Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0824U000142

Особливі позначки: відкрита

Дата реєстрації: 05-01-2024

Статус: Запланована

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Асєєва Людмила Анатоліївна
2. Liudmyla Asieieva

Кваліфікація:

Ідентифікатор ORCHID ID: Не застосовується

Вид дисертації: доктор філософії

Шифр наукової спеціальності: 125

Назва наукової спеціальності: Кібербезпека та захист інформації

Галузь / галузі знань: інформаційні технології

Освітньо-наукова програма зі спеціальності: Кібербезпека

Дата захисту: 15-02-2024

Спеціальність за освітою: Прикладна математика

Місце роботи здобувача:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Сектор науки: Не застосовується

III. Відомості про дисертацію

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): ДФ 26.861.003

Повне найменування юридичної особи: Державний університет інформаційно-комунікаційних технологій

Код за ЄДРПОУ: 38855349

Місцезнаходження: вул. Солом'янська, буд. 7, Київ, 03680, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Сектор науки: Університетський

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

Повне найменування юридичної особи: Державний університет інформаційно-комунікаційних технологій

Код за ЄДРПОУ: 38855349

Місцезнаходження: вул. Солом'янська, буд. 7, Київ, 03680, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Сектор науки: Університетський

V. Відомості про дисертацію

Мова дисертації: Українська

Коди тематичних рубрик: 50.37.23

Тема дисертації:

1. Управління інформаційною безпекою підприємства з використанням методів машинного навчання та нечіткої логіки.

2. Management of enterprise information security using machine learning and fuzzy logic.

Реферат:

1. Анотація. Асєєва Л.А. Управління інформаційною безпекою підприємства з використанням методів машинного навчання та нечіткої логіки. – Кваліфікаційна наукова праця на правах рукопису. Дисертація на здобуття наукового ступеня доктора філософії в галузі знань 12 – Інформаційні технології за спеціальністю 125 – Кібербезпека. – Державний університет інформаційно-комунікаційних технологій, Київ, 2023. Сучасні підприємства активно використовують інформаційні системи і технології в своїй діяльності, вони стали невід'ємною частиною бізнесу та повсякденного життя, тому забезпечення надійності та безпеки цих систем

є дуже важливим завданням. Одними з основних складових побудови та використання систем кіберзахисту є оцінка ризиків інформаційної безпеки та виявлення мережевих вторгнень. Дисертаційна робота присвячена вирішенню актуального наукового завдання з розробки моделей, методів та алгоритмів системи управління інформаційною безпекою у складі інформаційної системи підприємства на основі підходів машинного навчання та нечіткої логіки. Метою дисертаційної роботи є збільшення швидкодії і точності роботи аналітичного блоку системи управління інформаційною безпекою у складі інформаційної системи підприємства за рахунок розробки відповідних моделей, методів та алгоритмів на основі підходів машинного навчання та нечіткої логіки. Для досягнення зазначеної мети було виконано наступні часткові завдання: огляд існуючих підходів до управління інформаційною безпекою підприємства та забезпечення кібербезпеки; створення моделі оцінки ризиків інформаційної безпеки документів підприємства на основі нечіткої логіки і методу аналізу ієрархій; розробка гібридного методу виявлення вторгнень на основі моделі ансамблевого навчання з використанням алгоритмів нечіткої логіки; розробка методу обрання набору ознак для навчання моделей класифікації вторгнень з використанням алгоритмів машинного навчання і нечіткої логіки; дослідження ефективності запропонованих методів виявлення вторгнень та розробка рекомендацій щодо їх застосування в системі управління інформаційною безпекою підприємства. Наукова новизна отриманих результатів дослідження полягає в наступному. Вперше розроблено гібридний метод виявлення вторгнень до корпоративної мережі, новизна якого полягає у використанні ансамблевого підходу на базі алгоритмів нечіткої логіки для поєднання результатів класифікації даних окремими моделями машинного навчання, що забезпечило більш високу точність у порівнянні з існуючими методами. Отримав подальший розвиток метод обрання набору ознак для навчання класифікаторів вторгнень, який на відміну від інших базується на ансамблевому підході з використанням нечіткої логіки для оцінки важливості ознаки, що дало можливість підвищити надійність та зменшити розмірність набору ознак. Отримала подальший розвиток модель оцінки ризиків інформаційної безпеки документів підприємства за рахунок формалізації їх структури, операцій над ними та факторів порушення їх цілісності, конфіденційності та доступності на основі нечіткої логіки і методу аналізу ієрархій, що дало можливість врахувати невизначеність та розмитість інформації щодо складових небезпеки. Практичне значення одержаних результатів полягає в збільшенні швидкодії та точності роботи аналітичного блоку системи управління інформаційною безпекою у складі інформаційної системи підприємства. Застосування запропонованого методу обрання набору ознак для навчання моделей класифікації вторгнень дозволило зменшити час навчання на 50-60% та скоротити час виявлення можливого вторгнення на 30-40% за рахунок підвищення надійності та зменшення розмірності набору ознак. Використання результатів дослідження дозволяє збільшити точність виявлення вторгнень до корпоративної мережі підприємства у порівнянні з існуючими методами на 3-5%. Результати дисертаційної роботи прийнято до впровадження в ТОВ "Хуавей Україна", в ТОВ "РЕНТСОФТ", в навчальному процесі Державного університету інформаційно-комунікаційних технологій. Вирішене в даному дисертаційному дослідженні наукове завдання має істотне значення для теоретичних і прикладних основ оцінки ризиків інформаційної безпеки та побудови систем виявлення вторгнень при управлінні інформаційною безпекою підприємств. Ключові слова: інформаційна безпека, інформаційна технологія, машинне навчання, нечітка логіка, система виявлення атак, надійність розпізнавання подій, недоліки безпеки мережі, кібербезпека, управління ризиками кібербезпеки, модель, вразливості інформаційних систем, ансамблеве навчання, інформація, можливість правильного виявлення, обрання ознак.

