ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кваліфікаційна наукова
праця на правах рукопису

АСЄЄВА ЛЮДМИЛА АНАТОЛІЇВНА

УДК 004.056:004.896

ДИСЕРТАЦІЯ

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА З ВИКОРИСТАННЯМ МЕТОДІВ МАШИННОГО НАВЧАННЯ ТА НЕЧІТКОЇ ЛОГІКИ

125 – Кібербезпека

12 – Інформаційні технології

Подається на здобуття наукового ступеня доктора філософії.

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____Л.А. Асєєва

Науковий керівник:
БОНДАРЧУК Андрій Петрович,
доктор технічних наук, професор

КИЇВ – 2023

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.

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.

Тематика дисертаційного дослідження відповідає тимчасовому стандарту та фаховим компетентностям освітньо-наукової програми підготовки докторів філософії з кібербезпеки Державного університету інформаційно-комунікаційних технологій Міністерства освіти і науки України, а саме: фундаментальним науковим дослідженням теоретико-методологічних, науково-методичних та прикладних засад підвищення ефективності інноваційної та виробничої діяльності підприємства, а також проведення науково-дослідних та дослідно-конструкторських робіт, пов’язаних зі створенням та реалізацією політик безпеки у сфері інформаційно-комунікаційних технологій, дослідженням проблем розвитку та вдосконаленням технологій криптозахисту інформації, дослідженням методів і засобів підвищення живучості ІКС в умовах впливу кібернетичних атак тощо.

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. В умовах загального зростання рівня кіберзлочинності,

різноманіття форм та видів використання під час здійснення атак певними державами, організаціями чи окремими злочинцями вразливостей інформаційних технологій необхідне системне застосування методів та засобів кібербезпеки. Для забезпечення надійного захисту інформаційної системи підприємства звичайних антивірусів і брандмауерів вже недостатньо, тому значна увага приділяється теоретичним та практичним аспектам розробки багаторівневих систем управління інформаційною безпекою. Одними з основних складових побудови та використання таких систем є оцінка ризиків інформаційної безпеки та виявлення мережевих вторгнень.

Виявлення, аналіз, прогнозування та обробка ризиків інформаційної безпеки ґрунтується на використанні моделей та методів їх оцінки. Враховуючи наявність невизначеності та розмитості інформації про діяльність підприємств, нечітка логіка отримала широке застосування в таких моделях. Беручи до уваги, що вимірювання характеристик кібербезпеки досі залишається недостатньо розвинутою темою, в тому числі стосовно безпеки документів підприємства, подальші дослідження в цьому напряму є актуальними.

Однією з найважливіших складових захисту інформаційної системи підприємства є система виявлення вторгнень або англійською Intrusion Detection System (IDS). Сучасні IDS діляться на такі дві основні категорії: виявлення вторгнень на основі сигнатур (або «виявлення неправильного використання») та виявлення аномалій. Для виявлення загроз безпеці інформаційної системи на основі сигнатур IDS порівнює отримані дані з відомими моделями атак. Цей метод є дуже ефективним та надійним, однак він може виявити лише відомі атаки, які вже описані в базі даних системи. Підхід на основі виявлення аномалій передбачає побудову моделі нормальної поведінки інформаційної системи, а потім здійснення IDS пошуку відхилень в даних моніторингу. Це дозволяє виявити також і невідомі атаки, але часто створює значну кількість помилкових тривог. Враховуючи, що кібератаки стають все більш численними та

різноманітними, багато досліджень протягом останніх двох десятиліть було зосереджено на побудові IDS саме на основі виявлення аномалій. В межах цих досліджень активно застосовувалися методи та моделі машинного навчання, які здатні навчатися виявляти вторгнення безпосередньо з даних мережевого трафіку.

Відомі системи виявлення вторгнень мають певні недоліки, серед яких можна виділити потребу у великій кількості даних для навчання моделей, помилкові спрацювання внаслідок недостатньої кількості даних або обмеженої точності моделей, нестабільність моделей машинного навчання при роботі з великими обсягами даних, високу кількість помилок при виявленні аномалій, невміння розпізнати нові типи загроз, які не були включені до тренувальних даних, складність налаштування моделей машинного навчання і потребу в великій кількості обчислювальних ресурсів для їх тренування та експлуатації.

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.

У вступі обґрунтовано актуальність роботи та наведено її загальну характеристику. Перший розділ дослідження присвячено аналізу практичних та науково-методологічних підходів до управління інформаційною безпекою і виявлення вторгнень в інформаційну мережу підприємства. Перспективним напрямком розвитку систем виявлення вторгнень визначено використання ансамблевого методу навчання та засобів нечіткої логіки. У другому розділі проаналізовано фактори стратегії безпеки інформаційних технологій сучасного підприємства, проведено моделювання загроз інформаційної безпеки та інформаційних ризиків обробки документів підприємства на основі нечіткої логіки та методу аналізу ієрархій. У третьому розділі розглянуто ключові аспекти розробки методів виявлення вторгнень до інформаційної системи підприємства та обрання набору ознак для навчання моделей класифікації вторгнень. У четвертому розділі виконане дослідження ефективності запропонованих методів виявлення вторгнень та розробці рекомендацій щодо покращення структури та алгоритмів системи 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.

ANOTATION

Asieieva L.A. Management of enterprise information security using machine learning and fuzzy logic. − Qualifying scientific work, the manuscript.

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.

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 topic of the dissertation research corresponds to the temporary standard and professional competences of the educational and scientific program for training doctors of philosophy in cyber security of the State University of Information and Communication Technologies of the Ministry of Education and Science of Ukraine, namely: fundamental scientific research of theoretical-methodological, scientific-methodical and applied principles of improving the efficiency of innovative and production activities of the enterprise, as well as carrying out scientific research and research and development works related to the creation and implementation of security policies in the field of information and communication technologies, the study of development problems and the improvement of information cryptoprotection technologies, the study of methods and means of increasing the survivability of ICS in the conditions the impact of cyber attacks, etc.

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. In the conditions of the general increase in the level of cybercrime, the variety of forms and types of use during attacks by certain states, organizations or individual criminals of information technology vulnerabilities, the systematic application of cyber security methods and tools is necessary. To ensure reliable protection of the company's information system, ordinary antiviruses and firewalls are no longer enough, therefore considerable attention is paid to the theoretical and practical aspects of the development

of multi-level information security management systems. One of the main components of the construction and use of such systems is the assessment of information security risks and the detection of network intrusions.

Identification, analysis, forecasting and processing of information security risks is based on the use of models and methods of their assessment. Given the presence of uncertainty and blurring of information about the activities of enterprises, fuzzy logic has been widely used in such models. Taking into account that the measurement of cyber security characteristics still remains an underdeveloped topic, including regarding the security of company documents, further research in this direction is relevant.

One of the most important components of the protection of the company's information system is the intrusion detection system, or in English Intrusion Detection System (IDS). Modern IDSs fall into two main categories: signature-based intrusion detection (or "misuse detection") and anomaly detection.

In order to detect threats to the security of the information system based on signatures, IDS compares the received data with known attack patterns. This method is very effective and reliable, but it can only detect known attacks that are already described in the system database.

The approach based on the detection of anomalies involves building a model of the normal behavior of the information system, and then implementing an IDS search for deviations in the monitoring data. This allows detection of unknown attacks as well, but often creates a significant number of false alarms. Given that cyberattacks are becoming more numerous and diverse, much research over the past two decades has focused on building IDSs specifically based on anomaly detection. Within these studies, machine learning methods and models were actively used, which are capable of learning to detect intrusions directly from network traffic data.

Known intrusion detection systems have certain disadvantages, among which the need for a large amount of data for training models, false positives due to insufficient

data or limited accuracy of models, instability of machine learning models when working with large volumes of data, a high number of errors when detecting anomalies, the inability to recognize new types of threats that were not included in the training data, the complexity of setting up machine learning models and the need for a large amount of computing resources for their training and operation.

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 introduction substantiates the relevance of the work and gives its general characteristics. The first section of the study is devoted to the analysis of practical and scientific-methodological approaches to managing information security and detecting intrusions into the company's information network. The promising development direction of intrusion detection systems is defined as the use of the ensemble learning method and fuzzy logic tools. In the second section, the factors of the information technology security strategy of a modern enterprise are analyzed, the information security threats and information risks of the enterprise's document processing are modeled based on fuzzy logic and the method of analyzing hierarchies. In the third

chapter, the key aspects of the development of methods for detecting intrusions into the information system of the enterprise and the selection of a set of features for training intrusion classification models are considered. In the fourth chapter, a study of the effectiveness of the proposed methods of detecting intrusions and the development of recommendations for improving the structure and algorithms of the information security management system of the enterprise is carried out.

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 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.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА

Наукові праці, в яких опубліковані основні наукові результати дисертації:

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.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

8. Чичкарьов Є.А., Зінченко О.В., Бондарчук А.П., Асєєва Л.А. Використання алгоритмів машинного навчання і нечіткої логіки для виявлення мережевих вторгнень з використанням комплексу наборів даних. *«Systems and measures of artificial intelligence» AIIS'2023International scientific youth school*: Матеріали Міжнародної наукової молодіжної школи «Системи та засоби штучного інтелекту», м. Київ, 10–11 жовт.2023 р. / ІПШІ «Наука і освіта» Київ, 2023. С. 13 – 15.

9. Кожухівський А.Д., Асєєва Л.А. Оцінка ризиків конфіденційності документів проектів з застосуванням нечіткої логіки. *Проблеми інформатики та комп'ютерної техніки*: Праці Х-ї Міжнародної наук.-практ. конф. (ПІКТ – 2021),

м. Чернівці, 28 – 31 жовтня 2021 р. / Чернівці, 2021. С. 109–112.

10. Асєєва Л.А. Формалізація функції належності нечітких факторів управління інформаційною безпекою підприємства з використанням методу аналізу ієрархій. *IX Всеукраїнська науково-практична конференція з автоматичного управління* : Матеріали IX Всеукраїнської наук.-практ. конф. здобув. вищої освіти та молодих вчених з автоматичного управління присвяченої Дню космонавтики, м. Херсон, 12 – 14 квітня 2021 р. / Ред. Г.В. Рудакової та ін. Херсон: Видавництво ФОП Вишемирський В.С. Херсон, 2021. С. 36.

11. Кожухівський А.Д., Асєєва Л.А. Нечітке управління ризиками в інформаційній безпеці підприємства. *Комп'ютерна математика в науці, інженерії та освіті CMSEE-2020* : Матеріали V Всеукраїнської наук.-техн. конф., м. Полтава, 27 листопада 2020 р. / ред.: О.М. Гайтан – Полтава: Національний університет «Полтавська політехніка імені Юрія Кондратюка», 2020. С.69–70.

12. Асєєва Л.А. Підходи до класифікації складових небезпеки при побудові систем управління інформаційною безпекою підприємств. *VIII Всеукраїнська науково-практична конференція з автоматичного управління* : Матеріали VIII Всеукраїнської наук.-практ. конф. студентів, аспірантів та молодих вчених з автоматичного управління присвяченої Дню космонавтики, м.Херсон, 08 – 10 квітня 2020р./ Ред. Г.В. Рудакової та ін. Херсон: Видавництво ФОП Вишемирський В.С. Херсон, 2020. С.41.

13. Асєєва Л.А. Аналіз загроз інформаційної безпеки будівельного підприємства. *Проблеми інформатизації*: тези доп. тринадцятої міжнародної наук.-техн.конф., 11-12 квітня 2019 р./ Київ: ДУТ, НТУ; Полтава: ПНТУ; Катовице: КЕУ; Париж: Університет Париж VII Вєнсент-Сен-Дені; Вільнюс: ВДТУ; Харків : ХНДІТМ: Білорусь: БДАЗ; Кропивницький: ЛА НАУ, 2019. С.182.

14. Асєєва Л.А. Система управління інформаційною безпекою будівельного підприємства на принципах нечіткої логіки. *Проблеми*

інформатизації : тези доп. дванадцятої міжнародної наук.-техн. конф., 12 - 13 грудня. – 2018р./ Київ : ДУТ, НТУ; Полтава: ПНТУ; Катовице: КЕУ; Париж: Університет Париж VII Вєнсент-Сен-Дені; Вільнюс: ВДТУ; Харків : ХНДІТМ: Білорусь: БДАЗ, 2018. С.146–147.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ 18
ВСТУП 19
РОЗДІЛ 1. ОГЛЯД ІСНУЮЧИХ ПІДХОДІВ ДО УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ТА ВИЯВЛЕННЯ ВТОРГНЕНЬ В КОРПОРАТИВНУ МЕРЕЖУ ПІДПРИЄМСТВА 26
1.1 Загальна характеристика питань кібербезпеки інформаційних систем підприємств 26
1.2 Дослідження використання машинного та глибокого навчання у кібербезпеці 35
1.2.1 Методи протидії кібератакам 35
1.2.2 Використання методів обрання ознак і зменшення розмірності .. 37
1.2.3 Огляд застосування ансамблевого навчання для побудови систем виявлення вторгнень 41
1.3 Аналіз використання нечіткої логіки для моделювання ризиків інформаційної безпеки та побудови систем виявлення вторгнень 44
1.4 Огляд наборів даних для побудови систем виявлення вторгнень 46
1.5 Аналіз протиріч та постановка наукового завдання 48
Висновки до розділу 1 50
РОЗДІЛ 2. МОДЕЛЮВАННЯ ТА ФОРМАЛІЗАЦІЯ ФАКТОРІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА 52
2.1 Аналіз факторів стратегії безпеки інформаційних технологій сучасного підприємства 52

2.2 Моделювання загроз інформаційної безпеки та інформаційних ризиків роботи підприємства 64

Висновки до розділу 2 87

РОЗДІЛ 3. РОЗРОБКА МЕТОДІВ ТА МОДЕЛЕЙ ВИЯВЛЕННЯ ВТОРГНЕНЬ ДО ІНФОРМАЦІЙНОЇ СИСТЕМИ ПІДПРИЄМСТВА 89

3.1 Аналіз наборів даних для тренування моделей машинного навчання виявлення вторгнень та їх підготовка 89

3.1.1 Набір даних KDD Cup 1999 89

3.1.2 Набір даних NSL-KDD 91

3.1.3 Набір даних UNSW-NB15 96

3.1.4 Набір даних CSE-CIC-IDS2018 99

3.1.5 Набір даних Litnet-2020 103

3.2 Розробка методу обрання набору ознак для навчання класифікаторів вторгнень 104

3.2.1 Загальна характеристика методів вибору ознак 105

3.2.2 Попередня обробка даних 107

3.2.3 Методи вибору ознак 109

3.2.4 Дослідження методів відбору результативного набору ознак 115

3.2.5 Пропонований метод нечіткого обрання важливих ознак 118

3.3 Розробка гібридного методу ідентифікації вторгнень на основі ансамблевого навчання та алгоритмів нечіткої логіки 122

3.3.1 Порівняння варіантів класифікаторів для моделі ідентифікації вторгнень 122

3.3.2 Розробка структури модуля оцінювання системи виявлення вторгнень 125

3.3.3 Дослідження деяких ансамблевих класифікаторів 128

3.3.4 Алгоритм нечіткого голосування 130

3.3.5 Дослідження швидкості і точності класифікаторів для системи виявлення вторгнень 132

Висновки до розділу 3 134

РОЗДІЛ 4. РОЗРОБКА РЕКОМЕНДАЦІЙ З УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ТА ВИКОРИСТАННЯ СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ 136

4.1 Оцінка ефективності та достовірності застосування розроблених методів для виявлення вторгнень 136

4.2 Розробка рекомендацій щодо впровадження системи виявлення вторгнень в інформаційній системі підприємства 143

4.3 Розробка рекомендацій щодо оцінки ризиків в інформаційній системі підприємства 146

Висновки до розділу 4 151

ВИСНОВКИ 153

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 156

ДОДАТОК А. СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА 178

ДОДАТОК Б. АКТИ ВПРОВАДЖЕННЯ 182

ДОДАТОК В. ОПИС ОЗНАК НАБОРУ ДАНИХ CSE-CIC-IDS2018 186

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

IDS - Intrusion Detection System, система виявлення вторгнень

IPS - Intrusion Prevention System, система запобігання вторгнення

ML - Machine learning, машинне навчання

DL - Deep learning. глибоке навчання

DM - інтелектуальний аналіз даних

FS - feature selection, обрання ознак

DR - dimensionality reduction, зменшення розмірності

ШІ - штучний інтелект

KNN - K-найближчий сусід

IoT - Internet of things, Інтернет речей

CVSS - Common Vulnerability Scoring System

ЕЦП - електронний цифровий підпис

DTC - алгоритми дерева рішень

ВСТУП

Актуальність теми дослідження.

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. В умовах загального зростання рівня кіберзлочинності, різноманіття форм та видів використання під час здійснення атак певними державами, організаціями чи окремими злочинцями вразливостей інформаційних технологій необхідне системне застосування методів та засобів кібербезпеки. Для забезпечення надійного захисту інформаційної системи підприємства звичайних антивірусів і брандмауерів вже недостатньо, тому значна увага приділяється теоретичним та практичним аспектам розробки багаторівневих систем управління інформаційною безпекою. Одними з основних складових побудови та використання таких систем є оцінка ризиків інформаційної безпеки та виявлення мережевих вторгнень.

Виявлення, аналіз, прогнозування та обробка ризиків інформаційної безпеки ґрунтується на використанні моделей та методів їх оцінки. Враховуючи наявність невизначеності та розмитості інформації про діяльність підприємств, нечітка логіка отримала широке застосування в таких моделях. Беручи до уваги, що вимірювання характеристик кібербезпеки досі залишається недостатньо розвинутою темою, в тому числі стосовно безпеки документів підприємства, подальші дослідження в цьому напряму є актуальними.

Однією з найважливіших складових захисту інформаційної системи підприємства є система виявлення вторгнень або англійською Intrusion Detection System (IDS). Сучасні IDS діляться на такі дві основні категорії: виявлення вторгнень на основі сигнатур (або «виявлення неправильного використання») та виявлення аномалій.

Для виявлення загроз безпеці інформаційної системи на основі сигнатур IDS порівнює отримані дані з відомими моделями атак. Цей метод є дуже ефективним та надійним, однак він може виявити лише відомі атаки, які вже описані в базі даних системи.

Підхід на основі виявлення аномалій передбачає побудову моделі нормальної поведінки інформаційної системи, а потім здійснення IDS пошуку відхилень в даних моніторингу. Це дозволяє виявити також і невідомі атаки, але часто створює значну кількість помилкових тривог. Враховуючи, що кібератаки стають все більш численними та різноманітними, багато досліджень протягом останніх двох десятиліть було зосереджено на побудові IDS саме на основі виявлення аномалій. В межах цих досліджень активно застосовувалися методи та моделі машинного навчання, які здатні навчатися виявляти вторгнення безпосередньо з даних мережевого трафіку.

Відомі системи виявлення вторгнень мають певні недоліки, серед яких можна виділити потребу у великій кількості даних для навчання моделей, помилкові спрацювання внаслідок недостатньої кількості даних або обмеженої точності моделей, нестабільність моделей машинного навчання при роботі з великими обсягами даних, високу кількість помилок при виявленні аномалій, невміння розпізнати нові типи загроз, які не були включені до тренувальних даних, складність налаштування моделей машинного навчання і потребу в великій кількості обчислювальних ресурсів для їх тренування та експлуатації.

У зв’язку з цим існує необхідність вирішення 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.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційне дослідження відповідає вимогам статті 5 Закону України «Про пріоритетні напрями розвитку науки і техніки» від 11 липня 2001 рок № 2623 -III

(зі змінами та доповненнями від 12.01.2023 р.), пункту першого розділу другого «Переліку пріоритетних тематичних напрямів наукових досліджень і науково-технічних розробок на період до 2023 року», затвердженого Постановою КМУ від 7 вересня 2011 р. № 942.

Дисертаційна робота виконана відповідно з поточними та перспективними планами наукової та науково-технічної діяльності Державного університету інформаційно-комунікаційних технологій. Тематика дисертаційного дослідження відповідає тимчасовому стандарту та фаховим компетентностям освітньо-наукової програми підготовки докторів філософії з кібербезпеки Державного університету інформаційно-комунікаційних технологій Міністерства освіти і науки України, а саме: фундаментальним науковим дослідженням теоретико-методологічних, науково-методичних та прикладних засад підвищення ефективності інноваційної та виробничої діяльності підприємства, а також проведення науково-дослідних та дослідно-конструкторських робіт, пов'язаних зі створенням та реалізацією політик безпеки у сфері інформаційно-комунікаційних технологій, дослідженням проблем розвитку та вдосконаленням технологій криптозахисту інформації, дослідженням методів і засобів підвищення живучості ІКС в умовах впливу кібернетичних атак тощо.

Результати дисертаційної роботи є складовою науково-дослідної роботи "Забезпечення функціональної стійкості інформаційних систем підприємства в умовах впливу дестабілізуючих факторів із застосуванням нейронних мереж" (РК № 0121U107501).

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 необхідно виконати 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.

Об'єкт дослідження: процес управління інформаційною безпекою підприємства з використанням системи виявлення вторгнень.

Предмет дослідження: методи, моделі та архітектурні підходи до управління інформаційною системою підприємства з використанням системи виявлення на базі алгоритмів машинного навчання та нечіткої логіки.

Методи дослідження. В дослідженні використано методи: системного та порівняльного аналізу з метою визначення актуальності роботи та постановки наукового завдання; теорії множин для формалізації об'єктів предметної області та зв'язків між ними; нечіткої логіки в широкому розумінні для моделювання ризиків інформаційної безпеки, класифікації атак та оцінки важливості їх ознак; аналізу ієрархій для оцінки характеристик ризиків інформаційної безпеки; машинного навчання для виявлення вторгнень та обрання набору ознак для навчання класифікаторів.

Наукова новизна одержаних результатів полягає в наступному:

1. 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.

2. 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.
3. 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" (акт реалізації від 28.09.2023 р.), в ТОВ "РЕНТСОФТ" (акт реалізації від 26.09.2023 р.), в навчальному процесі Державного університету інформаційно-комунікаційних технологій (акт реалізації від 29.09.2023 р.).

Особистий внесок здобувача. Основні наукові та практичні результати дослідження отримані автором особисто. В дисертаційній роботі використані лише ті з результатів, що були опубліковані у наукових працях у співавторстві, які є індивідуальним внеском автора.

В роботах, які написані в співавторстві, автору належить: [1] – метод побудови набору важливих ознак для вирішення задачі навчання класифікаторів вторгнень; [2] – метод виявлення вторгнень на основі ансамблевого підходу на базі алгоритмів нечіткої логіки для поєднання результатів класифікації даних окремими моделями машинного навчання; [3] – модель оцінки ризиків інформаційної безпеки порушення доступності документів проекту на засадах нечіткої логіки; [4] – модель для оцінки можливості порушення цілісності документів та шкоди від такого порушення на основі математичного апарату нечіткої логіки; [5] – модель для оцінки ризику від порушення конфіденційності документа на засадах нечіткої логіки, яка дозволяє врахувати неповноту та розмитість даних; [6] – дослідження факторів інформаційної безпеки підприємства та рекомендації для її забезпечення.

Апробація результатів дисертації. Результати дослідження, представлені у дисертаційній роботі, доповідались на міжнародних та всеукраїнських конференціях: XXIII Міжнародна науково-технічна конференція «Штучний інтелект та інтелектуальні системи» (AIIS’2023) (10-11 жовтня, 2023, м. Київ); X Міжнародна науково-практична конференція «Проблеми інформатики та комп’ютерної техніки» (ПІКТ – 2021) (28 – 31 жовтня, 2021,м.Чернівці); IX Всеукраїнська науково-практична конференція здобувачів вищої освіти та молодих вчених з автоматичного управління (12 – 14 квітня, 2021,м. Херсон); V Всеукраїнська науково-технічна конференція «Комп’ютерна математика в науці, інженерії та освіті CMSEE-2020» (27 листопада, 2020, м. Полтава); VIII Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених з автоматичного управління (08 – 10 квітня, 2020, м. Херсон); Тринадцята

міжнародна науково-технічна конференція «Проблеми інформатизації» (11-12 квітня, 2019, м. Київ-м.Полтава-м.Катовице-м.Париж-м.Вільнюс-м.Харків-м.Мінськ); Дванадцята міжнародна науково-технічна конференція «Проблеми інформатизації» (12-13 грудня, 2018, м.Київ-м.Полтава-м.Катовице-м.Париж-м.Вільнюс-м.Харків-м.Мінськ).

Публікації. Результати дисертаційної роботи опубліковано у 14 наукових працях, у тому числі: 7 наукових статей [1-7], серед яких 1 стаття в іноземному науковому виданні, що індексується в наукометричній базі Scopus [3], та 6 наукових статей у періодичних виданнях України, що включені до переліку наукових фахових видань України, в яких можуть публікуватися результати дисертаційних робіт на здобуття наукових ступенів [1,2,4,5,6,7]; 7 тез доповідей в матеріалах наукових конференцій [8-14].

Структура і обсяг роботи. Дисертація складається зі вступу, 4 розділів, висновків, списку використаних джерел зі 169 найменувань та 3 додатків. Загальний обсяг дисертаційної роботи складає 189 сторінок, з яких 137 сторінок основного тексту.

РОЗДІЛ 1
ОГЛЯД ІСНУЮЧИХ ПІДХОДІВ ДО УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ТА ВИЯВЛЕННЯ ВТОРГНЕНЬ В КОРПОРАТИВНУ МЕРЕЖУ ПІДПРИЄМСТВА

В даному розділі наведено загальну характеристику питань кібербезпеки інформаційних систем підприємств, досліджено використання машинного та глибокого навчання у кібербезпеці, проведено аналіз використання нечіткої логіки для моделювання ризиків інформаційної безпеки та побудови систем виявлення вторгнень, виконано огляд наборів даних для побудови систем виявлення вторгнень та здійснено постановку задачі дослідження.

1.1 Загальна характеристика питань кібербезпеки інформаційних систем підприємств

Прийняття запобіжних заходів щодо реалізації так званої тріади цілей інформаційної безпеки, що полягає в забезпеченні конфіденційності, цілісності, доступності інформації є основним підходом у створенні систем кібербезпеки. З використанням персональних комп’ютерів та Інтернету виникли та продовжують вдосконалюватися прийоми добре обізнаних у відповідній області та високо мотивованих суб’єктів незаконного отримання інформації [15, 16]. Якщо раніше для цього необхідно було заволодіти і винести з об’єкта цілі купи паперових документів, або їх копій, подолати розвинуті перепони системи контролю фізичного доступу до місця знаходження інформації, то зараз величезні обсяги важливих відомостей можна просто «злити» на флешку, що міститься в брелоку, відправити по мережі, вдавшись до використання сімейства руткітів, троянів,

бекдор, кейлоггеров і ботнетів, отримати віртуальний доступ, або їх знищити за допомогою вірусів, влаштувавши атаку.

Відповідно до ISMS Framework, який розроблено міжнародною європейською агенцією з кібербезпеки, в основі побудови системи управління інформаційною безпекою є визначення підходів до виявлення, аналізу, прогнозування та обробки ризиків [17]. Але навіть у міру зростання ризиків та витрат на основі кібербезпеки, вимірювання кібербезпеки залишається недостатньо розвиненою темою, у якій немає стандартної систематики для таких термінів, як “вимірювання” та “показники”, тому розробка та узгодження надійних способів вимірювання ризиків та ефективності є актуальним для досліджень [18].

Підходи до формулювання основ та принципі побудови систем інформаційної безпеки виробничих підприємств викладено в [19 – 21]. В [22] проведені дослідження для формулювання визначення “інформація”, “інформаційна безпека”, “інформаційна безпека підприємства”, які проаналізовані у спробах вирішити проблеми забезпечення економічної безпеки підприємства як розвиток напрямку організаційно-управлінської діяльності підприємств з підкресленням особливого аспекту інформації і розширення комунікативних зв’язків. В тому числі визначені об'єкти, що входять в систему обмінних комунікативних зв'язків в процесу розвитку виробничо-господарської діяльності і формують його загрози: потоки інформації, інвестиції і фінансування, поставки тмц, придбання нових технологій, патентів, ліцензій, залученість кваліфікованого персоналу. Важливою складовою захисту інформації є кадри (персонал) як потенційне джерело розголошення комерційної таємниці навмисно чи не передбачено. Сформовано варіант концепції інформаційної безпеки підприємства [23].

Результати аналізу наявних робіт в галузі інформаційної безпеки дозволяють виділити два основні підходи до її забезпечення: оцінювання та

управління ризиками інформаційної безпеки та реалізація базового рівня інформаційної безпеки.

Оцінюванню та управлінню ризиками інформаційної безпеки присвячено роботи [24 – 27]. В цих роботах вирішуються такі основні завдання (зазвичай, після забезпечення базового рівня інформаційної безпеки):

- аналіз загроз і вразливостей в корпоративних інформаційних мережах, оцінка можливості їх реалізації та можливих збитків;
- оцінка ризиків інформаційної безпеки і визначення актуальних загроз для корпоративних інформаційних мереж;
- формування множини захисних заходів і зниження ризиків інформаційної безпеки до прийнятного рівня.

Існує кілька підходів до визначення поняття ризику інформаційної безпеки:

- оцінка можливого збитку, що наноситься організації або активу в результаті реалізації певної загрози [28];
- поєднання ймовірності події та її наслідків[29];
- подія, яка, якщо вона виникає, негативно впливає на здатність проекту досягати своїх цілей у результаті [30];
- можливість отримання збитку чи виникнення негативних наслідків [31].

Оцінка ризиків інформаційної безпеки часто застосовується для сучасних корпоративних інформаційних мереж, тому що вона дозволяє будувати ефективні системи захисту інформації враховуючи потенційно можливі збитки, а також досліджувати економічні деталі реалізації захисних заходів. Однак заявлені підходи не враховують в повній мірі структурування інформації підприємства у вигляді документів, неповноту та розмитість інформації, що обумовлюють необхідність подальших досліджень в цій галузі [11].

Для реалізації базового рівня інформаційної безпеки розроблено багато нормативних документів та стандартів [32 – 41]. Як правило, ці документи визначають та дозволяють вирішити дві основні задачі: переконатися в тому, що

компоненти комп’ютерної інформаційної мережі (КІМ) задовольняють всім обов'язковим вимогам стандартів і керівних документів та переконатися в тому, що компоненти КІМ захищені від усіх видів основних загроз. Щоб створювати та вдосконалювати ефективні системи інформаційної безпеки підприємств необхідно проаналізувати основні складові небезпеки [7].

Центром уваги фахівців у галузі кібербезпеки визначено вразливості, загрози, та атаки. Під атакою більшість авторів розуміють навмисне використання виявлених вразливостей чи спробу реалізації існуючих загроз комп'ютерних інформаційних систем як з конкретною метою, так і просто для розваги. За визначення CERT загрозами є будь-які обставини або події, які можуть спричинити шкоду системі або мережі [7,16].

Вразливості визначаються як [16]:

- функція або помилка в системі або програмі, яка дозволяє зловмисникам обходити заходи безпеки;
- аспект системи або мережі, що залишає її відкритою для атаки;
- відсутність або слабкість ризику зменшення гарантій, які мали б потенціал для того, щоб загроза могла відбуватися з більшою частотою чи більшим впливом;
- вада, яка робить ціль атаки сприйнятливою до нападу.

Три зазначені складові в кіберпросторі атаки, загрози, та вразливості є ключовими сутностями в структурі небезпеки та одночасно явищами через які небезпека реалізується [7]. У кіберзлочинців можуть бути різні мотиви для вибору цілі атаки. Вони постійно шукають та виявляють вразливі системи. Існуючі міжнародні кримінальні мережі спричиняють збитки, що обчислюються в мільярдах доларів [42, 43]. Незалежно від того, чи буде об’єкт атаки великою корпорацією або мікро-бізнесом, жодна організація не може бути гарантовано уникнути перевірки хакерів [44].

Вразливості програмного забезпечення перераховані в списку Common Vulnerabilities and Exposures (CVE), який є розробкою The MITRE Corporation, що спеціалізується в області системної інженерії та веде розробки й дослідження в інтересах органів державної влади США [45]. В результаті роботи сканерів вразливостей різних розробників перелік знайдених помилок описується із використанням списку CVE, чим дозволяє порозумітися фахівцям при описуванні явищ та допомагає уникати неоднозначності.

Результатом продовження роботи MITRE над CVE стала розробка CWE. Призначений для розробників і фахівців щодо забезпечення безпеки програмного забезпечення загальний перелік вразливостей і недоліків безпеки програмного забезпечення створено й поширено в фаховому середовищі CWE (Common Weakness Enumeration) у вигляді ієрархічного словника [7, 46]. Ідентифікатори CWE використовуються для відстеження проблем, що виникають під час діяльності з розробки програмних продуктів.

Розглянуті списки та класифікатори вразливостей і атак можуть бути використані для опису та дослідження складових небезпеки, в тому числі при створенні складових системи управління інформаційною безпекою окремого підприємства та розробки комплексу заходів для їх попередження [12].

На думку [47] основним засобом захисту інформаційних систем та мереж від інформаційно-руйнівних впливів (втручань) у вигляді кібернетичних вторгнень є системи виявлення та/або запобігання вторгненням (СВВ/СЗВ), основне завдання яких зводиться до оперативної їх ідентифікації (встановлення відповідності між об’єктом і його ідентифікатором (унікальним атрибутом) та в ідеальному випадку ініціювання ефективного захисного сценарію щодо припинення факту порушення конфіденційності, доступності та цілісності інформаційних ресурсів, сервісів. Практика застосування СВВ сформувала два напрями протидії кібернетичним вторгненням: виявлення зловживань (Misuse detection) та виявлення аномалій (Anomaly detection).

За даними [48] основним напрямом досліджень систем виявлення вторгнень є впровадження пошуку вторгнень на основі пошуку аномальної активності.

На думку [49] системи захисту комп'ютера від чужого вторгнення дуже різноманітні та класифікуються, як:

1) засоби власного захисту, передбачені загальним програмним забезпеченням;

2) засоби захисту у складі обчислювальної системи;

3) засоби захисту із запитом інформації;

4) засоби активного захисту;

5) засоби пасивного захисту та інші.

На думку [50], ефективність і якість функціонування інформаційно-керуючої системи суттєво залежить від достовірності інформації, що надходить на вхід керованих обчислювальних систем, від різних видів джерел інформації, які контролюють стан і параметри функціонування ІУС. Реальні джерела інформації мають граничну точність відображення контрольованої ними інформації.

Кібератака — це не що інше, як спосіб порушення функцій комп’ютера в мережі жертви або отримання несанкціонованого цифрового доступу до комп’ютера жертви шляхом усунення захисту. Згідно з визначенням Інституту досліджень технологій безпеки Дартмутського коледжу, кібератака розглядається як атака на комп’ютерну систему, яка порушує конфіденційність, цілісність або доступність інформації в цій системі. Кібератаки можна класифікувати за різними категоріями з різних точок зору. Найважливішими типами кібератак є відмова в обслуговуванні, логічна бомба, інструменти зловживання, сніфер, троянський кінь, вірус, хробак, надсилання спаму та ботнет (див. рис. 1.1). Приклади групування кібератак на основі наслідків, які вони завдають системі чи її архітектурі, за даними [51,52] наведено на рисунку 1.2.

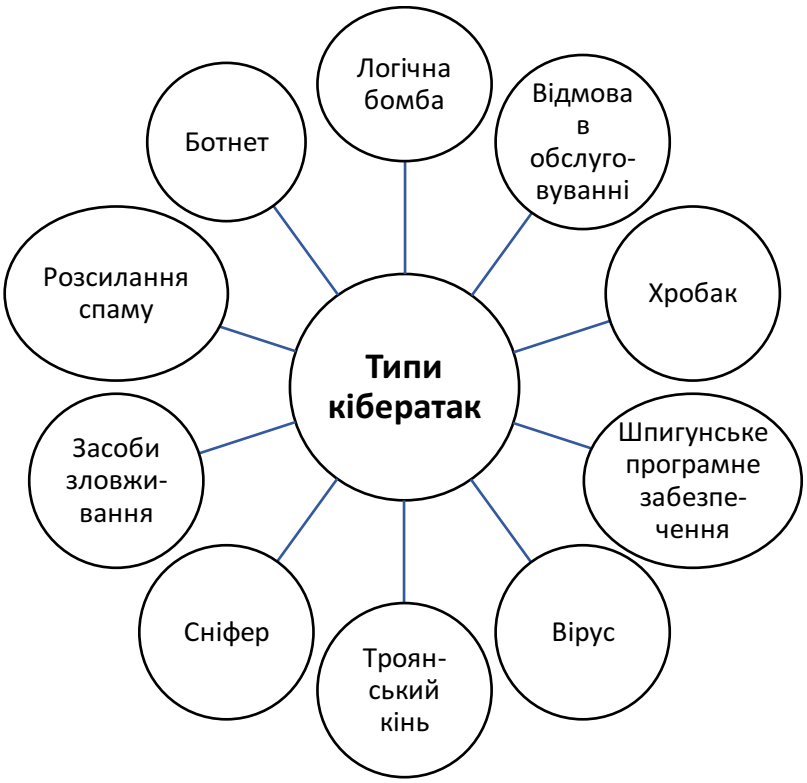


Рис. 1.1. Класифікація кібератак

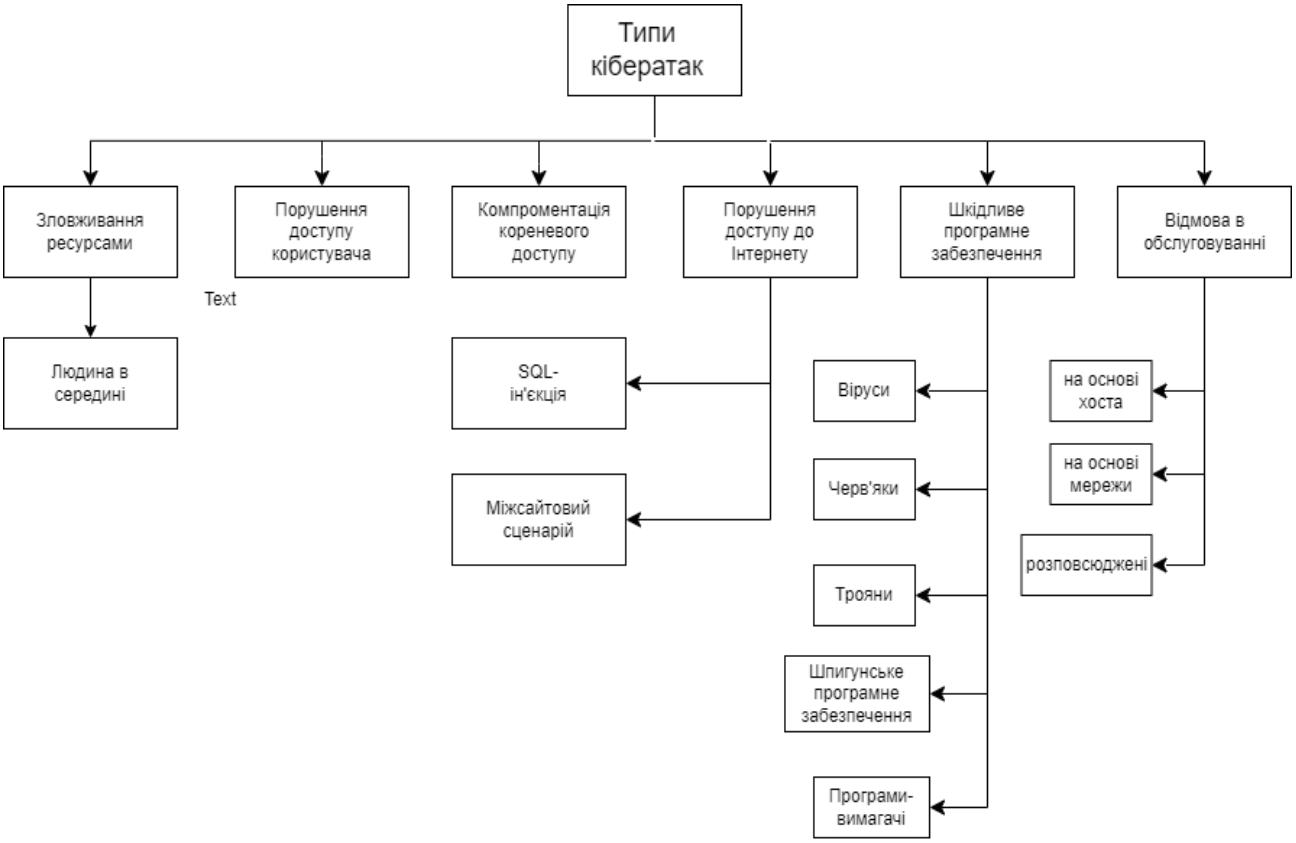


Рис. 1.2. Приклад групування кібератак основі наслідків, які вони завдають системі чи її архітектурі

Система виявлення вторгнень (intrusions detection system - IDS) складається з механізму виявлення вторгнень, а також механізму запобігання вторгненням. IDS, як правило, складається з поєднання програмного та апаратного забезпечення для спостереження та керування мережевими діями в мережі [53-56]. Детальна класифікація IDS (за даними [57]) наведена на рисунку 1.3.

