Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0823U100290

Особливі позначки: відкрита

Дата реєстрації: 17-05-2023

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Марченко Віталій Вікторович
2. Marchenko Vitalii Viktorovych

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: доктор філософії

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 125

Назва наукової спеціальності: Кібербезпека та захист інформації

Галузь / галузі знань:

Освітньо-наукова програма зі спеціальності: Не застосовується

Дата захисту: 15-05-2023

Спеціальність за освітою: Кібербезпека

Місце роботи здобувача: Державний університет телекомунікацій

Код за ЄДРПОУ: 38855349

Місцезнаходження: вул. Солом'янська, буд. 7, м. Київ, 03680, 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): ДФ 26.861.016

Повне найменування юридичної особи: Державний університет телекомунікацій

Код за ЄДРПОУ: 38855349

Місцезнаходження: вул. Солом'янська, буд. 7, м. Київ, 03680, 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: Державний університет телекомунікацій

Код за ЄДРПОУ: 38855349

Місцезнаходження: вул. Солом'янська, буд. 7, м. Київ, 03680, 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. Метод виявлення шкідливих процесів в інформаційній системі підприємства на основі ідентифікації та діагностування станів логічних об’єктів

2. The method of detecting harmful processes of the information system of the enterprise based on the identification and diagnosis of the states of logical objects

Реферат:

1. Дисертаційна робота присвячена розробці методу виявлення шкідливих процесів в інформаційній системі підприємства на основі ідентифікації та діагностування станів логічних об’єктів, методи кореляційної теорії, методи мета-аналізу, системного аналізу, методів машинного навчання Оскільки інформаційні технології стали невід'ємною частиною бізнесу та повсякденного життя - підприємства активно використовують інформаційні системи для забезпечення своєї діяльності, тому надійність та безпека цих систем є дуже важливою. Проте інформаційні системи підлягають різним шкідливим процесам, таким як хакерські атаки, віруси, збої у роботі обладнання та програмного забезпечення тощо. Ці шкідливі процеси можуть призвести до втрати даних, порушення роботи інформаційної системи та значного збитку для підприємства. Отже, розробка методу виявлення шкідливих процесів у інформаційній системі підприємства є дуже актуальною темою, яка може допомогти забезпечити безпеку та надійність роботи системи та запобігти можливим

шкідливим наслідкам. У вступі обґрунтовується важливість й актуальність теми дисертаційного дослідження, сформульовано мету та задачі роботи, визначено основні положення, наукову та практичну цінність отриманих результатів дослідження та введено особистий внесок автора. У першому розділі здійснено аналіз поточного стану та перспектив застосування методу виявлення шкідливих процесів в інформаційній системі підприємства, зокрема проблеми визначення в реальному часі та необхідних ресурсів на опрацювання великих даних. У прикінцевій частині першого розділу, враховуючи проведений аналіз та виявлені протиріччя, сформовано мету та часткові завдання дослідження, а саме: Мета. Підвищення ефективності роботи інформаційної системи підприємства за рахунок зменшення часу на пошук та вирішення проблем, що виникають у процесі її роботи шляхом вчасного виявлення можливих проблем та шкідливих процесів, що можуть впливати на її функціонування на основі ідентифікації та діагностування станів логічних об'єктів. У другому розділі розроблено розширену модель функціонування протоколу TCP на основі скінченних автоматів, що дозволяє наочно переглянути стани логічних об'єктів за допомогою матриць переходів станів, як в стані спокою так і допустимих переходів в розширеній матриці переходів станів TCP протоколу. У третьому розділі удосконалено вибір критеріїв параметрів логічних об'єктів, які підлягають ідентифікації та діагностуванню щодо виявлення шкідливих процесів та вибору оптимальних параметрів для машинного навчання, який базується на методі головних компонент на основі розширеного скінченного автомату TCP протоколу. Удосконалено метод машинного навчання на базі методу опорних векторів, з метою покращення ефективності виявлення шкідливих процесів в інформаційній системі. Досліджено ефективність методу виявлення шкідливих процесів в інформаційній системі підприємства. В результаті розроблені рекомендації щодо впровадження методу виявлення шкідливих процесів на основі ідентифікації та діагностуванні станів логічних об'єктів. Узагальнюючим результатом проведених досліджень є метод виявлення шкідливих процесів на основі ідентифікації та діагностування станів логічних об'єктів. Даний метод дозволяє підвищити ефективність ідентифікації та діагностування станів логічних об'єктів в інформаційній системі організації в реальному часі на 65-99% від існуючих сучасних методів та зменшення кількості хибно-позитивних спрацювань на 13-14%. В заключній частині роботи наведено загальні висновки щодо вирішення поставлених, у рамках дисертаційного дослідження завдання, та список використаних джерел, під час виконання роботи.