2. Anotation. Aseeva L.A. Management of information security of the enterprise using methods of machine learning and fuzzy logic. - Qualifying scientific work on manuscript rights. Dissertation for obtaining the scientific degree of Doctor of Philosophy in the field of knowledge 12 - Information technologies in the specialty 125 - Cybersecurity. - State University of Information and Communication Technologies, Kyiv, 2023. Modern enterprises actively use information systems and technologies in their activities, they have become an integral part of business and everyday life, therefore ensuring the reliability and security of these systems is a very important task. One of the main components of the construction and use of cyber protection systems is the assessment of information security risks and the detection of network intrusions. The dissertation work is devoted to the solution of the

actual scientific task of developing models, methods and algorithms of the information security management system as part of the information system of the enterprise based on the approaches of machine learning and fuzzy logic. The purpose of the dissertation is to increase the speed and accuracy of the analytical unit of the information security management system as part of the company's information system due to the development of appropriate models, methods and algorithms based on machine learning approaches and fuzzy logic. To achieve the specified goal, the following partial tasks were performed: review of existing approaches to managing information security of the enterprise and ensuring cyber security; creation of a risk assessment model for information security of enterprise documents based on fuzzy logic and the method of analyzing hierarchies; development of a hybrid intrusion detection method based on an ensemble learning model using fuzzy logic algorithms; development of a method for selecting a set of features for training intrusion classification models using machine learning algorithms and fuzzy logic; study of the effectiveness of proposed intrusion detection methods and development of recommendations for their application in the information security management system of the enterprise. The scientific novelty of the research results is as follows. For the first time, a hybrid method of detecting intrusions into the corporate network was developed, the novelty of which is the use of an ensemble approach based on fuzzy logic algorithms to combine the results of data classification by separate machine learning models, which ensured higher accuracy compared to existing methods. The method of selecting a set of features for training intrusion classifiers received further development, which, unlike others, is based on an ensemble approach using fuzzy logic to evaluate the importance of a feature, which made it possible to increase reliability and reduce the dimensionality of the set of features. The information security risk assessment model of the company's documents received further development due to the formalization of their structure, operations on them and factors of violation of their integrity, confidentiality and availability based on fuzzy logic and the method of analysis of hierarchies, which made it possible to take into account the uncertainty and blurring of information about the components of danger. The practical significance of the obtained results lies in increasing the speed and accuracy of the analytical unit of the information security management system as part of the company's information system. The application of the proposed method of selecting a set of features for training intrusion classification models made it possible to reduce the training time by 50-60% and reduce the time to detect a possible intrusion by 30-40% due to increasing reliability and reducing the dimensionality of the set of features. The use of research results allows to increase the accuracy of detection of intrusions into the company's corporate network by 3-5% compared to existing methods. The results of the dissertation work have been accepted for implementation in Huawei Ukraine LLC, in RENTSOFT LLC, in the educational process of the State University of Information and Communication Technologies. The scientific task solved in this dissertation study is of significant importance for the theoretical and applied foundations of information security risk assessment and the construction of intrusion detection systems in the management of information security of enterprises. Keywords: information security, information technology, machine learning, fuzzy logic, attack detection system, reliability of event recognition, network security flaws, cyber security, cyber security risk management, model, vulnerabilities of information systems, ensemble learning, information, possibility of correct detection, feature selection.