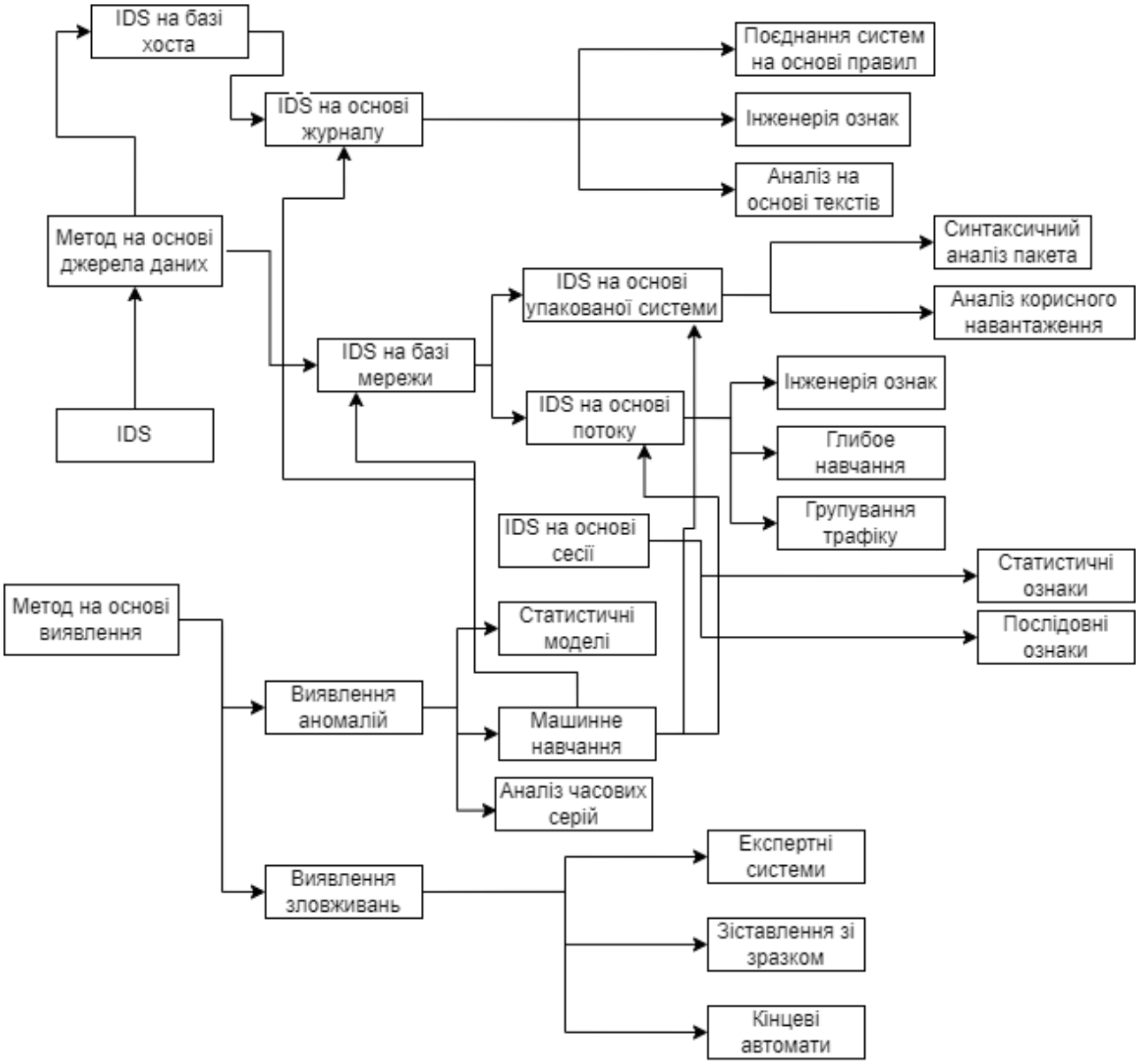


Рис. 1.3. Класифікація систем виявлення вторгнень (IDS)

Як видно на рисунку 1.3, за призначенням і механізмом виявлення IDS можна класифікувати на дві різні групи. Існує два типи методів класифікації IDS:

метод на основі виявлення та метод на основі джерела даних. Методи на основі виявлення також підрозділяються на виявлення на основі неправильного використання та виявлення на основі аномалій, тоді як методи на основі джерела даних класифікуються на методи на основі мережі та на основі хоста.

Ідея методу виявлення на основі сигнатур полягає в збереженні відомих або побачених атак як сигнатур у базі даних. Перевага методу виявлення зловживання полягає в тому, що він швидкий і має низький рівень помилкових тривог; недоліками є висока частота помилкових тривог для невідомих або нульових типів атак і те, що необхідно підтримувати велику базу даних. З іншого боку, виявлення на основі аномалій зберігає профіль для всіх нормальних дій і виявляє аномалії на основі ступеня відхилення від цього профілю. Перевагою виявлення на основі аномалій є його здатність виявляти невідомі атаки, а недоліками є висока частота помилкових тривог і неможливість визначити можливі причини порушення.

Метод на основі джерела даних полягає в тому, що вторгнення з певного хоста може бути легко виявлено IDS на основі хоста. Перевага цієї техніки в тому, що IDS можуть дуже точно виявляти поведінку мережевих об’єктів, таких як програми, файли та порти, а обмеження полягають у тому, що ця система залежить від ресурсів хоста та не може виявляти мережеві аномалії чи атаки. З іншого боку, мережеві IDS не залежать від ресурсів хоста та розгортаються на основних комутаторах, таких як маршрутизатори. Перевагами цієї системи є те, що вона не залежить від операційної системи (ОС) і здатна ідентифікувати конкретні типи мережевого протоколу. Основним обмеженням є те, що ця система призначена лише для моніторингу даних, що проходять через певну мережу.

Для покращання функціонування систем виявлення вторгнень активно застосовуються методи машинного навчання, тому необхідно їх розглянути більш детально.

1.2 Дослідження використання машинного та глибокого навчання у кібербезпеці

1.2.1 Методи протидії кібератакам

В останні роки методи обчислювального інтелекту, включаючи машинне навчання (ML), глибоке навчання (DL) і інтелектуальний аналіз даних (DM) використовувався для забезпечення кібербезпеки [58-60]. Ряд сучасних систем виявлення вторгнень використовують різні методи інтелектуального аналізу даних для виявлення атак і вторгнень. В основі таких систем лежать різні методики: методи Data Mining; пошук асоціативних правил; побудова імунних систем; марковскі процеси; дерева прийняття рішень; генетичні алгоритми; нейронні мережі. Експерименти [61] показали високу якість виявлення мережевих атак і довели правильність вибору методів інтелектуального аналізу даних і застосовність вироблених методик. За думкою [62, 63], ML надає великі функціональні можливості з організації кібербезпеки та є в планах використання бізнесу .

Глибоке навчання (DL) – це клас алгоритмів [64], який використовує кілька шарів для поступового вилучення функцій вищого рівня з вихідного входу. Основні відмінності між ML та DL полягають у наступному: алгоритми ML майже завжди вимагають структурованих даних, тоді як мережі DL покладаються на рівень штучних нейронних мереж (ANN). Часто в ML, втручання людини необхідне для отримання подальших результатів з більшим набором даних, тоді як в DL це не потрібно. Однією з основної концепцій DL є ANN.

Багато статей висвітлюють використання штучного інтелекту та методів глибокого навчання як заходів безпеки, а також як шкідливу кіберзброю. В роботі [65] проаналізовано декілька варіантів застосування штучного інтелекту у кібербезпеці (не обмежуючись глибоким навчанням), в тому числі нейронні

мережі та інтелектуальні агенти, а також випадки використання ШІ в програмах безпеки. Робота [66] розглядає виключно методи глибокого навчання, які посилюють заходи безпеки проти кібератак. Автори [65] дослідили різні моделі машинного навчання та представили їх у категоріях різних програм безпеки, таких як виявлення шкідливих програм, класифікація спаму та програми-вимагачі. Автори [67] поділили проблеми та атаки на три різні типи безпеки: фізичну, цифрову та соціальну. Розглянуто рекомендації, яких слід дотримуватися при роботі з ШІ, і стратегічний аналіз впливу ШІ в майбутньому на безпеку.

Автори [68] підкреслили вразливість алгоритмів машинного навчання до агресивних атак і необхідність точного налаштування параметрів і повторного навчання для кращих результатів. В роботі [69] розглянуто різні атаки на алгоритми машинного навчання та запропоновано засоби захисту від них. В роботі [70] було вивчено змагальні атаки на системи, що розгортають моделі глибокого навчання для аналізу зображень.

Впровадження методів машинного навчання у розробку IDS широко вивчалося протягом останнього десятиріччя [71]. Моделі машинного навчання показали перспективні результати в прогнозуванні або класифікації даних у багатьох областях досліджень, і в контексті IDS ML використовується для класифікації того, чи є трафік безпечним чи атакуючим [72].

Більшість досліджень використовують кілька моделей ML та кілька наборів даних для оцінки. У роботі [73] було побудовано десять моделей для IDS, включаючи як контрольовані, і неконтрольовані моделі машинного навчання. Автори оцінили кілька моделей машинного навчання та представили детальне порівняльне дослідження з допомогою набору даних CIDDS-001. У роботі [74] узагальнено результати понад 40 робіт, в яких реалізовано глибоке навчання для IDS, та описано 35 відомих наборів даних в області IDS. Автори також реалізували сім моделей глибокого навчання та порівняли продуктивність з підходами NaiveBayes, ANN, SVM та RandomForest. У дослідженні були

використані набори даних CSE-CIC-IDS2018 та Bot-IoT. Результат показує, що моделі глибокого навчання досягли рівня виявлення 95%, що перевищує рівень виявлення 90%, досягнутий іншими моделями. У роботі [75] порівнювалася продуктивності SVM, KNN та DT з використанням декількох наборів даних (CSE-CIC-IDS2018, UNSW-NB15, ISCX-2012, NSLKDD та CIDDS-001). Результати дослідження показали, що точність моделей варіювалася від 95% до 100%, крім набору даних UNSW-NB15. DT незмінно показує найкращі результати серед усіх реалізованих моделей незалежно від набору даних.

Незважаючи на наявність досвіду використання різноманітних класифікаторів для побудови систем виявлення вторгнень, досі незрозуміло, які методи машинного навчання є більш надійними та ефективними (особливо для створення динамічної IDS).

Важливим компонентом ефективної системи запобігання атакам є час перенавчання і класифікації, тому важливо розглянути шляхи прискорення процесу створення та налагодження системи. В першу чергу для цього необхідно зменшення часу обчислення, необхідного системам виявлення вторгнень [76]. Одним з варіантів вирішення цієї задачі є скорочення набору ознак.

1.2.2 Використання методів обрання ознак і зменшення розмірності

Для підвищення продуктивності IDS використовувались різні методи обрання ознак (FS) і зменшення розмірности (DR). Набори даних, які використовують для навчання систем виявлення вторгнень, відносно великі і мають досить велику розмірність простору ознак. Більшість досліджень використовують кілька моделей машинного навчання та кілька наборів даних для оцінки. Для великого набору даних важливо обрати метод вибору ознак для виключення непотрібних ознак та використовувати лише набір важливих ознак

як на етапі навчання, так і на етапі тестування. Вибір ознак - це процес зменшення кількості вхідних змінних при побудові прогнозної моделі. Оскільки IDS має справу з даними, які мають нерелевантні або надмірні ознаки, зменшення кількості ознак не лише зменшує обчислювальні витрати, а й покращує показник точності виявлення. Наприклад, у роботі [77] реалізовано класифікатори на базі алгоритмів Random Forest (RF), Bayes Net (BN), Random Tree (RT), Naive Bayes (NB), J48, проведено експерименти на наборі даних CICIDS-2017. Кількість релевантних та значущих ознак, отриманих за допомогою фільтації, суттєво впливає на підвищення точності виявлення та часу виконання.

Однак різні підходи до вибору набору релевантних ознак дають підмножини ознак, які не збігаються [78]. В роботі [79] досліджено ефективні методи вибору ознак поліпшення виявлення вторгнень з допомогою методів машинного навчання. Для аналізу сукупних ознак використовувалися різні методи класифікації (SVM, Decision Tree, Naive Bayes) для вибору ознак з високим рейтингом, які об'єднувалися і передавалися в класифікатор штучної нейронної мережі для того, щоб розрізнити напад і нормальну поведінку. Результати експериментів показують високу точність і ефективність запропонованого методу. У роботі [80] проведено дослідження з використання нейронних мереж для виявлення атак ботнетів під час навчання за набором даних CSE-CIC-IDS2018. За рахунок оптимізації гіперпараметрів було досягнуто точності 99,97% при середньому показнику помилкових спрацьовувань всього 0,001.

При порівнянні різних алгоритмів класифікації в роботі [81] найкращі результати (точність 99,98%, набір даних KDD99) автори отримали за допомогою нейронних мереж. Перевага класифікатора на основі нейронної мережі в порівнянні з алгоритмом SVM для набору даних NSL-KDD показана в [82]. Результати аналогічних досліджень представлені у роботах [83, 84], але найкращий показник точності (99,9%) був отриманий за допомогою комбінації

алгоритмів BayesNet та генетичного пошуку (GeneticSearch).

Метод вибору ознак, що базується на співвідношенні атрибутів (AR) для набору даних NSL-KDD, у поєднанні з кластеризацією k-Means і класифікацією XGBoost, був використаний у роботі [85].

У роботі [86] зменшення розмірності даних були використані методи вибору ознак з урахуванням кореляції (CFS) і класифікатора Naive Bayes (NB).

Для вибору результативних ознак набору даних NSL-KDD використовувався підхід хі-квадрат. Класифікація ознак виконувалася з допомогою алгоритму SVM [87].

У роботі [88] використано гібридний вибір ознак на основі правил та нейронна мережа глибокого навчання, досягнута точність розпізнавання склала 99,0% для NSL-KDD та 98,9% для UNSW-NB15. За даними [89] для набору даних NSL-KDD дві методики вибору функцій на основі рангу: посилення інформації та симетрична невизначеність разом із C4.5 забезпечують точність 99,68% та 99,64% із 17 та 11 функціями відповідно. Результати, отримані в цих двох випадках, є цілком задовільними порівняно з іншими дослідженнями, які вже проводяться в цій галузі.

У роботі [90] виконано порівняння методів вибору ознак (CFS, IGR, PCA) та алгоритмів класифікатора (NB, SVM, DT, NN, KNN) стосовно набору даних NSL-KDD. На думку авторів [90], найкращі результати забезпечили класифікатор KNN та метод вибору ознак IGR. За результатами порівняльного дослідження [91] алгоритм RandomForest за короткий час досяг хорошої точності без використання методів вибору ознак та зменшення розмірностей.

В роботі [92] представлено підхід для IDS на основі машинного навчання, в якому поєднано класифікатор дерева рішень (DT). Автори проаналізовали набір даних NSL-KDD. За допомогою методу відбору ознак на основі фільтрів було обрано 14 значущих ознак, це дослідження проводилося як для задач бінарної, так і багатокласової класифікації.

В роботі [93] для виявлення атак типу "розподілена відмова в обслуговуванні" (DDoS) було використано кілька фільтрів: хі-квадрат, приріст інформації, коефіцієнт посилення та алгоритм ReliefF для вибору оптимальної кількості ознак.

Автори [94] провели моделювання на наборах даних UNSW-NB15, NSL-KDD та KDDCup99. За допомогою роєвого інтелекту було обрано 10 об'єктів з KDDCup99, 14 об'єктів з набору даних UNSW-NB та 18 об'єктів з NSL-KDD, але для обрання ознак було використано алгоритми роєвого інтелекту.

В роботі [95] реалізували п'ять контрольованих моделей з використанням методу Extreme Gradient Boosting (XGBoost) для зменшення кількості ознак з 42 до 19 (з урахуванням їх важливості). При зменшенні кількості ознак для набору даних UNSW-NB15 автори спостерігали збільшення точності моделі DecisionTree з 88,13 до 90,85% при виконанні завдання двійкової класифікації.

Багато алгоритмів вибору ознак у випадку багатокласової класифікації ґрунтуються на взаємній інформації [96].

Побудова релевантного набору ознак на основі оцінки їх важливості використовується для навчання моделей машинного навчання. Аналіз важливості ознак грає істотну роль і для пояснення результатів машинного навчання [97, 98].

Наприклад, в роботі [99] було запропоновано двоетапний підхід до виявлення вторгнень. На першому етапі виконувалася бінарна класифікація. На другому етапі вихідні дані про атакуючий трафік передавалися в мультикласові класифікатори для ідентифікації кожної атаки. Для завдання бінарної класифікації автори [99] використовували метод вибору ознак на основі оцінки важливості після побудови моделі RandomForest.

Покращення надійності процедури вибору ознак можливе за рахунок використання ансамблевого методу оцінки важливості ознак (ensemble feature importance – EFI). У роботі [100] для оцінки важливості ознак запропоновано підхід, який базується на введенні характеристик (низька, середня та висока

важливість) для побудови нечіткої функції належності ознак до класу важливих. На думку авторів, нечіткі системи мають додаткову перевагу, пояснюючи оцінки важливості ознак лінгвістичними термінами, що полегшує для нефахівців розуміння моделей. За результатами розрахунків [100] з використанням різних синтетичних наборів даних із різним рівнем кількості ознак, нечітка ансамблева оцінка важливості ознак забезпечила більш точні результати порівняно з точними середніми або ансамблевими підходами на основі більшості голосів.

Для систем, критично важливих для безпеки, розуміння того, як генеруються вихідні дані машинного навчання, особливо важливим є для перевірки та діагностики моделі [101].

Таким чином, дослідження методів вибору ознак у даних мережевого трафіку з метою виявлення потенційних атак є актуальним завданням. Відомі набори даних для навчання систем виявлення вторгнень, містять ознаки, які можуть бути необов'язковими або нерелевантними. Використання відомих алгоритмів класифікації за умови вибору результативного набору ознак дає хороші результати точності розпізнавання атак, але однозначна оцінка найбільш ефективного алгоритму класифікації та способу відбору ознак та зменшення розмірності відсутня. Використання ансамблевого підходу і методів інтерполяції нечітких правил забезпечує більш точні і надійні результати обрання ознак і загальні можливості системи виявлення вторгнень, тому необхідно розглянути їх більш детально.

1.2.3 Огляд застосування ансамблевого навчання для побудови систем виявлення вторгнень

Для створення виявлення систем вторгнень є досить великий досвід використання різноманітних методів машинного навчання для виявлення та

класифікації загроз безпеці. Такі підходи до побудови систем виявлення вторгнень з використанням машинного навчання, реалізуються або за допомогою якого-небудь одного класифікатора або гібридної системи класифікаторів.

Системи на основі одного класифікатора використовують один алгоритм машинного навчання для виявлення аномалій, тоді як гібридна система використовує комбінацію більш ніж одного алгоритму машинного навчання, тобто використовує один класифікатор для попередньої обробки даних, а інший для навчання попередньо оброблених даних.

Для комбінування різних методів класифікації та прогнозу в системах виявлення вторгнень досить широко використовують алгоритми ансамблевого навчання. Метод ансамблевого навчання – це спосіб перегляду всіх методів навчання та алгоритмів одночасно, а не розгортання їх окремо [102]. Ансамблеве навчання покладається на набір комбінованих класифікаторів або предикторів замість окремих класифікаторів, тому ці набори класифікаторів навчаються та вивчаються на основі проведених шаблонів для вирішення тієї самої проблеми та отримання кращих результатів [103].

За даними [104] використання ансамблевих моделей навчання замість окремих в багатьох випадках може покращити ефективність виявлення IDS. Ці моделі є дуже корисними в деяких випадках, наприклад, початкові зразки невеликих наборів даних і зменшення витрат на обчислення. Значна частина проаналізованих в [105] статей надає перевагу використанню схеми голосування більшості, щоб підвищити продуктивність своїх IDS разом із методами обрання ознак (FS – feature selection) і зменшення розмірності (DR – dimensionality reduction).

Ансамблеве навчання поділяється на два основні типи: гомогенне або гетерогенне. Однорідний тип ансамблевого навчання передбачає використання різних підмножин даних для навчання базових класифікаторів (слабких учнів). Результат кожного класифікатора агрегується для підвищення точності. Цей тип

ансамблевого навчання підходить для великих наборів даних. Bagging і boosting є найпоширенішими типами однорідного ансамблевого навчання. Класифікатор Bagging – це ансамблевий мета-оцінювач, який встановлює кожен базовий класифікатор у випадкових підмножинах вихідного набору даних, а потім агрегує їхні індивідуальні прогнози (чи шляхом голосування, чи шляхом усереднення), щоб сформувати остаточний прогноз [105].

Метод VotingClassifier базується на ідеї поєднання концептуально різні класифікаторів машинного навчання та використання більшості голосів або середніх прогнозованих ймовірностей (м'яке голосування) для прогнозування міток класу. Такий класифікатор може бути корисним для набору однаково ефективних моделей, щоб збалансувати їх окремі слабкі сторони [106].

За даними [107, 108] переважна більшість робіт з ансамблевого навчання користуються однорідним ансамблем, де random forest, bagging, boosting були найпоширенішими методами ансамблю. Крім того, використовувалися мажоритарне голосування та стекова архітектура, особливо коли розглядалися різнорідні класифікатори. більшість проаналізованих статей вважають за краще використовувати схему мажоритарного голосування. Існує великий інтерес до застосування для IDS класифікатора випадкового лісу, тому що його реалізація різноманітна і застосування неважке [109].

У роботі [110] запропоновано ефективну систему виявлення вторгнень (IDS) для хмарного середовища, яка використовує методи вибору та класифікації ансамблю ознак. На думку авторів [110] пропонований метод на основі ансамблю ефективно визначає, чи є поведінка мережного трафіку нормальним або атакуючим.

Метод ансамблю поєднує кілька алгоритмів машинного навчання для отримання остаточного рішення. Він надійний і менш схильний до упередженості та дисперсії в порівнянні з неансамблевим підходом. Отже, ансамблевий підхід краще підходить для даного дослідження, ніж неансамблевий підхід.

1.3 Аналіз використання нечіткої логіки для моделювання ризиків інформаційної безпеки та побудови систем виявлення вторгнень

Апарат нечіткої логіки, запропонованої Л. Заде, активно застосовується при моделюванні ризиків інформаційної безпеки та побудові систем виявлення вторгнень.

Методи теорії нечітких множин дозволяють найповніше врахувати неточність, неповноту, і нечіткість знань експерта при оцінюванні факторів ризику інформаційної безпеки. При формування даних оцінювання в чіткому вигляді експерт не здатен адекватно відобразити умови реальності що призводить до недостовірності оцінок ризику [111, 112]. Реалізація методів нечіткої оцінки ризиків інформаційної безпеки представлені також в роботах [113, 114], в тому числі застосовано нечіткий аналог аналізу ієрархій [115]. Нечітка логіка застосовується для аналізу та виявлення передумов виникнення загроз інформаційної безпеки [116]. Нечітка логіка застосовувалася для моделювання ризиків інформаційної безпеки та рівня захищеності ERP систем [117].

Наявні методи кількісної оцінки і управління ризиками інформаційної безпеки на основі теорії нечітких множин дозволяють виконувати оцінку і управління ризиками в умовах нечіткості, неповноти інформації про загрози і вразливості, можливих суперечливостей оцінок факторів ризику, при яких експерти визначають збитки за окремими показниками нечіткого і якісного характеру, що свідчить про перспективність цього напрямку [10,11,12,14]. Однак наявні підходи потребують розвитку в частині управління ризиками інформаційної безпеки документів підприємства, в тому числі документів проекту, оскільки проектна побудована діяльності властива багатьом бізнес-структурам.

Одним із напрямків досліджень, що стосуються побудови IDS, є розробка систем з використанням нечіткої логіки. На думку [118], методи штучного

інтелекту, такі як дерева рішень, нейронні мережі та нечітка логіка, застосовуються для виявлення підозрілих дій у мережі, при цьому система на основі нечіткої інформації забезпечує значні переваги порівняно з іншими методами штучного інтелекту. В дослідженні [119] проведено дослідження можливостей використання методів інтерполяції нечітких правил (FRI) у сфері додатків IDS. На думку авторів [120], модель FRIIDS перевищує швидкість виявлення алгоритм машини опорних векторів у прикладі набору даних DDOS, де інші алгоритми (нейронна мережа, випадковий ліс і дерево рішень) зафіксували трохи більш високий рівень виявлення. В роботі [121] розробили метод динамічної інтерполяції нечітких правил для підвищення загальних можливостей системи, а також для ефективного виявлення атак. В роботі [122] була реалізована нова нечітка тимчасова функція, що включає згорткову нейронну мережу (FT-CNN), для виконання ефективної класифікації.

В роботі [123] запропоновано новий метод PCA-нечіткої кластеризації KNN, який означає сукупність аналізу основних компонентів та нечіткої кластеризації з методами вибору ознак K-найближчого сусіда. Однак для побудови запропонованої моделі виконується дві основні класифікації класів. Для того, щоб перевірити надійність моделі, використано відомий набір даних NSL-KDD, який використовується для аналізу аномалій. Цей набір даних заснований на контрольних даних, що використовуються для виявлення вторгнень, KDDCup 1999. Тому аналізується набір даних NSLKDD з використанням аналітики PCA-fuzzy Clustering-KNN і визначається продуктивність інциденту за допомогою алгоритмів машинного навчання.

В деяких дослідженнях побудовано комплексну архітектуру IDS з використанням комбінації вказаних підходів. Наприклад, в [124] запропонована нова ансамблева модель для IDS, заснована на двох алгоритмах: нечіткий вибір ознак ансамблю (FEFS) та об'єднання множинних класифікаторів (FMC). FEFS є об'єднання п'яти оцінок характеристик. Ці оцінки виходять з допомогою функцій

відстані класів об'єктів. Агрегація виконується з допомогою операції нечіткого об'єднання. З іншого боку, FMC є об'єднанням трьох класифікаторів. Він працює з урахуванням вирішальної функції ансамблю. Експерименти, проведені з набором даних KDDcup99, показали, що запропонована система працює краще ніж добре відомі методи, такі як машини опорних векторів (SVM), K-найближчий сусід (KNN) і штучні нейронні мережі (ANN).

Таким чином, застосування апарату нечіткої логіки в широкому розумінні надає суттєві переваги як в моделюванні ризиків інформаційної безпеки , так й при побудові систем виявлення вторгнень, особливо в комбінації з іншими підходами, тому це необхідно врахувати в подальших дослідженнях.

1.4 Огляд наборів даних для побудови систем виявлення вторгнень

Для розробки моделей машинного навчання виявлення вторгнень необхідні спеціалізовані набори даних, тому необхідно провести їх огляд. Набір CSE-CIC-IDS2018 є загальнодоступним набором даних про вторгнення. Цей набір даних було створено з урахуванням недоліків попередніх наборів даних про вторгнення. Набір CSE-CIC-IDS2018 – це один із найбільших наборів даних IDS із реальним мережевим трафіком і широким спектром атак. Він також містить звичайні дані та дані про вторгнення. Набір даних CSE-CIC-IDS2018 включає сім різних сценаріїв атак: Brute-force (Web, XSS, FTP, SSH), SQL Injection і DDoS (HOIC, LOIC- UDP, LOIC-HTTP), Heartbleed, Botnet, DoS (Hulk, SlowHTTPTest, GoldenEye, Slowloris), DDoS (HOIC, LOIC- UDP, LOIC-HTTP), Web attacks, і проникнення в мережу зсередини [125].

Набір даних KDDCup99 [126] містить 41 ознаку та охоплює чотири основні категорії атак: атаки зондування (атаки зі збором інформації), атаки на відмову в обслуговуванні (DoS), атаки користувача на root (U2R), атаки віддаленого до

локального (R2L), спостере-ження та інші зондування, наприклад, сканування портів (probing).

Набір NSL-KDD є поновленою версією набору даних KDDCup99 [127]. Це ефективний контрольний набір даних, який допоможе дослідникам порівняти різні методи виявлення вторгнень. Цей набір даних не має надлишкових записів, тому будь-яка модель, навчена на цьому наборі даних, не повинна бути схильна до повторних записів атак. Загалом у цьому наборі даних для одного запису є 43 ознаки. З 43 ознак 41 пов'язана з вхідним трафіком, а дві інші є мітками та балами вхідного трафіку. Цей набір даних має загалом чотири класи для різних атак: зондування, атак користувача на root (U2R), відмова в обслуговуванні (DoS) і віддале-на локальна атака (R2L).

Набір даних UNSW-NB15 містить понад два мільйони записів, 48 ознак і дев'ять різ-них типів атак: Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode та Worm [128].

Набір даних LITNET-2020 — це відносно новий набір даних, зібраний академічною мережею LITNET (Литовська науково-освітня мережа) у мережевому трафіку Литви в ре-жимі реального часу. Це реальний і сучасний мережевий набір даних на основі потоку [129], розроблений для тестування систем IDS. У цьому наборі даних було 85 функцій мережевого потоку та 12 типів атак

Слід зазначити, однією з проблем наборів даних для навчання є їх незбалансованість, що є класичною проблемою машинного навчання. Першим кроком у процесі створення моделі виявлення вторгнень є перебалансування даних для навчання, щоб отримати кращі результати в наборі перевірки. З метою вирішення проблем, спричинених нерівномірним розподілом даних, для побудови систем виявлення вторгнень досить часто використовується алгоритм SMOTE (Synthetic Minority Oversampling Technique). В основі алгоритму лежить ідея генерації деякої кількості штучних спостережень, які були б схожі на

спостереження, що є в міноритарному класі, але при цьому не дублювали їх. За даними, використання аугментації може значно покращити F1 класів з невеликою кількістю зразків (R2L, U2R), забезпечуючи підвищення загальної точності [130, 131].

В роботі [131] зазначено, що аугментація даних з використанням алгоритму SMOTE дозволила покращити ефективність і швидкість для бинарної та багатокласової класифікації з набору даних NSL-KDD.

Як зазначено в роботі [132], у випадку багатокласового набору даних працювати з даними складніше, й багатокласова класифікація в незбалансованому наборі даних залишається важливою темою дослідження. Автори [132] перевірили набір даних CICIDS-2017, щоб протестувати один із популярних підходів до вирішення проблеми дисбалансу в наборах даних із кількома класами, яким є техніка надмірної вибірки синтетичної меншості (SOMTE).

1.5 Аналіз протиріч та постановка наукового завдання

Як свідчить проведений аналіз, у фахівців з кібербезпеки наявний досить багатий досвід з розробки різних підходів до управління інформаційною безпекою підприємства та створення різних за архітектурою систем виявлення вторгнень, більшість з яких виконує аналіз мережевого трафіку з використанням методів інтелектуального аналізу даних або нейронних мереж глибокого навчання.

Незважаючи на велику кількість робіт з використання різноманітних класифікаторів для побудови систем виявлення вторгнень, досі незрозуміло, які саме методи машинного навчання є найбільш надійними та ефективними (особливо для створення динамічної системи виявлення вторгнень). Важливим

питанням роботи системи виявлення вторгнень є час перенавчання і класифікації, тому розробники докладають багато зусиль для його зменшення. Покращення результатів роботи систем виявлення вторгнень досягається за рахунок використання ансамблевих моделей навчання замість окремих, але питання вибору найкращої архітектури ансамблю і обрання окремих класифікаторів залишається відкритим.

Існує необхідність точного і надійного ідентифікування загроз в режимі реального часу шкідливих процесів (що потрібує збільшення обсягу набору даних для навчання системи), а з іншого боку, необхідне прискорення реагування і навчання системи (що, навпаки, вимагає зменшення обсягу набору даних для навчання системи). Тому підвищення продуктивності системи виявлення вторгнень потребує використання методів обрання ознак та зменшення розмірності простору ознак. Але вибір алгоритмів побудови системи ознак і зменшення розмірності пов’язаний з питанням обрання окремих класифікаторів ансамблевій моделі, тому теж залишається відкритим. Цікавим напрямком досліджень є застосування нечіткої логіки в поєднанні з ансамблевим навчанням.

Виявлення, аналіз, прогнозування та обробка ризиків інформаційної безпеки ґрунтується на використанні моделей та методів їх оцінки. Враховуючи наявність невизначеності та розмитості інформації про діяльність підприємств, нечітка логіка отримала широке застосування в таких моделях. Беручи до уваги, що вимірювання характеристик кібербезпеки досі залишається недостатньо розвинутою темою, в тому числі стосовно безпеки документів підприємства, подальші дослідження в цьому напряму є актуальними.

У зв’язку з цим існує необхідність вирішення 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 необхідно виконати наступні часткові завдання:

- 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.

Висновки до розділу 1

1. В результаті аналізу встановлено, що протягом останніх десятиліть для протидії кібератакам широке розповсюдження отримали системи виявлення вторгнень. Для побудови таких систем використовуються методи обчислювального інтелекту, в тому числі машинне навчання, глибоке навчання і інтелектуальний аналіз. Швидке збільшення мережевого трафіку, інтернет-технологій, збільшення обсягів даних, а також поява нових типів кіберзагроз вимагають удосконалення систем виявлення вторгнень, яке спрямоване на підвищення швидкості та сумарної ефективності їх роботи.

2. Існуючі підходи до управління інформаційною безпекою підприємств не враховують в повній мірі розмитість, неповноту та якісний характер інформації для оцінки вразливості та загроз, що обумовлює актуальність використання апарату нечіткої логіки при формалізації та побудові алгоритмів системи кібербезпеки.

3. Аналіз сучасної літератури показав, що перспективним напрямком розвитку систем виявлення вторгнень є використання гібридної ансамблевої моделі навчання на базі класифікатора голосування, алгоритмів нечіткої логіки та системи обрання ознак.

4. Відомі системи виявлення вторгнень мають певні недоліки, серед яких можна виділити потребу у великій кількості даних для навчання моделей, помилкові спрацювання внаслідок недостатньої кількості даних або обмеженої точності моделей, нестабільність моделей машинного навчання при роботі з великими обсягами даних, високу кількість помилок при виявленні аномалій, невміння розпізнати нові типи загроз, які не були включені до тренувальних даних, складність налаштування моделей машинного навчання і потребу в великій кількості обчислювальних ресурсів для їх тренування та експлуатації. Тому актуальною є розробка моделей, методів та алгоритмів системи управління інформаційною безпекою у складі інформаційної системи підприємства на основі підходів машинного навчання та нечіткої логіки. Зазначене було покладене в основу постановки задачі дослідження.

РОЗДІЛ 2
МОДЕЛЮВАННЯ ТА ФОРМАЛІЗАЦІЯ ФАКТОРІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Враховуючи результати проведеного в розділі 1 огляду існуючих підходів до управління інформаційною безпекою, в даному розділі проведено аналіз факторів стратегії безпеки інформаційних технологій сучасного підприємства та моделювання загроз та ризиків інформаційної безпеки на основі апарату нечіткої логіки.

2.1 Аналіз факторів стратегії безпеки інформаційних технологій сучасного підприємства

В даному підрозділі проведено аналіз сучасного стану інформаційної безпеки сучасних підприємств і сформовано рекомендації щодо побудови стратегії захисту інформаційних технологій. Для цього проаналізовано стан інформаційної безпеки підприємства, розглянуто проблеми, що виникають у роботі інформаційних систем та надаються рекомендації фахівцям підрозділів інформаційних технологій щодо їх вирішення.

Критична інфраструктура за своєю природою є цікавою метою для іноземної держави, навіть у мирний час. Наприклад, взаємопов'язаність об'єктів в енергетичній галузі підсилює вразливість системи, і кібератаки часто залишаються непоміченими протягом деякого часу. Вважається, що мережа електростанцій і ліній, що з'єднують будинки і підприємства, є однією з найбільш важливих інфраструктур в світі. Це також один з об'єктів, які найбільш часто піддаються нападам, з наслідками, що можуть потенційно вийти далеко за межі енергетичного сектора [6].

Звіт фінської компанії F-Secure [133] показує, що:

- різноманітні противники, кожен зі своєю мотивацією, постійно прагнуть скомпрометувати організації, які експлуатують критично важливу інфраструктуру;
- зловмисники мають більше часу, ніж їхні цілі, і на планування їх атаки йдуть місяці;
- люди є найслабшою ланкою у виробництві, а співробітники компанії, мабуть, стають метою злочинців;
- зловмисники продовжують домагатися успіху головним чином через відсутність в організаціях зрілих практик інформаційної безпеки;
- певні групи IT-фахівців продовжують шукати уразливі місця і шпигунські можливості, переслідуючи політичні цілі;
- існує безліч шкідливих програм / методів, націлених на виробничу (енергетичну) галузь, причому фішинг є найбільш поширеним методом початкової атаки ланцюжка поставок;
- утримати невелику поверхню атаки в енергетичній галузі просто неможливо.

Незважаючи на те, що порушення неминучі, організаціям для підтримки ефективності бізнесу необхідно переглянути свій стан інформаційної безпеки для впровадження новітніх технологій, таких як рішення для виявлення і реагування на складні загрози і цільові атаки (endpoint detection and response - EDR) [6].

У новому звіті Deloitte Global «Управління кіберризиками в електроенергетичному секторі» оцінюються найбільші кіберзагрози в електроенергетичному секторі та вказується, як компанії можуть управляти цими ризиками [134]. Виробничий сектор стикається з швидко зростаючим ландшафтом кіберзагроз – витонченість, частота атак, а також число учасників загроз зростає. Зокрема, енергетика є одним з провідних виробничих секторів, на які націлені кібератаки. Загрози можуть варіюватися від внутрішніх, таких як

атака незадоволених співробітників, до зовнішніх, від урядів ряду держав або організованої злочинності.

Виробничі компанії повинні зробити ряд кроків для подолання цих перешкод і управління кіберризиками на підприємстві [6].

1. Скласти карту активів інфраструктури та оцінити вразливості. Виробничі компанії повинні зіставити активи інфраструктури і розставити пріоритети по їх важливості. Потім вони повинні визначити вразливості активів і оцінити зрілість контрольного середовища для управління загрозами. І, нарешті, компанії повинні створити основу для захисту критично важливих активів з використанням людей, процесів і технологій.

2. Оцінити процеси забезпечення безпеки постачальників. Для управління кіберризиками в ланцюжку поставок багатообіцяючим першим кроком є участь у функції закупівель в ланцюжку поставок. Виробничі компанії повинні розуміти процеси кібербезпеки постачальників для продуктів і послуг і забезпечувати їх відповідність провідним галузевим практикам. Безсумнівно підвищують прозорість поставок довірчі принципи, закладені в практиках блокчейна.

