Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0824U001468

Особливі позначки: відкрита

Дата реєстрації: 08-04-2024

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Савенко Богдан Олегович
2. Bogdan O. Savenko

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: доктор філософії

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 123

Назва наукової спеціальності: Комп’ютерна інженерія

Галузь / галузі знань: інформаційні технології

Освітньо-наукова програма зі спеціальності: 123 Комп'ютерна інженерія

Дата захисту: 24-05-2024

Спеціальність за освітою: Комп'ютерна інженерія

Місце роботи здобувача:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): ДФ 70.052.036

Повне найменування юридичної особи: Хмельницький національний університет

Код за ЄДРПОУ: 02071234

Місцезнаходження: вул. Інститутська, буд. 11, Хмельницький, Хмельницький р-н., 29016, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

IV. Відомості про підприємство, установу, організацію, в якій було виконано дисертацію

Повне найменування юридичної особи: Хмельницький національний університет

Код за ЄДРПОУ: 02071234

Місцезнаходження: вул. Інститутська, буд. 11, Хмельницький, Хмельницький р-н., 29016, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

V. Відомості про дисертацію

Мова дисертації: Українська

Коди тематичних рубрик: 20.55

Тема дисертації:

1. Метод та частково централізовані системи виявлення зловмисного програмного забезпечення в комп'ютерних мережах
2. Method and partially centralized systems for detection of malicious software in computer networks

Реферат:

1. У дисертації здійснено аналіз методів синтезу архітектури розподілених систем, моделей показників оточуючого середовища для розподілених систем в корпоративних мережах, методів організації функціонування розподілених систем та методів виявлення зловмисного програмного забезпечення, зокрема worm-вірусів. В роботі розроблено метод синтезу математичних моделей рівнів безпеки компонентів системи для отримання нових аналітичних виразів комплексного опису оточуючого середовища корпоративних мереж і процесів, які відбуватимуться в частково централізованих розподілених системах, удосконалено модель частково централізованих розподілених систем, розроблено метод організації функціонування частково централізованих розподілених систем, розроблено метод виявлення worm-вірусів з використанням поділу їх на класи за спільними ознаками і визначеними критеріями за багатьма класами, а також розроблено відповідну розподілену систему, здійснено постановку експериментів і проведено з експериментальні дослідження з розробленою системою. Об'єктом дослідження є процес

синтезу частково централізованих розподілених систем виявлення зловмисного програмного забезпечення. Предметом дослідження є методи і розподілені системи з частковою централізацією для виявлення зловмисного програмного забезпечення в комп'ютерних мережах. Метою дисертаційного дослідження є покращення ефективності функціонування розподілених систем виявлення зловмисного програмного забезпечення в комп'ютерних мережах за рахунок синтезу в їх архітектурі принципів часткової централізації, самоорганізації та адаптивності. Наукова новизна одержаних результатів полягає в наступному: 1) удосконалено модель частково централізованих розподілених систем виявлення зловмисного програмного забезпечення, в якій синтезовано принципи самоорганізації та адаптивності таким чином, що така модель дала змогу створювати згідно неї системи виявлення зловмисного програмного забезпечення, функціонування яких ускладнює розуміння їх зловмисниками, дозволяє самостійно здійснювати прийняття рішень та гнучку перебудову архітектури, що покращує їх стійкість до зловмисних дій та виявлення зловмисного програмного забезпечення; 2) вперше розроблено метод синтезу математичних моделей рівнів безпеки компонентів системи для отримання нових аналітичних виразів комплексного опису оточуючого середовища корпоративних мереж і процесів, які відбуватимуться в розподілених системах, що дало змогу узгодити між собою характеристичні показники, які задані дискретними та неперевними величинами, та для формування нових характеристик; 3) розроблено новий метод організації функціонування частково централізованих розподілених систем, в якому проведено розподіл компонент системи по відношенню до центру прийняття рішень для реалізації часткової централізації, самоорганізації та адаптивності, що дало змогу задати механізми ускладнення розуміння принципу їх функціонування, самостійного прийняття рішень щодо подальших кроків, перебудови їх архітектури та наповнення системи методами виявлення зловмисного програмного забезпечення; 4) розроблено новий метод виявлення worm-вірусів, суть якого в здійсненні поділу їх на класи за спільними ознаками і визначеними критеріями за багатьма класами ознак та прийнятті рішення щодо віднесення worm-вірусу до певного класу частково централізованою розподіленою системою, що покращило достовірність виявлення, зокрема за рахунок приховування принципів функціонування системи. Розроблена частково централізована розподілена система виявлення зловмисного програмного забезпечення, зокрема worm-вірусів. має можливість її наповнення різними методами попередження, виявлення та протидії зловмисного програмного забезпечення та комп'ютерних атак, а також вона забезпечує належну стійкість та стабільність при функціонуванні в комп'ютерних мережах її компонентів. Особливістю розробленої частково централізованої розподіленої системи є складність в розумінні її функціонування зловмисниками, автоматичне та гнучке забезпечення переміщення центру між компонентами в процесі функціонування системи, автоматичне прийняття рішення щодо подальших кроків та не потребують при цьому залучення адміністратора. Крім того, реалізований метод виявлення worm-вірусів базується на багатокласовій класифікації об'єктів і результати його застосування для виявлення підтверджують ефективність запропонованого рішення. У результаті проведених експериментальних досліджень з розробленою системою було підтверджене коректне функціонування частково централізованої розподіленої системи, можливість застосування її до виявлення worm-вірусів, а також належні рівні стійкості та деградації системи. Результати роботи впроваджені на виробництві та в освітньому процесі університету.

