Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0823U100698

Особливі позначки: відкрита

Дата реєстрації: 26-09-2023

Статус: Наказ про видачу диплома

Реквізити наказу МОН / наказу закладу: Наказ НТУ "ХПІ" №2878СТ від 04.12.2023

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Челак Віктор Володимирович
2. Viktor V. Chelak

Кваліфікація:

Ідентифікатор ORCID ID: 0000-0001-8810-3394

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: ОП 28983 Комп’ютерна інженерія

Дата захисту: 16-11-2023

Спеціальність за освітою: 123 Комп'ютерна інженерія

Місце роботи здобувача: Національний технічний університет "Харківський політехнічний інститут"

Код за ЄДРПОУ: 02071180

Місцезнаходження: вул. Кирпичова, буд. 2, Харків, Харківський р-н., 61002, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): ДФ 64.050.099-2316

Повне найменування юридичної особи: Національний технічний університет "Харківський політехнічний інститут"

Код за ЄДРПОУ: 02071180

Місцезнаходження: вул. Кирпичова, буд. 2, Харків, Харківський р-н., 61002, 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: Національний технічний університет "Харківський політехнічний інститут"

Код за ЄДРПОУ: 02071180

Місцезнаходження: вул. Кирпичова, буд. 2, Харків, Харківський р-н., 61002, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

V. Відомості про дисертацію

Мова дисертації: Українська

Коди тематичних рубрик: 50.37.23, 50.41.27, 20.55, 20.55.01

Тема дисертації:

1. Методи та засоби захисту інформації в комп’ютерних системах та мережах

2. Methods and means of information security in computer systems and networks

Реферат/анотація:

1. Дисертаційна робота присвячена вирішенню актуальної науково-прикладної задачі, пов'язаної з розробкою та подальшим удосконалення методів та засобів ідентифікації стану комп'ютерних систем та мереж для захисту даних в умовах зовнішніх впливів. Метою дисертаційної роботи є розробка нових та удосконалення існуючих методів виявлення аномалій, загроз і шкідливого програмного забезпечення для підвищення точності та швидкості ідентифікації стану комп’ютерних систем та мереж на основі технології машинного навчання. Об’єкт дослідження – процес захисту даних в комп’ютерних системах та мережах в умовах зовнішніх впливів. Предмет дослідження – методи та засоби ідентифікації стану комп’ютерних систем та мереж на основі технології машинного навчання. За результатами дослідження отримано такі наукові результати: 1. Вперше запропоновано метод побудови дерева з багатовимірними вузлами рішень, що надало

можливість формувати деревоподібні моделі з урахуванням кореляційних зв'язків між показниками функціонування КС, дозволило підвищити точність ідентифікації її стану за рахунок кластеризації вихідних даних та збільшити оперативність ідентифікації завдяки зменшенню кількості розгалужень ДР; 2. Вперше запропоновано метод побудови нечіткого дерева рішень, який відрізняється від відомих наявністю спеціальної автоматизованої процедури формування нечітких множин та їх функцій належності, що дозволило підвищити точність та оперативність ідентифікації стану КС; 3. Удосконалено метод побудови дерева рішень, за рахунок використання у якості критерію прийняття рішень мінімальної помилки класифікації, використання направленого вибору ознак та застосування алгоритму бінарного пошуку для визначення оптимального значення порогу розщеплення вузла ДР, що дозволило зменшити час навчання моделі; 4. Удосконалено ансамблевий метод класифікації на основі мета-алгоритму бустінгу за допомогою використання у якості базових моделей розроблених дерев рішень та процедури попередньої обробки даних, що надало можливість підвищити точність ідентифікації стану КС. Практичне значення отриманих результатів полягає в наступному: - розроблено метод та програмне забезпечення побудови дерев з багатовимірними вузлами рішень, що дозволяє зменшити кількість розгалужень, підвищуючи оперативність ідентифікації стану комп'ютерних систем до 50% та точність до 12% (за умови наявності даних, які мають високі кореляційні коефіцієнти); - розроблено процедуру та програмне забезпечення формування нечітких множин та їх функцій належності для побудови нечітких дерев рішень, що дозволило підвищити точність класифікації до 30% (за умові великої кількості даних, які знаходяться на межі розмежування класів) та швидкість до 23%, порівнюючи з класичними дерева рішень; - удосконалено метод побудови дерева з одновимірними вузлами рішень та розроблено програмне забезпечення, що дозволило зменшити час навчання дерев рішень до 4,5 раз; - удосконалено ансамблевий метод класифікації на основі мета-алгоритму бустінгу та розроблено програмне забезпечення, яке моделює роботу методу, що дозволило підвищити точність класифікації до 32%. За результатами дослідження підтверджено практичну та теоретичну цінність розроблених методів, надано практичні рекомендації, щодо застосування розроблених методів та розглянуто перспективи їх подальшого розвитку.