3. Співпрацювати з колегами по галузі та державними установами. Управління ризиками кібербезпеки не повинно припинятися на рівні окремих підприємств. Компанії можуть поліпшити стан кібербезпеки, допомагаючи встановити галузеві стандарти, обмінюючись інформацією щодо загроз зі колегами і впроваджуючи нові технології. Зростаюча складність технологічного середовища є дуже важливим фактором для обміну інформацією про загрози.

4. Датчики і системи безпеки повинні обмінюватися інформацією про загрози в реальному часі, щоб відповідати швидкості атаки. Технологічні інновації та аналітика повинні визначати стратегію кібербезпеки кожної компанії. Нові інструменти стають все більш доступними, і можливості для моніторингу мереж в режимі реального часу, виявлення загроз і їх усунення швидко

розвиваються, забезпечуючи необхідний захист для галузей виробництва в цілому.

Керівники підрозділів IT-безпеки (Chief Information Security Officer - CISO), що працюють в промислових підприємствах, повинні розуміти ризики кібербезпеки, з якими вони стикаються, і точно визначати, що потрібно захищати.

Експерти, що володіють найкращими знаннями про підприємство (завод) і його системи, можуть дати оцінку, щоб допомогти новим CISO скласти уявлення про те, які у них уразливості і наскільки вони серйозні [133]. CISO повинні інформувати себе і свої команди про стандарти кібербезпеки для бізнесу, а потім впроваджувати і завжди дотримуватися цих стандартів. Наприклад, їм слід ознайомитися з ISA99 / IEC 62443, суворим стандартом для технологій промислової автоматизації [135].

Основою забезпечення інформаційної безпеки підприємства є її належне фінансування. Збільшити фінансування для забезпечення інформаційної безпеки – непросте завдання, особливо коли організація стикається з бюджетними обмеженнями [6].

Тому для отримання достатнього фінансування необхідно:

1. Визначити цінні активи підприємства та ризики, викликані організаційними недоліками. Слід описати найбільш важливі активи компанії і спрогнозувати, як атака на комп'ютерні системи може негативно вплинути на прибутковість та імідж бізнесу.

2. Розставити пріоритети і оцінити поточні ризики організації. Визначити п'ять основних ризиків інформаційної безпеки компанії – ті, які мають найбільший потенційний вплив на організацію – і оцініть сильні і слабкі сторони підприємства, а також прийнятні рівні ризику з точки зору людей, інформації, процесів, програм та інфраструктури.

3. Розробити план управління ризиками з точки зору:

– управління інформаційними активами;

– підвищення рівня безпеки;
– підвищення стійкості мережі.

4. Описати план безпеки для врахування поточних рівнів ризику:

– існуючі елементи управління, такі як покупка і впровадження послуг, ліцензії, розробка конфігурації, підтримка і таке інше;
– внутрішнє, зовнішнє або комбіноване рішення для захисту даних, щоб розширити можливості виявлення і зменшити ймовірність злому конфіденційної інформації і знизити ризик від критичного до низького;
– пропоновані контрольні ресурси для кожного кварталу.

Необхідно показати, чому запропонована стратегія інформаційної безпеки буде успішною, уточнити позитивні очікування після впровадження стратегії, встановити контрольні показники успіху і прогресу для програми врядування та інвестицій.

Концепція інформаційної мережі підприємства, повністю закритої всередині будівлі або віртуальної організації і, отже, більш зручною для захисту, фактично зникла. Це не новина для тих, хто в змозі захистити організацію від кібератак, і можна зрозуміти проблеми, з якими команди безпеки стикаються в цих обставинах [6, 13].

Зникнення периметра викликає розширення мережі організації, що включає в себе набагато більше пристроїв і місць розташування, багато з яких знаходяться за межами того, що раніше вважалося периметром. Багато пристроїв і таких місць знаходяться поза контролем команди безпеки. Gartner прогнозує [136], що скоро 27 відсотків корпоративного трафіку даних обійдуть захист периметра і будуть безпосередньо передаватися з мобільних і переносних пристроїв в хмару. Очікується, що число пристроїв IoT, які, як відомо, є слабкими з точки зору безпеки та вразливості, збільшиться майже втричі в наступні 6 років з 26,7 млрд. у 2019 до 75,4 млрд. у 2025 році.

Коли відділам інформаційних технологій підприємств потрібно тільки патрулювати периметр, обсяг вхідних і вихідних даних був керованим. Тепер обсяг даних, що генеруються, на кілька порядків перевищує можливості груп безпеки з контролю за всім цим. Ця розширена поверхня атаки включає IoT, персональні пристрої і хмару. Захист периметру легко обійти за допомогою розширених загроз, які ухиляються від виявлення [6].

Існує кілька методів і технологій, які дозволять групам безпеки ефективно захищати свою мережу, як тільки вони прийдуть до згоди з тим фактом, що периметр легко обходиться. Всі вони пов'язані з тими засобами, що зосереджені на виявленні зловмисного бокового руху в мережі, що є найбільш важливою метою для організацій сьогодні. Брандмауери, захист кінцевих точок і інші засоби захисту периметра важливі, але їх недостатньо.

В першу чергу слід забезпечити безпечне спілкування. Кожен вузол – це будь-який комп'ютер, пристрій або система, підключена до хмари або мережі, наприклад, ноутбук, смартфон і принтер із загальним доступом. Слід контролювати і аналізувати зв'язок між цими пристроями на предмет чого-небудь незвичайного або шкідливого. Якщо злочинець може зламати iPad, він може перейти звідти до інших пристроїв у середовищі підприємства, до інших вузлів мережі. З огляду на інтенсивність активності серед всіх вузлів зростаючої мережі, командам по забезпеченню безпеки може бути складно стежити за всіма оповіщенням. Один з варіантів – просто найняти більше аналітиків, але при нестачі навичок це теж може виявитися складним завданням. Деякі інструменти мережевої аналітики дозволяють користувачам встановлювати поріг для того, що буде генерувати попередження. Підвищення порогу зменшить кількість попереджень, але підвищить ризик пропуску атаки.

Інший варіант – використовувати штучний інтелект (ШІ). Рішення для забезпечення безпеки на базі ШІ може створювати моделі нормальної активності

і автоматично виділяти те, що є незвичайним або аномальним, що може вказувати на зловмисну діяльність.

Знання того, що щось передається між двома пристроями або вузлами, недостатньо. Необхідно проаналізувати характер спілкування. Знання того, що деякі рухи є аномальними або незвичайними в порівнянні з встановленими базовими рівнями, корисно. Це перший крок у виявленні загроз, що діють у мережі підприємства. Але є недолік у використанні тільки виявлення аномалій: не всі аномалії є шкідливими. Включення даних про відомі зловмисні дії в раніше згаданий аналіз на основі ШІ може відокремити шкідливі аномалії від доброякісних, майже виключити помилкові спрацьовування і зосередити зусилля груп безпеки на бічному русі, що представляє найбільший потенційний ризик [6].

Для захисту мережі тепер потрібні моніторинг і аналіз бокового руху в розширеній мережі. Це оптимально досягається за допомогою ШІ, який може спростити початковий аналіз мережевої активності, відфільтрувати те, що є нормальним, та зосередити зусилля на розслідуванні та усуненні загроз високого ризику.

Від глобальної економіки до щоденних індивідуальних взаємодій, все більше і більше часу люди проводять в Інтернеті. Проте, рівень уваги до захисту даних і захисту конфіденційності дій споживачів продукції підприємств є поки що недостатнім.

Біля 70 відсотків веб-сайтів США були сертифіковані для онлайн-аудиту довіри і рейтингу добробуту у 2019 році, що є найвищим показником за всю історію, в порівнянні з 52 відсотками в 2017 році, головним чином завдяки покращенням у аутентифікації електронної пошти та шифруванні сеансів [137].

В цілому, аудит виявив сильний крок в сторону шифрування: 93 відсотки сайтів шифрують всі веб-сеанси (в порівнянні з 52 відсотками у 2017 році). Аутентифікація електронної пошти також знаходиться на рекордно високому рівні; 76 відсотків сайтів використовують і SPF, і DKIM (проти 48 відсотків у 2017

році), а 50 відсотків мають запис DMARC (проти 34 відсотків раніше). Однією з можливостей покращання в цьому напрямі є використання механізмів звітності про вразливість, які різко зросли в онлайн-рітейлі, новинних і хостингових компаніях, але в цілому використовувалися тільки 11 відсотками організацій. Альянс онлайн-довіри домігся значних успіхів у просуванні більш високих стандартів безпеки в Інтернеті [138].

Впровадження 5G потенційно може привести до появи додаткових векторів загроз в мережах операторів, тому постачальники комунікаційних послуг (Communication Service Providers - CSPs) мають вирішити проблеми безпеки IoT, і, згідно з недавнім звітом Allot Telecom Trends [138], автоматизація з використанням замкнутого циклу (Closed Loop Automation - CLA) може допомогти їм вирішити цю проблему. Автоматизація із замкнутим контуром (CLA), яка використовує машинне навчання і штучний інтелект, пропонує безперервну оцінку стану мережі в реальному часі, доступності ресурсів і вимог до трафіку для виявлення перевантажень мережі, шкідливого трафіку на основі IoT. CLA допомагає виявляти та ізолювати нові аномалії і пом'якшувати загрози, перш ніж вони зможуть впливати на інформаційну мережу. Ця технологія одночасно допомагає підвищити продуктивність і забезпечує аналіз ємності, контроль якості і виявлення помилок.

Інформація безпека підприємства залежить в першу чергу від поведінки його співробітників [139]. Звинувачувати працівників в поведінці, до якої вони звикли в особистому житті, складно. Це може додати додаткову складність для IT-фахівців із захисту активів компанії, оскільки необхідно враховувати повсякденні звички співробітників, що може поставити під загрозу безпеку організації.

По-перше, співробітники мають потребу в навчанні. Тому ті, хто регулярно використовує загальнодоступні Wi-Fi, Bluetooth або USB-накопичувачі в особистому житті, повинні розуміти, чому вони небезпечні для роботи.

Потім організація повинна розвивати культуру спілкування – наприклад, якщо щось йде не так, співробітники також повинні відчувати себе досить комфортно, щоб повідомляти про проблеми в IT, перш ніж буде завдано значної шкоди. Співробітники повинні знати, що якщо вони втратять смартфон або ноутбук, вони повинні негайно повідомити про це IT.

Співробітники повинні знати проблеми з Wi-Fi і Bluetooth. Співробітники, яким доводиться платити за тарифні плани, звикли шукати відкриті з'єднання Wi-Fi всюди, де б вони не знаходилися. Звичайно, вони чули, що загальнодоступний Wi-Fi небезпечний, але якщо з ними нічого поганого не станеться під час його використання, вони часто проігнорують попередження. Важливо пояснити, як з'єднання Wi-Fi дозволяє хакеру легко розташуватися між пристроєм співробітника і точкою доступу, отримуючи доступ до кожної частини інформації, яку вони відправляють через Інтернет, включаючи всю їхню особисту інформацію, а також облікові дані для безпеки мережі бізнесу. Є навіть онлайн-уроки з мільйонами переглядів, щоб показати хакерам, як це зробити. Отримавши інформацію про співробітника, кіберзлочинці можуть легко увійти в систему і видати себе за них у будь-який час. Через загальнодоступний Wi-Fi хакери можуть також відправляти спливаючі повідомлення, що пропонують оновлення програмного забезпечення, де при натисканні вони встановлюють шкідливе ПЗ і заражають пристрій.

Використання Bluetooth також небезпечно. Як тільки пристрій заражено, він легко поширює шкідливе ПЗ на інші прилеглі пристрої, включаючи офісні комп'ютери. Хоча більшість пристроїв були виправлені для цієї конкретної проблеми, хакери, як правило, на крок попереду виробників пристроїв, а це може означати, що в майбутньому можуть виникнути інші неприємні сюрпризи [6].

Щоб уникнути проблем безпеки, пов'язаних з Wi-Fi, Bluetooth і іншими небезпечними сполуками, співробітникам підприємства слід використовувати віртуальну приватну мережу (VPN).

Однак мережі VPN складно налаштувати, і використання неправильного протоколу може привести до недоліків безпеки.

Окремо слід відмітити небезпеку USB-накопичувачів. Переважна більшість доступних даних на них не зашифровано, що дозволяє хакерам перепрограмувати їх за допомогою шкідливих програм. Оскільки вони такі маленькі, флешки також легко втратити.

Незахищені уразливості, а також зростаюча складність мереж і додатків підприємства створюють постійний ризик для його інформаційної безпеки.

Навчання співробітників відповідального використання своїх пристроїв і повідомленням про втрату або крадіжку є важливою частиною процесів інформаційної безпеки підприємства. Щодо основних правил кібергігієни [140, 141] слід впровадити:

- використання ліцензійні / легалізовані операційні системи, інші програмні продукти, своєчасно і систематично їх оновлюючи;
- користування антивірусним програмним забезпеченням з технологією евристичного аналізу;
- використання програмних міжмережевих екранів (брандмауерів) і штатні засоби захисту від шкідливого програмного забезпечення;
- регулярне резервне копіювання даних, зберігайте резервні копії на зовнішніх носіях інформації (SDD, HDD і т.д.) і налаштування функції «відновлення системи».

5. Унеможливлення підключень флешки і зовнішніх дисків, вставляння CD і DVD і т.д. в корпоративний комп'ютер, якщо немає довіри повністю їх джерелам. Існують техніки злому комп'ютера ще до того, як відкриється файл на флешці і задовго до того, як встановлений антивірус його просканує. Якщо знайдено пристрій всередині офісу або на вулиці, отримано його поштою або з доставкою, або незнайомець дав його з проханням роздрукувати документ, або просто відкрити і перевірити його вміст – є велика ймовірність, що пристрій є

небезпечним. При підключенні пристроїв мають бути забезпечена їх автоматична перевірка на наявність шкідливого програмного забезпечення. Має бути вимкнений автоматичний запуск змінних носіїв інформації (захист від autorun.inf).

6. Не зберігайте дані аутентифікації в легкодоступних місцях (наприклад, на робочому столі). Використовуйте для зберігання паролів спеціальні програмні засоби (наприклад, KeePass), створюйте стійкі паролі та не дублюйте їх в інших акаунтах.

7. Уникання використання Інтернет-банкінгу, електронних платіжних систем, введення аутентифікації даних при доступі до Інтернету через загальнодоступні (незахищені) бездротові мережі (в кафе, барах, аеропортах та інших громадських місцях).

8. Обережність з відкриттям вкладень до електронної пошти від невідомих осіб. Сьогодні найактуальнішим засобом розсилки шкідливого програмного забезпечення є електронна пошта. Під час роботи з поштою потрібно перевіряти розширення вкладених файлів і не відкривати файли навіть з безпечними розширеннями. Не переходити з невідомих посиланнях і не завантажувати файли, які мають потенційно небезпечне розширення (наприклад: .exe, .bin, .ini, .dll, .com, .sys, .bat, .js і т.д.) і навіть безпечне (наприклад: .docx, .zip, .pdf), адже можуть використовуватися уразливості, макроси і інші небезпеки. Звертання уваги на ім'я електронної пошти: навіть якщо воно здається легітимним, все одно потрібно перевірити (в телефонному режимі або будь-яким іншим способом), чи дійсно ця особа відправляла вам повідомлення з вкладенням.

Іноді, особливо під тиском часу, буває важко відрізнити шкідливі файли від легітимних. Користування сервісом VirusTotal для перевірки підозрілих файлів шляхом їх одночасного сканування більше 50 антивірусами. Це набагато ефективніше, ніж сканування файлів антивірусом в автономному режимі, але важливо враховувати той факт що завантаження файлів на VirusTotal надає доступ

до нього третій стороні. Важливо звернути увагу на те, що навіть якщо перевірка на VirusTotal не дала результату, це не виключає того, що файл може бути шкідливим.

9. При користуванні Інтернет-ресурсами (Інтернет-банкінгом, соціальними мережами, системами обміну повідомленнями, новинами, онлайн-іграми) не знімати підозрілі посилання (URL), особливо ті, що вказують на сайти, які зазвичай не відвідуються. Потрібна буди уважним до проявів Інтернет-шахрайства. Найпоширенішим засобом введення в оману в мережі Інтернет є фішинг. Особливу увагу слід звертати на доменне ім'я Інтернет-ресурсу, який запитує дані аутентифікації, перш ніж натиснути на посилання: зловмисники можуть замаскувати доменне ім'я, щоб воно виглядало знайомим (facelook.com, gooogle.com т.д.). В іншому випадку велика ймовірність потрапити на фішинг і самостійно «віддати» власні аутентифікаційні дані. У разі необхідності введення аутентифікації даних слід переконатися в тому, що використовується захищене з'єднання HTTPS, перевіряйте SSL-сертифікат сайту, щоб переконатися, що він не клонований або не підроблений.

Шкідливі URL-адреси можуть бути закодовані у вигляді QR-кодів і / або роздруковані на папері, в тому числі у формі скорочених URL, згенерованих спеціальними сервісами на зразок tinyurl.com, bit.ly, ow.ly тощо. Слід уникати введення цих посилання в браузер і сканування QR-коди корпоративним смартфоном, якщо немає впевненості в їх походженні. Слід використовувати VirusTotal для перевірки підозрілих посилань так само, як для сканування файлів.

10. Обережність щодо спливаючих вікон і повідомлень в вашому браузері, програмах, операційній системі і мобільному пристрої. Завжди читати зміст цих вікон і не натискати клавіш похапцем.

11. При використанні віддаленого доступу необхідно обмежити доступ за допомогою «білого списку» (IP whitelisting).

12. Встановлення обмеження кількості введення помилкових логінів / паролів. Регулярно переглядати журнали логування, планувальник завдань і автозавантаження на предмет несанкціонованих дій. Відстежувати за новинами нові кіберзагрози і швидко реагувати на нові виклики.

Результати аналізу факторів інформаційної безпеки закладають основу для моделювання загроз інформаційної безпеки та інформаційних ризиків роботи підприємства.

2.2 Моделювання загроз інформаційної безпеки та інформаційних ризиків роботи підприємства

Важливим елементом загального процесу управління ризиками безпеки є оцінка ризиків безпеки, що є процесами забезпечення того, щоб стан підприємства за ризиками був прийнятним. Прийнятні межі встановлюються вищим керівництвом і містять чотири основні складові: оцінка ризиків безпеки, тестування і нагляд, зниження ризиків і операційна безпека.

Оцінка ризиків інформаційної безпеки складається з трьох основних етапів: ідентифікація ризиків, аналіз ризиків, оцінка ризиків, яка може містити пов’язані етапи:

- визначення засобів захисту системи;
- виявлення загрози;
- виявлення уразливості;
- контрольний аналіз;
- визначення ймовірності;
- аналіз наслідків;
- ідентифікація ризику.

Повний процес оцінки ризику доповнюється також рекомендаціями з моніторингу та документуванням результатів. Враховуючи результати оцінок ризиків, приймається рішення про вибір засобів впливу на ризик, щоб зменшити шкоду від реалізації загроз в майбутньому.

В діяльності підприємства прояв змін та його поточний стан в певні моменту часу описують документи. Особливо це стосується підприємств, які використовують проектну модель діяльності. Проект розглядається як сукупність операцій із досягнення цілей при обмежені часу та ресурсів.

Документ за [32] – це матеріальний носій, що містить інформацію, основними функціями якого є її збереження та передавання у часі та просторі.

При дотриманні певної форми подання та формування цієї інформації документ містить такі обов'язкові ознаки як:

- функціональність: визначеність в межах існуючих суспільних відносин очікуваного впливу документа (в тому числі подальшого порядку дій) на його одержувачів після отримання та ознайомлення із вмістом;
- санкціонованість: визначеність фізичної і/або юридичної особи, яка відповідає у певний час за існування документа;
- реєстрованість: визначеність унікальної ідентифікації документа у множині документів.

За формою створення документи поділяють на паперові та електронні.

Електронний документ (ЕД) – це документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа, склад та порядок розміщення яких визначається законодавством [142]. При цьому ЕД може бути створений, переданий, збережений і перетворений електронними засобами у візуальну форму подання шляхом відображення даних, які він містить, електронними засобами або на папері у формі, придатній для сприймання його змісту людиною. Обов'язковими реквізитами ЕД є дані, без яких він не може бути підставою для його обліку і не матиме юридичної сили [142].

Критичність інформаційних активів, до яких відноситься документ, можливо розглядати як три наступні види: конфіденційність, цілісність та доступність.

Конфіденційність є властивістю інформації, при якій системи мають здатність забезпечувати зберігання її в таємниці від суб'єктів, які не уповноважені доступом до неї.

Цілісність – властивість інформації, що відповідає її існуванню в неспотвореному вигляді (незмінному по відношенню до якогось фіксованого стану).

Доступність – властивість інформації, при якій характерна здатність бути своєчасно наданій заінтересованим суб'єктам з відповідними повноваженнями.

Під час життєвого циклу кожного документу його створення, передачі, збереження і перетворення виникають загрози щодо конфіденційності, цілісності, доступності та достовірності. В умовах життєвого циклу проекту, що змінюються з часом, можливості виникнення ризиків поєднується із зацікавленістю акторів загроз, що залучаються до проекту явно, або потенційно і визначаються як розголошення або витік інформації, знищення, модифікація, блокування, несанкціонований доступ.

Для підприємства документ, що супроводжує проект, є одним з основних інформаційних активів. Документ характеризується формою (електронна, паперова, електронна з ЕЦП) та станом (проект документу, актуальний, недійсний). Документ існує в одному або декількох примірниках. Для паперового документа серед екземплярів виділяються оригінали та копії.

Позначимо документ в загальному випадку як $d_{lk}^{i} \in D$, де D - множина документів проекту; i –номер документа; l – форма документу, $l \in \{0,1,2,3\}$: 0-електронний екземпляр, 1- підписаний паперовий оригінал, 2-паперова копія, 3-електронний з ЕЦП; k - номер екземпляра документа [3-5].

Всі екземпляри *i*-го документа форми *l* позначимо як d_l^i, що визначається за формулою:

$$d_l^i = \bigcup_k d_{lk}^i \,. \tag{2.1}$$

Всі екземпляри документа *i*-го документа всіх форм позначимо як d^i (узагальнений документ), що визначається за формулою:

$$d^i = \bigcup_l d_l^i \,. \tag{2.2}$$

Стан документа представимо як функцію:

$$F_S : D \times T \to S \,, \tag{2.3}$$

де *D* – множина документів; *T* – вісь часу; *S* – множина станів документа *S* ={project, actual, inoperative}.

Множину документів *D* розіб'ємо по їх видам:

$$D = \bigcup_{j=1}^{n} D_j \,, D_j \bigcap D_m = \varnothing, j \neq m \,. \tag{2.4}$$

Протягом життєвого циклу документа з ним може виконуватися безліч різних операцій, серед яких створення, редагування, погодження, затвердження, використання, утилізація, архівування тощо. Позначимо множину операцій над

документом d^i як P_i. Кожна операція $p_{ij} \in P_i$ передбачає використання певного програмного та технічного забезпечення, обладнання, роботу певного персоналу із різним рівнем доступу тощо. Позначимо ISP_{ij} множину інформаційних систем, що використовуються під час виконання операції $p_{ij} \in P_i$ над документом.

Кожному співробітнику $StaffP_{ij}$ в межах операції $p_{ij} \in P_i$ при використанні інформаційного активу IA_m ставиться у відповідність рівень на виконання певних дій AL_{ijm}, який може приймати значення із множини {read , write , execute}. Відповідно до загально прийнятої практики в операційних системах, права на читання (read, позначається як: r або «4» в бітовій масці) – право читати файл, наприклад, за допомогою текстового редактора або переглядати вміст директорії; права на запис (write, позначається як: w або «2» в бітовій масці) – право робити запис і редагування в файлі, або створювати і видаляти файли в каталозі; право на виконання (execute, позначається як: x або «1» в бітовій масці) – право запускати файл (програму, записану в файлі) або переходити в саму директорію, якщо при цьому немає права на читання, тоді користувач просто не побачить наповнення папки.

Для виконання операції $p_{ij} \in P_i$ може залучатися як співробітник підприємства, так і співробітник підрядника чи замовника (власника). Сукупність операцій P_i по документу d^i може бути представлена у вигляді мережевого графу, що відображає технологічну схему обробки документа. При цьому можуть створюватися різні екземпляри документів в різних формах $d^i_{lk} \in D$, тобто кожній операції $p_{ij} \in P_i$ у загальному випадку співставлений деякий набір документів [].

Загрози інформаційної безпеки при обробці документа d^i в загальному випадку пов’язані з конфіденційністю, цілісністю та доступністю.

Будемо розраховувати інтегральний показник ризику IR^i по документу d^i як:

$$IR^i = RConf^i + RIn^i + RAv^i, \qquad (2.5)$$

де $RConf^i$ – рівень ризику порушення конфіденційності документу d^i; RIn^i – рівень ризику порушення цілісності d^i; RAv^i – рівень ризику порушення доступності d^i.

Під порушенням конфіденційності документа розуміють фактор стороннього ознайомлення з інформацією документа, він стає відомим тому, хто не володіє повноваженнями доступу до нього [9]. Воно має місце, коли отримано доступ до деякої інформації обмеженого доступу, що зберігається тому числі в комп'ютерній системі або передається від однієї системи до іншої [5].

Рівень ризику порушення конфіденційності $RConf^i$ документу d^i визначимо як [5,9]:

$$RConf^i = PConf^i \cdot UConf^i, \qquad (2.6)$$

де $PConf^i$ – оцінка можливості загрози порушення конфіденційності документа d^i; $UConf^i$ – оцінка шкоди від загрози порушення конфіденційності документа d^i.

Розрахунок оцінки можливості порушення конфіденційності $PConf^i$ документа d^i здійснюється так [5,9]:

$$PConf^i = \max_{p_{ij} \in P_i} PConf_j^i, \qquad (2.7)$$

де $PConf_j^i$ – оцінка можливості порушення конфіденційності документа d^i під час операції $p_{ij} \in P_i$.

До опису факторів ризику інформаційної безпеки проекту застосуємо лінгвістичний підхід. Це забезпечить створення кількісних оцінок для елементів моделі в умовах нечіткої інформації про значення рівня ризику, шкоди від загрози, можливостей виникнення певних загроз, рівнів незахищеності з вразливостями [117].

Для розрахунку оцінки $PConf_j^i$ можливості порушення конфіденційності документа d^i під час операції $p_{ij} \in P_i$ пропонується нечітка модель, узагальнена структура якої наведена на рисунку 2.1 [5].

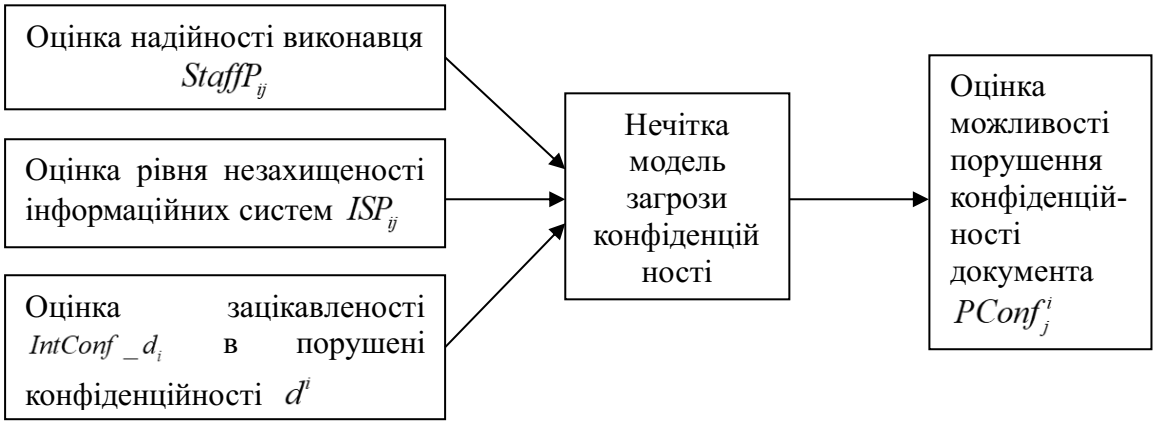


Рис. 2.1. Нечітка модель оцінки можливості загрози порушення конфіденційності документа

Як видно на рисунку 1, в нечіткій моделі вхідними є лінгвістичні змінні:

- рівень надійності виконавця операції $StaffP_{ij}$;
- оцінка рівня незахищеності інформаційних систем ISP_{ij};

– оцінка зацікавленості $IntConf_d_i$ сторонніх акторів в порушені конфіденційності документа d^i.

Для спрощення будемо вважати, що у операції $p_{ij} \in P_i$ лише один виконавець. Цього можна легко досягнути, врахувавши дане припущення при формуванні множини операцій над документом. Для оцінки рівня надійності виконавця може бути використана відповідна модель, побудована на засадах нечіткої логіки. В такому випадку для проведення розрахунків слід застосувати ієрархічне нечітке логічне виведення.

Для оцінки рівня незахищеності інформаційних систем пропонується використати стандарт CVSS [143] і розрахувати показник вразливості інформаційних систем ISP_{ij} операції $p_{ij} \in P_i$. На основі цього показника запропонована лінгвістична змінна $LevelISP_{ij}$, опис якої відповідно до методики інфологічного моделювання [144] наведено у вигляді фрейму на рисунку 2.2.

Рівень незахищеності інформаційних систем $LevelISP_{ij}$ при використанні оцінок вразливостей за CVSS	
Тип	Input
Блок змінних	
Оцінка вразливостей по стандарту CVSS	Множина допустимих значень $\{1\ldots10\}$
Блок термів	
None	Лінійна z-образна функція належності $\mu(x,0,0.1)$
Low	Трикутна функція належності $\mu(x,0.1,3.9,4)$
Medium	Трапецевидна функція належності $\mu(x,3.9,4.0,6.9,7)$
High	Трапецевидна функція належності $\mu(x,6.9,7.0,8.9,9)$
Critical	трикутна функція належності $\mu(x,8.9,9,10)$
Опис процедури формування нових термів відсутня	
Опис процедури формування функцій належності термів відсутня	

Рис. 2.2. Опис лінгвістичної змінної рівня незахищеності інформаційних систем

З метою формування функцій належності термів лінгвістичної змінної $LevelISP_{ij}$ використана обробка експертних оцінок на основі методу аналізу ієрархій Сааті.

Для кількісної оцінки рівня зацікавленості в порушені конфіденційності документа $IntConf_d_i$ пропонується застосувати метод аналізу ієрархій [145], спираючись на експертні оцінки на основі трирівневої ієрархії в вигляді дерева декомпозицій по акторам загроз та видам документів, представленої на рисунку 2.3. Оцінювати рівень зацікавленості в порушенні конфіденційності за замовчуванням запропоновано для виду документу. В тих випадках, коли це припущення не може бути застосовано, рівень зацікавленості встановлюється експертом [5].

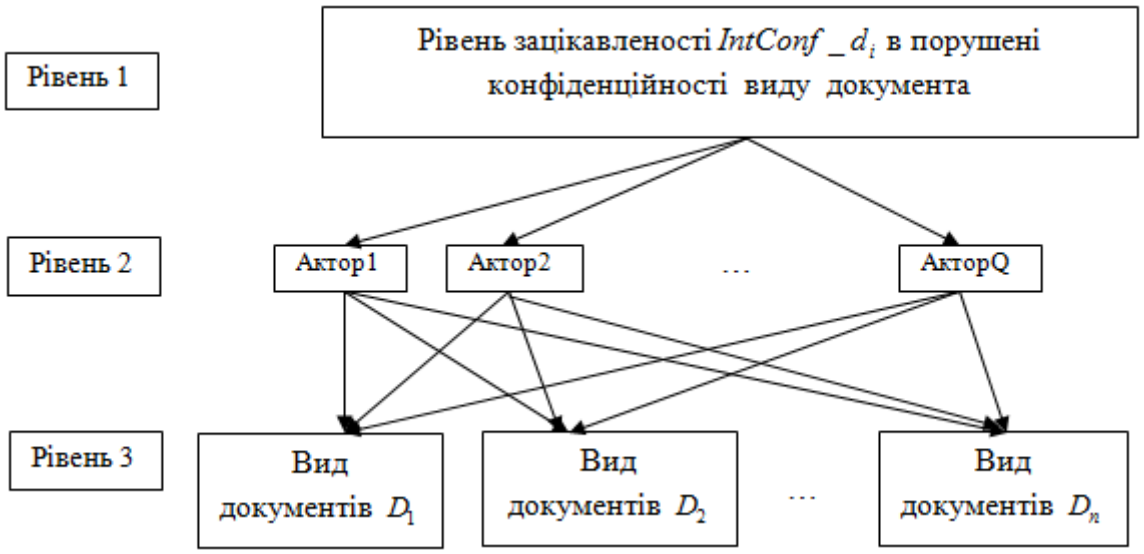


Рис. 2.3. Дерево критеріїв оцінки рівня зацікавленості в порушенні конфіденційності документу

Розрахунок оцінки $UConf^i$ шкоди від загрози порушення конфіденційності документа d^i вимагає введення множини частинних показників, що впливають

на даний збиток/шкоду. Узагальнений перелік частинних показників розроблено і представлено у таблиці 2.1 [3].

Таблиця 2.1

Перелік частинних показників збитку/шкоди

№	Назва показника	Група показників
1	Збиток авторитету організації	Зовнішня збиток/шкода
2	Збиток авторитету держави на міжнародній арені	
3	Судові витрати	
4	Негативна реакція на рівні уряду держави	
5	Публікація негативних матеріалів у пресі	
6	Можливість здійснення терористичних актів	
7	Можливість звершення техногенних катастроф	
8	Звільнення фахівців організації	Внутрішній збиток/шкода
9	Зниження рівня інформаційної безпеки	
10	Втрата або руйнування активів організації	
11	Вплив на прийняті персоналом організації рішення в бізнес-процесів	
12	Необхідність перевірки і відновлення цілісності активу	
13	Погіршення емоційного клімату в колективі	
14	Дезорганізація діяльності	
15	Необхідність ручного виконання робіт	
16	Зниження конкурентоспроможності організації	Фінансовий збиток
17	Втрати вигоди при укладанні договорів	
18	Зниження ліквідності і курсової вартості акцій	
19	Неможливість організації виконати свої зобов'язання перед клієнтами і постачальниками	
20	Необхідність проведення додаткових досліджень	
21	Можливість розкрадання активів і проведення неврахованих операцій	
22	Зниження цін на продукцію, обсягів продажів	
23	Втрата можливостей патентування, продажу ліцензій	
24	Випередження конкурентами виведення аналогічної продукції на ринок	
25	Відмова від стратегічних рішень, що стали неефективними	
26	Погіршення умов отримання кредитів	
27	Падіння рентабельності виробництва	
28	Зниження рівня співпраці з діловими партнерами	
29	Масові крадіжки, шахрайства	

Показники розподілені за трьома групами: зовнішній збиток/шкода організації, внутрішній збиток/шкода організації, фінансові збитки організації. Для розрахунку оцінки $UConf^i$ пропонується використати метод аналізу ієрархій на основі дерева критеріїв, яке складається з рівня частинних показників шкоди, видів документів проекту та документів, розподілених по видам. Шкода від порушення конфіденційності оцінюється в грошовому еквіваленті або у балах, які можуть бути використані при прийнятті рішень стосовно заходів кібербезпеки.

Під загрозою цілісності документа в загальному випадку розуміють пошкодження і знищення інформації, перекручення інформації – як не навмисне в разі помилок і збоїв, так і зловмисне.

Рівень ризику порушення цілісності RIn^i документу d^i визначимо як [4]:

$$RIn^i = PIn^i \cdot UIn^i, \tag{2.8}$$

де PIn^i – оцінка можливості загрози порушення цілісності документа d^i, яка приймає значення з відрізку [0,1]; UIn^i – оцінка шкоди від загрози порушення цілісності документа d^i.

Формула для розрахунку оцінки можливості порушення цілісності PIn^i документа d^i має вид [4]:

$$PIn^i = \prod_{p_j \in P_i} PIn_j^i, \tag{2.9}$$

де PIn_j^i – оцінка можливості порушення цілісності документа d^i під час виконання операції $p_{ij} \in P_i$.

Враховуючи, що інформація щодо ризиків інформаційної безпеки документів при виконанні проектів в багатьох галузях є нечіткою, для оцінки можливості загрози порушення цілісності документу та шкоди від цього порушення в роботі запропоновано застосувати лінгвістичний підхід на основі нечіткої логіки [10].

З метою розрахунку оцінки PIn_j^i можливості порушення цілісності документа d^i при виконанні операції $\boldsymbol{d^i}$ розроблена нечітка модель, вхідні та вихідні змінні якої наведені на рисунку 2.4 [4].

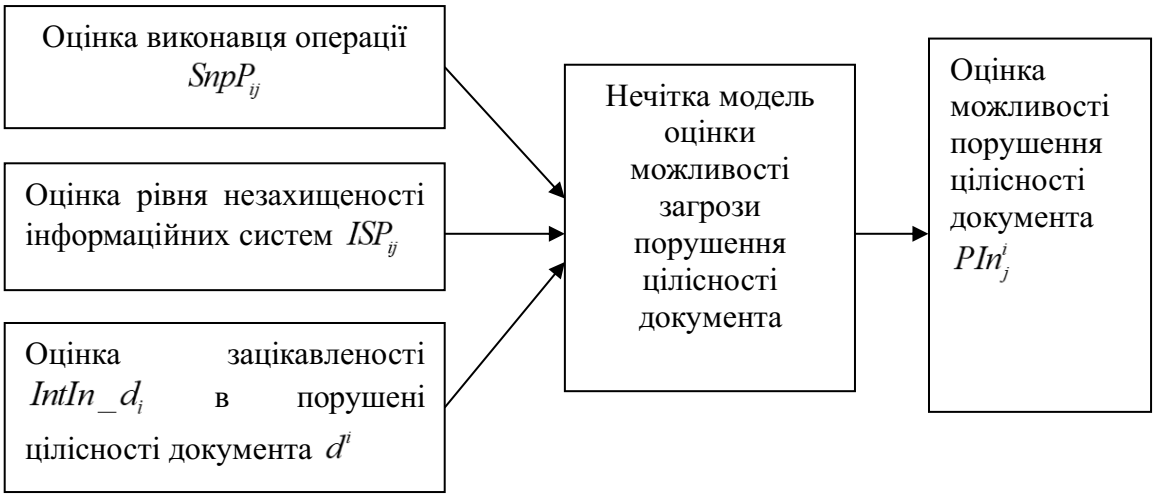


Рис. 2.4. Вхідні та вихідні змінні нечіткої моделі оцінки можливості загрози порушення цілісності документа

З рисунку 2.4 видно, що в даної нечіткої моделі вхідні лінгвістичні змінні:

- оцінка виконавця операції $SnpP_{ij}$;
- оцінка рівня незахищеності інформаційних систем ISP_{ij};
- оцінка зацікавленості $IntIn_d_i$ зовнішніх акторів в порушені цілісності документа d^i.

З метою спрощення приймемо припущення, що у кожної операції $p_{ij} \in P_i$ завжди один виконавець, чого легко можна досягнути при формуванні множини

операцій для документа. Оцінка виконавця операції $SnpP_{ij}$ характеризує можливість пошкодження ним документа зумисно або через недостатній рівень кваліфікації. Для розрахунку даної оцінки розроблена відповідна нечітка підмодель.

Розрахунок рівня незахищеності інформаційних систем ISP_{ij}, що використовуються при виконанні операції, слід виконувати на основі стандарту CVSS [143]. Результати розрахунку показника вразливості інформаційних систем є значенням базової вхідної змінної, для якої сформована відповідна лінгвістична змінна.

Оцінка $IntIn_d_i$ зацікавленості зовнішніх акторів в порушенні цілісності документа формалізована у вигляді лінгвістичної змінної, яка відповідно до методу інфологічного моделювання предметних областей задач нечіткого управління [144] представлена у вигляді фрейму на рисунку 2.5 [4].

