Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0422U100014

Особливі позначки: відкрита

Дата реєстрації: 05-01-2022

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Саприкін Олександр Сергійович
2. Saprykin Oleksandr Sergiyovych

Кваліфікація:

Ідентифікатор ORCHID ID: Не застосовується

Вид дисертації: кандидат наук

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: 09-12-2021

Спеціальність за освітою: Комп’ютерні системі та мережі

Місце роботи здобувача: Фізична особа-підприємець Саприкін Олександр Сергійович

Код за ЄДРПОУ: 3117306710

Місцезнаходження: вул. Клочківська, 191, м. Харків, Харківський р-н., Харківська обл., 61145, Україна

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Сектор науки: Не застосовується

III. Відомості про дисертацію

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, буд. 14, м. Харків, Харківський р-н., Харківська обл., 61166, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Сектор науки: 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, буд. 14, м. Харків, Харківський р-н., Харківська обл., 61166, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Сектор науки: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 50.37.23, 50.39, 50.41.27

Тема дисертації:

1. Моделі автоматизованого аналізу та діагностування поліморфних вірусів у комп'ютерних системах та мережах

2. Models for automated analysis and diagnosis of polymorphic viruses in computer systems and networks

Реферат:

1. Мета дослідження – істотне зменшення часу і вартості розпізнавання поліморфних мутаторів шляхом розробки і впровадження федеративної архітектури cloud-edge комп'ютингу на основі ML-sandbox і векторно-логічних методів пошуку zero-day шкідливих кодів для захисту інфраструктури кіберфізичного простору. Поліморфний мутатор – механізм управління логічною і синтаксичною модифікацією коду шкідливої програми для її маскування від детектування існуючими антивірусними сервісами. Наукова новизна результатів досліджень: 1) вперше запропоновано федеративну ML-архітектуру sandbox комп'ютингу; 2) удосконалено структурну модель ML-комп'ютингу; 3) удосконалено матрично-логічний метод діагностування шкідливих кодів; 4) удосконалено векторно-матричний метод діагностування

шкідливих кодів; 5) вперше запропоновано методи: детектування модифікованих шкідливих кодів; детектування досліджуваного зразка заздалегідь встановленими антивірусними рішеннями; діагностування поліморфних шкідливих програм за допомогою Yara правил; створення URL сигнатур нового покоління, що дає можливість скоротити розмір бази даних на 75%

2. The aim of the study is to significantly reduce the time and cost of recognizing polymorphic mutators by developing and implementing a federated cloud-edge computing architecture based on ML-sandbox and vector-logical methods for finding zero-day malicious codes to protect cyberspace infrastructure. Polymorphic mutator is a mechanism for controlling the logical and syntactic modification of malicious code to mask it from detection by existing antivirus services. Scientific novelty of research results: 1) proposed a federal ML-architecture sandbox computing; 2) improved structural model of ML-computing; 3) improved matrix-logical method of diagnosing malicious code; 4) improved vector-matrix method of diagnosing malicious codes; 5) proposed methods: detection modified malicious codes; detection of the test sample by pre-installed anti-virus solutions; diagnosing polymorphic malware using Yara rules; creation of URLs of signatures of new generation, it allows to reduce the size of a database by 75%

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. Чумаченко Світлана Вікторівна
2. Chumachenko Svitlana Viktorivna

Кваліфікація: 01.05.02

Ідентифікатор ORCHID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Сектор науки: Не застосовується

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Мірошник Марина Анатоліївна
2. Miroshnyk Maryna Anatoliivna

Кваліфікація: 05.13.05

Ідентифікатор ORCHID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Сектор науки: Не застосовується

Власне Прізвище Ім'я По-батькові:

1. Леонов Сергій Юрійович
2. Leonov Sergiy Yuriyovych

Кваліфікація: 05.13.05

Ідентифікатор ORCHID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Сектор науки: 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	Хаханов Володимир Іванович
Відповідальний за підготовку облікових документів	
Реєстратор	
Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності	Юрченко Т.А.