2. The dissertation work is devoted to the solution of an actual scientific and applied problem related to the development and further improvement of methods and means of identifying the state of computer systems and networks for data protection in conditions of external influences. The purpose of the dissertation is to develop new and improve existing methods for detecting anomalies, threats and malware to increase the accuracy and speed of identifying the state of computer systems and networks, which is based on machine learning methods. Object of research is the process of data protection in computer systems and networks in conditions of external influences. The subject of research is methods and means of identifying the computer systems and networks state based on machine learning techniques. Scientific novelty of the results. As a result of the dissertation work, the scientific direction related to the development of methods and means of identifying the state of computer systems and networks for data security was further developed. The following scientific results were obtained within this area: 1. For the first time, a method of building a tree with multidimensional decision nodes was proposed, which made it possible to build tree models taking into account the correlations between the features of computer systems functioning, increased the accuracy of identifying its state by clustering the initial data and increased the identification velocity by reducing the number of decision trees' branches. 2. For the first time, a method for constructing a fuzzy decision tree is proposed, which differs from the known ones by the presence of a special automated procedure for the formation of fuzzy sets and their membership functions, which made it possible to increase the accuracy and velocity of identifying the state of a computer system. 3. The method of constructing a decision tree has been improved, which differs from the known ones by using the minimum classification error as a decision-making criterion and by applying a binary search algorithm to determine the optimal value of threshold for splitting a decision tree node. 4. The ensemble classification method based on the meta-algorithm boosting has been improved by using the proposed decision trees as basic models and a special data preprocessing procedure, which made it possible to increase the accuracy of identifying the computer systems' state. The practical significance of the obtained results include the following: – A method and software for constructing trees with

multidimensional decision nodes has been developed, which allows reducing the number of branches, increasing the speed of identifying the computer systems' state by up to 50% and accuracy by up to 12%. – The procedure and software for the formation of fuzzy sets and their membership functions for the construction of fuzzy decision trees were developed, which allowed to increase the classification accuracy by up to 30% (with a large amount of data on the verge of class delimitation) and speed by up to 23% compared to classical decision trees. – The method of building a tree with one-dimensional decision nodes was improved and software was developed that reduced decision trees training time by up to 4.5 times. – The ensemble classification method based on the meta-algorithm of boosting was improved and software was developed that simulates the method, which increased the classification accuracy by up to 32%. The research results confirmed the practical and theoretical significance of the developed methods, provided practical recommendations for the application of the developed methods and considered the prospects for their further development.

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:

- 1. S. Y. Gavrylenko, V. V. Chelak, S. G. Semenov Development of Method for Identification the Computer System State based on the Decision Tree with Multi-Dimensional Nodes / Radio Electronics, Computer Science, Control (RECSC), Zaporizhzhia, No. 2 (2022), P. 113-122. (А)
- 2. V. Chelak, S. Gavrylenko Method of Computer System State Identification based on Boosting Ensemble with Special Preprocessing Procedure / Advanced Information Systems, Kharkiv, 2022, Vol. 6 No. 1, P. 12-18, 2022. (Б)
- 3. Гавриленко С. Ю., Челак В. В. Розробка методу ідентифікації стану комп'ютерної системи на основі нечітких дерев рішень / Системи управління, навігації та зв'язку, Полтава, 2023, Випуск 1 (71), С. 78-83. (Б)
- 4. Семенов С. Г., Гавриленко С. Ю., Челак В. В. Розробка шаблонів ідентифікації стану комп'ютерних систем на основі BDS-тестування / Вісник Національного технічного університету "ХПІ". Серія: Інформатика та моделювання, Харків, № 21 (2016), С. 118-125. (Б)
- 5. S. Yu. Gavrylenko, M. S. Melnyk, V. V. Chelak Development of a Heuristic Antivirus Scanner Based on the File`s PE-Structure Analysis / Інформаційні технології та комп'ютерна інженерія, Вінниця, 2017, № 3(40), P. 23-29. (Б)
- 6. Гавриленко С. Ю., Челак В. В., Василев В. А. Система ідентифікації шкідливого програмного забезпечення на основі контекстно-вільних граматик / Сучасні інформаційні системи, Харків, 2018, Том 2 № 2, С. 101-105. (Б)
- 7. Гавриленко С. Ю., Челак В. В., Давидов В. В. Розробка системи фіксації аномальних станів комп'ютера / Вісник Національного технічного університету "ХПІ". Серія: Інформатика та моделювання, Харків, № 42 (2018), С. 109-121. (Б)
- 8. Гавриленко С. Ю., Семенов С. Г., Челак В. В. Розробка методу виявлення аномальної поведінки комп'ютерної системи на основі імовірнісного автомата / Безпека інформації, Київ, 2018, Т. 24 № 3, С. 163-168. (Б)
- 9. S. Gavrylenko, V. Chelak, O. Hornostal, V. Vassilev Development of a method for identification the state of a computer system using fuzzy cluster analysis / Advanced Information Systems, Kharkiv, 2020, Vol. 4 No. 2, P. 8-11. (Б)
- 10. V. V. Chelak, S. Y. Gavrylenko, N. Bilogorskiy Investigation of Intrusion in Computer Systems Based on the Hurst Exponent / Advanced Information Systems, Kharkov, 2017, vol. 1, no. 2, pp. 58-61.