Рівень зацікавленості в порушені цілісності документу	
Тип	Input
Блок змінних	
Рівень зацікавленості	Множина допустимих значень [0…9]
Блок термів	
низький	Лінійна z-образна функція належності $\mu(x,2,3)$
середній	Трикутна функція належності $\mu(x,3,5,3)$
високий	Лінійна s-образна функція належності $\mu(x,7,8)$
Опис процедури формування нових термів - відсутня	
Опис процедури формування функцій належності термів - відсутня	

Рис. 2.5. Опис лінгвістичної змінної рівня зацікавленості в порушенні цілісності документа

Для лінгвістичної змінної оцінки рівня зацікавленості в порушенні цілісності документу, що представлена на рисунку 2.5, значення базової змінної з множини допустимих значень формується на основі методу аналізу ієрархій Сааті з використанням експертних оцінок зацікавленості в порушенні цілісності для дерева рішень, в якому на передостанньому та останньому рівнях знаходяться множини зовнішніх акторів та множин видів документів. Таким чином, оцінка зацікавленості в порушенні цілісності конкретного документу d^i приймається рівною зацікавленості для всього виду документів. Однак при наявності виключень з цього правила можливо доповнення дерева ієрархії рівнем документів чи безпосереднє встановлення значення експертом.

Використовуючи запропоновані лінгвістичні змінні та їх терми для розрахунку оцінки можливості загрози порушення цілісності документа d^i сформована база правил нечіткого логічного виведення у вигляді нечітких продукцій. В загальному випадку множину правил цієї нечіткої бази знань можна представити у вигляді [4]:

$$\text{Правило } R\text{: <Якщо> } \bigcap_{i=1}^{N} A_i \ \text{ <ТО> } \bigcap_{j=1}^{M} C_j \ , \qquad (2.10)$$

де N – кількість підумов, що входять до антецеденту правила; M – кількість підвисновків, що входять в консеквент правила; A_i – підумова, що входить до антецеденту правила та є нечітким висловлюванням, що позначає прийняття певною лінгвістичною змінною значення з множини свої термів; C_j – підвисновок, що входить до консеквента правила та є нечітким висловлюванням, що позначає прийняття певною лінгвістичною змінною значення з множини свої термів.

На основі бази правил нечітких продукцій (2.10) з використанням методу Мамдані розраховується оцінка PIn_j^i можливості загрози порушення цілісності документа d^i, при виконанні операції $p_{ij} \in P_i^{lk}$. Потім по формулі (2.9)

розраховується загальна оцінка PIn^i можливості загрози порушення цілісності документа d^i.

Для обчислення оцінки UIn^i шкоди від виконання загрози порушення цілісності документа d^i сформована множина Y частинних показників, з яких складається величина збитків або шкоди на основі таблиці 2.1. Ці показники характеризують зовнішній збиток або шкоду для підприємства, внутрішній збиток або шкоду підприємства та його фінансові збитки. Розрахунок значення UIn^i пропонується здійснювати за допомогою методу аналізу ієрархій Сааті на основі дерева критеріїв, представленого на рисунку 2.6 [4].

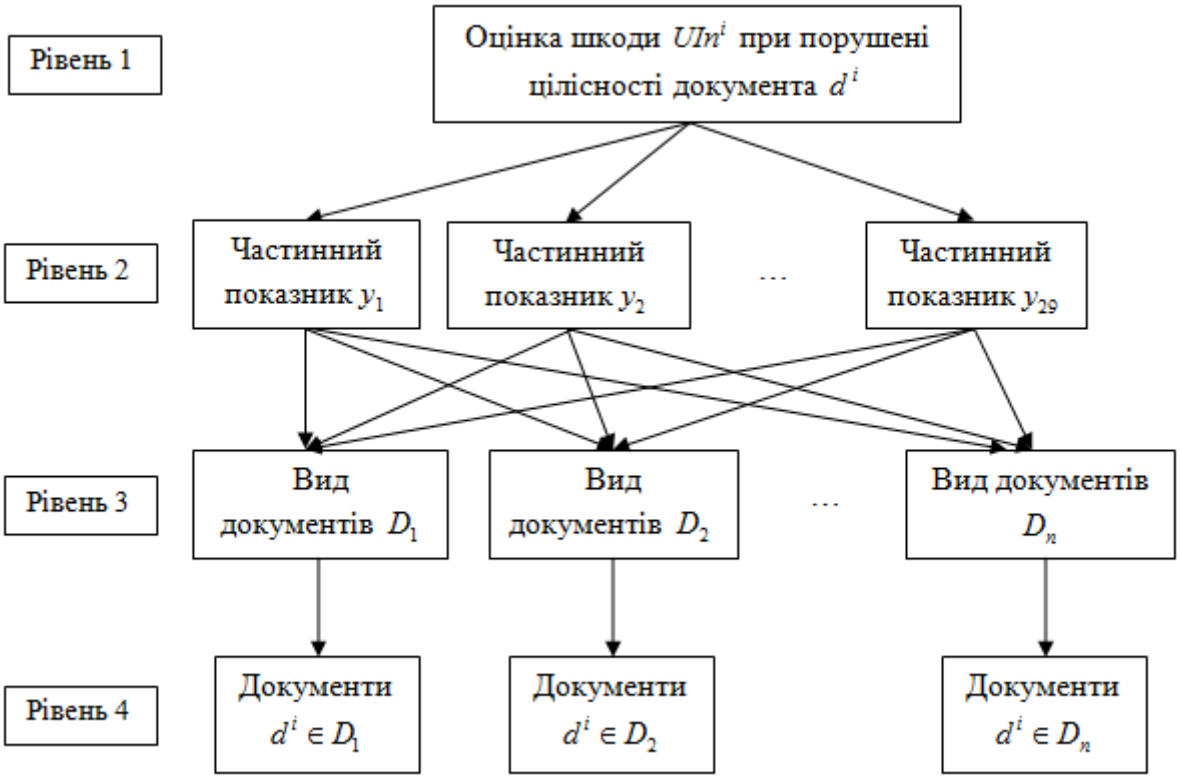


Рис. 2.6. Дерево ієрархії критеріїв оцінки шкоди при порушенні цілісності документу

Як видно на рисунку 2.6, дерево критеріїв для оцінки шкоди від порушення цілісності документів має чотири рівні. Крім частинних показників шкоди з множини Y, використовуються множини видів документів, що формуються для кожної галузі індивідуально. Приклад сформованих множин видів документів для будівельного підприємства наведено в таблиці 2.2 [4].

Таблиця 2.2

Види документів проектів будівельного підприємства

Вид документу	Опис
D_1	комерційні пропозиції;
D_2	обов'язкові для подання та забезпечення проектування об'єкта вихідні дані (містобудівні умови та обмеження, технічні умови, завдання на проектування);
D_3	договори та специфікації до них;
D_4	проектна документація на різних її стадіях після схвалення та/або після затвердження, як підставою для розроблення наступних стадій проектування (техніко-економічне обґрунтування, техніко-економічний розрахунок або «Ескізний проект»), що розробляється на об'єкт будівництва в цілому чи з відображенням окремих черг чи пускових комплексів;
D_5	в визначених регуляторами випадках документи щодо експертизи проектів;
D_6	дозвільні документи та ліцензії;
D_7	креслення;
D_8	витяги;
D_9	документи, що містять фінансові оцінки стадій та черг чи пускових комплексів по роботах, що передбачаються, кошториси;
D_{10}	документи, що містять фінансові оцінки стадій та черг чи пускових комплексів по виконаним роботам, акти виконаних робіт;
D_{11}	тендерні документі;
D_{12}	інші юридично значимі документи.

Шкода оцінюється в балах чи в грошову еквіваленті.

Рівень ризику порушення доступності RAv^i документу d^i визначимо як [3]:

$$RAv^i = PAv^i \cdot UAv^i, \qquad (2.11)$$

де PAv^i – оцінка можливості загрози порушення доступності документа d^i; UAv^i – оцінка шкоди від загрози порушення доступності документа d^i.

Розрахунок оцінки можливості загрози порушення доступності документа d^i здійснюється як:

$$PAv^i = \min_{l,k} \{ \max_{p_{ij} \in P_i^{lk}} PAv_j^i \}, \qquad (2.12)$$

де PAv_j^i – можливості загрози порушення доступності документа d^i під час операції $p_{ij} \in P_i^{lk}$, де P_i^{lk} –множина операцій, в якій використовується документ $d_{lk}^i \in D$ в l-формі та k-екземплярі.

До опису факторів ризику інформаційної безпеки проекту застосуємо лінгвістичний підхід. Це забезпечить створення кількісних оцінок для елементів моделі в умовах нечіткої інформації про значення рівня ризику, шкоди від загрози, можливостей виникнення певних загроз, рівнів незахищеності з вразливостями [117].

Для розрахунку можливості PAv_j^i порушення доступності документа d^i при виконанні операції $p_{ij} \in P_i^{lk}$ пропонується нечітка модель, узагальнена структура якої наведена на рисунку 2.7 [3].

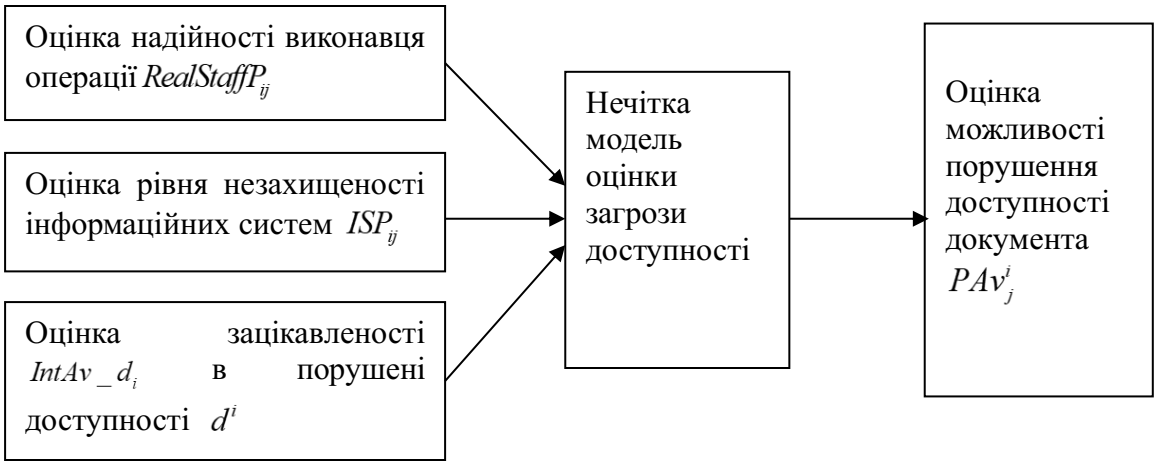


Рис. 2.7. Нечітка модель оцінки можливості загрози порушення доступності документа

Як видно на рисунку 1, в нечіткій моделі оцінки можливості загрози порушення доступності документа вхідними є лінгвістичні змінні:

– рівень надійності виконавця операції $RealStaffP_{ij}$;
– оцінка рівня незахищеності інформаційних систем ISP_{ij};
– оцінка зацікавленості $IntAv_d_i$ сторонніх акторів в порушені доступності документа d^i.

Для спрощення будемо вважати, що у операції $p_{ij} \in P_i$ лише один виконавець. Цього можна легко досягнути, врахувавши дане припущення при формуванні множини операцій над документом. Для оцінки рівня надійності виконавця може бути використана відповідна модель, побудована на засадах нечіткої логіки . В такому випадку для проведення розрахунків слід застосувати ієрархічне нечітке логічне виведення.

Для оцінки надійності $RealStaffP_{ij}$ виконавця операції $p_{ij} \in P_i$ пропонується нечітка модель, структура якої наведена на рисунку 2.8 [3].

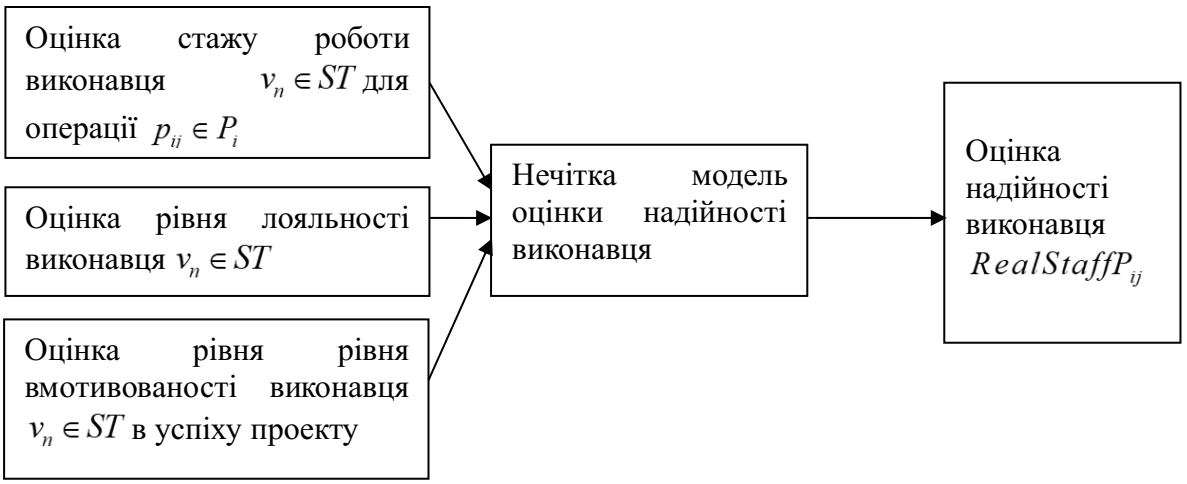


Рис. 2.8. Нечітка модель оцінки надійності виконавця

В нечіткої моделі оцінки надійності виконавця вхідними є наступні лінгвістичні змінні із наведеними відповідними характеристиками:

– стаж роботи виконавця *ExpStaffP* ;

– оцінка лояльності виконавця *SatStaffP* ;

– рівня вмотивованості виконавця в успіху проекту *MotStaffP* .

Опис зазначених вище вхідних лінгвістичних змінних наведено на рисунках 2.9 – 2.11 відповідно до методики інфологічного моделювання задач нечіткого управління [144].

Стаж роботи виконавця *ExpStaffP* **.**	
Тип	Input
Блок змінних	
Стаж роботи	Множина допустимих значень {0...55 років}
Блок термів	
Без стажу	Лінійна z-образна функція належності $\mu(x, 0.5, 1)$
Початківець	Трикутна функція належності $\mu(x, 0.5, 2, 3)$
Досвідчений	Лінійна s-образна функція належності $\mu(x, 1.5, 3)$
Опис процедури формування нових термів - відсутня	
Опис процедури формування функцій належності термів - відсутня	

Рис. 2.9. Опис лінгвістичної змінної стажу роботи виконавця *ExpStaffP*

Лояльність виконавця *SatStaffP*	
Тип	Input
Блок змінних	
Рівень лояльності	Множина допустимих значень $\{0\ldots10\}$
Блок термів	
нелояльний	Лінійна z-образна функція належності $\mu(x, 0.5, 1)$
нейтральний	Трикутна функція належності $\mu(x, 0.5, 2, 3)$
лояльний	Лінійна s-образна функція належності $\mu(x, 2, 3)$
Опис процедури формування нових термів - відсутня	
Опис процедури формування функцій належності термів - відсутня	

Рис. 2.10. Характеристики лінгвістичної змінної лояльності виконавця *SatStaffP*

Вмотивованість виконавця в успіху проекту *MotStaffP*	
Тип	Input
Блок змінних	
Рівень мотивації	Множина допустимих значень $\{0\ldots10\}$
Блок термів	
низький	Лінійна z-образна функція належності $\mu(x, 0.5, 2)$
нейтральний	Трикутна функція належності $\mu(x, 0.5, 2, 3)$
високий	Лінійна s-образна функція належності $\mu(x, 2, 3)$
Опис процедури формування нових термів - відсутня	
Опис процедури формування функцій належності термів - відсутня	

Рис. 2.11. Характеристики лінгвістичної змінної лояльності виконавця *MotStaffP*

Опис вихідної лінгвістичної змінної надійності виконавця *StaffP* наведено на рисунку 2.12.

Надійність виконавця *StaffP*	
Тип	Output
Блок змінних	
Рівень надійності	Множина допустимих значень $\{0\ldots10\}$
Блок термів	
ненадійний	Лінійна z-образна функція належності $\mu(x,2,5)$
сумнівний	трикутна функція належності $\mu(x,2,5,8)$
надійний	Лінійна s-образна функція належності $\mu(x,5,8)$
Опис процедури формування нових термів використання квантифікаторів дуже надійний, більш-менш-надійний, дуже ненадійний, несумнівний	
Опис процедури формування функцій належності термів дуже надійний $(\mu(x,5,8))^2$; більш-менш-надійний $\sqrt{\mu(x,5,8))}$; дуже ненадійний $(\mu(x,2,5))^2$; несумнівний $1-\mu(x,2,5)$	

Рис. 2.12. Характеристики лінгвістичної змінної надійності виконавця *StaffP*

Для оцінки рівня незахищеності інформаційних систем пропонується використати стандарт CVSS [14] і розрахувати показник вразливості інформаційних систем ISP_{ij} операції $p_{ij} \in P_i$. На основі цього показника запропонована лінгвістична змінна $LevelISP_{ij}$, опис якої відповідно до методики інфологічного моделювання [144] наведено у вигляді фрейму на рисунку 2.13.

Рівень незахищеності інформаційних систем *LevelISP* **при використанні оцінок вразливостей за CVSS**	
Тип	Input
Блок змінних	
Оцінка вразливостей по стандарту CVSS	Множина допустимих значень $\{1\ldots10\}$
Блок термів	
None	Лінійна z-образна функція належності $\mu(x,0,0.1)$
Low	Трикутна функція належності $\mu(x,0.1,3.9,4)$
Medium	Трапецевидна функція належності $\mu(x,3.9,4.0,6.9,7)$
High	Трапецевидна функція належності $\mu(x,6.9,7.0,8.9,9)$
Critical	трикутна функція належності $\mu(x,8.9,9,10)$
Опис процедури формування нових термів - відсутня	
Опис процедури формування функцій належності термів - відсутня	

Рис. 2.13. Опис лінгвістичної змінної рівня незахищеності інформаційних систем

Для формування функцій належності термів лінгвістичної змінної $LevelISP$ використана обробка експертних оцінок на основі методу аналізу ієрархій Сааті.

З метою оцінки рівня зацікавленості в порушені доступності документу $IntAv_d_i$ пропонується застосувати метод аналізу ієрархій, спираючись на оцінки експертів відповідно до трирівневої ієрархії по акторам загроз та видам документів, що показана на рисунку 2.14. За замовчуванням оцінювати рівень зацікавленості в порушенні доступності документу запропоновано як для його виду. В інших випадках, коли зазначене припущення не може бути застосовано, ця оцінка встановлюється експертом.

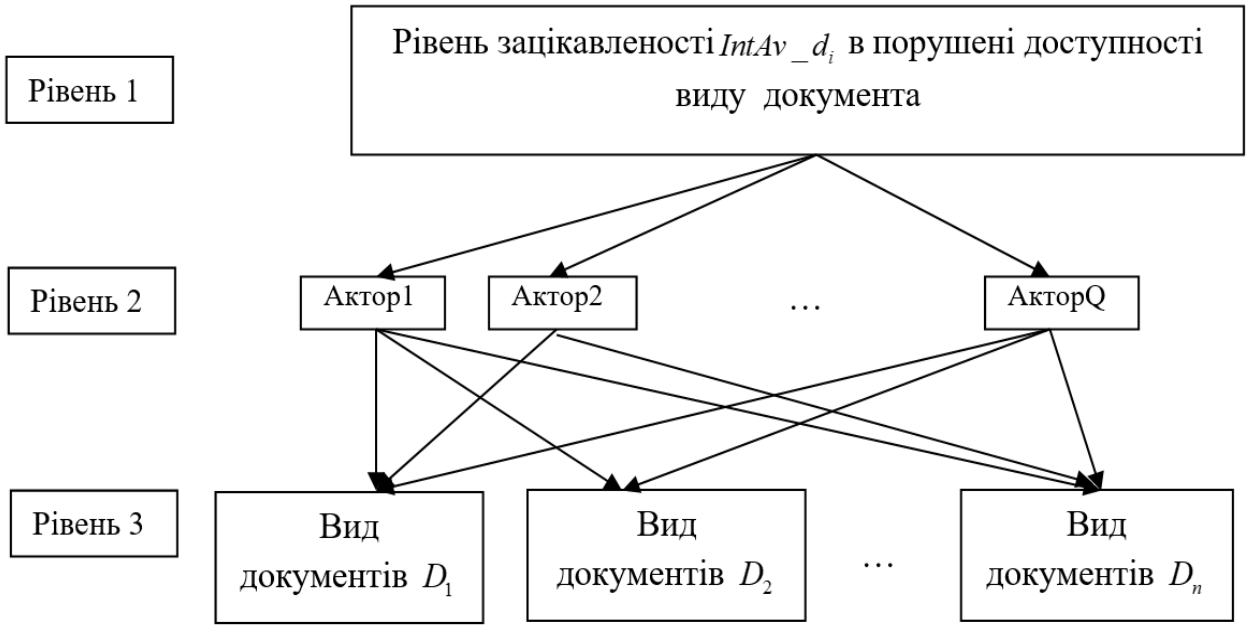


Рис. 2.14. Дерево критеріїв оцінки рівня зацікавленості в порушенні доступності документу

Опис лінгвістичної змінної можливості порушення доступності документу наведено на рисунку 2.15.

Рівень можливості порушення доступності PAv документа	
Тип	Output
Блок змінних	
Назва звичайної змінної	Множина допустимих значень [0,1]
Блок термів	
низький	Лінійна z-образна функція належності $\mu(x, 0, 0.5)$
середній	Трикутна функція належності $\mu(x, 0, 0.5, 1)$
високий	Лінійна s-образна функція належності $\mu(x, 0.5, 1)$
Опис процедури формування нових термів - відсутня	
Опис процедури формування функцій належності термів - відсутня	

Рис. 2.15. Опис лінгвістичної змінної можливості порушення доступності документу

На основі запропонованих лінгвістичних змінних та їх термів будуються в формі (2.10) нечіткі продукційні правила для виконання розрахунків по моделям.

Використовуючи один з алгоритмів нечіткого логічного виведення, наприклад, метод Мамдані, на основі бази правил нечіткої моделі оцінки можливості порушення доступності документа розраховується можливість PAv_j^i порушення доступності документа d^i при виконанні операції $p_{ij} \in P_i^{lk}$. Далі з використанням формули (2.12) розраховується загальна оцінка PAv^i можливості загрози порушення доступності документа d^i. Порушенням доступності документу вважається створення таких умов або здійснення дій, які унеможливлюють чи ускладнюють доступ до нього. Доступ є заблокованим або, якщо і є можливим, то за такий час, який не забезпечить досягнення тих чи інших цілей чи ведення бізнес-процесів. Під загрозою доступності документа розуміють його блокування або знищення, які пов’язують з діями користувачів, внутрішніми відмовами інформаційної системи, відмовами інфраструктури, що підтримує інформаційну систему. Наприклад, неможливість працювати із

необхідним документом через відсутність відповідної підготовки (недолік загальної комп'ютерної освіти, невміння інтерпретувати вхідні чи вихідні повідомлення, необізнаність з необхідними методиками, невміння працювати з документацією).

Для розрахунку кількісної оцінки ризику порушення доступності документу відповідно до формули (2.11) необхідно розрахувати оцінку UAv^i шкоди від загрози порушення доступності документа d^i [3].

Розрахунок оцінки UAv^i шкоди від загрози порушення доступності документа d^i вимагає створення множини частинних показників, що формують даний збиток чи шкоду. Узагальнений перелік цих частинних показників представлено у таблиці 2.1. Показники розподілені за трьома групами: зовнішній збиток чи шкода підприємству, внутрішній збиток чи шкода підприємству, фінансові збитки підприємства. Розрахунок величини UAv^i пропонується здійснювати з використанням методу аналізу ієрархій, дерево критеріїв якого складається з рівней частинних показників шкоди, видів документів проекту та документів, розподілених по видам. Шкода від порушення доступності оцінюється в грошовому еквіваленті або у балах, які можуть бути використані при формуванні рішень стосовно забезпечення інформаційної безпеки.

Інтегральний показник ризику IR^i по документу d^i розраховується по формулі (2.5) та може бути використаний при розробці заходів кіберзахисту як окремого документа, так і їх сукупності, наприклад пакету документів проекту.

Висновки до розділу 2

1. Проведено аналіз стану інформаційної безпеки сучасного виробничого підприємства та розглянуті фактори, які на неї впливають. По кожному напрямку

забезпечення інформаційної безпеки сформовані рекомендації фахівцям відділу інформаційних технологій. Розглянуто кроки до прискорення реакції на загрози, залучення для підвищення рівня кібербезпеки штучного інтелекту та хмарних технологій. Результати можуть бути застосовані для розробки стратегії інформаційної безпеки підприємств, в тому числі компаній, що використовують у своїй роботі сучасні технології 5G та сервіси IoT.

2. Розроблено модель оцінки ризиків інформаційної безпеки документів підприємства. Представлено формальний опис множини документів підприємства в вигляді узагальненої ієрархічної структури, формалізовано зв'язок документів з операціями, що над ними виконуються, та інформаційними системами, які використовуються під час цих операцій. Враховуючи невизначенісь та розмитість даних, на засадах нечіткої логіки з використанням методу аналізу ієрархій розроблено підмоделі для оцінки загроз порушення конфіденційності, цілісності та доступності документа. Запропоновано підходи для оцінки шкоди від порушення конфіденційності, цілісності та доступності документу та спосіб розрахунку загальної оцінки ризику інформаційної безпеки документу.

3. Представлена модель оцінки ризиків інформаційної безпеки документів може бути використана в процесах прийняття рішень стосовно інформаційної безпеки проектів в організаціях, які мають проектні види діяльності, в тому числі на IT- підприємствах, в компаніях будівельної галузі, підприємствах критичної інфраструктури та інших. Запропоновані підходи можуть слугувати основою для створення у складі інформаційної системи підприємства підсистеми управління інформаційною безпекою для автоматизації розрахунків оцінок ризиків кібербезпеки та виявлення вторгнень до корпоративної інформаційної мережі.

РОЗДІЛ 3
РОЗРОБКА МЕТОДІВ ТА МОДЕЛЕЙ ВИЯВЛЕННЯ ВТОРГНЕНЬ ДО ІНФОРМАЦІЙНОЇ СИСТЕМИ ПІДПРИЄМСТВА

Спираючись на результати проведеного в розділі 1 огляду існуючих підходів до управління інформаційною безпекою та моделювання факторів інформаційної безпеки в розділі 2, в даному розділі виконано аналіз наборів даних для тренування моделей машинного навчання виявлення вторгнень, розроблено метод обрання набору ознак для навчання класифікаторів вторгнень та гібридний метод ідентифікації вторгнень на основі ансамблевого навчання та алгоритмів нечіткої логіки.

3.1 Аналіз наборів даних для тренування моделей машинного навчання виявлення вторгнень та їх підготовка

3.1.1 Набір даних KDD Cup 1999

Дані були зібрані в 1998 році за допомогою програми оцінки DARPA IDS. Приблизно 4 900 000 векторів було створено протягом семи тижнів перевантаження мережі. Було визначено чотири типи імітованих атак: користувач на root (U2R), віддалений на локальний (R2L), зондування та відмова в обслуговуванні (DoS). Кожен із цих типів атак позначається окремою абревіатурою (DoS). Кожну з 41 характеристики в цьому наборі даних можна віднести до одного з трьох окремих класів:

(1) - фундаментальні характеристики;

(2) - характеристики трафіку;

(3) - характеристики вмісту.

З моменту свого першого випуску в 1999 році набір даних KDD99 в основному використовувався для оцінки продуктивності систем виявлення аномалій. Ця колекція даних була зібрана з використанням інформації, зібраної з програми оцінки IDS DARPA 1998 року. Колекція DARPA98 складається з приблизно 4 терабайтів необроблених (двійкових) дампів TCP, зібраних протягом семитижневого періоду мережевої активності. Ця інформація може бути розділена приблизно на 5 мільйонів записів підключення, причому кожен запис містить приблизно 100 байт інформації. За двотижневий пробний період на цій платформі було здійснено близько двох мільйонів реєстрацій підключень. Навчальний набір даних KDD містить близько 4 900 000 різних векторів підключення. Кожен вектор з'єднання містить 41 характеристику, на яку можна атакувати як у стандартному режимі, так і в режимі атаки [146,147].

Можна виділити чотири різні форми імітаційних атак [146,147]:

1. Зловмисник може здійснити атаку на відмову в обслуговуванні, також відому як DoS-атака. Ця атака може включати перевантаження комп'ютера чи пам'яті в режим надто зайнятого або повного завантаження для ефективної обробки справжніх запитів або запобігання авторизованим користувачам доступу до системи. Обидва з ці методи є вважається " відмова з обслуговування»
2. Під час атаки User-to-Root зловмисник спочатку отримує доступ до системи за допомогою аналізу пароля, атаки за словником або соціальної інженерії, а потім використовує вразливість системи, щоб отримати доступ root (U2R). Експлойти користувача до root – це різновид атак, які дозволяють будь-якому користувачеві отримати адміністративні привілеї для системи. Цей тип уразливості безпеки відомий як «атака користувача на root».
3. Атака хробака відбувається, коли зловмисник має можливість передавати пакети через мережу, але не має облікового запису в цій

системі. Такий напад є успішним, лише якщо мережа не захищена паролем. Локальний зловмисник використовує вразливість, щоб отримати доступ до системи так само, як і користувач.

4. Прагнення зібрати якомога більше інформації про комп'ютерну систему чи мережу. Цей вид атаки має на меті обійти засоби захисту, призначені для захисту мережі.

Вибір для отримання навчальних даних з одного розподілу ймовірностей і тестових даних з окремого розподілу ймовірностей робить роботу більш реалістичною.

3.1.2 Набір даних NSL-KDD

Ця збірка даних пропонує пропозиції щодо покращення набору даних KDD 1999. Переважна більшість досліджень щодо виявлення вторгнень вказує на те, що набір даних NSL-KDD дає точніші результати при порівнянні продуктивності обох наборів даних.

Набір даних NSL-KDD в основному складається з чотирьох типів нападів:

1. DoS — це абревіатура від «відмова в обслуговуванні», що означає атаку, під час якої ціль не в змозі відповідати на дійсні запити або обробляти їх, оскільки всі її ресурси вичерпано. До такого типу флуду належать, наприклад, синхронні флуди. У цьому контексті особливо актуальні терміни «вихідні байти» і «відсоток пакетів з помилками». Ставка _ пакет помилка і джерело байт спосіб передавання.
2. Метою атак зі скануванням портів, а також інших типів пробних атак, таких як шпигунство, є отримання інформації про віддалену ціль. Цей розділ має містити посилання на « час підключення» та «вихідні байти».

3. Атаки U2R включають неавторизований доступ до прав локального суперкористувача (root). Використовуючи стандартний обліковий запис, зловмисник підключається до цільової системи та намагається отримати права root або адміністратора, використовуючи вразливість у системі жертви, таку як атака переповнення буфера. Це часто називають атакою U2R. U2R – це абревіатура від «несанкціонований доступ до привілеїв локального суперкористувача (root)». Двома ключовими характеристиками є «кількість ініційованих підказок оболонки» та «кількість створених файлів». І те, і інше можна знайти в стовпці під назвою «кількість створених файлів».

4. Фраза «remote -to-local» (R2L) означає, що зловмисник зламав віддалену робочу станцію, щоб отримати доступ до локальної системи. Поширена практика «вгадування » паролів є чудовим прикладом. Однак дані про « кількість невдалих спроб входу» на рівні хоста набагато важливіші, ніж дані про «тривалість з'єднання» та «запитані послуги» на рівні мережі.

Попередником набору даних *NSL-KDD Dataset* є безліч *KDD99 Dataset*. *KDD99* де-факто є першим стандартом в області *Dataset* для систем виявлення вторгнень, створеним для проведення порівняльного тестування адаптивних алгоритмів у системах виявлення вторгнень [146,147].

Через розвиток систем виявлення вторгнень, у реалізації *KDD99* було виявлено велику кількість недоліків [148], які згодом були усунені шляхом реалізації *NSL-KDD Dataset*, що містить ряд переваг у порівнянні з *KDD99* серед яких можна виділити такі як:

– видалення ряду записів з метою усунення впливу частотних характеристик (надмірність, дублювання) на адаптивний механізм;
– найбільш продуманий підхід до формування тестових та навчальних множин і т.д.

Склад та опитування набору *NSL-KDD Dataset* представлений у таблиці 3.1 та таблиці 3.2.

Таблиця 3.1

Набір даних *NSL-KDD Dataset*

№	Найменування множини	Опис
1	*KDDTrain+*	навчальна вибірка з мітками атаки та рівнем складності
2	*KDDTrain+20%*	20% підмножина *KDDTrain+*
3	*KDDTest+*	перевірочна множина з мітками атаки та рівнем складності
4	*KDDTest-21*	множина з *KDDTest+* яке не включає записи рівень атак, яких вище значення 21

Таблиця 3.2

Розподіл записів за множинами в *NSL-KDD Dataset*

Найменування множини	Записів	Нормальних запитів	Кількість			
			DoS	Probe	U2R	R2L
KDDTrain+20%	25192	13449	9234	2289	11	209
		53.39%	36.65%	9.09%	0.04%	0.83%
KDDTrain+	125973	67343	45927	11656	52	995
		53.46%	36.46%	9.25%	0.04%	0.79%
KDDTest+	22544	9711	7458	2421	200	2754
		43.08%	33.08%	10.74%	0.89%	12.22%

Об'єкти в *NSL-KDD Dataset* являють собою з'єднання - послідовність пакетів (*TCP, UDP, ICMP*), зафіксовану в певний проміжок часу, в яку укладено потік даних від *IP* адреси джерела до *IP*- адреси призначення відповідно до певного протоколу [149].

Набір даних містить 4 категорії загроз:

- *Denial of Service (dos)*. Набір атак, у яких зловмисник обмежує доступ верифікованим користувачам до конкретного сервісу через певний протокол (*Back, Land, Neptune, Pod, Smurf, Teardrop, Apache2, Udpstorm, Processtable, Worm*).
- *Remote to Local (r2l)*. Набір атак, у яких зловмисник намагається отримати доступ ззовні до локальної машини користувача (*Guess_Password, Ftp_write, Imap, Phf, Multihop, Warezmaster, Warezclient, Spy, Xlock, Xsnoop, Snmpguess, Snmpgetattack, Httptunnel, Sendmail, Named*).
- *User to Root (u2r)*. Набір атак, в яких зловмисник маючи доступ до машині жертви намагається отримати права більш привілейованого користувача (*Buffer_overflow, Loadmodule, Rootkit, Perl, Sqlattack, Xterm, Ps*).
- *Probe*. Набір атак, в яких зловмисник намагається отримати відомості про інфраструктуру користувача (*Satan, Ipsweep, Nmap, Portsweep, Mscan, Saint*).

Хоча розмірність вектора (кількість атрибутів у запиті) *NSL-KDD Dataset* дорівнює 43, для реальної роботи використовується 41 атрибут, а 42-й атрибут представляє категорію загрози, 43-ий - про складність реалізації атаки (від найпростішого до найскладнішого). Таким чином, формальна модель запиту для набору даних *NSL-KDD Dataset* являє собою вектор розмірності 41.

Повний список атрибутів записів запитів *NSL-KDD Dataset* представлений у таблиці 3.3.

Таблиця 3.3

Атрибут	**Опис**	**Атрибут**	**Опис**
1. тривалість	Тривалість з'єднання	*22. is guest login*	1 якщо "Гість", інакше 0
2. protocol type	Тип протоколу (tcp, udp тощо)	*23. count*	кількість підключень до того ж хосту, що і поточне з'єднання протягом останніх двох секунд
3. service	Сервіс призначення (telnet, ftp тощо)	*24. srv count*	кількість підключень до того ж сервісу, що і поточне з'єднання протягом останніх двох секунд

Продовження таблиці 3.3

Атрибут	**Опис**	**Атрибут**	**Опис**
4. flag	Статус прапора з'єднання	*25. serror rate*	% з'єднань у яких помилка в "SYN" пакеті
5. source bytes	Кількість байт відправлених за адресою призначення	*26. srv serror rate*	% з'єднань у яких помилка в "SYN" пакеті
6. destination bytes	Кількість байт відправлених від відправника адресату	*27. rerror rate*	% з'єднань у яких помилка в "REJ" пакеті
7. land	1 якщо з'єднання з/в той самий хост/порт, інакше 0	*28. srv rerror rate*	% з'єднань у яких помилка в "REJ" пакеті
8. wrong fragment	Кількість помилкових фрагментів	*29. same srv rate*	% з'єднань до одного і того ж сервісу
9. urgent	Кількість термінових пакетів	*30. diff srv rate*	% з'єднань до різних сервісів
10. hot	Кількість "гарячих" індикаторів	*31. srv diff host rate*	% з'єднань до різних хостів
11. failed logins	Кількість невдалих спроб авторизації	*32. dst host count*	Кількість з'єднань мають однакові порти
12. logged in	1 якщо догляд успішний, інакше 0	*33. dst host srv count*	Кількість з'єднань мають однакові хости та однакові послуги
13. Compromised	Кількість скомпрометованих умов	*34. dst host same srv rate*	% з'єднань мають однакові хости та однакові сервіси
14. root shell	1 якщо видано право root, інакше 0	*35. dst host diff srv rate*	% різних сервісів на поточному хості
15. su attempted	1 якщо "su root" успішно, інакше 0	*36. dst host same src port rate*	% з'єднань на поточному хості, що мають аналогічний порт
16. root	Кількість "root" сесій	*37. dst host srv diff host rate*	% з'єднань поточного сервісу, що отримується від інших хостів
17. file creations	Кількість операцій зі створення файлів	*38. dst host serror rate*	% з'єднань до поточного хосту у яких S0 помилок
18. shells	Кількість запущених з оболонок	*39. dst host srvb serror rate*	% з'єднань до поточного хосту та сервісу у яких S0 помилка
19. access files	Кількість операцій з отримання доступу до файлів	*40. dst host rerror rate*	% з'єднань до поточного хзосту у яких є помилка RST
20. outbound cmds	Кількість вихідних команд у ftp сесії	*41. dst host srv rerror rate*	% з'єднань до поточного хосту та сервісу у яких є будь-яка помилка RST
21. is hot login	1 якщо авторизація була "гарячої", інакше 0		

Кожен зразок у NSL-KDD містить 41 ознаку, класифікація яких наведена в таблиці 3.4.

Таблиця 3.4

Опис даних з набору NSL-KDD.

Атрибути	Опис
1–9	Basic features of network connections
10–22	Content-related traffic features
23–31	Time-related traffic features
32–41	Host-based traffic features

3.1.3 Набір даних UNSW-NB15

Набір даних UNSW-NB15 досить великий, він містить майже 2 мільйони векторів, був опублікований у 2015 році лабораторією Cyber Range Австралійського центру кібербезпеки (ACCS) і є широко використовуваним набором даних системи виявлення мережевих вторгнень (NIDS) [128].

Він містить гібрид нормального та ненормального мережевого трафіку, створеного за допомогою інструменту IXIA PerfectStorm, цей трафік було зафіксовано як файли pcap, 35 ознак було вилучено за допомогою Argus і Bro-IDS, 12 додаткових ознак було згенеровано з відповідних даних.

Набір даних UNSW-NB15 містить такі 9 категорій атак:

- Analysis: загрози, націлені на веб-додатки за допомогою портів, електронних листів і сценаріїв.
- Backdoor: Техніка, спрямована на обхід механізмів безпеки, покладаючись на певні клієнтські програми.
- Відмова в обслуговуванні (Denial of Service - DoS): спроба перевантажити ресурси комп’ютерної системи з метою запобігання доступу або доступності її даних.