2. The dissertation analyzes the methods of synthesis of the architecture of distributed systems, models of indicators of the environment for distributed systems in corporate networks, methods of organizing the functioning of distributed systems and methods of detecting malicious software, in particular worm viruses. The work developed a method of synthesizing mathematical models of security levels of system components to obtain new analytical expressions for a comprehensive description of the environment of corporate networks and processes that will take place in partially centralized distributed systems, improved the model of partially centralized distributed systems, developed a method of organizing the functioning of partially centralized distributed systems, developed method of detecting worm viruses using their division into classes based on common features and defined criteria for many classes, as well as developed a corresponding distributed system, set up experiments and carried out experimental studies with the developed system. The object of the study is the

process of synthesis of partially centralized distributed systems for detecting malicious software. The subject of research are methods and distributed systems with partial centralization for detecting malicious software in computer networks. The aim of the dissertation research is to improve the effectiveness of distributed systems for detecting malicious software in computer networks due to the synthesis of the principles of partial centralization, self-organization and adaptability in their architecture. The scientific novelty of the obtained results is as follows: 1) the model of partially centralized distributed malware detection systems was improved, which synthesized the principles of self-organization and adaptability in such a way that such a model made it possible to create malware detection systems according to it, the functioning of which makes it difficult for attackers to understand them, allows independent decision-making and flexible restructuring of the architecture, which improves their resistance to malicious actions and detection of malicious software; 2) for the first time, a method of synthesizing mathematical models of the security levels of system components was developed to obtain new analytical expressions for a comprehensive description of the surrounding environment of corporate networks and processes that will take place in distributed systems, which made it possible to reconcile the characteristic indicators, which are set by discrete and continuous values, and for formation of new characteristics; 3) a new method of organizing the functioning of partially centralized distributed systems was developed, in which the distribution of system components in relation to the decision-making center was carried out for the implementation of partial centralization, self-organization and adaptability, which made it possible to set mechanisms for complicating the understanding of the principle of their functioning, independent decision-making regarding further steps , rebuilding their architecture and filling the system with methods of detecting malicious software; 4) a new method of detecting worm viruses was developed, the essence of which is to divide them into classes based on common features and defined criteria according to many classes of features and to make a decision to assign a worm virus to a certain class by a partially centralized distributed system, which improved the reliability of detection, in particular due to hiding the principles of system functioning. A partially centralized distributed system for detecting malicious software, in particular worm viruses, has been developed. has the ability to fill it with various methods of prevention, detection and countermeasures against malicious software and computer attacks, and it also ensures proper stability and stability when functioning in computer networks of its components. The peculiarity of the developed partially centralized distributed system is the difficulty in understanding its functioning by attackers, automatic and flexible provision of the transfer of the center between components during the functioning of the system, automatic decision-making regarding further steps and do not require the involvement of the administrator. In addition, the implemented method of detection of worm viruses is based on a multi-class classification of objects, and the results of its application for detection confirm the effectiveness of the proposed solution. As a result of the experimental studies with the developed system, the correct functioning of the partially centralized distributed system, the possibility of its application to the detection of worm viruses, as well as the appropriate levels of stability and degradation of the system were confirmed. The results of the work are implemented in production and in the educational process of the university.

