of this representation and used it (redundancy) for the hidden extra data embedding into FPGA-based components program code. On the foundation of the mentioned models a steganography-oriented method of the monitoring digital watermark embedding into the space of FPGA-based components program code has been developed. The developed method is characterized by the usage of natural functional redundancy of the FPGA chip program code and allows to hide the presence of monitoring data and the fact of integrity/authenticity monitoring execution in regard to the corresponding FPGA-based components. These features of the method make its results more strong to the traditional stegoanalysis. The steganography-oriented method of FPGA-based components integrity monitoring, which stores the monitoring data by embedding them into the components program code in the form of digital watermark, was developed. This permits increasing the monitoring reliability due to hiding both the monitoring data and the fact of monitoring execution under the conditions of probable attacks on monitoring data. The estimation method of monitoring reliability of information objects integrity of the FPGA program code under the conditions of combined usage of traditional and steganographic approaches to the monitoring data storing, has been developed. The research of this method and estimation of steganographic constituent contribution in providing the monitoring system reliability under the conditions of attacks on the monitoring data have been carried out. A model of FPGA-based components integrity life cycle is proposed. On the basis of this model a method of computational complexity decrease of the stage of FPGA-based components validation before integrity monitoring starting has been developed. The method is founded on the analysis of LUT units activeness at their outputs and address inputs. This permits simplifying the stage of FPGA-based components validation due to the preliminary estimation of the LUT units dynamics activeness at the specific operation modes in the specific scenarios of integrity violation. On the foundation of the obtained theoretical principles a set of software and hardware modules, which in total provide the processes of integrity and authenticity monitoring of the computer system FPGA-based components in accordance with the proposed steganography-oriented approach has been developed. The usage of the developed software and hardware set as well as the proposed models and methods under the conditions of attacks on the monitoring data has allowed to increase the reliability of the mentioned types of monitoring as compared to the one (reliability), which is provided by the well-known means of monitoring. Wherein the developed means permit increasing the monitoring reliability not only due to the introduction of the extra protection stages of monitoring data but also by creating the new qualities which are substantial for the processes of integrity and authenticity monitoring of FPGA program code, namely: hiding the presence of monitoring data and the fact of monitoring procedure execution with respect to the given FPGA-based component; the formation of integrated whole of FPGA

program code object and monitoring data; the absence of monitoring data effect on both the operation and characteristics of FPGA-based component and a size of its program code

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. Дрозд Олександр Валентинович
2. Drozd Oleksandr

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. Дрозд Олександр Валентинович
2. Drozd Alexander

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. Саченко Анатолій Олексійович
2. Sachenko Anatoliy O.

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. Романюк Олександр Никифорович
2. Romaniuk Oleksandr N.

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. Романкевич Віталій Олексійович

2. Romankevich Vitaliy O.

Кваліфікація: д. т. н., 05.13.13

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 Антощук Світлана Григорівна

Власне Прізвище Ім'я По-батькові головуючого на засіданні Антощук Світлана Григорівна

Відповідальний за підготовку облікових документів

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності Юрченко Т.А.