- Експлойти (Exploits): послідовності команд, що контролюють поведінку хоста через відому вразливість.
- Fuzzers: Атака, під час якої зловмисник надсилає великі обсяги випадкових даних, що спричиняє збій системи, а також має на меті виявити вразливі місця системи безпеки.
- Загальний (Generic): метод, який націлений на криптографію та викликає колізію з кожним блоковим шифром.
- Розвідка (Reconnaissance): метод збору інформації про хост мережі, також відомий як зондування.
- Shellcode: зловмисне програмне забезпечення, яке проникає в програмний код для керування хостом жертви.
- Черв'яки (Worms): атаки, які розмножуються та поширюються на інші комп'ютери.

Розподіл атак у наборі даних є незбалансованим, загалом набір даних містить 2390275 загальних зразків, які мають розподіл 96,02% доброякісних, 1,32% атак експлойтів, 0,93% атак з розмиванням, 0,69% загальних атак, 0,53% розвідувальних атак, 0,24% DoS атак, 0,10% аналітичних атак, 0,09% бекдор-атак, 0,06% атак shellcode та < 0,01% атак хробаків.

Розподіл лише шкідливих зразків у наборі даних наочно показано на рисунку 3.1.

Як видно на рисунку 3.1, це представляє проблему для точної класифікації атак менш поширених категорій і запобігання переобладнанню до найбільшого класу.

Незбалансованість набору даних є загальною рисою наборів даних мережевих IDS.

Перелік ознак і їх типи у наборі даних UNSW-NB15 наведено в таблиці 3.5.

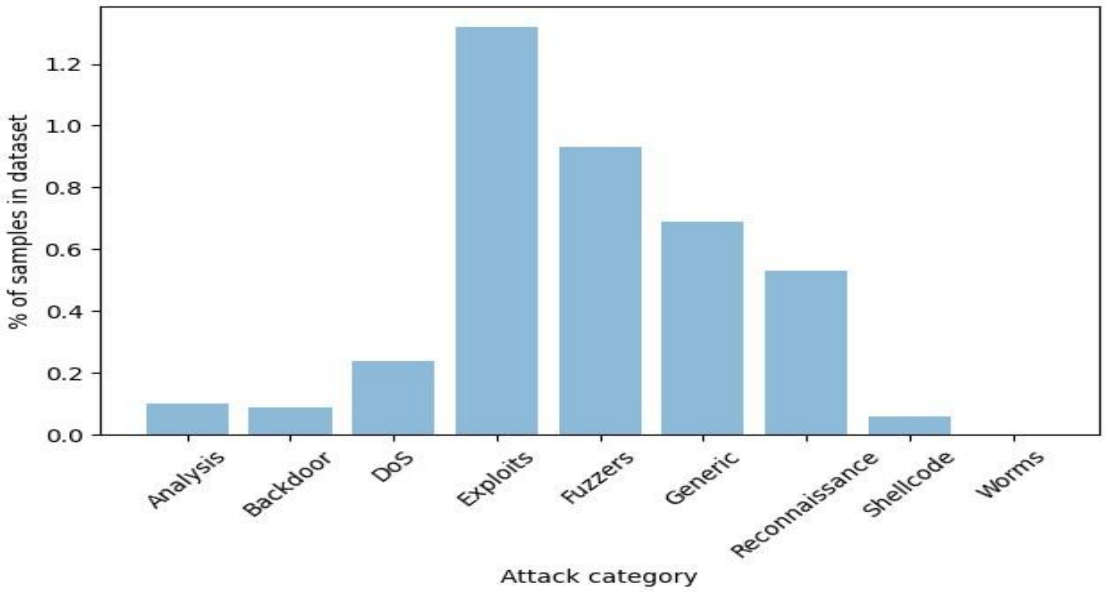


Рис. 3.1. Розподіл класів набору даних за винятком доброякісних зразків

Таблиця 3.5.

Опис ознак і їх тип у наборі даних UNSW-NB15

Name	**Type**	**Name**	**Type**	**Name**	**Type**
srcip	nominal	Djit	Float	Dpkts	integer
sport	integer	Stime	Timestamp	swin	integer
dstip	nominal	Ltime	Timestamp	dwin	integer
dsport	integer	Sintpkt	Float	stcpb	integer
proto	nominal	Dintpkt	Float	dtcpb	integer
state	nominal	Tcprtt	Float	smeansz	integer
dur	Float	Synack	Float	dmeansz	integer
sbytes	Integer	Ackdat	Float	ct_src_dport_ltm	integer
dbytes	Integer	is_sm_ips_ports	Binary	ct_dst_sport_ltm	integer
sttl	Integer	ct_state_ttl	Integer	ct_dst_src_ltm	integer
dttl	Integer	ct_flw_http_mthd	Integer	trans_depth	integer
sloss	Integer	is_ftp_login	Binary	res_bdy_len	integer
dloss	Integer	ct_ftp_cmd	integer	Sjit	Float
service	nominal	ct_srv_src	integer	attack_cat	nominal
Sload	Float	ct_srv_dst	integer		
Dload	Float	ct_dst_ltm	integer		
Spkts	integer	ct_src_ ltm	integer		

3.1.4 Набір даних CSE-CIC-IDS2018

Цей набір даних було схвалено Комітетом безпеки зв'язку (CSE) і Канадський інститут кібербезпеки для використання в дослідницьких проектах (CIC).

Розподілена відмова в обслуговуванні, розподілена відмова в обслуговуванні (DDoS), веб-атаки, ботнет і проникнення включені в колекцію CSE-CIC-IDS2018. Для формування набору даних було використано програму під назвою CIC Flow Meter, щоб отримати 80 показників мережевого потоку із змодельованого мережевого трафіку.

Набір даних CSE-CIC-IDS2018 є прикладом набору даних, створеного за допомогою систематичних профілів. Цей збір даних надасть описи вторгнень і моделі розповсюдження для програм, протоколів і мережевих компонентів нижчого рівня, які базуються на реальності.

Однією з реалістичних особливостей цього набору даних є 83% доброякісного відсотка трафіку. Оскільки очікується, що більша частина трафіку також буде нормальною в реальній топології, навчання моделі детектора аномалій є дуже критичним, використовуючи цей створений безпечний трафік. Це покращить здатність нашої моделі відрізняти безпечний трафік від атакуючого чи підозрілого трафіку, що зменшить частоту хибних спрацьовувань і підвищить точність.

Кожна атака була здійснена з однієї або кількох машин за межами цільової мережі. Подібно до мережевих топологій у реальному світі, було розгорнуто 5 різних підмереж, що імітують різні відділи та серверні кімнати компанії.

Розподіл мережевого трафіку цього набору даних наведено в таблиці 3.6. Усі 14 типів атак зіставлені зі сценаріями атак.

Таблиця 3.6

Розподіл атак набору даних

Сценарій атаки	**Назва атаки**	**Розподіл (%)**
Доброякісний	Жодного	83.07
DDoS	None	7,786
	DDoS	
	DDOS-LOIC-UDP	
DoS	DDOS-HOIC	4,031
	DoS-GoldenEye	
	DoS-Slowloris	
	DoS-SlowHTTPTest	
Брут сила	DoS-Hulk	2,347
	FTP-BruteForce	
Ботнет	SSH-BruteForce	1,763
Інфільтрація	Bot	0,997
Веб -атака	Infiltration	0,006
	Brute Force -Web	
	Brute Force -XSS	

У таблиці В.1 Додатку В наведено список вилучених характеристик мережевого трафіку та їх опис. На додаток до 75 функцій для мережевого потоку трафіку також було додано 5 додаткових функцій для категоризації трафіку: *FlowID , SourceIP , DestinationIP , SourcePort , DestinationPort* і *Protocol.*

Набір даних CSE-CIC-IDS2018 є незбалансованим (як і UNSW-NB15 або LITNET – див. нижче). Проблема незбалансованої класифікації (при виконання багатокласової класифікації) спричинена чисельно співвідношенням доброякісного трафіку до всього трафіку. Таблиця 3.7 демонструє, що доброякісність становить значну частину даних із 13 484 708 записами, або 83% від загальної кількості, тоді як на кожен тип нападу припадає менше 5% записів,

або приблизно три мільйони записів, або 17% усіх записів, у той час як доброякісні записи становлять 13 484 708 записів, або 83% від загальної кількості

Таблиця 3.7

Розподіл даних CSE-CIC-IDS2018

Тип класу	**Номер**	**Об'єм (%)**
Доброякісний	13484708	83,0700
DDOS атака-HOIC	686012	4,2260
DDoS-атаки-LOIC-HTTP	576191	3,5495
DoS-атаки-Халк	461912	2,8455
Бот	286191	1,7630
FTP-BruteForce	193360	1.1912
SSH-Bruteforce	187589	1,1556
Інфільтрація	161934	0,9976
DoS-атаки-SlowHTTPTest	139890	0,8618
DoS-атаки - GoldenEye	41508	0,2557
DoS-атаки-Slowloris	10990	0,0677
DDOS атака-LOIC-UDP	1730	0,0107
Груба сила - Web	611	0,0038
Груба сила -XSS	230	0,0014
SQL ін'єкція	87	0,0005
Всього	**16,232,943**	**100**

Для використання набору даних CSE-CIC-IDS2018 необхідно виконати декілька попередніх кроків, перш ніж його можна буде використовувати для аналізу з використанням алгоритмів машинного навчання.

Для підготовки набору даних було застосовано наступні кроки [150]:

Крок 1. Видалені повторювані заголовки з набору даних, які відображаються як рядки.

Крок 2. Значення Infinity та inf замінені на одне (було обрано “inf”).

Крок 3. Видалені пробіли та несловесні символи з назви стовпця.

Набір даних CSE-CIC-IDS2018 після його очищення було проаналізовано, дані було розбито на дві групи: доброякісний/нормальний трафік і атакуючий трафік (таблиця 3.8). Результати класифікаціх даних за типом атаки на основі мітки типу атаки наведені в таблиці 3.9.

Таблиця 3.8

Кількість атак і доброякісного трафіку для набору даних CSE-CIC-IDS2018

Label	Number	Percentage
Benign	13,484,708	83.07%
Attack	2,748,235	16.93%
Total	16,232,943	

Таблиця 3.9

Типи атак і їх частка для набору даних CSE-CIC-IDS2018

Назва	Кількість	Частка, %
Benign	13484708	83.0700%
DDOS attack-HOIC	686012	4.2260%
DDoS attacks-LOIC-HTTP	576191	3.5495%
DoS attacks-Hulk	461912	2.8455%
Bot	286191	1.7630%
FTP-BruteForce	193360	1.1912%
SSH-Bruteforce	187589	1.1556%
Infiltration	161934	0.9976%
DoS attacks-SlowHTTPTest	139890	0.8618%
DoS attacks-GoldenEye	41508	0.2557%
DoS attacks-Slowloris	10990	0.0677%
DDOS attack-LOIC-UDP	1730	0.0107%
Brute Force –Web	611	0.0038%
Brute Force -XSS	230	0.0014%
SQL Injection	87	0.0005%

Набір даних CSE-CIC-IDS2018 містить шість різних сценаріїв атак: Brute Force, Botnet, DoS, DDoS, Web Attacks, and Infiltration. Кожен зразок у CSE-CIC-IDS2018 містить 83 функції, перелічені в таблиці 3.10.

Таблиця 3.10.

Групування ознак набора даних CSE-CIC-IDS2018

Attributes	Description
1–4	Basic features of network connections
5–16	Features of network packets
17–22	Features of network flows
23–45	Statistic of network flows
46–63	Content-related traffic features
64–67	Features of network subflows
68–79	General purpose traffic features
80-83	Basic features of network connections

3.1.5 Набір даних Litnet-2020

Набір LITNET-2020 – це новий анотований мережевий набір даних для виявлення мережевих вторгнень, отриманий дослідниками з Каунаського технологічного університету (KTU) із реального трафіку литовської академічної мережі LITNET. Середовище збору даних, порівняння набору даних з іншими нещодавно опублікованими наборами даних про вторгнення в мережу та опис атак, представлених у наборі даних LITNET-2020, представлено [151]. Набір даних містить безпечний трафік академічної мережі та 12 типів атак, згенерованих у керованій KTU мережі LITNET з 6 березня 2019 року по 31 січня 2020 року. Мережевий трафік було зафіксовано за допомогою двійкового формату nfcapd з відкритим кодом, анонімно та оброблено у форматі CSV, містить 39 603 674 записи з мітками часу. Інструменти сценаріїв Nfsen, MeSequel і Python використовувалися для генерації додаткових функцій і попередньої обробки з полями даних у форматі CSV, названими відповідно до полів, згенерованих Nfdump. 49 атрибутів, які є специфічними для протоколу NetFlow v9, як визначено в RFC 3954 (Claise, 2004), використовуються для формування основи

набору даних, далі розширено додатковими полями прапорів часу та tcp (у символьному форматі), які можна використовувати для ідентифікації атак. Додано ще 19 спеціальних атрибутів атаки. Представлення класів у LITNET-2020 незбалансоване в діапазоні приблизно від 1 : 30 до 1 : 100 000.

У наступній таблиці 3.11 наведено підсумок представлення класу цього набору даних.

Таблиця 3.11

Представлення класу набору даних LITNET-2020.

Клас трафіку	Мітка	Кількість записів[1]	Частка, %
Benign	немає	36 423 860	91,9709%
SYN Flood	tcp_syn_f	1 580 016	3,9896%
Code Red	tcp_red_w	1 255 702	3,1707%
Smurf	icmp_smf	118 958	0,3004%
UDP Flood	udp_f	93 583	0,2363%
LAND DoS	tcp_land	52 417	0,1324%
W32.Blaster	tcp_w32_w	24 291	0,0613%
ICMP Flood	icmp_f	23 256	0,0587%
HTTP Flood	http_f	22 959	0,0580%
Port Scan	tcp_udp_win_p	6 232	0,0157%
Reaper Worm	udp_reaper_w	1 176	0,0030%
Spam botnet	smtp_b	747	0,0019%
Fragmentation	udp_0	477	0,0012%

[1]Підраховується кількість записів перед видаленням позначки часу та відповідних дублікатів записів.

3.2 Розробка методу обрання набору ознак для навчання класифікаторів вторгнень

Сучасні IDS повинні відповідати вимогам і зростаючим потребам у вдосконаленні технологій. Для успішної роботи IDS необхідна високоефективна класифікація з використанням даних, які раніше не були відомі системі. IDS

зазвичай обробляють досить великий обсяг даних, які містять різні надлишкові ознаки, що призводить до низького рівня точності та тривалого часу обробки [82]. Це робить вибір ознак для класифікації важливим питанням. Для скорочення часу навчання моделі класифікації та підвищення рівня її точності важливим питанням є вибір найважливіших ознак із набору даних. У цьому дослідженні досліджувалися різні методи вибору ознак і ансамблю, щоб створити ефективну IDS з високою точністю розпізнавання загроз.

3.2.1 Загальна характеристика методів вибору ознак

У цьому підрозділі розглянуто основні концепції вибору ознак. Залежно від взаємодії з моделлю класифікації методи вибору ознак можна розділити на методи фільтрації, обгортки та вбудовані методи [152].

Відомі також гібридні та ансамблеві методи вибору ознак. Гібридний підхід поєднує два різних методи для використання переваг обох підходів, при цьому загальною комбінацією є методи фільтра і оболонки. Техніка ансамблю об'єднує ансамбль методів обрання ознак або підмножин даних та ознак, потім тим чи іншим способом формує загальний результат.

Методи типу фільтра вибирають ознаки, оцінюючи внутрішні властивості даних з урахуванням статистичних показників, не розглядаючи ефективності перехресної перевірки.

Їх легко масштабувати стосовно багатовимірних наборів даних незалежно від алгоритму навчання; вони відносно прості та швидкі у обчисленнях; і вони стійкі до перенавчання. У цих методах кожному об'єкту надається бал, який визначається обраним статистичним методом. Після цього всі ознаки ранжуються в порядку зменшення, а об'єкти з низькими оцінками видаляються з використанням порогового значення. Інші ознаки становлять підмножину ознак і потім вводяться у модель класифікації. Отже, вибір ознак проводиться один раз,

а потім можна використовувати різні класифікатори. Цей підхід має два основних недоліки: ознаки вибираються незалежно від класифікатора та ігноруються взаємозалежності ознак.

Деякі поширені статистичні показники, що використовуються в цьому методі, є приріст інформації (IG), кореляція Пірсона (PCC), хі-квадрат ($\chi 2$), взаємна інформація (MI) і симетрична невизначеність (SU).

У цій методології визначається стратегія пошуку можливих підмножин ознак і алгоритм класифікації навчається з використанням цих підмножин ітеративним способом. На відміну від методів фільтрації, методи-оболонки взаємодіють із класифікатором, проте оцінка підмножин ознак виходить із використання конкретної моделі класифікації, що робить такі методи специфічними для моделей.

Ці методи надають неоптимальні підмножини ознак для навчання моделей, оскільки оцінка всіх можливих підмножин недоцільна з обчислювальної точки зору.

Пошук для створення підмножин ознак може здійснюватися за допомогою таких схем, як прямий вибір, зворотний вибір, покроковий вибір або евристичний пошук. Спочатку додається ознака з найбільшим вкладом (найкращою оцінкою). Потім вибирається інша ознака, що забезпечує найкращу продуктивність (performance) разом із ознаками, які було додано раніше. Цей процес триває доти, доки включення нової ознаки не перестане покращувати продуктивність класифікатора. При зворотному виключенні алгоритм починається з усіх доступних ознак і відкидає рекурсивно найбільш незначні ознаки з моделі. Цей процес виключення повторюється доти, доки видалення ознак не перестане покращувати продуктивність моделі. Для покрокового вибору цей метод є комбінацією прямого вибору та зворотного виключення. Він починається з порожнього набору, і кожної ітерації додається найважливіша функція. При додаванні нової ознаки раніше вибрані ознаки видаляються, якщо якась із них

стала незначною. Евристичний пошук пов'язаний з оптимізацією та спрямований на оптимізацію цільової функції в оцінці різних підмножин [153].

Ці методи включають переваги методів фільтра і оболонки і одночасно виконують побудову набору ознак і моделі. Як і методи-оболонки, вони специфічні для моделі класифікації, але мають меншу обчислювальну складність, ніж методи-оболонки [152].

Ще один метод інтеграції алгоритму відбору ознак і створення моделі – це дерева рішень. Ці методи є непараметричними, в них об'єкти розглядаються як вузли. Деревоподібні стратегії, що використовуються випадковими лісами, накопичують різну кількість дерев рішень і ранжують вузли (тобто ознаки) щодо зменшення impurity (наприклад Gini impurity) по всіх деревах, наприклад, дереву класифікації та регресії (CART) [154].

Традиційні підходи вибору ознак мають низку недоліків. Наприклад, методи фільтрації оцінюють значущість кожної ознаки індивідуально, не зважаючи на відносини та взаємодії між ознаками. Методи-обгортки можуть забезпечити оптимальне підмножина ознак, але їх складність робить їх недосконалими. Вони не є кращими, особливо у комбінаторних методах, таких як ансамблеві методи. Крім того, вони не застосовуються до даних з невеликою кількістю вибірок через перенавчання. Вбудовані методи і оболонки, специфічні для моделі, тому можуть надавати інший підбір ознак для одного і того ж набору даних. Основним недоліком таких методів є їх нездатність ефективно видаляти надлишкові ознаки та ефективно зберігати інформативні ознаки [155, 156].

3.2.2 Попередня обробка даних

IDS має включати обробку даних, оскільки це початковий крок у спрощенні навчання моделі машинного навчання. Ефективна підготовка даних безпосередньо впливає на продуктивність моделі класифікації, і за допомогою

відповідних процедур можна вирішити технічні проблеми з попередньою обробкою даних і підвищити рівень продуктивності.

Попередня обробка даних передбачає наступні операції:

- виявлення/усунення невідповідностей, очищення даних;
- виправлення помилок в даних;
- масштабування та нормалізація.

Дані про вторгнення з відомих наборів даних та реальні дані трафіку в корпоративних мережах мають деякі особливості:

- в одній виборці зазвичай присутні ознаки різних типів – числові та категоріальні;
- для більшості аналізованих наборів даних розглядається як бінарна, так і багатокласова класифікація;
- кількість ознак варіюється від вибірки до вибірки;
- зв'язок відгуку та окремих ознак може бути як лінійним, так і нелінійним, або практично відсутнім.

Для систем виявлення вторгнень, які покладаються на статистичні ознаки, отримані з даних, нормалізація є важливим кроком у попередній обробці даних. Вхідні дані зазвичай повинні бути нормалізовані для методів, заснованих на машинному навчанні, щоб усунути зміщення, яке може виникнути внаслідок варіацій у величинах значень змінних. Якщо існує істотна різниця між найвищим і найнижчим значеннями даних, необхідна нормалізація. Нормалізуючи дані, нормалізується діапазон значень, що покращує продуктивність моделі. Найпоширеніший метод нормалізації, StandardScaler, коригує дані, щоб мати середнє значення 0 і стандартне відхилення 1. Трансформація неперервних і квазінеперервних ознак використовує стандартизацію. Зменшуючи середнє значення та масштабуючи дані до однієї дисперсії, він нормалізує дані.

Це можна позначити як $x_{sc} = \frac{x-\mu}{\sigma}$, де $\mathcal{X}_{sc}$ - нове згенероване значення, μ - середнє значення, а σ — стандартне відхилення, де $\sigma = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(x_i - \mu)^2}$.

3.2.3 Методи вибору ознак

Після попередньої обробки було виконано декілька спроб обрати найважливіші ознаки в наборі даних за допомогою відповідних алгоритмів. Час навчання та класифікації та інші показники класифікатора оцінювались разом із точністю результатів.

Для вибору ознак було використані декілька варіантів обрання ознак:

– чисто статистичні методи оцінки важливості ознак, розраховані на лінійний зв'язок ознак та класу відгуку (тест χ^2; F-classif; Correlation);
– метод з використанням оцінки важливості ознак за критерієм середнього зменшення помилок класифікації (mean decrease in impurity – MDI; для розрахунку важливості використовували ExnraTreeClassifier);
– метод оцінки важливості ознак на взаємної інформації (mutual information).

Кореляція є ефективним методом вимірювання залежності між змінними. Коефіцієнт кореляції Пірсона (Pearson Correlation Coefficient - PCC) є статистичним показником, який вимірює силу та напрямок лінійного зв'язку між двома випадковими величинами [157]. Для двох безперервних змінних *X* і *Y* PCC (*X*, *Y*) обчислюється за допомогою наступного рівняння:

$$PCC(X,Y) = \frac{\sum_i (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_i (x_i - \bar{x})^2 \sum_i (y_i - \bar{y})^2}} , \quad (3.1)$$

де $\bar{x}$ є середнім *X* , $\bar{y}$ є середнім *Y*.

Значення *PCC(X, Y)* нормалізується на інтервал між −1 та 1. Якщо значення дорівнює −1 або 1, це означає, що існує сильна кореляція між двома змінними, а коли воно дорівнює 0, це означає що дві змінні незалежні одна від одної.

Оскільки PCC не може виявити зв'язок між двома нелінійними залежними змінними, а його обчислення вимагає, щоб усі характеристики мали значення, дослідники запропонували інші методи вимірювання кореляції, такі як хі-квадрат, інформаційний приріст (information gain - IG) і взаємна інформація (mutual information - MI), які згадано нижче.

Тест χ^2 (хі-квадрат) — це перевірка статистичної гіпотези, яка вимірює відхилення від очікуваного розподілу, якщо припустити, що ознака фактично не залежить від значення класу [158, 159]. Чим вище значення хі-квадрат, тим релевантнішою є ознака щодо класу.

Її розрахунок здійснюється за загальновідомою формулою:

$$\chi^2 = \sum_{i=1}^{n_I} \sum_{j=1}^{n_c} \frac{\left[A_{ij} - \frac{R_i B_j}{N}\right]^2}{\frac{R_i B_j}{N}} , \qquad (3.2)$$

де n_I – кількість інтервалів, n_c – кількість класів, N – загальна кількість екземплярів, A_{ij} кількість випадків в інтервалі i і класі j, R_i позначає кількість екземплярів в інтервалі i, а B_j кількість екземплярів у класі j.

Основна ідея тесту χ^2 полягає в тому, щоб визначити, чи є теорія правильною чи ні, спостерігаючи за відхиленням між фактичним значенням і теоретичним значенням. Зокрема, часто припускають, що дві змінні незалежні одна від одної (нульова гіпотеза), а потім спостерігають відхилення між фактичним значенням і теоретичним значенням (теоретичне значення відноситься до «значення, яке повинні мати дві змінні, якщо вони дійсно незалежні один від одного») ступінь. Якщо відхилення досить мале, ми

приймаємо нульову гіпотезу. Якщо відхилення досягає певного рівня, ми вважаємо, що таке відхилення навряд чи спричинене випадковістю чи неточністю, тобто дві змінні фактично корелюють, що означає, що нульова гіпотеза відхиляється та вибирається альтернативна гіпотеза.

Під час вибору ознак нам потрібно лише виконати тест хі-квадрат між кожною ознакою та кожною категорією, а потім відсортувати результати в порядку спадання. Нарешті, до результуючої вибірки входять кілька функцій з відносно великими значеннями хі-квадрат.

Тест χ^2 має деякі недоліки. Він підраховує, чи існує певна функція в екземплярі певної категорії, але не враховує, скільки разів функція з'являється в екземплярі. Це зробить його упередженим до низькочастотних слів. Тому тест хі-квадрат зазвичай потрібно поєднувати з іншими методами розрахунку (такими як IG), щоб максимізувати сильні сторони та уникнути слабких сторін.

Дисперсійний аналіз (ANOVA) — це техніка статистичного аналізу, яка використовується для порівняння середніх значень кількох груп, щоб визначити, чи існує значна різниця між ними. Подібно до підходу хі-квадрат, перед його використанням необхідна дискретизація. Ключова ідея дисперсійного аналізу полягає в тому, щоб порівняти загальну дисперсію даних із варіацією всередині груп і варіацією між групами.

Внутрішньогрупова сума квадратів (SSW) вимірює варіацію в межах груп. Визначається як:

$$SSW = \sum_{i=1}^{k}[(n_i - 1) \cdot SS(i)], \tag{3.3}$$

де n_i – це кількість екземплярів у групі i, а $SS(i)$ – це дисперсія групи i.

Сума квадратів між групами (SSB) [63] вимірює варіацію між середніми значеннями груп. Визначається як:

$$SSB = K \cdot \sum (\bar{x}_i - \bar{\bar{x}})^2,$$

де K – кількість груп, $\bar{x}_i$ є середнім для групи i, а $\bar{\bar{x}}$ є середнім для всіх випадків.

Загальна сума квадратів (SST) становить:

$$SST = SSW + SSB. \tag{3.4}$$

Нульова гіпотеза ANOVA полягає в тому, що всі групи мають однакове середнє, тобто значення досліджуваної ознаки не впливають на кінцевий клас. Альтернативна гіпотеза полягає в тому, що принаймні одна група має інше середнє значення. Нульова гіпотеза перевіряється за допомогою F-відношення, яке є відношенням SSB до SSW. F-відношення вище порогового значення (так зване критичне F-значення) вказує на те, що існує значна різниця між середніми значеннями груп, і тому нульову гіпотезу можна відхилити:

$$F = \frac{SSB}{SSW}. \tag{3.5}$$

Критичне значення F – це значення F-розподілу, яке визначається ступенями свободи для чисельника ($df_{SSB} = K - 1$ та ступенями свободи для знаменника ($df_{SSW} = N - K$). Тут N — кількість екземплярів.

Ентропія описує невизначеність випадкової величини. Приріст інформації вказує на ступінь зменшення невизначеності випадкової величини за певних умов. Рівняння (3.6) визначає ентропію змінної X, а рівняння (3.7) визначає умовну ентропію X з огляду на відкриття Y:

$$H(X) = -\sum_{x \in X} p(x) log_2\big(p(x)\big), \tag{3.6}$$

$$H(X|Y) = -\sum_{y \in Y} p(y) \sum_{x \in X} p(x|y) log_2\big(p(x|y)\big) . \tag{3.7}$$

Поєднуючи рівняння (3.6) і (3.7), ми отримуємо рівняння для отримання інформації [160]:

$$IG(X, Y) = H(X) - H(X|Y) = H(Y) - H(Y|X) . \quad (3.8)$$

Рівняння (3.8) є симетричним, тому результат не залежить від порядку випадкових величин.

Найважливіші ознаки забезпечують найбільший зріст інформації. Оскільки цей метод використовує алгоритм дерева рішень, він також повинен належати до вбудованого методу. Його поточне обмеження полягає в тому, що потрібно покращити точність деяких другорядних класів.

Збільшення інформації – це популярний підхід до вибору ознак, який передбачає визначення найбільш відповідних функцій у наборі даних, які можуть допомогти зробити точні прогнози. Ось кроки для обробки вибору функції за допомогою отримання інформації:

1. Обчислити інформаційний приріст для кожної ознаки: інформаційний приріст вимірює зменшення ентропії (тобто невизначеності), яке є результатом поділу даних на основі певної ознаки. Ознаки з вищим приростом інформації більш корисні для прогнозування. Їх треба ранжувати на основі їх інформаційного приросту: після того, як було обчислено інформаційний приріст для кожної ознаки, можна розташувати їх у порядку спадання на основі їхніх інформаційних значень. Ознаки з найбільшим приростом інформації є найбільш релевантними і повинні бути обрані для моделі.
2. Обрати перші N ознак: залежно від розміру та складності набору даних, можливо, слід вибрати лише перші N ознак із найбільшим приростом інформації. Це допоможе зменшити розмірність даних і підвищити ефективність моделі.

3. Навчити моделі з вибраним набором ознак: якщо визначено основні функції за допомогою отримання інформації, навчити потрібну модель можна, використовуючи лише ці ознаки. Це допоможе підвищити точність і можливість інтерпретації моделі. Загалом використання отримання інформації для вибору ознак може допомогти покращити продуктивність і ефективність моделей машинного навчання шляхом зменшення розмірності ваших даних і визначення найбільш релевантних функцій.

Взаємна інформація [161] є мірою взаємозалежності між двома змінними, визначеними як рівняння (3.9) для безперервних випадкових змінних і рівняння (3.10) для дискретних випадкових змінних.

Видно, що MI та IG мають схожі вирази:

$$I(X,Y) = H(X) - H(X|Y), \tag{3.9}$$

$$I(X,Y) = \sum_{y \in Y} \sum_{x \in X} p(x,y) log \frac{p(x,y)}{p(x)p(y)}. \tag{3.10}$$

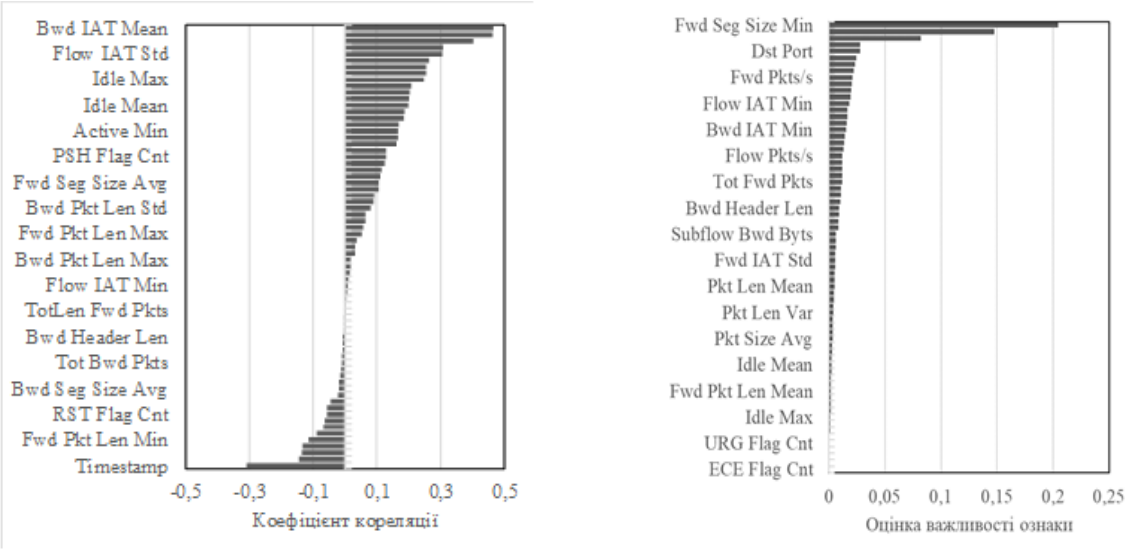
Взаємна інформація між ознакою-кандидатом X_k і міткою класу Y виражається як $I(X_k, Y)$, тоді як умовна взаємна інформація між X_k та іншими ознаками X_j у вибраному наборі S із міткою класу Y виражається через $I(Xj , X_k|Y)$.

Взаємна інформація може бути використана для вимірювання кореляції між ознаками та категоріями та видалення цих нерелевантних ознак. Однак обчислення взаємної інформації є витратною операцією, тому для даних великої розмірності її використання обмежено.

3.2.4 Дослідження методів відбору результативного набору ознак

Алгоритми, засновані на ідеї дерева, є досить успішними при проведенні класифікації різних вибірок, які використовуються для побудови класифікаторів IDS. Досить точний і швидкий результат отримано також з використанням алгоритму k найближчих сусідів (див. підрозділ 3.3).

Критерії для обрання набору ознак надають досить неоднозначні результати (див. рис. 3.2).



а) Кореляційна діаграма наявності атаки і ознак набору даних CSE-CIC-IDS2018

б) Діаграма MDI для ознак набору даних CSE-CIC-IDS2018

Рис. 3.2. Варіанти критеріїв обрання ознак для набору даних CSE-CIC-IDS2018

Відомі методи обрання ознак, які використовуються по одному, нерідко дають різні результуючі набори даних. Приклад обчислення кореляції ознак

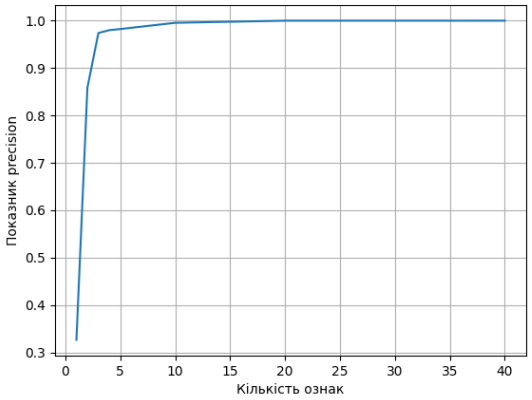
набору даних CSE-CIC-IDS2018 і наявності атаки наведено на рис. 3.2а.

Після аналізу поведінки компонентів пропонованої системи було додано ще один варіант обрання ознак, більш адекватний саме для класифікаторів на основі дерев: вибір ознак за критерієм середнього зменшення помилок класифікації (mean decrease in impurity - MDI).

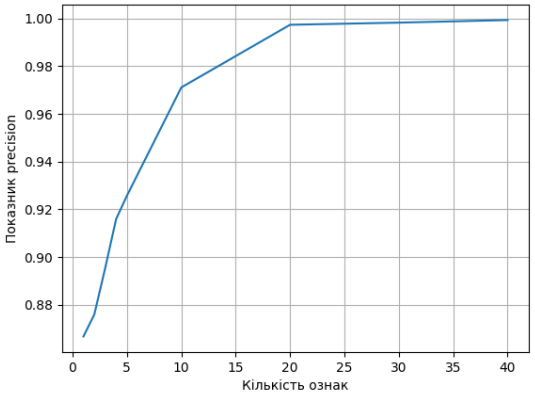
Приклад обчислення вибору ознак за критерієм середнього зменшення помилок класифікації для набору даних CSE-CIC-IDS2018 наведено на рис. 3.2б.

Як видно з наведених діаграм, кількість ознак у результуючому наборі даних для навчання класифікатора залежить від критерію вибору цих ознак. Те ж саме питання виникає й для обрання ознак за допомогою тестів χ^2 або fuzzy logic[2]. При цьому точність класифікації за таким зменшеним набором не змінюється, але пояснення, чому саме такий набор даних дає можливість відслідкувати вторгнення, метод обрання ознак не надає.

Приклад змінення точності класифікації даних KDD99 та NSL-KDD в залежності від кількості ознак, які включено в модель, наведено на рис. 3.3 (для побудови цих рисунків відбір ознак було здійснено за критерієм f_classif).



а) набір даних KDD99



б) набор даних NSL-KDD

Рис. 3.3. Зростання точності класифікації моделі в залежності від частки кількості використаних ознак

Кількість ознак, які забезпечують досить високу точність класифікації, складає 25-50% вихідного набору даних. Показники точності та час навчання трьох класифікаторів (ExtraTreeClassifier – ETC; DesignTreeClassifier – DTC; K nearest neibours – KNN) з використанням оригінальних наборів даних або наборів даних зі скороченою кількістю ознак наведені в таблиці 3.12.

Таблиця 3.12

Порівняння точності і часу навчання моделі на наборах даних з різною кількістю ознак (вихідний набор даних KDDCup99)

Параметр	Класифікатор		
	KNN	DTC	ETC
Точність, %			
41 ознака (вихідний)	99,9	100	100
21 ознака	99,9	100	100
Час навчання, с			
41 ознака (вихідний)	0,0945	1,836	0,214
21 ознака	0,0628	1,225	0,177

У цій таблиці представлені дані KDDCup99, хоча аналогічні результати були отримані й для інших наборів даних – LITNET, ISD2018.

Як видно з таблиці 3.12, скорочення кількості ознак помітно зменшує час навчання моделі, але не впливає на точність моделі. Для зменшення точності моделі скорочення кількості ознак повинно бути значним (див. рис. 3.3).

Але якщо слідкувати за переліком ознак, які були обрані за важливістю, то перелік обраних ознак залежить від метода оцінки. Приклад послідовності включення ознак в результуючий набір з використанням трьох критеріїв наведено в таблиці 3.13. Для побудови таблиці 3.13 було використано три критерії важливості ознак: критерій F-значення ANOVA (f_classif), критерій середнього зменшення помилок класифікації (mean decrease in impurity - MDI), критерій взаємної інформації (mutual_info_classif). Критерії взаємної інформації або важливості перестановки (permutation importance) розраховуються досить

повільно, тому для обрання ознак за запропонованим підходом не використовувались [1].

Таблиця 3.13

Результати обрання ознак за важливістю з використанням різних критеріїв (набір даних KDD99)

Кіль-кість ознак	Критерій f_classif	Критерій MDI	Критерій mutual_info_classif
1	['wrong_fragment']	['count']	['count']
2	['wrong_fragment' 'srv_count']	['count' 'same_srv_rate']	['src_bytes' , 'count']
3	['wrong_fragment' 'srv_count' 'same_srv_rate']	['service' 'serror_rate' 'dst_host_same_srv_rate']	['service' , 'src_bytes' , 'count']
4	['wrong_fragment' 'count' 'srv_count' 'same_srv_rate']	['srv_serror_rate' 'dst_host_count' 'dst_host_srv_count' 'dst_host_same_src_port_rate']	['service' , 'src_bytes' , 'count', 'dst_host_same_src_port_rate']
5	['protocol_type' 'wrong_fragment' 'count' 'srv_count' 'same_srv_rate']	['protocol_type' 'srv_serror_rate' 'diff_srv_rate' 'dst_host_srv_count' 'dst_host_srv_rerror_rate']	['service' , 'src_bytes' 'count', 'srv_count', 'dst_host_same_src_port_rate']

Таким чином, досить складно з’ясувати, якщо використовувати відомі алгоритми обрання ознак, який саме набір ознак забезпечить досить високу точність класифікації спостережень, й буде досить швидко виконувати навчання моделі і класифікацію даних [1,2,8].

3.2.5 Пропонований метод нечіткого обрання важливих ознак

Припустимо, що набір даних, для якого необхідно побудувати оцінку важливості ознак, містить M ознак. Усі ознаки перетворюються на числові та

нормалізуються.

Для оцінки важливості ознак використовуємо N методів, кожен з яких надає оцінку важливості ознаки j $(j \in 1 \dots M)$ з використанням метода i $(i \in 1 \dots N)$, яка дорівнює f_j^i.