- 11. G. Semenov, S. Gavrilenko, V. Chelak Developing parametrical criterion for registering abnormal behavior in computer, and telecommunication systems on the basis of economic test / Actual problems of economics, Kiev, 2016, vol. 4(178), pp. 451-459.
- 12. Гавриленко С.Ю., Челак В. В. Аналіз змін фрактальних властивостей завантаження центрального процесора та мережевої карти, спричинених впливом шкідливого програмного забезпечення / STANDART: науково-техн. журнал агенції "УЗСТАНДАРТ", Узбекистан, 2017, № 4, С. 14-17.
- 13. S. Gavrylenko, V. Chelak, M. Kazarinov Method of Identifying the State of Computer System under the Condition of Fuzzy Source Data / International Journal of Computer Science and Security (IJCSS), 2020, vol. 14 (5), pp. 174-186.
- 14. S. Gavrylenko, V. Chelak, O. Gornostal, S. Gornostal Identification of the computer system state based on multidimensional discriminant analysis / Proceedings of the 29th International Scientific Symposium Metrology and Metrology Assurance, Sozopol, Bulgaria, 2019, pp. 192-196.
- 15. S. Gavrylenko, V. Chelak, O. Hornostal Research of Intelligent Data Analysis Methods for Identification of Computer System State / Proceedings of the 30th International Scientific Symposium Metrology and Metrology Assurance (MMA), Sozopol, Bulgaria, 2020, pp. 1-5.
- 16. S. Gavrylenko, V. Chelak, O. Hornostal Ensemble approach based on bagging and boosting for identification the computer system state / Proceedings of the 31th International Scientific Symposium Metrology and Metrology Assurance, Sozopol, Bulgaria, 2021, pp. 1-7.
- 17. S. Gavrylenko, V. Chelak, O. Hornostal Construction Method of Fuzzy Decision Trees for Identification the Computer System State / Proceedings of the 32th International Scientific Symposium Metrology and Metrology Assurance, Sozopol, Bulgaria, 2022, pp. 1-5.
- 18. S. Gavrylenko, O. Hornostal, V. Chelak Research of Methods of Identifying the Computer Systems State based on Bagging Classifiers / IEEE 3rd KhPI Week on Advanced Technology (KhPIWeek), Kharkiv, Ukraine, 2022, pp. 1-6.
- 19. Гавриленко С.Ю., Челак В. В. Розробка системи ідентифікації шкідливого програмного забезпечення на основі контекстно-вільних граматик / XII Міжнар. науково-практ. конф. магістрантів та аспірантів, ч. 1, Харків, 2018, с. 152-153.
- 20. S. Y. Gavrylenko, V. V. Chelak, A. A. Gornostal Development of a heuristic scanner for an antivirus program on the basis of the Mamdani fuzzy logic method / Proceedings of the 28th International Scientific Symposium Metrology, and Metrology Assurance, Sozopol, Bulgaria, 2018, pp. 129-133.
- 21. Челак В. В., Гавриленко С. Ю., Павлова М. В. Розробка структурно-функціональної моделі ідентифікації аномального стану комп'ютерної системи / Матеріали XVIII Міжнар. науково-техн. конф. Проблеми інформатики та моделювання, Харків, 2018, с. 28-29.
- 22. Гавриленко С.Ю., Челак В. В., Челак Є. В. Розробка алгоритму відновлення вихідного стану програм / Матеріали V Міжнар. конф. Інформатика, управління та штучний інтелект, Харків, 2018, с. 20.
- 23. V. Chelak, E. Chelak, S. Gavrylenko Neural Networks as Decision-Making Apparatus in Antivirus Systems / Proceedings of the 6th International Scientific Conference Problems of Informatization, Kharkiv, 2018, p. 20.
- 24. V. Chelak, S. Gavrylenko, E. Chelak Computer system anomalous state detection method based on fuzzy logic / Матеріали IX Міжнар. науково-техн. конф. Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління, Харків, 2019, с. 94.
- 25. V. V. Chelak, E. V. Chelak, S. Yu. Gavrylenko Effectiveness Evaluation of Methods, and Means of Information Security in Computer Systems, and Networks / Proceedings of the 6th International Informatics, management and artificial intelligence, Kharkiv, 2019, p. 121.
- 26. Челак В.В., Гавриленко С. Ю. Дослідження ансамблевих методів оцінки стану комп'ютерної системи / Матеріали XXVIII Міжнар. науково-практ. конф. (MicroCAD-2020) Інформаційні технології: наука, техніка, технологія, освіта, здоров'я, Kharkiv, 2020, с. 193.
- 27. V. Chelak, S. Gavrylenko Development of Computer State Identification Method Based on Boosting Ensemble / Proceedings of the 5th International Scientific, and Technical Conference Computer and

Information Systems, and Technologies, Kharkiv, 2021, pp. 53-54.
- 28. Челак В. В., Гавриленко С. Ю. Розробка методу побудови дерева з багатовимірними вузлами рішень для задач ідентифікації стану комп'ютерної системи / Матеріали VIII Міжнар. науково-техн. конф. Інформатика, управління та штучний Інтелект (ІУШІ-2021), Kharkiv, 2021, с. 143.
- 29. Челак В. В., Гавриленко С. Ю. Розробка методу побудови нечітких дерев рішень для задач ідентифікації стану комп'ютерної системи / Матеріали IX Міжнар. науково-техн. конф. (ІУШІ-2022) Інформатика, управління та штучний інтелект, Харків, 2022, с. 138.
- 30. Bezpieczeństwo w cyberprzestrzeni społeczna przestrzeń internetu w kontekście wartości i zagrożeń security in cervatury, the social internet space in context values, and hazards / V. Chelak, E. Chelak, S. Gavrylenko, S. Semenov / "Development of anomalous computer behavior detection method based on probabilistic automaton", Slupsk-Charkow, 2019, pp. 237-258.

