Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0420U102287

Особливі позначки: відкрита

Дата реєстрації: 18-12-2020

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Погорелов Володимир Володимирович
2. Pogorelov Volodymyr

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: кандидат наук

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 05.13.21

Назва наукової спеціальності: Системи захисту інформації

Галузь / галузі знань: Не застосовується

Освітньо-наукова програма зі спеціальності: Не застосовується

Дата захисту: 26-11-2020

Спеціальність за освітою: 123 Комп'ютерна інженерія

Місце роботи здобувача: Національний авіаційний університет

Код за ЄДРПОУ: 01132330

Місцезнаходження: пр. Космонавта Комарова, буд. 1, м. Київ, Київська обл., 03058, 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 26.062.17

Повне найменування юридичної особи: Національний авіаційний університет

Код за ЄДРПОУ: 01132330

Місцезнаходження: пр. Космонавта Комарова, буд. 1, м. Київ, Київська обл., 03058, 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 авіаційний університет

Код за ЄДРПОУ: 01132330

Місцезнаходження: пр. Космонавта Комарова, буд. 1, м. Київ, Київська обл., 03058, 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. Нейромережеві моделі та методи розпізнавання комп'ютерних вірусів

2. Neural models and methods for computer viruses recognition

Реферат:

1. У роботі вирішено актуальну науково-прикладну задачу підвищення ефективності протидії комп'ютерним вірусам, за рахунок дослідження і розробки нових нейромережевих моделей, методів і засобів розпізнавання комп'ютерних вірусів, здатних оперативно пристосовуватись до умов використання і реагувати на виникнення нових видів вірусів. У дисертаційній роботі проведено аналіз сучасних нейромережевих моделей та методів розпізнавання комп'ютерних вірусів, що показав наявність низки недоліків, пов'язаних з високою потребою в обчислювальних ресурсах, низькою адаптованістю до проведення аналізу обфускованого програмного коду та недостатньою ефективністю розпізнавання. Розроблено концептуальну модель оцінювання глибоких нейронних мереж. Розроблено модель формування параметрів навчальних прикладів глибокої нейронної мережі. Розроблено метод визначення архітектурних параметрів глибокої нейронної мережі, призначеної для розпізнавання вірусів. Отримав подальший розвиток метод нейромережевого розпізнавання комп'ютерних вірусів. Розроблене спеціалізоване програмне забезпечення, що базується на створених нейромережевих методах та моделях, дозволило забезпечити достатню точність

розпізнавання комп'ютерних вірусів та забезпечити оперативність створення алгоритмів функціонування апаратно-програмних засобів захисту інформації.

2. In terms of the work, it is resolved the actual scientific and applied task of increasing the effectiveness of computer viruses detection by researching and developing new neural network models, methods and means of recognizing computer viruses that can quickly adapt to the conditions of use and respond to the emergence of new types of viruses. The prospects of application in the circuit of anti-virus protection systems and neural network tools for malware recognition are substantiated. The possibility of using of neural network model both in behavioral analyzers and when using signature analysis is shown. Also for domestic anti-virus protection systems, the set of expected conditions of application for the specified neural network means is defined. A conceptual model for assessing deep neural networks has been developed, which, due to the interrelated principles of permissibility of use, determining a set of effective types and evaluating the effectiveness of a type of deep neural network, makes it possible to determine a variety of modern neural network models for building effective antivirus tools. The model for construction of parameters of educational examples for a deep neural network was developed that is based on formal representation of encoded values of API-functions calls, bytes of sequence of N-grams, opcodes, the main registers of the processor, and also results of static analysis of samples of malicious and safe programs, two-dimensional interpretation of binary code, parameters of the values state dependence graph. The model allows to build means of the neural network analysis of the obfuscated code. A method for determining the architectural parameters of a deep neural network designed for virus recognition has been developed, which because of the use of the proposed conceptual model for assessing deep neural networks and model for construction of training examples used to implement the stages of determining the basic conditions of application, neural network model and the most effective architecture, as well as the constrcution of parameters of educational examples and determining the parameters of the architecture of the most effective type of deep neural network, allows you to form a set of values that ensure the adaptability of such a network to certain conditions of use. The method of neural network recognition of computer viruses was further developed, which provides sufficient error of recognition under different conditions by determining the conditions of creation and application of neural network means, processes of forming portraits of viruses and secure programs, as well as determining architectural parameters of deep neural network, verification and evaluation of neural network means. The method takes into account the limitations related to creation of a training sample and the limitations related to the computing resources of the anti-virus protection system. The specialized software is developed that is based on the created neural network methods and models and allows providing sufficient accuracy of computer viruses recognition and providing efficiency of algorithms

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. Терейковський Ігор Анатолійович

2. Tereykovskyy Ihor A.

Кваліфікація: д. 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

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Опірський Іван Романович

2. Opirskyy Ivan R.

Кваліфікація: д. 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. Фесенко Андрій Олексійович

2. Фесенко Андрій Олексійович

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

Рецензенти

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради Корченко Олександр Григорович

Власне Прізвище Ім'я По-батькові головуючого на засіданні Корченко Олександр Григорович

Відповідальний за підготовку облікових документів

Реєстратор

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