Введемо універсальну множину U з переліком граничних значень рівня важливості ознаки від 0 до 1 (наприклад, важливість ознаки j при оцінці методом i висока, якщо $f_j^i > 0.8$). Лінгвістична змінна буде мати 3 (низька, помірна і висока важливість, як в роботах [56, 58]) або 5 термів (важливість висока, достатньо висока, середня, достатньо низька, низька).

Для результуючої оцінки важливості ознак за усіма методами було використовується алгоритм Мамдані [83]. У кінцевий набір даних включаються ознаки, важливість яких на рівні висока та досить висока. Для підвищення надійності і узагальнення методу оцінка важливості ознак може виконуватись для вибірок із початкового набору даних із подальшим обчисленням середнього результату або за допомогою алгоритму голосування.

Запропонований гібридний метод вибору ознак було реалізовано за наступним алгоритмом:

Крок 1. Видалення постійних ознак, які відображають однакове значення (одне для всіх спостережень набору даних). Ця ознака не надає інформації, яка б дозволила моделям машинного навчання розрізняти або передбачати цілі. Видалення постійних ознак здійснюється шляхом видалення ознак з нульовою дисперсією або видалення ознак, які мають стандартне відхилення 0 [162].

Крок 2. Видалення квазіконстантних ознак, які відображають однакове значення для більшості спостережень набору даних. Загалом такі ознаки надають дуже мало інформації, яка дозволяє моделям машинного навчання розрізняти або прогнозувати цілі. Видалення квазіконстантних ознак здійснюється шляхом видалення ознак з низькою дисперсією або видалення функцій (наприклад, які мають VarianceThreshold 0,01) [162].

Крок 3, Розрахунок декількох критеріїв вибору ознак з різних груп (група статистичних критеріїв - тест χ^2, F-classif, Correlation; оцінки важливості ознак за критерієм середнього зменшення помилок класифікації - MDI; в деяких випадках метод оцінки важливості ознак на взаємної інформації). У таблиці 3.14 наведено інтерпретацію абсолютних величин коефіцієнту кореляції або важливості ознак, які можна використовувати як межи універсальної множини.

Таблиця 3.14

Приклад створення універсальної множини за значеннями коефіцієнта кореляції та рівня важливості ознак

Абсолютна величина	Інтерпретація коефіцієнту кореляції	Інтерпретація важливості ознаки за критерієм MDI
0.00-0.10	Незначна кореляція	Неважлива ознака
0.10-0.39	Низька кореляція	Слабка важливість
0.40-0.69	Середня кореляція	Середня важливість
0.70-0.89	Висока кореляція	Важлива ознака
0.90-1.00	Дуже висока кореляція	Дуже важлива ознака

Крок 4. Для результуючої оцінки важливості ознак за усіма методами було використано алгоритм Мамдані [83]. У кінцевий набір даних включаються ознаки, важливість яких на рівні висока та досить висока.

Приклад реалізації розглянутого алгоритму наведено в таблиці 3.15. Розрахунки виконано для набору даних CSE-CIC-IDS2018, оцінки важливості ознак виконувалась за допомогою різних класифікаторів.

Таблиця 3.15

Результати обрання ознак для кількох алгоритмів класифікатора

Алгоритм класифікації	Вибрані ознаки (ознаки, які залишилися)
Random Forest	flow_duration, totlen_fwd_pkts, fwd_pkt_len_mean, flow_byts_s, flow_pkts_s, flow_iat_min, fwd_iat_tot, fwd_iat_min, bwd_pkts_s, init_fwd_win_byts, init_bwd_win_byts, fwd_seg_size_min
Extra Trees	
Decision Tree	

Декілька варіантів результатів класифікації в залежності від меж групи важливих ознак (обирати лише дуже важливі і з дуже високою кореляцією, або важливі теж) наведено в таблицях 3.16 (бінарна класифікація) і 3.17 (багатокласова класифікація). В обох випадках було використано ExtraTreeClassifier.

Як можна побачити з наведених таблиць, запропонований алгоритм забезпечує стабільність обрання набору ознак, досить високу точність навчання моделі зі скороченою кількістю ознак. Зменшення розмірності простору ознак забезпечує й прискорення навчання та класифікації спостережень (див. нижче).

Таблиця 3.16

Оцінка ефективності двокласової моделі класифікації

Selected features subset	Accuracy	Precision	Recall	F1-Score
12 features*	0.989	0.989	0.989	0.989
9 features (проміжний вариант)	0.988	0,988	0.988	0.988
7 features **	0.987	0.987	0.987	0.987

* жорсткий варіант відбору ознак (лише дуже важливі ознаки і ознаки з дуже високою кореляцією)

** помірний варіант - важливі і дуже важливі ознаки та ознаки з високою кореляцією і дуже високою кореляцією.

Таблиця 3.17

Оцінка ефективності багатокласової моделі класифікації (ExtraTreeClassifier)

Selected features subset	Accuracy	Precision	Recall	F1-Score
12 features*	0.983	0.977	0.983	0.979
9 features (проміжний вариант)	0.982	0.977	0.982	0.979
7 features **	0.981	0.977	0.981	0.978

* жорсткий варіант відбору ознак (лише дуже важливі ознаки і ознаки з дуже високою кореляцією)

** помірний варіант - важливі і дуже важливі ознаки та ознаки з високою кореляцією і дуже високою кореляцією.

3.3 Розробка гібридного методу ідентифікації вторгнень на основі ансамблевого навчання та алгоритмів нечіткої логіки

3.3.1 Порівняння варіантів класифікаторів для моделі ідентифікації вторгнень

Системи виявлення вторгнень зосереджуються на виявленні поведінки для обробки аномалій або атак. Вона розпізнає будь-який порушений мережевий трафік за цим шаблоном, який може призвести до атаки на інфраструктуру. Раціональний підхід полягає в тому, щоб навчати систему на цьому шаблоні поведінки за допомогою кількох методів. Для комбінування різних методів класифікації та прогнозу в системах виявлення вторгнень досить широко використовують алгоритми ансамблевого навчання.

Метод ансамблевого навчання – це спосіб перегляду всіх методів навчання та алгоритмів одночасно, а не розгортання їх окремо [66]. Останнім часом методи ансамблевого навчання використовувались для вирішення кількох складних проблем. Ансамблеве навчання покладається на набір комбінованих класифікаторів або предикторів замість окремих класифікаторів, тому ці набори класифікаторів навчаються та вивчаються на основі проведених шаблонів для вирішення тієї самої проблеми та отримання кращих результатів [67].

Існують чотири різні типи технік ансамблевого навчання, як-от bagging, boosting, stacking, voting. Під час голосування потужність кількох окремих класифікаторів полегшує застосування правила комбінування для прийняття рішень.

Кожен алгоритм машинного навчання має різні обмеження, як-от низьке зміщення та незначна дисперсія. Ансамблеве навчання розглядає обмеження автономних методів машинного навчання. Парадигма такого навчання об’єднує різноманітні моделі (слабкі учні) для створення однієї оптимальної прогнозної

моделі, яка дає більш точні результати, ніж одна модель [67]. Прогнози, зроблені кожною моделлю в складі ансамблю (базовим учнем), поєднуються за допомогою голосування або усереднення.

Ансамблеве навчання поділяється на два основні типи: гомогенне або гетерогенне. Однорідний тип ансамблевого навчання передбачає використання різних підмножин даних для навчання базових класифікаторів (слабких учнів). Результат кожного класифікатора агрегується для підвищення точності. Цей тип ансамблевого навчання підходить для великих наборів даних. Bagging і boosting є найпоширенішими типами однорідного ансамблевого навчання. Класифікатор Bagging – це ансамблевий мета-оцінювач, який встановлює кожен базовий класифікатор у випадкових підмножинах вихідного набору даних, а потім агрегує їхні індивідуальні прогнози (чи шляхом голосування, чи шляхом усереднення), щоб сформувати остаточний прогноз [68]. Таку метаоцінку зазвичай можна використовувати як спосіб зменшити дисперсію оцінки чорної скриньки (наприклад, дерева рішень), вводячи рандомізацію в процедуру її побудови, а потім створюючи з неї ансамбль.

У гетерогенних моделях ансамблевого навчання різні базові класифікатори використовуються для навчання на однакових даних. Ця техніка добре працює для невеликих наборів даних. Прикладом гетерогенної моделях ансамблевого навчання є stacking.

VotingClassifier базується на ідеї поєднання концептуально різні класифікаторів машинного навчання та використання більшості голосів або середніх прогнозованих ймовірностей (м’яке голосування) для прогнозування міток класу. Такий класифікатор може бути корисним для набору однаково ефективних моделей, щоб збалансувати їх окремі слабкі сторони [69].

Для організації ансамблевого навчання в цій роботі було використано декілька алгоритмів, які забезпечили найкращі результати.

Класифікація на основі найближчих сусідів — це тип навчання на основі екземплярів або неузагальнюючого навчання: воно не намагається побудувати загальну внутрішню модель, а просто зберігає екземпляри навчальних даних. Класифікація обчислюється простою більшістю голосів найближчих сусідів кожної точки: точці запиту призначається клас даних, який має найбільше представників у найближчих сусідах точки [70].

Класифікація k-сусідів у KNeighborsClassifier є найпоширенішим методом. Оптимальний вибір значення k сильно залежить від даних: загалом більше пригнічує вплив шуму, але робить межі класифікації менш чіткими.

DT є одним із найбільш широко використовуваних для класифікації та виявлення вторгнень. DT складається з трьох основних компонентів, а саме вузла рішення (ідентифікує тестовий атрибут), гілки (можливий вибір на основі значення тестового атрибута) і кінцевого вузла (класу, членом якого є екземпляр). Спочатку вивчається та моделюється набір даних, а потім у алгоритмі DT формується дерево. Коли тестові дані надаються DT, вони будуть класифіковані на основі процедури класифікації попереднього набору даних. Виконується перевірка для класифікації з використанням значення тестового атрибута та процедури прийняття рішення (позначеної кореневим вузлом). Клас (звичайний, атакуючий) призначається тестовим даним, коли досягається кінцевий вузол. DT краще працює для великих наборів даних [71]. DT має такі переваги, як краща продуктивність виявлення, точність узагальнення тощо.

RF або ліси випадкових рішень є методом ансамблевого навчання, у якому будується значна кількість декорельованих дерев, а потім усереднюється [72]. RF генерує ліс дерева рішень із довільно розділеного набору даних на вибірки. Для кожного атрибута створюється окреме дерево рішень залежно від незалежної випадкової вибірки. Для класифікації тестових даних отримують прогнози з кожного дерева, і, нарешті, клас призначається тестовим даним за допомогою більшості голосів або техніки усереднення.

Extra Tree — це набір моделей на основі ML, які поєднують класифікації з кількох невідрізаних DT на різних підвибірках цілі, щоб підвищити точність узагальнення, бути обчислювально ефективними та запобігти надмірній підгонці [73]. Весь навчальний екземпляр використовується для вирощування дерев, і вузли в кожному дереві розділяються шляхом абсолютного випадкового вибору точок розрізу. Ці прогнози зроблені за допомогою схеми голосування більшості для завдань класифікації або усереднення значень прогнозу для завдань регресії.

3.3.2 Розробка структури модуля оцінювання системи виявлення вторгнень

Сучасні IDS повинні відповідати вимогам і зростаючим потребам у вдосконаленні технологій. Для успішної роботи IDS необхідна високоефективна класифікація з використанням даних, які раніше не були відомі системі. IDS зазвичай обробляють досить великий обсяг даних, які містять різні надлишкові ознаки, що призводить до низького рівня точності та тривалого часу обробки [81]. Це робить вибір ознак для класифікації важливим питанням. Для скорочення часу навчання моделі класифікації та підвищення рівня її точності важливим питанням є вибір найважливіших ознак із набору даних [82]. У цьому дослідженні досліджувалися різні методи вибору ознак і ансамблю, щоб створити ефективну IDS з високою точністю розпізнавання загроз. На рис. 3.4 показана структура модуля оцінювання з вибором ознак та ансамблевим класифікатором.

Після попередньої обробки були обрані найважливіші ознаки в наборі даних за допомогою запропонованого підходу (див. вище). Час навчання та класифікації та інші показники класифікатора оцінювались разом із точністю результатів.

- В якості метакласифікатора використовувались декілька варіантів:
- алгоритм RandomForest;

– алгоритм VotingClassifier;

– алгоритм нечіткого обрання результатів оцінювання;

– алгоритм StackingClassifier.

Для уточнення класифікації використовувались варіанти:

– нечіткий класифікатор FuzzyKNN;

– алгоритм BaggingClassifier з використанням генерування випадкових наборів даних.

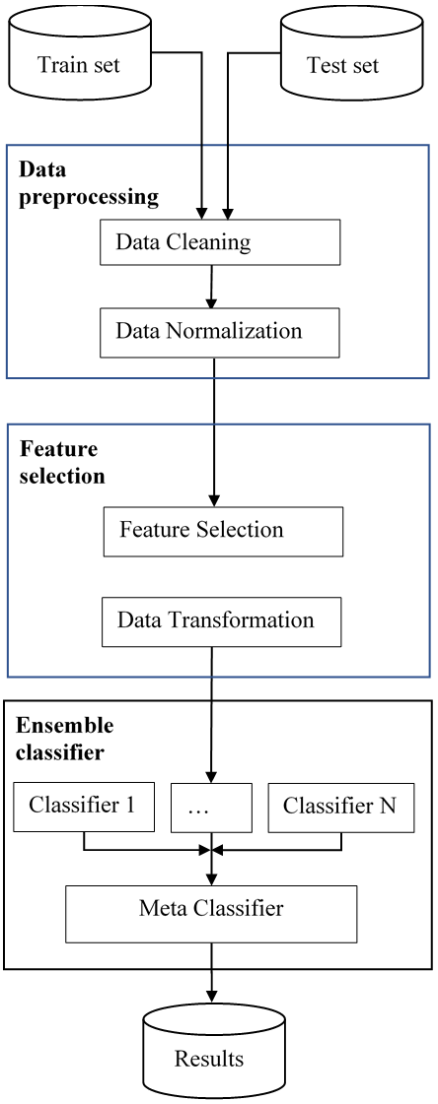


Рис. 3.4. Структура модуля оцінювання з вибором ознак та ансамблевим класифікатором

Основні результати роботи одиничних класифікаторів наведені в таблиці 3.18. Позначки в таблиці: KNN – класифікатор KNeibourClassifier (метод найближчих сусідів); DTC – класифікатор DecignTreeClassifier; ETC – класифікатор ExtraTreeClassifier; RFC- класифікатор RandomForestClassifier; MLP – класифікатор MLPClassifier (багатошаровий персептрон); ADA - класифікатор ADABoost; LR – логістична регресія.

Таблиця 3.18

Результати без недостатньої вибірки та вибору ознак (IDS2018)

Класифікатор	Точність, %	Показник F1	Час навчання, с
KNN	99.99	0,999	0.0945
DTC	100,00	1.00	1,836
ETC	100,00	1.00	0,214
RFC	100,00	1.00	22,01
MLP	99.5	0,995	206,67
ADA	68,0	0,716	37,48
LR	94,9	0,952	54,31

Результати показують, що алгоритми, засновані на дереві, є досить успішними при проведенні класифікації різних вибірок, які було використано для побудови класифікатора IDS. Оскільки метою дослідження є розробка ансамблевої моделі з набором даних, вибраних за ознаками, на наступному кроці всі алгоритми були використані з набором даних, після застосування RFE або MDI. Приклад результатів наведено в таблиці 3.19.

Таблиця 3.19

Результати для набору даних зі скороченою кількістю ознак

Класифікатор	Точність,%	Показник F1	Час навчання, с
KNN	99.99	0,999	0,0628
DTC	100,00	1.00	1,225
ETC	100,00	1.00	0,177
RFC	100,00	1.00	28,38
MLP	99.6	0,995	202,15
ABC	94,2	0,940	44,81
LR	93,4	0,936	61,95

Алгоритми LogisticRegression, AdaBoost, MultiLayerPerceptron довго навчаються і для досягнення високих показників точності потрібують налагодження. Коли час прогнозування та рівень точності оцінюються разом, було знайдено, що алгоритми дерева рішень (DTC), найближчих сусідів (KNN) та додаткових дерев (ETC) дають результати з високою точністю та швидким часом прогнозування. Тому ці три алгоритми були обрані для моделі ансамблю [1,2,8].

3.3.3 Дослідження деяких ансамблевих класифікаторів

Питання вибору найкращого класифікатора для роботи системи виявлення вторгнень можна вирішити за допомогою ансамблевого навчання.

Для обрання найзручнішої технології було виконано дослідження впливу варіанта побудови ансамблевої моделі на час її навчання і можливості підвищення точності класифікації.

Якість відповідей класифікаторів (моделей) порівнювалося з використанням наступних метрик:

- частка правильних відповідей (accuracy);
- точність (precision, наскільки можна, можливо довіряти класифікатору);
- повнота (recall, як багато об'єктів класу «є атака» визначає класифікатор);
- F1-міра (F1-measure, гармонійне середня між точністю та повнотою).

При визначенні значень метрик якості використовуються елементи матриці помилок (confusion matrix), відповідні кількості правильних та неправильних відповідей за результатами тестування класифікатора (табл. 3.20).

Таблиця 3.20

Опис матриці помилок класифікатора

Відповіді	Відповідь класифікатора: клас 0, «ні атаки»	Відповідь класифікатора: клас 1, « є атака»
Правильна відповідь: клас 0, «немає атаки»	TN	FP
Правильна відповідь: клас 1, « є атака»	FN	TP

Позначення в таблиці 3.20:

- TP (True Positive) позначає істинно-позитивна відповідь,
- TN (True Negative) - істинно негативна відповідь,
- FP (False Positive) - хибно-позитивна відповідь (хибне спрацювання, помилка першого роду),
- FN (False Negative) - помилково-негативна відповідь (перепустка атаки, помилка другого роду).

З урахуванням наведених позначень використовувані метрики якості визначаються наступними виразами:

$$Accuracy = \frac{TP + TN}{TP + FP + FN + TN}; \tag{3.11}$$

$$Precision = \frac{TP}{TP + FP}; \tag{3.12}$$

$$Recall = \frac{TP}{TP + FN}; \tag{3.13}$$

$$F1 = \frac{2 \cdot Precision \cdot Recall}{Precisiom + Recall}; \tag{3.14}$$

Деяке підвищення точності оцінювання було досягнуто за рахунок використання стандартних варіантів метакласифікаторів (VotingClassifier, StackingClassifier, RandomForestClassifier). Було побудовано декілька моделей з використанням різних алгоритмів класифікації, які навчались на підмножинах зі зменшеною кількістю ознак, або на наборах даних вихідного розміру.

При відповідному налаштуванні точність класифікації за рахунок використання ансамблевого підходу трохи збільшується, але обрання Stacking або Bagging класифікаторів як основи навчання моделі для усіх наборів даних збільшує час навчання більш ніж на порядок (в залежності від базових класифікаторів або кількості підмножин даних). При збільшенні кількості спостережень в наборі даних для навчання ефект зростання часу навчання стає більш помітним.

Тому при подальшій роботі вибір результатів класифікації встановлювався переважно за допомогою алгоритму VotingClassifier. Його ідея полягає в тому, щоб поєднати концептуально різні класифікатори машинного навчання та використовувати більшість голосів або середні передбачені ймовірності (м’яке голосування) для прогнозування міток класу. Такий класифікатор може бути корисним для набору однаково ефективних моделей, щоб збалансувати їх окремі слабкі сторони.

Але при підрахунку кінцевого результату голосування виникає проблема обгрунтованості простого голосування. Перспективним рішенням буде використання нечіткої логіки для узагальнення результатів, отриманих за допомогою різних класифікаторів.

3.3.4 Алгоритм нечіткого голосування

Розглянемо роботу класифікатора голосування (VotingClassifier, soft mode). Припустимо, що набір, для якого необхідно побудувати оцінку результату, містить

M класифікаторів. Для кожного з окремих класифікаторів отримаємо імовірність належності спостереження до усіх класів. Припустимо, що є N класів.

Розглянемо об'єкт $\boldsymbol{x}$ (спостереження), нехай $d_{i,j}(x) \in [0,1]$ є ступенем належності, який класифікатор i $(i \in 1 \dots M)$ пропонує для класу j $(j \in 1 \dots N)$.

Введемо універсальну множину U з переліком граничних значень рівня належності спостереження до якогось класу від 0 до 1. Лінгвістична змінна може містити 3 (низька, помірна і висока імовірність), або 5 термів (імовірність висока, достатньо висока, середня, достатньо низька, низька).

У системах із декількома класифікаторами (ансамблях класифікаторів) рішення кількох класифікаторів агрегуються для отримання однієї (чіткої або м'якої) мітки класу [163, 164].

Матриця $\{d_{i,j}(x)\}$ має назву **профіль рішення** для **x**.

Нечіткі функції агрегації (правила агрегації) базуються на нечіткому прийнятті рішень. Загальна підтримка для класу j розраховується з використанням матриці профілю рішень для цього класу, який є j - м стовпцем матриці. Враховуючи функцію агрегування A, результат м'якого ансамблю для класу j є [163,164]:

$$d_{e,j}(x) = A\left(d_{1,j}(x), d_{2,j}(x), \dots , \qquad d_{M,j}(x)\right) \tag{3.15}$$

Найчастіше в якості функції агрегації використовують мінімум, максимум або середнє значення. Враховуючи ціль дослідження, в якості агрегуючої функції було використано найбільше значення (максимум).

3.3.5 Дослідження швидкості і точності класифікаторів для системи виявлення вторгнень

Показники точності та час роботи цих алгоритмів у результаті роботи з оригінальними наборами даних і наборами даних зі скороченою кількістю ознак наведені вище в таблиці 3.12. Результати навчання і використання моделі ансамблю наведено в таблиці 3.20.

Таблиця 3.20

Результати дослідження ансамблевих класифікаторів

Набір даних	Кількість ознак	Класифікатор	Точність, %	Час навчання, с
KDDCup99	41	RF	99,55	22,55
	41	RF	100,0	12,57
	20	Voting	99,34	2.26
	20	Fuzzy	99,14	2,36
NSL-KDD	41	RF	99,99	9,53
	16	RF	100,0	9,18
	16	Voting	99,34	1,31
	16	Fuzzy	99,14	1,43
UNSW-NB15 (скорочений набір)	44	RF	99,99	17,66
	21	RF	99,99	12,40
	21	Voting	99,34	2,01
	21	Fuzzy	99,33	2,22
IDS 2018 (одна доба)	79	RF	99,99	172.1
	21	RF	99,99	121,4
	21	Voting	99,99	8,51
	21	Fuzzy	99,99	9,02

Як видно з цієї таблиці, точність класифікації при навчанні моделі на наборі даних лише з важливими ознаками практично не знижується.

Вплив кількості ознак, на час навчання класифікаторів і ансамбля VotingClassifier в цілому наведено на рис. 3.5.

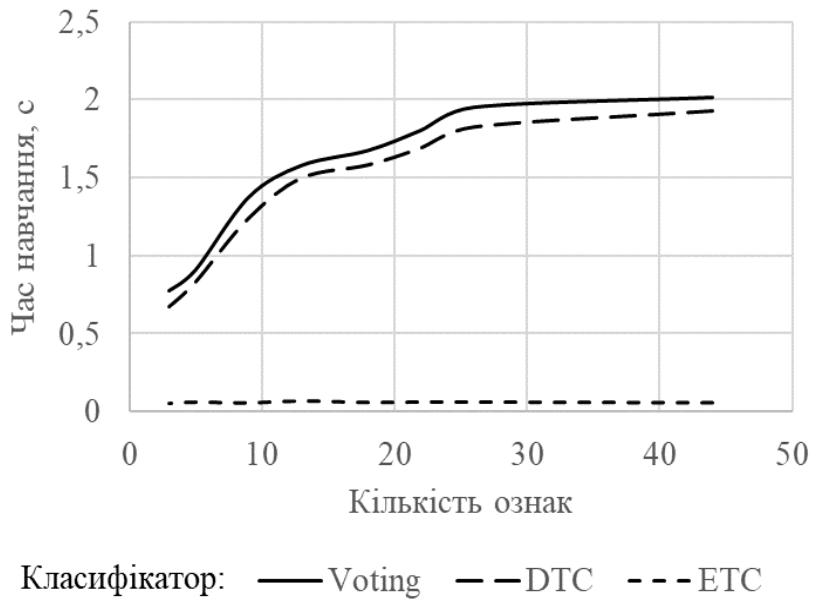


Рис. 3.5. Залежність часу навчання деяких класифікаторів ансамблю від кількості ознак (навчання на частині набору даних UNSW-NB15)

Час навчання Voting-класифікатора залежить від базових класифікаторів, які використано для його побудови. Наприклад, якщо для побудови вотуючого класифікатора користуватись RandomForestClassifier (та ще два інші) і порівнювати швидкість навчання із безпосередньо RandomForestClassifier, то час навчання вотуючого класифікатора зростає на 10-15 %. Якщо порівнювати, наприклад, швидкість навчання вотуючого класифікатора на базі KNearestNeiborClassifier, ExtraTreeClassifier, DesignTreeClassifier з навчанням RandomForestClassifier, то час навчання вотуючого класифікатора значно менше (в залежності від набору даних, який обрано для навчання, але щонайменше на 60-70%). Час навчання класифікатора з використанням нечіткого ансамбля (див. алгоритм вище) практично не відрізняється від часу навчання класифікатора голосування (більше приблизно на 10-15%).

Для ExtraTreeClassifier час навчання практично не залежить від кількості ознак. Для DesignTree або KNeibors (і, як наслідок, для класифікатора Voting в

цілому) час навчання помітно зростає зі збільшенням кількості ознак.

Зменшення кількості ознак на усіх наборах даних впливає на точність оцінювання досить неоднозначно. Поки група ознак в наборі даних для навчання містить перши за списком ознаки з найбільшим впливом, точність моделі знаходиться на початковому рівні – більш, ніж 99%. При виключенні з моделі хоча б однієї з ознак з великим впливом, точність моделі стрибкоподібно знижується.

В деяких розрахунках визначення вагових коефіцієнтів для визначення результатів голосування здійснювалося за допомогою евристичного набору нечітких правил.

Таким чином, запропонований підхід до побудови ансамблю дозволив підтримати високий рівень точності (краще 99%) і низький рівень помилок після навчання на наборі даних зі зменшеною кількістю ознак.

Висновки до розділу 3

1. Виконано дослідження точності роботи деяких класифікаторів на наборах даних для навчання моделей виявлення вторгнень. Найкращі результати класифікації для усіх досліджених наборів даних забезпечили класифікатори на основі дерев: DecignTreeClassifier, ExtraTreeClassifier, RandomForestClassifier.

2. Встановлено, що зменшення кількості ознак на усіх наборах даних впливає на точність оцінювання відповідно до критерію середнього зменшення помилок класифікації. Поки група ознак в наборі даних для навчання містить перші за списком ознаки з найбільшим впливом, точність моделі знаходиться на початковому рівні, але при виключенні з моделі хоча б однієї з ознак з великим впливом, точність моделі стрибкоподібно знижується.

3. Запропоновано метод побудови набору важливих ознак для вирішення задач класифікації. Цей метод заснований на ідеє використання ансамбля

оцінювачів важливості ознак з підведенням підсумків і кінцевого результату ансамбля за допомогою алгоритмів нечіткої логіки. В якості оцінювачів важливості ознак було використано статистичні критерії (χ^2, f_classif, коефіцієнт кореляції), критерій середнього зменшення помилок класифікації (mean decrease in impurity - MDI), критерій взаємної інформації (mutual_info_classif).

4. Розроблено новий 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.

5. Найкращі показники за швидкістю навчання забезпечив класифікатор VotingClassifier, побудований на базі алгоритмів з максимальною швидкістю навчання. Час навчання класифікатора з використанням нечітких правил практично не відрізняється від часу навчання класифікатора голосування (більше приблизно на 10-15%). За рахунок виключення із моделі несуттєвих ознак досягається помітне збільшення швидкості навчання (до 60-70%).

РОЗДІЛ 4
РОЗРОБКА РЕКОМЕНДАЦІЙ З УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ТА ВИКОРИСТАННЯ СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ

В даному розділі проведене дослідження ефективності запропонованих методів виявлення вторгнень, представлені рекомендації з використання отриманих у розділах 2 та 3 результатів в системі інформаційної безпеки підприємства.

4.1 Оцінка ефективності та достовірності застосування розроблених методів для виявлення вторгнень

Для перевірки запропонованих в дисертаційному дослідженні підходів щодо розробки системи виявлення вторгнень, створення ансамблевого класифікатора з використанням нечіткої логіки, створення метода обрання набору релевантних ознак з використанням ансамблевого навчання і нечіткої логіки в інформаційній системі підприємства проведено практичну реалізацію на підприємстві, зміст якої полягає у наступному. В якості даних для перевірки та оцінки ефективності розробленого методу було прийнято рішення використовувати реальну мережеву топологію, схема якої наведена на рис. 4.1. Для скорочення часу дослідження і спрощення формування атак для генерації трафіка була створена модель з аналогічною топологією (тестовий стенд) за допомогою пакету GNS3 [169]. На рис. 4.1 показано структура мережі для виконання дослідження, в якої є умовна мережа жертви та умовна мережа зловмисника, розділеними типовим брандмауером.

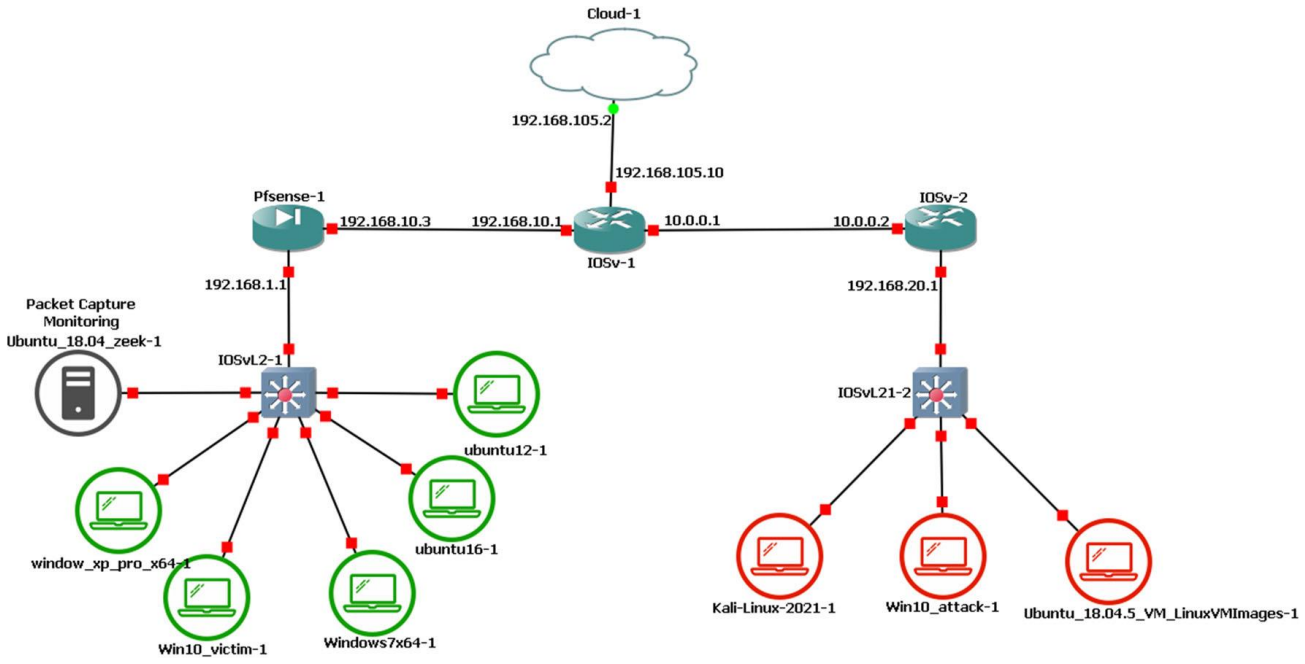


Рис. 4.1 – Топологія інформаційної мережі для виконання досліджень

За замовчуванням сторона локальної мережі (LAN) брандмауера є надійною мережею, тоді як сторона глобальної мережі (WAN) брандмауера є ненадійною. В загальному випадку трафік, ініційований з WAN до LAN, блокується. Цей трафік було дозволено, щоб мати можливість виконувати сценарії мережевих атак. Мережа жертви також має доступ до Інтернету через трансляцію мережевих адрес (NAT).

Було припущено, що мережевий трафік «жертви» записується за допомогою відомого інструменту мережевого запису та обробки Wireshark. В якості операційної системи використовується Ubuntu. Уся комунікація, що відбувається через мережу жертви, віддзеркалюється на цю віртуальну машину. Тут цей трафік записується для кількох сценаріїв атак і пересилається на cicflowmeter.

CICFlowMeter — генератор і аналізатор потоку мережевого трафіку. Його

можна використовувати для створення двонаправлених потоків, де перший пакет визначає напрямок вперед (від джерела до пункту призначення) і назад (від пункту призначення до джерела), отже, більше 80 статистичних характеристик мережевого трафіку, таких як тривалість, кількість пакетів, кількість байтів, Довжину пакетів тощо можна розрахувати окремо в прямому та зворотному напрямках.

Експериментальне дослідження та оцінка ефективності розробленого методу виявлення вторгнень в ІС підприємства на основі ансамблевого метода класифікації проводилися з використанням мови програмування Python в середовищі спеціально розробленого додатка. Цей додаток імпортував необхідні компоненти з пакету scikit-learn, а також ілюстративні бібліотеки matplotlib і seaborn.

Було досліджено декілька властивостей створеної системи: точність класифікації, час навчання моделі, час виконання класифікації тестової вибірки (на деяких вибірках – для бінарної та багатокласової класифікації) [1,2,8].

На наступної стадії був виконаний аналіз реального трафіка в мережі реальної інформаційної мережі підприємства.

Приклад порівняння результатів порівняння роботи класифікаторів з оцінкою часу розпізнавання тестової вибірки наведено в таблиці 4.1.

Таблиця 4.1

Оцінка продуктивності навчених моделей на наборі даних CSE-CIC-IDS2018

Model	**Accuracy**	**Precision**	**Recall**	**F-score**	**AUC**	**Test Time (s)**
DTC	99.59	99.59	99.59	99.59	99.76	0.18
ETC	99.71	99.72	99.71	99.61	99.97	0.17
RFC	99.69	99.69	99.67	99.67	99.98	2.83
Voting	99.78	99.79	99.77	99.77	99.97	0.46
Votind+Fuzzy	99.76	96.96	96.43	96.43	96.81	0.49

Як видно з цієї таблиці, точність моделей з класифікатором голосування трохи вище у порівнянні з ExtraTreeClassifier або DesignTreeClassifier, а час виконання класифікації для розглянутої вибірки трохи вище (тестова вибірка обсягом 15% від навчальної).

Для варіанту мультикласової класифікації результати дослідження наведено в таблиці 4.2. Розрахунки було виконано для набору даних CSE-CIC-IDS2018, класи відповідають групам атак, які представлено в тому наборі.

Таблиця 4.2

Продуктивність моделей IDS у виявленні та класифікації кожного класу мережевого трафіку (набір даних CIC-IDS-2018)

Class	**Voting (hard)**			**Voting+Fuzzy**		
	Precision	**Recall**	**F-score**	**Precision**	**Recall**	**F-Score**
Benign	0.9966	0.9990	0.9978	0.9999	0.9999	0.9998
Bot	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
Brute Force	0.9999	1.0000	1.0000	1.0000	0.9999	0.9999
DoS	0.9999	1.0000	1.0000	1.0000	0.9999	1.0000
DDoS	0.9999	0.9999	0.9999	0.9999	1.0000	0.9999
Infiltration	0.9966	0,9967	0.9964	1.0000	1.0000	1.0000
Web Attack	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000

Результати показують, що для різних атак у наборі даних CSE-CIC-IDS2018 обидві моделі IDS показали високі показники точності та F-оцінки, досягнувши 100% у правильній класифікації класів. Якщо говорити точніше, стандартний VotingClassifier з простим голосуванням і VotingClassifier з нечітким голосуванням показали практично однакові результати на наборі даних 2018 року. Однак покращений класифікатор трохи перевершив стандартний, виявив атаку інфільтрації з відкликанням, яке досягло 100% проти 99,67% у стандартного класифікатора Результати загалом показують низьку ймовірність помилкових тривог в обох сценаріях[1,2,8].

Для перевірки зроблених висновків і розроблених технологічних рішень

декілька експериментів було виконано з контролем мережевого трафіка за допомогою пристрою моніторінгу пакетів. За рахунок генерування трафіку було створено власний новий набір даних, який включає всі атаки, перелічені CSE-CIC-IDS2018. Схема генерації набору даних показана на рисунку 4.2.

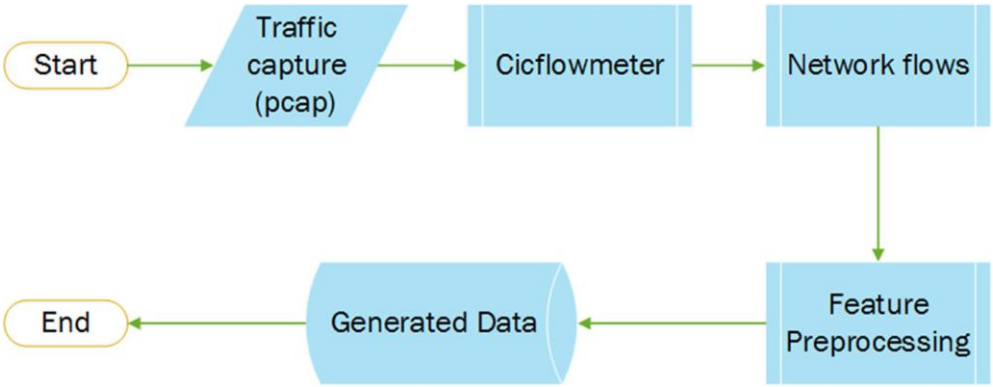


Рис. 4.2 Схема створення набору даних

Кількість випадків атак для згенерованого трафіка на 300 тис. записів представлена на рисунку 4.3.

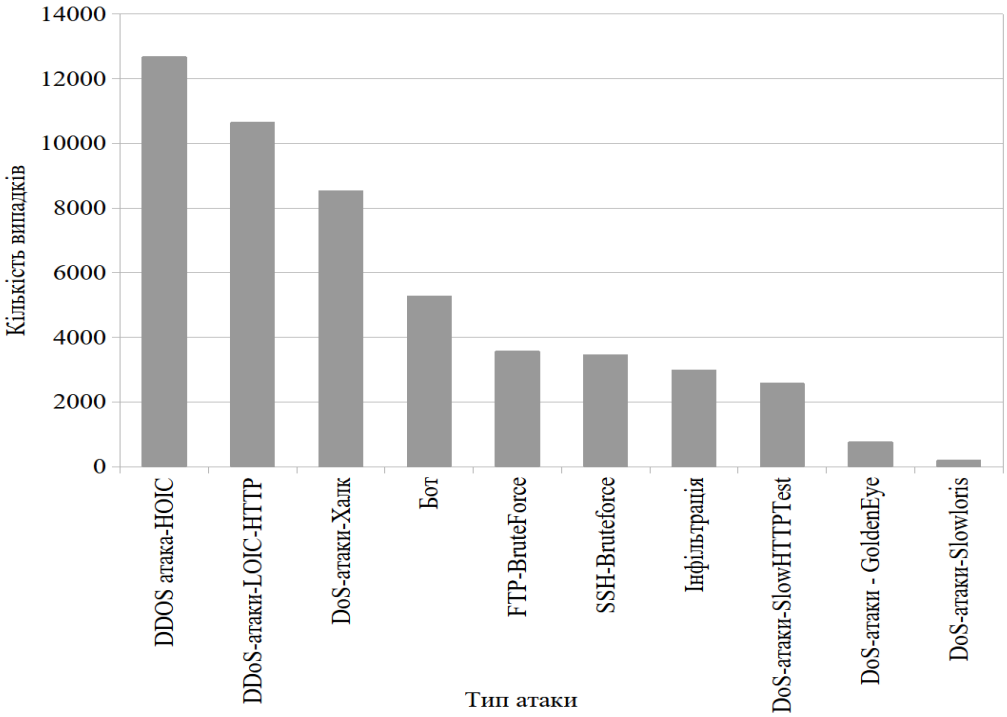


Рис. 4.3 Кількість випадків атак для згенерованого трафіка

Cicflowmeter бере файл запису трафіку та створює файл CSV на основі цих тих же ознак, які є в наборі даних CSE-CIC-IDS2018. Ці характеристики базуються на інформації заголовків рівня 3 і 4 OSI та іншій інформації про мережевий трафік, що базується на часі та обсязі, такій як кількість байтів, пакетів і тривалість у прямому та зворотному напрямках.