Наукова (науково-технічна) продукція: методи, теорії, гіпотези; програмні продукти, програмно-технологічна документація

Соціально-економічна спрямованість: підвищення захисту інформації в комп'ютерних системах та мережах

Охоронні документи на ОПІВ:

Впровадження результатів дисертації: Впроваджено

Зв'язок з науковими темами: 0122U200526 0122U200527

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Гавриленко Світлана Юріївна

2. Svitlana Y. Gavrylenko

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

Ідентифікатор ORCID ID: 0000-0002-6919-0055

Додаткова інформація: https://www.scopus.com/authid/detail.uri?authorId=57189042150; https://scholar.google.com.ua/citations?user=4Vn1dBkAAAAJ&hl=ua; https://www.webofscience.com/wos/author/record/2299382

Повне найменування юридичної особи: Національний технічний університет "Харківський політехнічний інститут"

Код за ЄДРПОУ: 02071180

Місцезнаходження: вул. Кирпичова, буд. 2, Харків, Харківський р-н., 61002, 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. Трубчанінова Карина Артурівна

2. Karyna A. Trubchaninova

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

Ідентифікатор ORCID ID: 0000-0003-2078-2647

Додаткова інформація: https://www.scopus.com/authid/detail.uri?authorId=57208109791;
https://www.webofscience.com/wos/author/record/2514056;
https://scholar.google.com.ua/citations?user=tFdGngkAAAAJ&hl=uk

Повне найменування юридичної особи: Український державний університет залізничного транспорту

Код за ЄДРПОУ: 01116472

Місцезнаходження: майдан Фейєрбаха, буд. 7, Харків, Харківський р-н., 61050, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Коваленко Андрій Анатолійович

2. Andrii A. Kovalenko

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

Ідентифікатор ORCID ID: 0000-0002-2817-9036

Додаткова інформація: https://www.scopus.com/authid/detail.uri?authorId=56423229200;
https://www.webofscience.com/wos/author/record/283165;
https://scholar.google.com.ua/citations?user=9KzEtDMAAAAJ&hl=ua

Повне найменування юридичної особи: Харківський національний університет радіоелектроніки

Код за ЄДРПОУ: 02071197

Місцезнаходження: проспект Науки, буд. 14, Харків, Харківський р-н., 61166, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Кучук Георгій Анатолійович

2. Heorhii A. Kuchuk

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

Ідентифікатор ORCID ID: 0000-0002-2862-438X

Додаткова інформація: https://www.scopus.com/authid/detail.uri?authorId=57057781300; https://www.webofscience.com/wos/author/record/2485726; https://scholar.google.com.ua/citations?user=gHejYRUAAAAJ&hl=uk

Повне найменування юридичної особи: Національний технічний університет "Харківський політехнічний інститут"

Код за ЄДРПОУ: 02071180

Місцезнаходження: вул. Кирпичова, буд. 2, Харків, Харківський р-н., 61002, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Подорожняк Андрій Олексійович
2. Andrii O. Podorozhniak

Кваліфікація: к.т.н., доцент, 05.12.17

Ідентифікатор ORCID ID: 0000-0002-6688-8407

Додаткова інформація: https://www.scopus.com/authid/detail.uri?authorId=57202229410; https://www.webofscience.com/wos/author/record/909299; https://scholar.google.com.ua/citations?user=gbxjOTEAAAAJ&hl=uk

Повне найменування юридичної особи: Національний технічний університет "Харківський політехнічний інститут"

Код за ЄДРПОУ: 02071180

Місцезнаходження: вул. Кирпичова, буд. 2, Харків, Харківський р-н., 61002, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради	Заковоротний Олександр Юрійович
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Заковоротний Олександр Юрійович
Відповідальний за підготовку облікових документів	Зайцев Юрій Іванович
Реєстратор	УкрІНТЕІ

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності



Юрченко Тетяна Анатоліївна