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. Чичкарьов Є., Зінченко О., Бондарчук А., Асєєва Л. Метод вибору ознак для системи виявлення вторгнень з використанням ансамблевого підходу та нечіткої логіки. Кібербезпека: освіта, наука, техніка. 2023. № 1(21). С. 234–251.

- 2. Чичкарьов Є., Зінченко О., Бондарчук А., Асєєва Л. Виявлення мережевих вторгнень з використанням алгоритмів машинного навчання і нечіткої логіки. Кібербезпека: освіта, наука, техніка. 2023. № 3(19). С. 209–225.
- 3. Oleksii M.Shushura, Liudmyla A.Asieieva, Oleksiy L. Nedashkivskiy,Yevhen V. Havrylko, Yevheniia O. Moroz, Saule S. Smailova, Magzhan Sarsembayev. Simulation of information security risks of availability of project documents based on fuzzy logic. Informatyka, Automatyka, Pomiary W Gospodarce I Ochronie Środowiska. 2022. 12(3). P.64–68.
- 4. Асєєва Л.А. Шушура О.М. Нечітке моделювання ризиків порушення цілісності документів проекту. Телекомунікаційні та інформаційні технології. 2021. № 4 (73). С. 20–27.
- 5. Асєєва Л.А. Шушура О.М. Оцінка ризиків конфіденційності інформаційної безпеки проектів на основі нечіткої логіки. Телекомунікаційні та інформаційні технології. 2021. № 1 (70). Київ 2021. С. 88–95.
- 6. Шушура О.М., Довбешко С.В., Золотухіна О.А., Асєєва Л.А. Фактори створення стратегії безпеки інформаційних технологій сучасного підприємства. Телекомунікаційні та інформаційні технології. 2019. №2(63). С.5–13.
- 7. Асєєва Л.А. Аналіз основних складових небезпеки при побудові системи інформаційної безпеки підприємства. Сучасний захист інформації. 2019. №2(38). С.42–46.

Наукова (науково-технічна) продукція:

Соціально-економічна спрямованість:

Охоронні документи на ОПІВ:

Впровадження результатів дисертації: Впроваджено

Зв'язок з науковими темами:

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Бондарчук Андрій Петрович

2. Andrii P. Bondarchuk

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

Ідентифікатор ORCHID ID: 0000-0001-5124-5102

Додаткова інформація:

Повне найменування юридичної особи: Державний університет інформаційно-комунікаційних технологій

Код за ЄДРПОУ: 38855349

Місцезнаходження: вул. Солом'янська, буд. 7, Київ, 03680, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Сектор науки: Університетський

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Аль-Амморі Алі Нурддинович

2. Ali N. Al-Ammori

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

Ідентифікатор ORCHID ID: 0000-0002-0375-6108

Додаткова інформація:

Повне найменування юридичної особи: Національний транспортний університет

Код за ЄДРПОУ: 02070915

Місцезнаходження: вул. М. Омеляновича-Павленка, буд. 1, Київ, 01010, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Сектор науки: Університетський

Власне Прізвище Ім'я По-батькові:

1. Толюпа Сергій Васильович

2. Serhii V. Toliupa

Кваліфікація: д.т.н., професор, 05.12.02

Ідентифікатор ORCHID ID: 0000-0002-1919-9174

Додаткова інформація:

Повне найменування юридичної особи: Київський національний університет імені Тараса Шевченка

Код за ЄДРПОУ: 02070944

Місцезнаходження: вул. Володимирська, буд. 60, Київ, 01033, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Сектор науки: Університетський

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Гайдур Галина Іванівна

2. Halyna I. Haidur

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

Ідентифікатор ORCHID ID: 0000-0003-0591-3290

Додаткова інформація:

Повне найменування юридичної особи: Державний університет інформаційно-комунікаційних технологій

Код за ЄДРПОУ: 38855349

Місцезнаходження: вул. Солом'янська, буд. 7, Київ, 03680, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Сектор науки: Університетський

Власне Прізвище Ім'я По-батькові:

1. Савченко Віталій Анатолійович

2. Vitalii A. Savchenko

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

Ідентифікатор ORCHID ID: 0000-0002-3014-131X

Додаткова інформація:

Повне найменування юридичної особи: Державний університет інформаційно-комунікаційних технологій

Код за ЄДРПОУ: 38855349

Місцезнаходження: вул. Солом'янська, буд. 7, Київ, 03680, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Сектор науки: Університетський

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради	Сторчак Каміла Павлівна
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Сторчак Каміла Павлівна
Відповідальний за підготовку облікових документів	Вишнівський В.В.
Реєстратор	УкрІНТЕІ

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності

Юрченко Тетяна Анатоліївна