Заголовок рівня 3 визначає IP-адресу джерела, IP-адресу призначення та тип служби, тоді як рівень 4 містить різноманітні прапори заголовка, включаючи порти джерела та призначення, порядковий номер, номер підтвердження та інші прапори, такі як URG, ACK, PSH, RST, SYN і FIN. Генеруються потоки TCP і UDP. Потоки UDP зазвичай закінчуються тайм-аутом потоку, тоді як потоки TCP закінчуються пакетом FIN або тайм-аутом потоку. Стандартний час очікування для потоків становить 120 000 000 мікросекунд або 120 с.

Порівняльні результати базових моделей і моделей ансамблю (див. таб. 4.3 та 4.4) на створеному новому наборі даних показують, що різні моделі застосовуються до нашого згенерованого набору даних, а зважений бал F1 запропонованого ансамблевого підходу з нечіткими правилами є найвищим (98,24%). Ці результати доводять перевагу запропонованого ансамблевого підходу при навчанні й формування тестового набора даних з використанням створеного набору даних.

Таблиця 4.3

Порівняння результатів моделей глибокого машинного навчання та моделей ансамблю на наборі даних

Тип моделі	Особливості моделі	Зважене значення F1-критерію (%)
MLP	4 шари	95.40
RandomForest		96.50
Ensemble	Majority based voting ensemble (ETC, KNN, DTC)	97.70
Ensemble (Voting+Fuzzy)	**Fuzzy-logic ensemble approach** Base learner: KNN, ETC, DTC	**98.24**

Таблиця 4.4. Оцінка продуктивності навчених моделей на новому наборі даних

Набір даних	Кількість ознак	Класифікатор	Точність, %	Час навчання, с	Час тестування, с
NSL-KDD	41	RF	99,99	9,53	0,14
	16	RF	100,0	9,18	0,12
	16	Voting	99,34	1,31	0,13
	11	Ensemble (Voting+Fuzzy)	99,14	1,11	0,11
IDS 2018 (одна доба)	79	RF	99,99	172.1	2,83
	21	RF	99,99	121,4	2,01
	21	Voting	99,99	8,51	2,13
	11	Ensemble (Voting+Fuzzy)	99,93	5,96	1,39
Створений набір даних	79	RF	99,99	126,5	2,09
	21	RF	99,99	89,4	1,49
	21	Voting	99,99	7,11	1,58
	11	Ensemble (Voting+Fuzzy)	99,91	5,03	1,03

Як видно з таблиці 4.4, використання розробленого класифікатора дозволяє зменшити час тестування вибірки на наявність/відсутність атаки більш, ніж на 30% на усіх протестованих наборах даних. Значно скорочується також час навчання моделі зі зменшеною кількістю релевантних ознак. Таким чином, 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.

Отже, на основі проведеного дослідження можна зробити висновок, що вдосконалений ансамблевий класифікатор з підведенням підсумків голосування на базі нечітких правил є найефективнішим. Застосування цього методу дозволяє значно знизити час виявлення вторгнень і підвищити точність оцінювання, що сприяє підвищенню рівня безпеки інформаційної систем.

4.2 Розробка рекомендацій щодо впровадження системи виявлення вторгнень в інформаційній системі підприємства

На основі результатів дослідження ефективності та достовірності застосування розроблених методів виявлення вторгнень та обрання набору ознак на основі використання ансамблевого класифікатора з системою нечітких правил, можна рекомендувати впровадження побудованої на них системи виявлення вторгнень в інформаційну систему підприємства після мережевого екрану. Приклад інтеграції системи виявлення вторгнень в архітектуру інформаційної системи підприємства наведено на рис. 4.4.

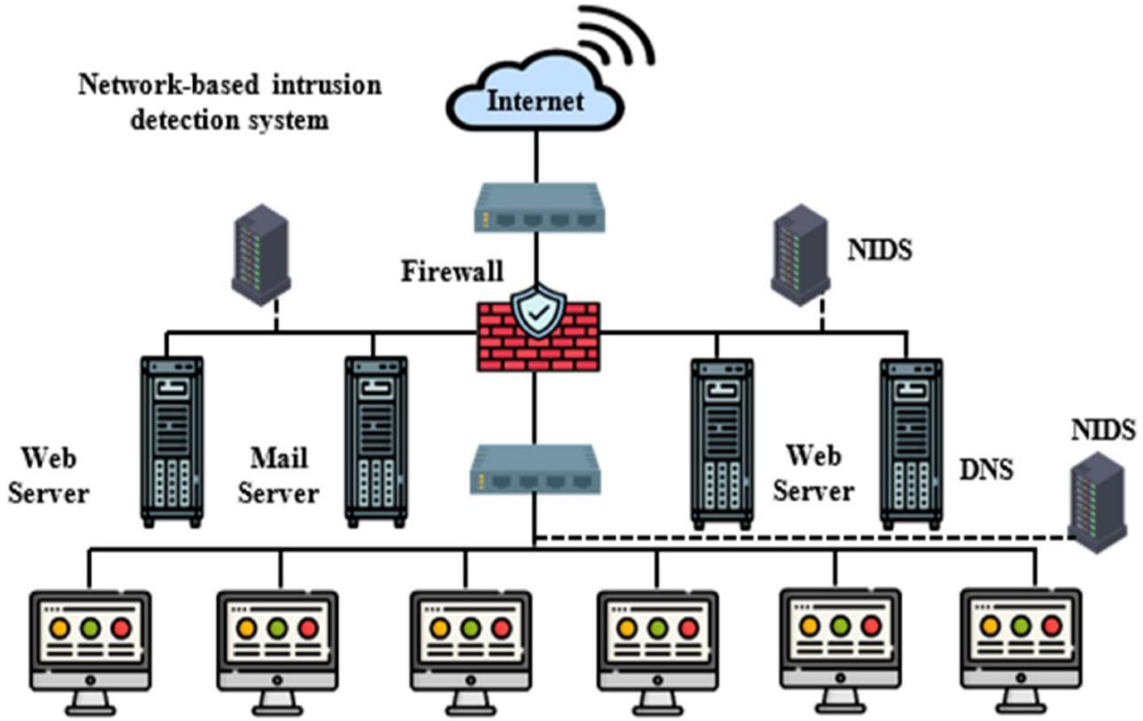


Рис. 4.4. Структура інформаційної системи підприємства з системою виявлення вторгнень

Застосування розроблених методів в системі виявлення вторгнень передбачає етапи.

1. Початкова стадія – підготовка або відбір набору даних для навчання системи (або використання відомих наборів даних).

2. Попередня підготовка даних (очищення, трансформація, масштабування даних).

3. Вибір набору ознак відповідно до типу атаки, який чекає система, або ітераційно для усіх типів атак, які підтримує датасет.

4. Навчання моделі. Обирається або одна модель (бінарна класифікація) або ітераційно навчається декілька моделей для різних типів атак.

5. Виявлення присутності атак. Якщо є виявлення атаки, система формує повідомлення.

6. Виявлення тривоги: якщо на етапі виявлення відхилення від нормального функціонування було виявлено потенційну загрозу безпеці інформаційної системи, то на цьому етапі генерується тривога. Тривога може бути надіслана адміністратору системи або відповідному відділу, щоб вжити заходів щодо подальшого аналізу інциденту та його припинення.

Опис роботи системи виявлення вторгнень в інформаційній системі підприємства зображений на рис. 4.5.

Якщо на етапі виявлення відхилення атак відсутні будь-які ознаки потенційних атак або інших шкідливих процесів, то система отримує наступний вектор даних і знову виконує оцінку загроз.

Таким чином, розроблена система виявлення вторгнень в інформаційній системі підприємства на основі ансамблевого навчання і скорочення розмірності простору ознак дозволяє автоматично виявляти потенційні атаки інформаційної системи та реагувати на них вчасно [1,2,8].

Це значно зменшує ризик виникнення інцидентів та збільшує рівень безпеки інформаційних систем підприємства та її функціонування в цілому.

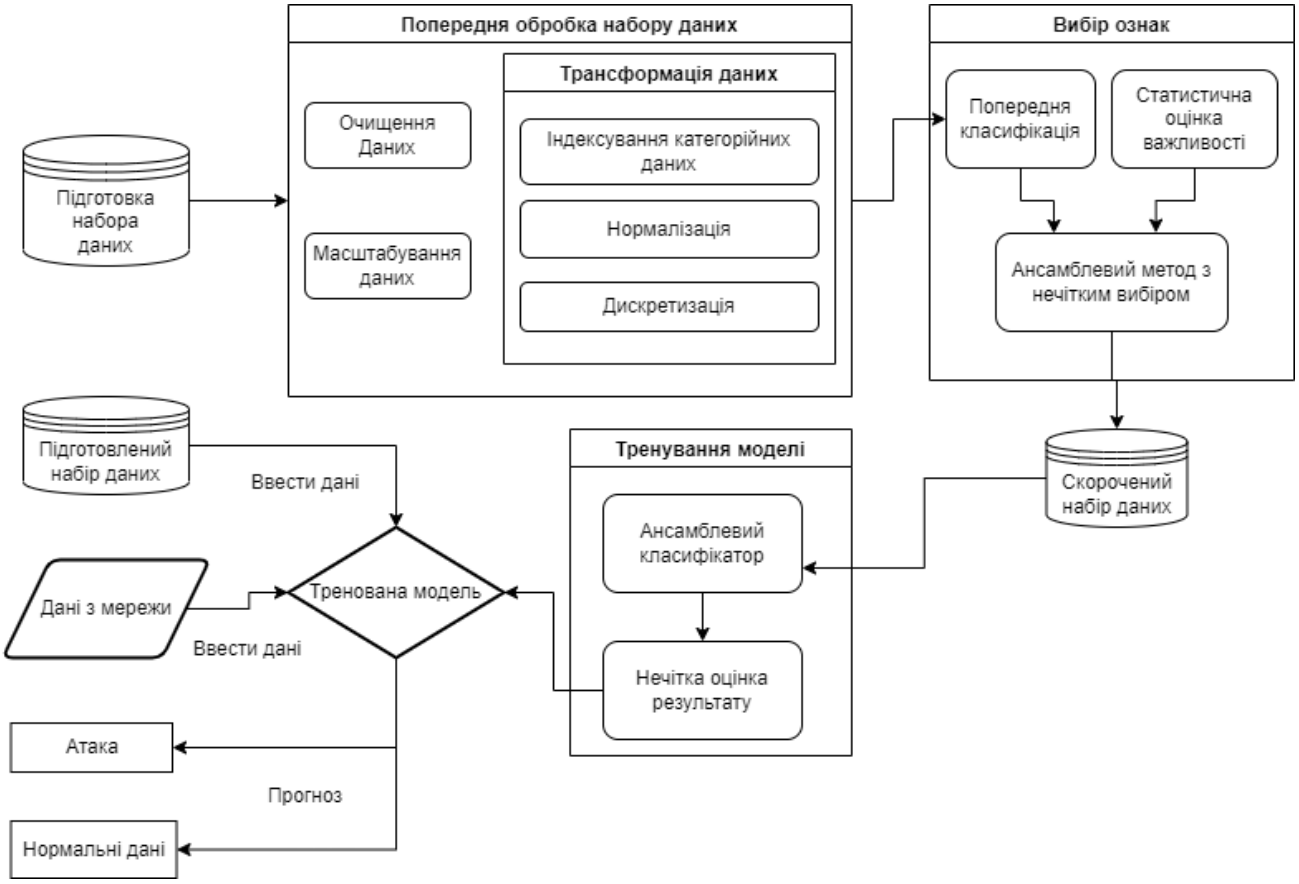


Рис. 4.5. Послідовність роботи системи виявлення вторгнень

Загальні рекомендації щодо впровадження розробленого методу виявлення вторгнень:

1. Забезпечити належне збирання та аналіз даних для побудови набора даних для навчання моделі IDS (або декількох моделей).
2. Використовувати необхідні алгоритми і програмні засоби для зручного і вчасного формування набору даних, щоб уникнути помилок та впевнитись у точності результатів.
3. Контролювати критерії формування набору ознак для побудови моделі IDS, щоб забезпечити її точність та надійність, уникнути перенавчання.
4. Використовувати сучасні стандарти та протоколи для забезпечення взаємодії між системами та компонентами.

5. Забезпечити постійний моніторинг стану інформаційної системи в цілому та системи виявлення вторгнень системи.

6. Регулярно проводити навчання моделі на нових накопичених даних для забезпечення її актуального стану та ефективності IDS.

7. Налагодити процедуру автоматичного оповіщення у разі виявлення вторгнень, налагодити системи автоматичного ранжування загроз і повідомлень (див. п. 4.3).

8. Врахувати особливості інформаційної системи підприємства, її топологію та можливі загрози при впровадженні системи ідентифікації вторгнень.

9. Забезпечити надійне зберігання конфіденційної інформації, яка пов'язана з функціонуванням системи виявлення вторгнень.

10. Проводити систематичний аналіз і контроль ефективності та результативності системи виявлення вторгнень для її налагодження і покращення роботи відповідних алгоритмів.

4.3 Розробка рекомендацій щодо оцінки ризиків в інформаційній системі підприємства

Система виявлення вторгнень відіграє важливу роль у безпеці та стійкості системи активного захисту від атак зловмисників. Вони еволюціонували від пакетних сніфферів, використовуваних як інструмент усунення несправностей мережі для виявлення несправного обладнання та програмного забезпечення шляхом створення журналів, що показують активність мережевих пакетів. До появи мережевих комутаторів продукти IDS можна було підключити до будь-

якого порту мережевого концентратора та мали хороші шанси контролювати мережеві пакети в сегменті локальної мережі. Багато дослідників запропонували та впровадили різні моделі для IDS, але вони часто генерують занадто багато помилкових спрацьовувань через їх спрощений аналіз.

Загалом, зменшення кількості помилкових спрацьовувань і встановлення пріоритету для найбільш критичних атак є основними цілями підходів IDS до керування сповіщеннями. Крім того, ці методи допомагають адміністраторам безпеки зрозуміти ситуацію, виявлену IDS.

Атака може справді відбутися, і мережевий адміністратор повинен мати можливість правильно її ідентифікувати, тому йому потрібно вручну проаналізувати кожне сповіщення IDS, незалежно від того, чи є воно помилковим чи справжнім. Отже, це займає досить багато часу. Оскільки кількість повідомлень (можливо, помилкових) досить велика, серед них може бути прихованим сповіщення про справжні атаки.

Оптимальним способом вирішення цієї проблеми є використання рішення IDS, яке має можливість визначати пріоритети сповіщень, обчислювати ризик кожного з них і співвідносити їх, тим самим допомагаючи адміністратору мережі зосередити зусилля на виявленні реальних загроз.

Таким чином, автоматизована операція необхідна для обробки сповіщень і надання належної оцінки шкоди адміністратору безпеки.

Розглянемо модель оцінки ризиків як метод пріоритезації сповіщень відповідно до рівня ризику кожного з них, а також оцінюємо ризик кластера сповіщень. Ризик оцінюється як комбінація певних параметрів, отриманих із кожного сповіщення.

IDS генерує велику кількість сповіщень про можливі атаки, і через таку велику кількість адміністратори безпеки перевантажені, і стає важко вручну відрізнити справжні атаки від помилкових.

Для вирішення цієї проблеми було запропоновано два рішення [165]:

1. Покращення пристроїв моніторингу, вдосконалення механізму виявлення вторгнення, оптимізація сигнатур вторгнень, вдосконалення розміщення IDS. Це рішення обіцяє зменшити кількість сповіщень, але воно вимагає попереднього знання адміністратора системи безпеки щодо механізму виявлення.

2. Покращення керуванням оповіщеннями IDS, що містить агрегацію, кластеризацію, кореляцію та злиття.

Розглянемо міру ризиків, які пов’язані з повідомленнями IDS.

Оцінимо ризик як сукупність показників, отриманих із самих сповіщень і можливих цілей атаки.

Результати оцінки ризику можна використовувати для фільтрації повідомлень, щоб виділити підмножину з найвищими ризиками.

Введемо градацію ризиків: сповіщення, створені IDS, можуть бути високого ризику, середнього ризику або низького ризику.

Системи виявлення вторгнень, працюючи на основі сигнатур, використовуються для створення сповіщень про мережевий трафік.

Як приклад можна розглянути Snort або Suricata, які є IDS із відкритим вихідним кодом на основі сигнатур. Такі системи отримують онлайн-трафік, а потім створюють файли журналу сповіщень. Алгоритм зіставлення шаблонів використовується для фільтрації сповіщень і класифікації їх за різною формою.

Повідомлення про можливі вторгнення обробляються синтаксичним аналізатором з використанням типів та форматів згенерованих сповіщень після їх обробки.

Оцінка ризику – це процес виявлення ризиків безпеці, пов’язаних із системою, і визначення їхньої ймовірності виникнення, їх впливу та заходів безпеки, які б пом’якшили цей вплив. Ризики можна визначити як можливість того, що дана загроза використовуватиме вразливі місця об'єкту або групи об'єктів, щоб спричинити втрату або пошкодження об'єктів. Основна мета оцінки

ризиків полягає у визначенні відповідних засобів контролю для зменшення або усунення цих ризиків [166].

За даними [167], стандартний ризик оцінюється шляхом розгляду ймовірності успішних атак і відповідної серйозності цих атак.

Загалом існує чотири етапи оцінки ризику, а саме:

- ідентифікація загроз;
- ідентифікація вразливостей;
- визначення ризику;
- рекомендація щодо контролю.

Шаблон атаки – це абстрактний механізм для опису того, як виконується тип спостережуваної атаки. Шаблон атаки включає опис контексту, в якому він застосовний, а також (на відміну від типових шаблонів) дає рекомендовані методи пом'якшення наслідків [168].

Коли відбувається атака, вона використовує кілька шляхів (від розвідки до експлуатації), використовуючи сценарії, визначені в процесі індикаторами та симптомами, з метою отримання несанкціонованого доступу до даних. Аналіз впливу спрощує процес моніторингу та мінімізує кількість помилкових тривог.

Кожен сценарій атаки впливає на конфіденційність, доступність і/або цілісність. Власник даних щодо агента ризику визначить вплив кожного показника, симптому та вразливості залежно від характеру даних.

Можливість того, що ця подія відбудеться, визначається як ймовірність. Оцінка ризику виявленої атаки змінюється та спрощує діагностику тривог (хибнопозитивна або успішна атака), у той же час симптоми та сценарій індикаторів атаки підвищують ймовірність агента ризику.

Аналіз шаблону атаки використовує агент ризику для обчислення балів усіх індикаторів і симптомів, а потім для визначення характеру пакета.

Простий механізм визначення ризику – оцінити його добуток ймовірності (Pe) порушення безпеки, загрози та її потенційного впливу або наслідків (Ie):

$$Re = Pe * Ie, \tag{4.1}$$

де Re – оцінка ризику.

Вплив Ie (або наслідок) означає ступінь, до якого подія ризику може вплинути на підприємство, виражену в термінах: конфіденційність, цілісність і доступність.

Для розрахунку ризиків конфіденційності, цілісності та доступності слід застосовувати моделі, представлені у розділі 2.

Кореляція використовується для агрегування сценаріїв атак і симптомів, створених усіма зондами в хмарному середовищі.

Рівняння (4.1) представляє формулу оцінки ризику ймовірності Pe, тоді як (Ie) може бути присвоєно значення за числовим масштабом. Кожен показник Is, Vulnerability Ve, Symptoms Sy має різний вплив. Значення Pe буде збільшено з кожним виявленням шаблону атаки.

Використовуючи формулу оцінки ризику всіх підозрілих дій, ми можемо отримати оцінку ризику для кожної атаки:

$$Ra = \frac{1}{n} \sum Ie \cdot Pe, \tag{4.2}$$

де

$$Ie = \sum (Is + Ve + Sy). \tag{4.3}$$

Вплив Ie та ймовірність Pe кожного симптому та атаки будуть визначені власником даних і адміністратором системи в агенті ризику, розгорнутому в корпоративній мережі. Мета такої кореляції полягає в тому, щоб отримати поведінку зловмисника та ризик, пов’язаний з кожною дією, шляхом розрахунку впливу та переманити потенційного зловмисника з критичної системи.

Значення Ra, пов’язане з кожною атакою, визначатиме, чи є дія успішною атакою чи хибним позитивним результатом залежно від чутливості цільових даних, пов’язаних зі значеннями ризику.

IDS/IPS виконують чотири важливі функції безпеки: вони відстежують, аналізують, виявляють і реагують на всі підозрілі дії, як показано на функціональному рівні.

IDS/IPS виявляє вторгнення, аналізуючи зібрані дані на всіх хмарних рівнях на основі бази знань і онтології моделі атаки, обчислює ризик атаки, а потім вирішує, чи є вона підозрілою дією чи хибно-позитивним.

Система виявлення вторгнень визначає вплив і ймовірність кожного виявленого симптому. Вона визначатиме вплив кожної моделі атаки, а потім ризик атаки. Впровадження такої методики дозволяє мінімізувати кількість хибно-визначених тривог і підвищити ефективність системи виявлення вторгнень.

Висновки до розділу 4

1. В результаті дослідження встановлено, що запропонована нова модель IDS з використанням методів ансамблевого навчання на скорочених за допомогою алгоритмів вибору ознак великих наборах даних дозволяє значно знизити час виявлення вторгнень і підвищити точність оцінювання, що сприяє підвищенню рівня безпеки інформаційної систем. Результати дослідження можуть бути використані в подальших наукових дослідженнях в галузі захисту інформації та забезпечення безпеки технічних систем.

2. Встановлено, що для різних атак покращений класифікатор VotingClassifier з нечітким голосуванням показав високі показники точності та F-оцінки, досягнувши 100% у правильній класифікації класів, і перевершив стандартний, виявив атаку інфільтрації з відкликанням, яке досягло 100% проти 99,67% у стандартного класифікатора. Результати загалом показують низьку

ймовірність виникнення помилкових тривог.

3. Розроблено рекомендації щодо впровадження моделі IDS з використанням методів ансамблевого навчання на скорочених за допомогою алгоритмів вибору ознак великих наборах даних в інформаційну систему підприємства та описаний алгоритм роботи розробленого методу.

4. Розроблено рекомендації щодо оцінки ризиків в інформаційній системі підприємства. Передбачено, що система виявлення вторгнень визначатиме вплив кожної моделі атаки, а потім ризик атаки. Впровадження такої методики дозволяє мінімізувати кількість хибно-визначених тривог та підвищити ефективність системи виявлення вторгнень.

ВИСНОВКИ

В результаті дисертаційного дослідження, виконаного автором, вирішено актуальне наукове завдання з розробки моделей, методів та алгоритмів системи управління інформаційною безпекою у складі інформаційної системи підприємства на основі підходів машинного навчання та нечіткої логіки. Вирішене наукове завдання має істотне значення для теоретичних і прикладних основ оцінки ризиків інформаційної безпеки та побудови систем виявлення вторгнень при управлінні інформаційною безпекою підприємств. Відсутність аналогічних рішень робить результати дослідження актуальними та пріоритетними.

В дисертаційному дослідженні отримані такі основні результати:

1. В результаті аналізу існуючих підходів до управління інформаційною безпекою та виявлення вторгнень в корпоративну мережу підприємства встановлено, що протягом останніх десятиліть для протидії кібератакам широке розповсюдження отримали системи виявлення вторгнень. Для побудови таких систем використовуються методи обчислювального інтелекту, в тому числі машинне навчання, глибоке навчання та інтелектуальний аналіз. Швидке збільшення мережевого трафіку, розвиток інтернет-технологій, збільшення обсягів даних, а також поява нових типів кіберзагроз вимагають удосконалення систем виявлення вторгнень, яке спрямоване на підвищення швидкості та сумарної ефективності їх роботи. Існуючі підходи до управління інформаційною безпекою підприємств не враховують в повній мірі розмитість, неповноту та якісний характер інформації для оцінки вразливостей та загроз, що обумовлює актуальність використання апарату нечіткої логіки при формалізації та побудові алгоритмів системи кібербезпеки.

2. 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.

3. 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.

4. 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.

5. У результаті дослідження та проведення експерименту щодо виявлення вторгнень в інформаційній системі підприємства було встановлено, що 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%. Основні наукові результати дослідження реалізовані у практичній діяльності ТОВ "Хуавей Україна" і ТОВ "РЕНТСОФТ", та впроваджені в навчальний процес Державного університету інформаційно-комунікаційних

технологій, що підтверджено відповідними актами.

6. Таким чином, мета дослідження, яка полягає в збільшенні 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, досягнута та всі часткові завдання дослідження вирішено повністю.

7. Результати роботи можуть бути використані в подальших наукових дослідженнях в галузі захисту інформації та забезпечення кібербезпеки інформаційних систем. Напрями подальших досліджень за тематикою дисертації можуть охоплювати аналіз та вдосконалення методів машинного та глибокого навчання, що використовуються для виявлення вторгнень в інформаційних системах підприємств, розвиток моделей оцінки ризиків інформаційної безпеки з використанням нечіткої логіки та нейро-нечіткого моделювання.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

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.

8. Чичкарьов Є.А., Зінченко О.В., Бондарчук А.П., Асєєва Л.А. Використання алгоритмів машинного навчання і нечіткої логіки для виявлення мережевих вторгнень з використанням комплексу наборів даних. *«Systems and*

measures of artificial intelligence» AIIS'2023International scientific youth school: Матеріали Міжнародної наукової молодіжної школи «Системи та засоби штучного інтелекту», м. Київ, 10–11 жовт.2023 р. / ІПШІ «Наука і освіта» Київ, 2023. С. 13 – 15.

9. Кожухівський А.Д., Асєєва Л.А. Оцінка ризиків конфіденційності документів проектів з застосуванням нечіткої логіки. *Проблеми інформатики та комп'ютерної техніки*: Праці Х-ї Міжнародної наук.-практ. конф. (ПІКТ – 2021), м. Чернівці, 28 – 31 жовтня 2021 р. / Чернівці, 2021. С. 109–112.

10. Асєєва Л.А. Формалізація функції належності нечітких факторів управління інформаційною безпекою підприємства з використанням методу аналізу ієрархій. *IX Всеукраїнська науково-практична конференція з автоматичного управління* : Матеріали IX Всеукраїнської наук.-практ. конф. здобув. вищої освіти та молодих вчених з автоматичного управління присвяченої Дню космонавтики, м. Херсон, 12 – 14 квітня 2021 р. / Ред. Г.В. Рудакової та ін. Херсон: Видавництво ФОП Вишемирський В.С. Херсон, 2021. С. 36.

11. Кожухівський А.Д., Асєєва Л.А. Нечітке управління ризиками в інформаційній безпеці підприємства. *Комп'ютерна математика в науці, інженерії та освіті CMSEE-2020* : Матеріали V Всеукраїнської наук.-техн. конф., м. Полтава, 27 листопада 2020 р. / ред.: О.М. Гайтан – Полтава: Національний університет «Полтавська політехніка імені Юрія Кондратюка», 2020. С.69–70.

12. Асєєва Л.А. Підходи до класифікації складових небезпеки при побудові систем управління інформаційною безпекою підприємств. *VIII Всеукраїнська науково-практична конференція з автоматичного управління* : Матеріали VIII Всеукраїнської наук.-практ.конф. студентів, аспірантів та молодих вчених з автоматичного управління присвяченої Дню космонавтики, м.Херсон, 08 – 10 квітня 2020р./ Ред. Г.В. Рудакової та ін. Херсон: Видавництво ФОП Вишемирський В.С. Херсон, 2020. С.41.

13. Асєєва Л.А. Аналіз загроз інформаційної безпеки будівельного

підприємства. *Проблеми інформатизації*: тези доп. тринадцятої міжнародної наук.-техн.конф., 11-12 квітня 2019 р./ Київ: ДУТ, НТУ; Полтава: ПНТУ; Катовице: КЕУ; Париж: Університет Париж VII Вєнсент-Сен-Дені; Вільнюс: ВДТУ; Харків : ХНДІТМ: Білорусь: БДАЗ; Кропивницький: ЛА НАУ, 2019. С.182.

14. Асєєва Л.А. Система управління інформаційною безпекою будівельного підприємства на принципах нечіткої логіки. *Проблеми інформатизації* : тези доп. дванадцятої міжнародної наук.-техн.конф., 12 - 13 грудня. – 2018р./ Київ : ДУТ, НТУ; Полтава: ПНТУ; Катовице: КЕУ; Париж: Університет Париж VII Вєнсент-Сен-Дені; Вільнюс: ВДТУ; Харків : ХНДІТМ: Білорусь: БДАЗ, 2018. С.146–147.

15. Dasgupta D., Akhtar Z., Sen S. Machine learning in cybersecurity: a comprehensive survey. *The journal of defense modeling and simulation: applications, methodology, technology*, 2020. Vol. 19, № 1. P. 57–106. DOI:https://doi.org/10.1177/1548512920951275.

16. Cherian Samuel. Cybersecurity: Global, Regional and Domestic Dynamics. *Institut for Defence Studies and Analyses. New Delhi.* Monograph series No42. dec2014. P.10 – 84c.

17. Bharadwaj R. K. Manthaa, Borja Garcia de Sotob. Cyber security challenges and vulnerability assessment in the construction industry. *Conference Creative Construction 2019*. Budapest, Hungary. 2019. 29 June - 2 July. DOI:10.3311/CCC2019-005. PP 30–37.

18. NIST. Measurements for Information Security. Created September 15, 2020, Updated December 3, 2020. Режим доступу: URL :https://www.nist.gov/cybersecurity/measurements-information-security (дата звернення 31.03.2022).

19. Смачило Т.В., Кахній М.І. Теоретичні засади управління системою інформаційної безпеки підприємства. *Young Scientist* • № 12.1 (40).dec.,2016.

Режим доступу: URL: http://molodyvcheny.in.ua/files/journal/2016/12.1/227.pdf (дата звернення 31.03.2022).

20. Такій Д. М., Журан О. А. Управління інформаційною безпекою підприємства для утримання конкурентних позицій на ринку. ОНПУ. Режим доступу URL : http://dspace.opu.ua/jspui/bitstream/123456789/7134/1/%D0%A2%D0%B5%D0%B7%D0%B8%D1%81%D1%8B%20%D0%96%D1%83%D1%80%D0%B0%D0%BD_%D0%A2%D0%B0%D0%BA%D0%B8%D0%B9.pdf. (дата звернення 31.03.2021).

21. Ананченко О.Є. Питання формування організаційної структури системи управління інформаційною безпекою підприємства. *Сучасний захист інформації* 2016. №1. Режим доступу URL: http://journals.dut.edu.ua/index.php/dataprotect/article/view/536 (дата звернення 31.03.2021).

22. Куркин М. В. Управление экономической безопасностью предприятия : монография. / М. В. Куркин. – Днепропетровск : АРТ-ПРЕСС, 2004. – 452 с.

23. Куркін М. В. Управління інформаційною безпекою та забезпечення стабільності інформаційної безпеки підприємства. 2014. Режим доступу URL: https://cybersafetyunit.com/upravlinnya-informatsiynoyu-bezpekoyu-ta-zabezpechennya-stabilnosti-informatsiynoyi-sistemi-pidpriyemstva-2/(дата звернення 31.03.2019).

24. PCI DSS Risk Assessment Guidelines Режим доступу URL: https://www.pcisecuritystandards.org/documents/PCI_DSS_Risk_Assmt_Guidelines_v1.pdf(дата звернення 31.03.2021).

25. Generic SCADA Risk Management Framework For Australian Critical Infrastructure Developed by the IT Security Expert Advisory Group (ITSEAG) (Revised March 2012) Режим доступу URL: https://www.tisn.gov.au/Documents/SCADA-Generic-Risk-Management-

Framework.pdf(дата звернення 31.03.2022).

26. Thomas R. Peltier . Information Security Risk Analysis 1st Edition. P.296. Режим доступу URL: https://www.academia.edu/40140524/Information_security_risk_analysis_thomas_r_peltier (дата звернення 31.03.2020).

27. Risk management guide for dod acquisition Sixth Edition (Version 1.0) Режим доступу URL: https://www.acq.osd.mil/damir/documents/DAES_2006_RISK_GUIDE.pdf(дата звернення 31.03.2022).

28. Special Publication (NIST SP) - 800-30 Rev 1. September 17, 2012. Режим доступу URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30.pdf (дата звернення 31.03.2021).

29. The Security Risk Management Guide Режим доступу URL: http://go.microsoft.com/fwlink/?linkid=30794(дата звернення 31.03.2021).

30. Garvey P.R. Analytical Methods for Risk Management: A Systems Engineering Perspective. Chapman-Hall/CRC-Press, Taylor & Francis Group (UK), Boca Raton, London, New York, 2008. ISBN: 1584886374.

31. Alberts C. Managing information security risks. The OCTAVE™ approach / C. Alberts, A. Dorofee. – Addison Wesley, 2002. – 512 p.

32. Про інформацію: Закон України від 02.10.1992р. станом 06.06.2020р. № 2657-XII Верховна Рада України; Законодавство України. Режим доступу URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text(дата звернення 04.10.2022).

33. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994р. станом 15.03.2022р. № 80/94-ВР Верховна Рада України; Законодавство України. Режим доступу URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення 04.06.2022).

34. Про захист персональних даних: Закон України «»Закон України від 01.06.2010р. станом 27.10.2022р. № 2297-VI Верховна Рада України; Законодавство України. Режим доступу URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення 04.11.2022).

35. BSI-Standart 200-2. IT Grundschutz Metholodody Режим доступу URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/International/bsi-standard-2002_en_pdf.pdf?__blob=publicationFile&v=1(дата звернення 31.03.2019).

36. NIST.SP.800-53 Security and Privacy Controls for Federal Information Systems and Organizations Режим доступу URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf(дата звернення 31.03.2019).

37. ДСТУ 3396.2-96 «Захист інформації. Технічний захист інформації. Терміни та визначення» Режим доступу URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=38934&cat_id=38836(дата звернення 31.03.2020).

38. НД ТЗІ 1.1-003-99 «Термінологія у галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу» Режим доступу URL: https://tzi.com.ua/downloads/1.1-003-99.pdf(дата звернення 31.03.2020).

39. Концепція технічного захисту інформації в Україні, затверджена постановою Кабінету Міністрів України від 08.10.97 р. № 1126. Режим доступу URL: https://zakon.rada.gov.ua/laws/show/1126-97-%D0%BF#Text(дата звернення 31.03.2020).

40. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу, затверджений наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від 28.04.99 р. № 22 Режим доступу URL: http://www.dsszzi.gov.ua/control/uk/publish/article?art_id=46074&cat_id=38835

(дата звернення 31.03.2022).

41. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу, затверджений наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від 28.04.99 р. № 22 Режим доступу URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article ?showHidden=1&art_id=105861&cat_id=38835&ctime=1359461827897(дата звернення 31.03.2022).

42. Granville K. Recent cyberattacks. 2015. feb. 5. Режим доступу URL: URL: https://www.nytimes.com/interactive/2015/02/05/ technology/recent-cyberattacks.html?_r=1(дата звернення 31.03.2019).

43. Rossi B. Top 10 most devastating cyber hacks of 2015. 2015. Dec. 10 Режим доступу URL: https://www.information-age.com/top-10-most-devastating-cyber-hacks-2015-123460657/(дата звернення 31.03.2019).

44. James A. Lewis. Rethinking Cybersecurity: Stratedy, Mass Effect and States. *CSIS*. Jan.2018. P.50.

45. Cve details. Режим доступу URL: https://www.cvedetails.com/vulnerability-search.php(дата звернення 31.03.2019).

46. CWE List. View the List of Weaknesses Apr. 13 2018. Режим доступу URL: https://cwe.mitre.org/data/index.html (дата звернення 31.01.2019).

47. Толюпа С., Лукова-Чуйко Н., Шестак Я. Засоби виявлення кібернетичних атак на інформаційні системи. *Інфокомунікаційні технології та електронна інженерія.* 2021. № 2 (2), с. 19–31. DOI:https://doi.org/10.23939/ictee2021.02.019.

48. Риндич Є.В., Коняшин В.В., Зайцев С.В., Усов Я.Ю. Особливості створення мережевої системи виявлення вторгнень у комп’ютерні системи. *Математичні машини і системи*. 2018. № 3. С.89–96.

49. Al-Ammouri A., Lebid I., Dekhtiar M., Lebid I., Al-Ammori H.

Development of a mathematical model of reliable structures of information-control systems. *Eastern-European Journal of Enterprise Technologies*. 2022. №5(9(119)). С.68–78. DOI:https://doi.org/10.15587/1729-4061.2022.265953.

50. Al-Ammouri Ali, Al-Ammori Hasan, Klochan A., Tymchenko O., Al-Ahmad A. Methods for improving the data reliability in information and control systems. *Electronics and Control Systems*. 2018. Vol.4, №58. С.27–34. DOI:https://doi.org/10.18372/1990-5548.58.13506.

51. Abdulkareem Al-Enezi K, Alshaikhli I, Alkandari A, et al. A survey of intrusion detection system using case study Kuwait Governments entities. In:proceedings of the 2014 3rd international conference on advanced computer science applications and technologies (ACSAT ’14). *IEEE Computer Society,* USA, Amman, Jordan. 2014.29–30 Dec. P.37–43.

52. Li Yuchong, Liu Qinghui. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports.* 2021.Nov. Vol. 7. P. 8176–8186. DOI:https://doi.org/10.1016/j.egyr.2021.08.126.

53. Tong W., Lu L., Li Z., et al. A survey on intrusion detection system for advanced metering infrastructure. In: *Sixth international conference on instrumentation & measurement, computer, communication and control (IMCCC)*. *IEEE.* Harbin, China. 21–23 July. 2016. P.33–37.

54. Gardiner J and Nagaraja S. On the security of machine learning in malware c & c detection: a survey. *ACM Comput Surv*. 2016. V.49. P1–39.

55. Siddique K., Akhtar Z., Aslam Khan F., et al. KDD cup 99 data sets: a perspective on the role of data sets in network intrusion detection research. *Computer.* 2019. Vol.52. P.41–51.

56. Siddique K, Akhtar Z, Khan MA, et al. Developing an intrusion detection framework for high-speed big data networks: a comprehensive approach. *KSII Trans Internet Inform Syst*. 2018. Vol.12. P. 4021–4037.

57. Liu H., Lang B. Machine learning and deep learning methods for intrusion

detection systems: A survey. *Applied Sciences.* 2019. 9(20). P.4396. DOI:https://doi.org/10.3390/app9204396.

58. Shanbhogue R.D., Beena B.M. Survey of data mining (DM) and machine learning (ML) methods on cyber security. *Ind J Sci Techno.l* 2017. Vol. 10 P. 1153–1176.

59. Liu Q., Li P., Zhao W., et al. A survey on security threats and defensive techniques of machine learning: a data driven view. *IEEE Access* . 2018. Vol.6 P. 12103–12117.