2. The dissertation is devoted to the development of a method for detecting malicious processes in the information system of the enterprise based on the identification and diagnosis of the states of logical objects, methods of correlation theory, methods of meta-analysis, system analysis, methods of machine learning Since information technologies have become an integral part of business and everyday life - enterprises actively use information systems to support their activities, therefore the reliability and security of these systems is very important. However, information systems are subject to various malicious processes, such as hacker attacks, viruses, hardware and software malfunctions, etc. These malicious processes can lead to data loss, disruption of the information system and significant damage to the enterprise. Therefore, the development of a method for detecting malicious processes in an enterprise's information system is a very relevant topic that can help ensure the safety and reliability of system operation and prevent possible harmful consequences. The introduction substantiates the importance and relevance of the topic of the dissertation research, formulates the purpose and tasks of the work, defines the main provisions, scientific and practical value of the obtained research results, and introduces the author's personal contribution. In the first section, an analysis of the current state and prospects for the application of the method of detecting malicious processes in the information system of the enterprise is carried out, in particular, the problems of real-time determination and the necessary resources for processing big data. In the final part of the first chapter, taking into account the conducted analysis and the revealed contradictions, the goal and partial tasks of the research were formed, namely: Goal. Increasing the efficiency of the enterprise's information system by reducing the time it takes to search for and solve problems that arise during its operation through the timely detection of possible problems and harmful processes that can affect its functioning based on the identification and diagnosis of the states of logical objects. In the second section, an extended model of the operation of the TSR protocol based on finite automata is developed, which allows you to

visually review the states of logical objects with the help of state transition matrices, both in the rest state and admissible transitions in the extended state transition matrix of the TSR protocol. In the third section, the selection of criteria for the parameters of logical objects that are subject to identification and diagnosis for the detection of malicious processes and the selection of optimal parameters for machine learning, which is based on the method of principal components based on the extended finite automaton of the TSR protocol, is improved. The method of machine learning based on the method of support vectors has been improved in order to improve the effectiveness of detecting malicious processes in the information system. The effectiveness of the method of detecting harmful processes in the information system of the enterprise was investigated. As a result, recommendations were developed for the implementation of the method of detecting malicious processes based on the identification and diagnosis of the states of logical objects. The general result of the conducted research is a method of detecting malicious processes based on the identification and diagnosis of states of logical objects. This method makes it possible to increase the efficiency of identification and diagnosis of the states of logical objects in the organization's information system in real time by 65-99% compared to existing modern methods and to reduce the number of false positives by 13-14%. The final part of the work contains general conclusions regarding the solution of the tasks set as part of the dissertation research, and a list of the sources used during the work.

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. Гайдур Галина Іванівна
2. Haidur Halyna I.

Кваліфікація: д. т. н., 05.13.06

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. Казмірчук Світлана Володимирівна
2. Kazmirchuk Svitlana V.

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. Радівілова Тамара Анатоліївна
2. Radivilova Tamara 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

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Кожухівський Андрій Дмитрович
2. Kozhuhivskij Andrii Dmitrovich

Кваліфікація: д.т.н., 01.05.02

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. Ахрамович Володимир Миколайович
2. Akhramovych Volodymyr M.

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

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради Вишнівський Віктор Вікторович

Власне Прізвище Ім'я По-батькові головуючого на засіданні Вишнівський Віктор Вікторович

Відповідальний за підготовку облікових документів

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності

Юрченко Т.А.