Державний реєстраційний номер ДіР:

Пріоритетний напрям розвитку науки і техніки: Інформаційні та комунікаційні технології

Стратегічний пріоритетний напрям інноваційної діяльності: Розвиток сучасних інформаційних, комунікаційних технологій, робототехніки

Підсумки дослідження: Нове вирішення актуального наукового завдання

Публікації:

- Lysenko S., Savenko B. Distributed Discrete Malware Detection Systems Based on Partial Centralization and Self-Organization. International Journal of Computing. 2023. Vol. 22. Pp. 117-139
- Kashtalian A., Lysenko S., Savenko B., Sochor T., Kysil T. Principle and method of deception systems synthesizing for malware and computer attacks detection. Radioelectronic and Computer Systems. 2023. Vol.

0(4). Pp. 112-151.

- Савенко Б. О. Метод синтезу математичних моделей рівнів безпеки для частково централізованих розподілених систем виявлення зловмисного програмного забезпечення. Вчені записки Таврійського національного університету імені В.І. Вернадського. Серія: Технічні науки. 2023. № 3. Ч. 1. С. 217-227.
- Савенко Б. О. Метод виявлення worm-вірусів згідно багатокласової класифікації. (2024). Вісник Хмельницького національного університету. Серія: Технічні науки, 331(1), 18-28.

Наукова (науково-технічна) продукція:

Соціально-економічна спрямованість:

Охоронні документи на ОПІВ:

Впровадження результатів дисертації: Впроваджено

Зв'язок з науковими темами: 0121U109936 0124U000980

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Лисенко Сергій Миколайович
2. Sergiy M. Lysenko

Кваліфікація: д. т. н., професор, 05.13.06

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Хмельницький національний університет

Код за ЄДРПОУ: 02071234

Місцезнаходження: вул. Інститутська, буд. 11, Хмельницький, Хмельницький р-н., 29016, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Мухін Вадим Євгенійович
2. Vadym Mukhin

Кваліфікація: д. т. н., професор, 05.13.05

Ідентифікатор ORCID ID: 0000-0002-1206-9131

Додаткова інформація:

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

Код за ЄДРПОУ: 02070921

Місцезнаходження: проспект Берестейський, буд. 37, Київ, 03056, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Поночовний Юрій Леонідович
2. Yuriy L. Ponochovnyi

Кваліфікація: д. т. н., професор, 05.13.06

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Полтавський державний аграрний університет

Код за ЄДРПОУ: 00493014

Місцезнаходження: вул. Сковороди, буд. 1/3, Полтава, Полтавський р-н., 36003, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: https://ror.org/01s344n79

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Кльоц Юрий Павлович
2. Yuri Klots

Кваліфікація: к. т. н., доц., 05.13.05

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Хмельницький національний університет

Код за ЄДРПОУ: 02071234

Місцезнаходження: вул. Інститутська, буд. 11, Хмельницький, Хмельницький р-н., 29016, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Бармак Олександр Володимирович

2. Olexander V. Barmak

Кваліфікація: д. т. н., професор, 05.13.06

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Хмельницький національний університет

Код за ЄДРПОУ: 02071234

Місцезнаходження: вул. Інститутська, буд. 11, Хмельницький, Хмельницький р-н., 29016, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради	Говорущенко Тетяна Олександрівна
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Говорущенко Тетяна Олександрівна
Відповідальний за підготовку облікових документів	Кондратюк К.Р
Реєстратор	УкрІНТЕІ
Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності	Юрченко Тетяна Анатоліївна