Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0419U003850

Особливі позначки: відкрита

Дата реєстрації: 02-10-2019

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Адамов Олександр Семенович

2. Adamov Oleksandr S.

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: 26-09-2019

Спеціальність за освітою: 8.05010201 Комп'ютерні системи та мережі

Місце роботи здобувача: Харківський національний університет радіоелектроніки

Код за ЄДРПОУ: 02071197

Місцезнаходження: проспект Науки, 14, м. Харків, Харківський р-н., Харківська обл., 61166, 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 64.052.01

Повне найменування юридичної особи: Харківський національний університет радіоелектроніки

Код за ЄДРПОУ: 02071197

Місцезнаходження: проспект Науки, 14, м. Харків, Харківський р-н., Харківська обл., 61166, 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: Харківський національний університет радіоелектроніки

Код за ЄДРПОУ: 02071197

Місцезнаходження: проспект Науки, 14, м. Харків, Харківський р-н., Харківська обл., 61166, 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, 20.55, 28.31.04

Тема дисертації:

1. Моделі і методи захисту кіберпростору на основі аналізу великих даних з використанням машинного навчання

2. Cyberspace protection models and methods based on big data analysis using machine learning

Реферат/анотація:

1. Мета дослідження – істотне скорочення часу виявлення і блокування кібератак, спрямованих на кіберпростір суб'єкта, шляхом використання розроблених матричних моделей і логічних методів тестування, перевірки та діагностування за рахунок введення обчислювальної надмірності в інфраструктуру кіберпростору. Наукова новизна результатів досліджень: 1) Удосконалено структурно-логічні моделі і методи перевірки кіберпростору для тестування і діагностування шкідливих компонентів, які відрізняються використанням методу дедуктивного паралельного аналізу обчислювальної системи для перевірки та діагностування malware. 2) Запропоновано нові методи синтезу еталонних логічних схем malware-функціональностей, які характеризуються використанням сигнатурно-кубітних структур, що дає можливість паралельно моделювати malware-driven великі дані для визначення належності поточного коду до існуючих деструктивних компонентів у malware бібліотеці. 3) Розроблено нову модель активного online cyber security комп'ютингу, яка характеризується сигнатурно-кубітним поданням інформації, що дає можливість

підвищувати швидкодію процесів моніторингу вхідних потоків malware-даних і управління видаленням деструктивних компонентів. 4) Запропоновано новий метод атрибутно-орієнтованого розпізнавання URL-адрес з використанням частотних паттернів і метод перевірки поліморфних шкідливих програм на основі врахування контрольних сум Portable Executable секцій у виконуваних файлах і застосування апарату інтелектуального аналізу даних. 5) Удосконалено засоби захисту кіберпростору, які відрізняються використанням моделей і методів сигнатурно-логічного тестування атак, пошуку криптопримітивів у троянських програмах-шифрувальниках на основі використання алгоритмів машинного навчання, що дає можливість істотно зменшити час відновлення працездатності обчислювальної структури.

2. The purpose of the study is to significantly reduce the time of detection and blocking of cyber attacks aimed at the cyberspace of the subject, using the developed matrix models and logical methods of testing, testing and diagnosing by introducing computational redundancy into the cyberspace infrastructure. The scientific novelty of research results: 1) Structural and logical models and methods for testing cyberspace for testing and diagnosing malicious components have been improved, which differ in using the method of deductive parallel analysis of a computing system to check and diagnose malware. 2) New methods for synthesizing reference logic circuits of malware-functionalities are proposed, which are characterized by the use of signature-qubit structures, which makes it possible to simulate malware-driven big data in parallel to determine whether the current code belongs to existing destructive components in the malware library. 3) A new model of active online cybersecurity computing has been developed, which is characterized by a signature-qubit representation of information, which makes it possible to increase the speed of monitoring the input malware-data streams and controlling the removal of destructive components. 4) Developing a method of attribute-based URL recognition using frequency patterns and a method for testing polymorphic malware based on the accounting of the Portable Executable checksums of sections in the executable file and using the data mining apparatus. 5) Cyberspace protection tools have been improved, which differ in the use of models and methods of signature-logic testing of attacks, the search for crypto-primitives in ransomware based on the use of machine learning algorithms, which makes it possible to significantly reduce the recovery time of the computing structure.

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. Хаханов Володимир Іванович

2. Hahanov Vladimir I.

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. Хажмурадов Манап Ахмадович
2. Khazhmuradov Manap A.

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

Власне Прізвище Ім'я По-батькові:

1. Мірошник Марина Анатоліївна
2. Miroshnyk Maryna A.

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	Хаханов Володимир Іванович
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Путятін Євгеній Петрович
Відповідальний за підготовку облікових документів	
Реєстратор	
Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності	Юрченко Т.А.