60. 8b. Catania C. A., Garino C. G. Automatic network intrusion detection: Current techniques and open issues. *Computers & Electrical Engineering.* 2012. Vol. 38(5). P. 1062–1072. DOI:https://doi.org/10.1016/j.compeleceng.2012.05.013

61. Toliupa, S., Pliushch, O., Parkhomenko, I. Побудова систем виявлення атак в інформаційних мережах на нейромережевих структурах. *Кібербезпека: освіта, наука, техніка.* 2020. №2(10). С.169–183. DOI:https://doi.org/10.28925/2663-4023.2020.10.169183.

62. Ivanichenko, Y., Sablina, M., & Kravchuk, K. (2021). Використання машинного навчання в кібербезпеці. *Кібербезпека: освіта, наука, техніка*. №4(12). С.132–142. DOI:https://doi.org/10.28925/2663-4023.2021.12.132142.

63. [12] Gulrajani, F. Ahmed, M. Arjovsky, V. Dumoulin, A. Courville. Improved training of wasserstein GANs. In Proc. of the 31st *International Conference on Neural Information Processing Systems* .2017. P. 5769–5779.

64. Sharma, B., Mangrulkar, R. Deep learning applications in cyber security: a comprehensive review, challenges and prospects. *International Journal of Engineering Applied Sciences and Technology.*2019. Vol.4(8). P.148–159.

65. Dilek S., Çakir H., Aydin, M. Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review. *International Journal of Artificial Intelligence & Applications*. 2015. Vol.6(1). P. 21.

66. Berman D. S., Buczak A. L., Chavis J. S., & Corbett C. L. A survey of deep

learning methods for cyber security. *Information.* 2019. Vol.10(4). P. 122.

67. Brundage M., Avin S., Clark J., Toner H., Eckersley P., Garfinkel B., Anderson H. The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. 2018. arXiv preprint arXiv:1802.07228.

68. Apruzzese G., Colajanni M., Ferretti L., Guido A., Marchetti M. On the effectiveness of machine and deep learning for cyber security. In 2018 10th International Conference on Cyber Conflict (CyCon). *IEEE*. 2018, May. P. 371–390.

69. Bae H., Jang J., Jung D., Jang H., Ha H., Yoon S. Security and Privacy Issues in Deep Learning. 2018. arXiv preprint arXiv:1807.11655.

70. Akhtar N., & Mian A. Threat of adversarial attacks on deep learning in computer vision: A survey. *IEEE Access.*2018. Vol.6. P.14410–14430.

71. García-Teodoro, P., Díaz-Verdejo, J., Maciá-Fernández, G., Vázquez, E. Anomaly-based network intrusion detection: Techniques, systems and challenges. *Comput. Secur*. 2009. Vol.28. P.18–28.

72. Chua T.-H., Salam I. Evaluation of Machine Learning Algorithms in Network-Based Intrusion Detection Using Progressive Dataset. *Symmetry.* 2023. Vol.15. P.1251. DOI:https://doi.org/10.3390/sym15061251.

73. Verma, Abhishek & Ranga, Virender. On Evaluation of Network Intrusion Detection Systems: Statistical Analysis of CIDDS-001 Dataset Using Machine Learning Techniques. *Pertanika Journal of Science and Technology*. 2018. Vol.26. P.1307–1332. DOI:https://doi.org/10.36227/techrxiv.11454276.v1.

74. Ferrag Mohamed Amine, Maglaras Leandros, Moschoyiannis Sotiris, Janicke Helge. Deep Learning for Cyber Security Intrusion Detection: Approaches, Datasets, and Comparative Study. *Journal of Information Security and Applications.* 2019. P.50. DOI:https://doi.org/10.1016/j.jisa.2019.102419.

75. 24. Kilincer I. F., Ertam F., & Sengur A. Machine learning methods for cyber security intrusion detection: Datasets and comparative study. *Computer Network*s. 2021. Vol.188. P.107840. DOI:https://doi.org/10.1016/j.comnet.2021.107840.

76. Khraisat A., Gondal I., Vamplew P., & Kamruzzaman J. Survey of intrusion detection systems: techniques, datasets and challenges. *Cybersecurit.*2019. Vol.2(1). P. 1–22. DOI: https://doi.org/10.1186/s42400-019-0038-7.

77. Rahman M. A., Asyhari A. T., Wen O. W., Ajra H., Ahmed Y., Anwar F. Effective combining of feature selection techniques for machine learning-enabled IoT intrusion detection. *Multimedia Tools and Applications*. 2021. Vol.80(20). P.31381–31399. DOI:https://doi.org/https://doi.org/10.1007/s11042-021-10567-y.

78. Alkasassbeh M. An empirical evaluation for the intrusion detection features based on machine learning and feature selection methods. 2017. DOI:https://doi.org/10.48550/arXiv.1712.09623.

79. Kaja, Nevrus & Shaout, Adnan & Ma Di. An intelligent intrusion detection system. *Applied Intelligence*. 2019.Vol. 49. P.3235–3247. DOI:https://doi.org/ 10.1007/s10489-019-01436-1.

80. Kanimozhi V. & Jacob Prem. Artificial Intelligence based Network Intrusion Detection with Hyper-Parameter Optimization Tuning on the Realistic Cyber Dataset CSE-CIC-IDS2018 using Cloud Computing. 2019. P.0033–0036. DOI:https://doi.org/10.1109/ICCSP.2019.8698029.

81. Javadpour Amir, Abharian Sanaz, Wang Guojun. Feature Selection and Intrusion Detection in Cloud Environment Based on Machine Learning Algorithms. *ISPA* 2017. P.1417–1421. DOI:https://doi.org/10.1109/ISPA/IUCC.2017.00215.

82. K.A. Taher, B.M.Y. Jisan and M.M. Rahman. Network intrusion detection using supervised machine learning technique with feature selection, in: 2019 International conference on robotics, electrical and signal processing techniques (ICREST). *IEEE*. 2019. P.643–646 DOI:doi:https://doi.org/10.1109/icrest.2019.8644161.

83. G. Kocher and G. Kumar. Analysis of machine learning algorithms with feature selection for intrusion detection using UNSW-NB15 dataset. Available at SSRN 3784406. *International Journal of Network Security & Its Applications (IJNSA)*. 2021.

Vol.13. №1.P.21–31. DOI:https://doi.org/10.5121/ijnsa.2021.13102.

84. Alkasassbeh Mouhammd. An empirical evaluation for the intrusion detection features based on machine learning and feature selection methods. *Journal of Theoretical and Applied Information Technology*. 2017. Vol.95. P.5962–5976. DOI:https://doi.org/10.48550/arXiv.1712.09623.

85. Pattawaro Apichit, Polprasert Chantri. Anomaly-Based Network Intrusion Detection System through Feature Selection and Hybrid Machine Learning Technique. *16th International Conference on ICT and Knowledge Engineering (ICT&KE)*. 2018. P.1–6. DOI:https://doi.org/10.1109/ICTKE.2018.8612331.

86. Kumar Kaushal. Network Intrusion Detection with Feature Selection Techniques using Machine-Learning Algorithms. *International Journal of Computer Applications.* 2016. Vol.150. P.1–13. DOI:https://doi.org/10.5120/ijca2016910764.

87. X. Zheng, Y. Wang, L. Jia, D. Xiong and J. Qiang. Network Intrusion Detection Model based on Chi-square Test and Stacking Approach. *7th International Conference on Information Science and Control Engineering (ICISCE).* Changsha, China. 2020. P. 894–899. DOI:https://doi.org/ 10.1109/ICISCE50968.2020.00185.

88. Choudhary, Sarika & Kesswani, Nishtha. Analysis of KDD-Cup'99, NSL-KDD and UNSW-NB15 Datasets using Deep Learning in IoT. *Procedia Computer Scienc*e. 2020. Vol.167. P.1561–1573. DOI:https://doi.org/10.1016/j.procs.2020.03.367.

89. Hota H. & Shrivas, Akhilesh. Decision Tree Techniques Applied on NSL-KDD Data and Its Comparison with Various Feature Selection Techniques. *Smart Innovation, Systems and Technologies*. 2014. Vol. 27. P.205–212. DOI:https://doi.org/10.1007/978-3-319-07353-8_24.

90. A. Rashid, M. J. Siddique and S. M. Ahmed. Machine and Deep Learning Based Comparative Analysis Using Hybrid Approaches for Intrusion Detection System. *2020 3rd International Conference on Advancements in Computational Sciences (ICACS).* Lahore, Pakistan. 2020. P. 1–9.

DOI:https://doi.org/10.1109/ICACS47775.2020.9055946.

91. Malhotra Heena, Sharma Prabha. Intrusion Detection using Machine Learning and Feature Selection. *International Journal of Computer Network and Information Security.* 2019. Vol.11. P.43–52. DOI:https://doi.org/10.5815/ijcnis.2019.04.06.

92. Ingre B., Yadav A. Performance analysis of NSL-KDD dataset using ANN. In: *2015 International Conference on Signal Processing And Communication Engineering Systems (SPAC-ES). IEEE.* 2015. P. 92–96. DOI:https://doi.org/10.1109/spaces.2015.7058223.

93. Osanaiye O., Cai H., Choo K.-K. R., Dehghantanha A., Xu Z., Dlodlo M. Ensemble-based multi-filter feature selection method for DDoS. detection in cloud computing. EURASIP *Journal on Wireless Communications and Networking*. 2016. Vol.1. P.1–10. DOI:https://doi.org/10.1186/s13638-016-0623-3.

94. Liu H., Yan X., Wu Q. An Improved Pigeon-Inspired Optimisation Algorithm and Its Application in Parameter Inversion. *Symmetry*. 2019. Vol.11(10). P. 1291. DOI:https://doi.org/10.3390/sym11101291.

95. Kasongo S. M., Sun Y. Performance Analysis of Intrusion Detection Systems Using a Feature Selection Method on the UNSW-NB15 Dataset. *Journal of Big Data.* 2020. Vol. 7(1). P.105. DOI: https://doi.org/10.1186/s40537-020-00379-6.

96. Wang X., Zhou Y. Multi-Label Feature Selection with Conditional Mutual Information. *SSRN Electronic Journal.* 2022. Режим доступу URL: DOI:https://doi.org/10.2139/ssrn.4153295. (дата звернення 30.12.2022).

97. Sara Hooker, Dumitru Erhan, Pieter-Jan Kindermans, Been Kim. Evaluating feature importance estimates. 2018. Режим доступу URL:

https://doi.org/10.48550/arXiv.1806.10758.(дата звернення 04.12.2019).

98. Rengasamy D., Rothwell B. C., Figueredo, G. P. Towards a More Reliable Interpretation of Machine Learning Outputs for Safety-Critical Systems Using Feature Importance Fusion. *Applied Sciences*. 2021. Vol.11(24). P.11854.

DOI:https://doi.org/10.3390/app112411854.

99. Souhail et. al., M. Network Based Intrusion Detection Using the UNSW-NB15 Dataset. *International Journal of Computing and Digital Systems*. 2019. Vol.8(5). P. 477–487. DOI:https://doi.org/10.12785/ijcds/080505.

100. Rengasamy, Divish Mafeni Mase, Jimiama Rothwell, Benjmain Torres, Mercedes Alexander, Morgan Winkler, David Figueredo, Grazziela. Feature Importance in Machine Learning Models. *A Fuzzy Information Fusion Approach. Neurocomputing.* 2022. P.511. DOI:https://doi.org/10.1016/j.neucom.2022.09.053.

101. Barredo Arrieta A., Díaz-Rodríguez N., Del Ser J., Bennetot A., Tabik S., Barbado A., Garcia S., Gil-Lopez S., Molina D., Benjamins R., Chatila R., Herrera F. Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. *Information Fusion.* 2020. Vol.58. P.82–115. DOI:https://doi.org/10.1016/j.inffus.2019.12.012

102. Rani D., Gill N. S., Gulia P., & Chatterjee J. M. An ensemble-based multiclass classifier for intrusion detection using internet of things. *Computational Intelligence and Neuroscience*. 2022. P.1–16. DOI:https://doi.org/10.1155/2022/1668676.

103. Guo G. A machine learning framework for intrusion detection system in iot networks using an ensemble feature selection method. In 2021 *IEEE 12th annual information technology, electronics and mobile communication conference (IEMCON)*, *IEEE.* (2021). DOI:https://doi.org/10.1109/iemcon53756.2021.9623082.

104. Thockchom N., Singh M.M. & Nandi U. A novel ensemble learning-based model for network intrusion detection. *Complex Intell. Syst*. 2023. Vol.9. P.5693–5714. DOI:https://doi.org/10.1007/s40747-023-01013-7.

105. A. Subasi, S. Algebsani, W. Alghamdi, E. Kremic, J. Almaasrani, N. Abdulaziz. Intrusion detection in smart healthcare using bagging ensemble classifier. in *International Conference on Medical and Biological Engineering.* 2021. P. 164–171. DOI:https://doi.org/10.1007/978-3-030-73909-6_18.

106. Khan Muhammad Almas, Khattak Muazzam, Latif Shahid, Shah Awais, Rehman Mujeeb, Boulila Wadii, Driss Maha, Ahmad Jawad. Voting Classifier-Based Intrusion Detection for IoT Networks. *Advances on Smart and Soft Computing*.2022. P.313–328. DOI:https://doi.org/10.1007/978-981-16-5559-3_26.

107. Alotaibi Yazeed, Ilyas Mohammad. Ensemble-Learning Framework for Intrusion Detection to Enhance Internet of Things' Devices Security. *Sensors*. 2023. Vol.23. P.5568. DOI:https:// doi.org/10.3390/s23125568.

108. Aleesa Ahmed, Bahaa Bilal, Zaidan A., Sahar Nan. Review of intrusion detection systems based on deep learning techniques: coherent taxonomy, challenges, motivations, recommendations, substantial analysis and future directions. *Neural Computing and Applications*. 2020. P.32. DOI:https:/ doi.org/10.1007/s00521-019-04557-3.

109. Bayu Adhi Tama, Sunghoon Lim. Ensemble learning for intrusion detection systems: A systematic mapping study and cross-benchmark evaluation. *Computer Science Review*. 2021. Vol.39. P.100357. DOI:https:// doi.org/10.1016/j.cosrev.2020.100357.

110. S. Krishnaveni, S. Sivamohan, S. Sridhar, S. Prabakaran. Efficient feature selection and classification through ensemble method for network intrusion detection on cloud computing. *Cluster Computing* .2021. Vol.24(3). P.1761–1779. DOI:https://doi.org/10.1007/s10586-020-03222-y

111. Ye S.C., Wu K.H., Niu Y.G. A method for information security risk assessment based on fuzzy operator. *Advanced Materials Research.* 2014. Vol.850-851. P. 454-457.

112. Ming-Chang Lee. Information Security Risk Analysis Methods and Research Trends: AHP and Fuzzy Comprehensive Method. National Kaohsiung University of Applied Science, Taiwan. *International Journal of Computer Science & Information Technology (IJCSIT)*. 2014. Vol 6, No1, Feb.2014. P.29-45. DOI : 10.5121/ijcsit.2014.6103 .

113. Lee Z.J., Chang L.Y. Apply fuzzy decision tree to information security assessment . *International Journal of Fuzzy Systems*. 2014. Vol. 16, Issue 2. P. 265–269.

114. Tamjidyamcholo A., Yamchello H.T., Bin M.S., Gholipour R.Application of fuzzy set theory to evaluate the rate of aggregative risk in information security: *Proceedings of 2013 International Conference on Research and Innovation in Information Systems: ICRIIS 2013*. Kuala Lumpur, Malaysia,27 November. P. 410–415.

115. Peng X., Cui J.Q. Network security risk assessment based on fuzzy analytical hierarchy process. *Applied Mechanics and Materials.* 2014. Vol. 631-632. P. 971–975.

116. Довбешко С.В., Толюпа С.В., Шестак Я.В. Застосування методів інтелектуального аналізу даних для побудови систем виявлення атак. *Сучасний захист інформації* . 2019. No1(37). С 6–15.

117. Міщенко А.В., Курило О.В., Золотухіна О.А. Нечітка модель оцінки ризиків інформаційної безпеки та підтримки рівня захищеності ERP-систем. *Телекомунікаційні та інформаційні технології*. 2020. №1(66). С.142-151. DOI: 10.31673/2412-4338.2020.011451

118. R. Shanmugavadivu, Dr.N.Nagarajan. Network Intrusion Detection System using Fuzzy Logic. *Indian Journal of Computer Science and Engineering.* 2011. Vol.2. Режим доступу URL:https://www.researchgate.net/publication/50417996_Network_Intrusion_Detection_System_using_Fuzzy_Logic(дата звернення 04.12.2019).

119. Almseidin M., Kovács S. Intrusion Detection Mechanism Using Fuzzy Rule Interpolation. 2019. ArXiv, abs/1904.08790.

120. M. Nalayini C., Katiravan, J. A. New IDS for Detecting DDoS Attacks in Wireless Networks using Spotted Hyena Optimization and Fuzzy Temporal CNN. *Journal of Internet Technology*. 2023. Vol.24(1). P.23–34. Режим доступу URL:

https://jit.ndhu.edu.tw/article/view/2836(дата звернення 31.03.2023).

121. Naik Nitin, Diao Ren, Shen, Qiang. Dynamic Fuzzy Rule Interpolation and Its Application to Intrusion Detection. *IEEE Transactions on Fuzzy Systems*. 2017. P. 1–1. DOI:https:// doi.org/10.1109/TFUZZ.2017.2755000.

122. Deka Rup,Bhattacharyya Dhruba K., Kalita Jugal. Active learning to detect DDoS attack using ranked features. *Computer Communications*. 2019. P.145. DOI:https:// doi.org/10.1016/j.comcom.2019.06.010.

123. Benaddi Hafsa, Ibrahimi Khalil, Benslimane Abderrahim. Improving the Intrusion Detection System for NSL-KDD Dataset based on PCA-Fuzzy Clustering-KNN. *WINCOM*. 2018. P. 1–6. DOI:https:// doi.org/10.1109/WINCOM.2018.8629718.

124. Pullagura Indira, Anuradha G. A novel ensemble modeling for intrusion detection system. *International Journal of Electrical and Computer Engineering (IJECE)*. 2020. Vol.10. P.1963–1971. DOI:https:// doi.org/10.11591/ijece.v10i2.pp1963-1971.

125. IDS 2018 Intrusion CSVs (CSE-CIC-IDS2018). Режим доступу URL: https://www.kaggle.com/datasets/solarmainframe/ids-intrusion-csv(дата звернення 04.05.2020).

126. Aggarwal P., Sharma S. K. Analysis of KDD dataset attributes - class wise for intrusion detection. *Procedia Computer Science.* 2015. Vol.57. P.842–851. DOI:https://doi.org/10.1016/j.procs.2015.07.490.

127. NSL-KDD dataset. Режим доступу URL: http://www.unb.ca/research/iscx/dataset/iscx-NSL-KDD-dataset.html. (дата звернення 01.06.2022).

128. Moustafa Nour, Slay Jill. UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). 2015. Режим доступу URL: https://doi.org/10.1109/MilCIS.2015.7348942. (дата звернення 04.06.2019).

129. Damasevicius R., Venckauskas A., Grigaliunas S., Toldinas J., Morkevicius N., Aleliunas T., Smuikys, P. LITNET-2020: An annotated real-world network flow dataset for network intrusion detection. *Electronics.* 2020. Vol.9(5). P. 800. DOI:https://doi.org/10.3390/electronics9050800.

130. Tian Luyao, Lu Yueming. An Intrusion Detection Model Based on SMOTE and Convolutional Neural Network Ensemble. *Journal of Physics: Conference Series*. 2021. Vol.1828. P.012024. DOI:https://doi.org/10.1088/1742-6596/1828/1/012024.

131. Alshamy Reem, Ghurab Mossa, Othman Suad, Alshami Faisal. Intrusion Detection Model for Imbalanced Dataset Using SMOTE and Random Forest Algorithm. 2021. Режим доступу URL: DOI:https://doi.org/10.1007/978-981-16-8059-5_22. (дата звернення 04.05.2022).

132. A. Abdullah Alfrhan, R. Hamad Alhusain, R. Ulah Khan. SMOTE: Class Imbalance Problem In Intrusion Detection System. *2020 International Conference on Computing and Information Technology (ICCIT-1441*), Tabuk, Saudi Arabia. 2020. P. 1–5. DOI:https://doi.org/10.1109/ICCIT-144147971.2020.9213728.

133. Cyber espionage and sabotage attacks pose an increasing threat to the energy industry. *Help Net Security*. Режим доступу URL: https//www.helpnetsecurity.com/2019/04/17/energy-industry-threat/ (дата звернення 04.05.2019).

134. Evaluating the biggest cyber threats to the electric power sector. Режим доступу URL: https//www.helpnetsecurity.com/2019/02/04/cyber-threats-electric-power-sector/ (дата звернення 04.05.2019).

135. Zeljka Zorz, Building a sound security strategy for an energy sector company. *Help Net Security* .2019. July 30 Режим доступуURL: https://www.helpnetsecurity.com/2018/07/30/security-strategy-energy-sector-company/(дата звернення 04.05.2019).

136. Which organizations place a premium on security and privacy? Режим доступу URL:https//www.helpnetsecurity.com/2019/04/18/2018-online-trust-audit-

and-honor-roll (дата звернення 04.05.2019).

137. John DiLullo, The perimeter is vanishing, how will you secure your network? *Help Net Security.* 2019. Apr. 18. Режим доступу URL: https//www.helpnetsecurity.com/2019/04/18/secure-vanishing-perimeter/ (дата звернення 04.05.2019.

138. One hundred percent of endpoint security tools eventually fail. *Help Net Security* .2019). April 18. Режим доступу URL:https://www.helpnetsecurity.com/2019/04/18/2019-global-endpoint-security-trends-report/(дата звернення 04.05.2019).

139. Robert MacDonald, Employee cybersecurity essentials part 2: Lost devices and unsafe connections. *Help Net Security* .2019. April 6. Режим доступу URL: https//www.helpnetsecurity.com/2019/04/16/employee-cybersecurity-essentials-part-2-lost-devices-and-unsafe-connections/(дата звернення 08.05.2019).

140. Bad security hygiene still a major risk for enterprise IT networks Режим доступу URL:https //www.helpnetsecurity.com/2019/04/16/bad-security-hygiene/(дата звернення 08.05.2019).

141. Basic rules of cyber hygiene, April 20 (2019). Режим доступу URL: https://cert.gov.ua/recommendations/21(дата звернення 10.05.2019).

142. Про електронні документи та електронний документообіг :Закону України від 22.05.2003р. станом 01.08.2022р. № 851-IVВерховна Рада України; Законодавство України. Режим доступу URL: https://zakon.rada.gov.ua/laws/show/851-15#Text (дата звернення 04.10.2022).

143. Common Vulnerability Scoring System v3.1. Режим доступу URL:https://www.first.org/cvss/v3.1/user-guide(дата звернення 10.01.2021).

144. Shushura O. M. Infological modeling of information systems subject industries IN solving of fuzzy control tasks. *Зв'язок.* 2018. № 2. С. 53–56.

145. Т. Саати. Принятие решений. Метод анализа иерархий. – М. Радио и связь, 1993. — 278 с.

146. Levin I. KDD-99 Classifier Learning Contest I. Levin. LLSoft's Results Overview. *SIGKDD Explorations* 2010. P. 67–75.

147. Lippmann R. P. Evaluating Intrusion Detection Systems: The 1998 DARPA off-line intrusion detection evaluation // R. P. Lippmann, D. J. Fried, I. Graf, J. W. Haines, K. Kendall, D. McClung, D. Webber, S. Webster, D. Wyschograd, R. Cunninghan, M. Zissman. – DARPA, 2000.

148. Tavallaee M.,A. Tavallaee, E. Bagheri ,W. Lu A. Ghorbani.Detailed Analysis of the KDD CUP 99 Data Set : *Submitted to Second IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA)* 2009.

149. Knowledge discovery in databases DARPA. Archive University of California. Режим доступу URL: http://www.kdd.ics.uci.edu/ databases/kddcup99/task.html (дата звернення: 29.01.2019).

150. Prihantono Y., Kalamullah Ramli. Model-Based Feature Selection for Developing Network Attack Detection and Alerting System. Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi). 2022. Vol.6(2), P. 322–329. DOI:https://doi.org/10.29207/resti.v6i2.3989.

151. Damaševičius R., Venčkauskas Alg., Grigaliunas S., Toldinas J., Morkevicius N., Aleliūnas T., Smuikys P. LITNET-2020: An Annotated Real-World Network Flow Dataset for Network Intrusion Detection. *Electronics.* 2020. Vol. 9. 800. DOI:https://doi.org/10.3390/electronics9050800.

152. Jundong Li, Kewei Cheng, Suhang Wang, Fred Morstatter, Robert P. Trevino, Jiliang Tang, and Huan Liu. Feature Selection: A Data Perspective. *ACM Comput*. 2017. Surv. 50, 6. Article 94 (Nov.2018), 45p. DOI:https://doi.org/10.1145/3136625

153. Huan Liu and Lei Yu. Toward Integrating Feature Selection Algorithms for Classification and Clustering. *IEEE Trans. on Knowl. and Data Eng.* 2005. Vol.17, No.4, Apr.2005. P. 491–502. DOI:https://doi.org/10.1109/TKDE.2005.66

154. Breiman L. Classification and Regression Trees (1st ed.). Routledge.

2017. Режим доступу URL: DOI:https://doi.org/10.1201/9781315139470(дата звернення: 29.01.2022).

155. Khaire U., Dhanalakshmi, R. Stability of Feature Selection Algorithm: A Review. *Journal of King Saud* University - Computer and Information Sciences. 2019. P.34. DOI:https://doi.org/10.1016/j.jksuci.2019.06.012.

156. Kamalov F., Thabtah F., Leung H.H. Feature Selection in Imbalanced Data. Ann. Data. Sci. (2023). Vol. 10. P.1527–1541 DOI:https://doi.org/10.1007/s40745-021-00366-5

157. Teukolsky S.A., Flannery B.P., Press W.H.,Vetterling W.T. Numerical Recipes in C; SMR.693; *WH Press: Cambridge, MA, USA*, 1992.

158. Li Y., Fang B.X., Chen, Y., Guo, L. A lightweight intrusion detection model based on feature selection and maximum entropy model: *In Proceedings of the 2006 International Conference on Communication Technology, Guilin, China, 27–30 November 2006*. 2006.P. 1–4.

159. Liu H., Setiono R. Chi2: Feature selection and discretization of numeric attributes: *In Proceedings of the 7th IEEE International Conference on Tools with Artificial Intelligence, Herndon, VA, USA, 5–8 November 1995*. 1995. P. 388–391.

160. Salzberg, S.L. C4.5: Programs for Machine Learning by J. Ross Quinlan. Morgan Kaufmann Publishers, Inc., 1993, Mach. 1994. Learn 16. P. 235–240 Режим доступу URL: https://doi.org/10.1007/BF00993309 (дата звернення 02.06.2022)

161. Cover T.M., Thomas J.A. Elements of Information Theory. Wiley: Hoboken, NJ, USA. 2012.

162. S. Galli, Feature Selection for Machine Learning - Code Repository. Режим доступу URL: https://github.com/solegalli/feature-selection-formachine-learning, Feb. 2018. (дата звернення 02.06.2022)

163. Uriz Mikel, Paternain Daniel, Dominguez-Catena Iris, Sola Humberto, Galar Mikel. Unsupervised Fuzzy Measure Learning for Classifier Ensembles From Coalitions Performance. *IEEE Access.* 2020. P. 1–1.

DOI:https://doi.org/10.1109/ACCESS.2020.2980949.

164. Kuncheva L.I. Fuzzy Classifier Design. *Springer-Verlag*. Heidelberg, May 2000. DOI:https://doi.org/10.1007/978-3-7908-1850-5.

165. Chakir El. Mostapha, Moughit Mohamed, Idrissi Khamlichi Youness. Building an Efficient Alert Management Model for Intrusion Detection Systems. *Advances in Science, Technology and Engineering Systems Journal(ASTESJ)*. 2018. Vol.3. P.18–24. DOI:https://doi.org/10.25046/aj030103.

166. Youssef Ben , Nada Mannane, Bendriss Elmehdi, Boubker Regragui. Intrusion detection in cloud computing based attack patterns *and risk assessment. Advances* in Science, Technology and Engineering Systems Journal. 2017. Vol.2. P.479–484. DOI:https://doi.org/10.25046/aj020361.

167. Charhi Y. Ben., Mannane N., Bendriss E. , Regragui B. Intrusion detection in cloud computing based attacks patterns and risk assessment: *2016 Third International Conference on Systems of Collaboration (SysCo)*. *Casablanca Morocco*. 2016, P. 1–4. DOI:https://doi: 10.1109/SYSCO.2016.7831341.

168. Ekelhart A., Fenz S., Klemen M., Weippl E. Security Ontologies: Improving Quantitative Risk Analysis: 2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07), Waikoloa, HI, USA. 2007. P. 156a–156a, DOI:https://doi: 10.1109/HICSS.2007.478.

169. GNS3. The software that empowers network professionals. Режим доступу URL: https://www.gns3.com/ (дата звернення 20.07.2022).

ДОДАТОК А
СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА

Наукові праці, в яких опубліковані основні наукові результати дисертації:

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.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

8. Чичкарьов Є.А., Зінченко О.В., Бондарчук А.П., Асєєва Л.А. Використання алгоритмів машинного навчання і нечіткої логіки для виявлення мережевих вторгнень з використанням комплексу наборів даних. *«Systems and measures of artificial intelligence» AIIS'2023International scientific youth school*: Матеріали Міжнародної наукової молодіжної школи «Системи та засоби штучного інтелекту», м. Київ, 10–11 жовт.2023 р. / ІПШІ «Наука і освіта» Київ, 2023. С. 13 – 15.

9. Кожухівський А.Д., Асєєва Л.А. Оцінка ризиків конфіденційності документів проектів з застосуванням нечіткої логіки. *Проблеми інформатики та комп'ютерної техніки*: Праці Х-ї Міжнародної наук.-практ. конф. (ПІКТ – 2021), м. Чернівці, 28 – 31 жовтня 2021 р. / Чернівці, 2021. С. 109–112.

10. Асєєва Л.А. Формалізація функції належності нечітких факторів управління інформаційною безпекою підприємства з використанням методу аналізу ієрархій. *IX Всеукраїнська науково-практична конференція з автоматичного управління* : Матеріали IX Всеукраїнської наук.-практ. конф. здобув. вищої освіти та молодих вчених з автоматичного управління присвяченої Дню космонавтики, м. Херсон, 12 – 14 квітня 2021 р. / Ред. Г.В. Рудакової та ін. Херсон: Видавництво ФОП Вишемирський В.С. Херсон, 2021. С. 36.

11. Кожухівський А.Д., Асєєва Л.А. Нечітке управління ризиками в інформаційній безпеці підприємства. *Комп'ютерна математика в науці, інженерії та освіті CMSEE-2020* : Матеріали V Всеукраїнської наук.-техн. конф., м. Полтава, 27 листопада 2020 р. / ред.: О.М. Гайтан – Полтава: Національний університет «Полтавська політехніка імені Юрія Кондратюка», 2020., С.69–70.

12. Асєєва Л.А. Підходи до класифікації складових небезпеки при побудові систем управління інформаційною безпекою підприємств. *VIII Всеукраїнська науково-практична конференція з автоматичного управління* : Матеріали VIII

Всеукраїнської наук.-практ.конф. студентів, аспірантів та молодих вчених з автоматичного управління присвяченої Дню космонавтики, м.Херсон, 08 – 10 квітня 2020р./ Ред. Г.В. Рудакової та ін. Херсон: Видавництво ФОП Вишемирський В.С. Херсон, 2020. С.41.

13. Асєєва Л.А. Аналіз загроз інформаційної безпеки будівельного підприємства. *Проблеми інформатизації*: тези доп. тринадцятої міжнародної наук.-техн.конф., 11-12 квітня 2019 р./ Київ: ДУТ, НТУ; Полтава: ПНТУ; Катовице: КЕУ; Париж: Університет Париж VII Вєнсент-Сен-Дені; Вільнюс: ВДТУ; Харків : ХНДІТМ: Білорусь: БДАЗ; Кропивницький: ЛА НАУ, 2019. С.182.

14. Асєєва Л.А. Система управління інформаційною безпекою будівельного підприємства на принципах нечіткої логіки. *Проблеми інформатизації* : тези доп. дванадцятої міжнародної наук.-техн.конф., 12 - 13 грудня. – 2018р./ Київ : ДУТ, НТУ; Полтава: ПНТУ; Катовице: КЕУ; Париж: Університет Париж VII Вєнсент-Сен-Дені; Вільнюс: ВДТУ; Харків : ХНДІТМ: Білорусь: БДАЗ, 2018. С.146–147.

Відомості про апробацію результатів дисертації

1. XXIII Міжнародна науково-технічна конференція «Штучний інтелект та інтелектуальні системи» (AIIS’2023) (10-11 жовтня 2023, м.Київ.);

2. X Міжнародна науково-практична конференція «Проблеми інформатики та комп’ютерної техніки» (ПІКТ – 2021) (28 – 31 жовтня 2021, м.Чернівці);

3. IX Всеукраїнська науково-практична конференція здобувачів вищої освіти та молодих вчених з автоматичного управління (12 – 14 квітня 2021, м. Херсон);

4. V Всеукраїнська науково-технічна конференція «Комп’ютерна

математика в науці, інженерії та освіті CMSEE-2020» (27 листопада 2020, м. Полтава);

5. VIII Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених з автоматичного управління (08 – 10 квітня 2020, м. Херсон);

6. Тринадцята міжнародна науково-технічна конференція «Проблеми інформатизації» (11-12 квітня 2019, Київ-Полтава-Катовице-Париж-Вільнюс-Харків-Мінськ) ;

7. Дванадцята міжнародна науково-технічна конференція «Проблеми інформатизації» (12-13 грудня 2018 Київ-Полтава-Катовице-Париж-Вільнюс-Харків-Мінськ).

ДОДАТОК Б

АКТИ ВПРОВАДЖЕННЯ

HUAWEI

ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ «ХУАВЕЙ УКРАЇНА»
LIMITED LIABILITY COMPANY "HUAWEI UKRAINE"
ТОВ «ХУАВЕЙ УКРАЇНА» / LLC "HUAWEI UKRAINE"

03124, Київ, вул. Радищева, буд. 10/14, (ідентифікаційний код: 33501267), тел. 498-77-18, факс 498-77-19
10/14, Radischeva street, Kiev, 03124, Ukraine, (Company Code: 33501267), tel. 498-77-18, fax 498-77-19

ЗАТВЕРДЖУЮ
Заступник директора з питань персоналу
ТОВ "Хуавей Україна"
_____ В.Б. Білавка
(підпис, ініціали, прізвище)
«26» 09 2023 р.

АКТ
про реалізацію результатів дисертаційної роботи
Асєєвої Людмили Анатоліївни
на тему: «Управління інформаційною безпекою підприємства з використанням методів машинного навчання та нечіткої логіки»

Результати наукових досліджень Асєєвої Людмили Анатоліївни, а саме гібридний метод виявлення вторгнень до корпоративної мережі та метод обрання ознак для навчання моделей класифікації вторгнень, використано в науково-дослідних і дослідно-конструкторських роботах, що ведуться в ТОВ "Хуавей Україна".

Застосування розроблених Асєєвою Л.А. методів дає можливість збільшити швидкодію та точність роботи аналітичного блоку системи управління інформаційною безпекою у складі інформаційної системи підприємства. Перевірка на контрольних наборах даних виявила, що використання вказаних методів дозволяє скоротити час навчання моделей класифікації вторгнень в середньому на 52,4%, зменшити час виявлення вторгнень в середньому на 36,2% та збільшити точність виявлення в середньому на 3,8%.

Заступник директора з питань персоналу ТОВ "Хуавей Україна" В.Б. Білавка

www.huawei.com

ЗАТВЕРДЖУЮ

Директор ТОВ «РЕНТСОФТ»

_____ С.М. Лисенко

«26» 09 _____ 2023 року

АКТ

про реалізацію результатів наукових досліджень Асєєвої Людмили Анатоліївни на тему: «Управління інформаційною безпекою підприємства з використанням методів машинного навчання та нечіткої логіки» за спеціальністю 125 «Кібербезпека», а саме:

- гібридного методу виявлення вторгнень до корпоративної мережі, що використовує ансамблевий підхід на базі алгоритмів нечіткої логіки для поєднання результатів класифікації даних окремими моделями машинного навчання;
- методу обрання набору ознак для навчання класифікаторів вторгнень, який базується на ансамблевому підході з використанням нечіткої логіки для оцінки важливості ознаки;
- моделі 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.

Використання вказаних наукових результатів дозволяє збільшити точність виявлення вторгнень до корпоративної мережі підприємства у порівнянні з існуючими методами на 3-5%. Застосування запропонованого Асєєвою Л.А. 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.

Зазначені результати дають можливість підвищити рівень інформаційної безпеки підприємства.

Даний акт не є підставою для фінансових взаєморозрахунків.

Керівник проектів з впровадження
інформаційних систем, доктор технічних наук О.М. Шушура

„ЗАТВЕРДЖУЮ"

Проректор з навчально-виховної та наукової роботи ДУІКТ, доктор технічних наук, професор

Любов БЕРКМАН

_____ 2023р.

АКТ

використання у навчальному процесі Навчально-наукового інституту інформаційних технологій результатів дисертаційної роботи асистента кафедри комп'ютерної інженерії Державного університету інформаційно-комунікаційних технологій Асєєвої Людмили Анатоліївни на тему: «Управління інформаційною безпекою підприємства з використанням методів машинного навчання та нечіткої логіки» на здобуття наукового ступеня доктора філософії за спеціальністю 125 – Кібербезпека.

Комісія у складі:

голова – директор Наукового центру, кандидат технічних наук, професор Дробик О.В.; члени комісії – завідувачка кафедри штучного інтелекту, доктор технічних наук, доцент Зінченко О.В.; завідувачка кафедри комп'ютерної інженерії, кандидат технічних наук, доцент Лащевська Н.О.

розглянула дисертаційну роботу Асєєвої Людмили Анатоліївни на тему: «Управління інформаційною безпекою підприємства з використанням методів машинного навчання та нечіткої логіки» та публікації автора за матеріалами дисертаційної роботи. Результати впроваджено в начальний процес Навчально-наукового інституту інформаційних технологій, а саме:

1. 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.

2. 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.

3. 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.

На основі аналізу представлених матеріалів комісія встановила, що отримані наукові результати використовуються в навчальному процесі Державного університету інформаційно-комунікаційних технологій при викладанні навчальних дисциплін: «Захист інформації в інформаційно-комунікаційних системах», «Штучний інтелект» ОКР «Бакалавр» спеціальності 122 «Комп'ютерні науки» та «Моделі та методи прийняття рішень в комп'ютерних системах» ОКР «Магістр» спеціальності 123 «Комп'ютерна інженерія».

Голова комісії

Директор Наукового центру,
кандидат технічних наук, професор Олександр ДРОБИК

Члени комісії

Завідувачка кафедри штучного інтелекту,
доктор технічних наук, доцент Ольга ЗІНЧЕНКО

Завідувачка кафедри комп'ютерної інженерії,
кандидат технічних наук, доцент Наталія ЛАЩЕВСЬКА

ДОДАТОК В

ОПИС ОЗНАК НАБОРУ ДАНИХ CSE-CIC-IDS2018

Таблиця В.1

Ознаки набору даних CSE-CIC-IDS2018

№	Назва ознаки	Опис
1.	Flow Duration	Flow duration
2.	Tot Fwd Pkts	Total packets in the forward direction
3.	Tot Bwd Pkts	Total packets in the backward direction
4.	TotLen Fwd Pkts	Total size of packet in forward direction
5.	Fwd Pkt Len Max	Maximum size of packet in forward direction
6.	Fwd Pkt Len Min	Minimum size of packet in forward direction
7.	Fwd Pkt Len Mean	Average size of packet in forward direction
8.	Fwd Pkt Len Std	Standard deviation size of packet in forward direction
9.	Bwd Pkt Len Max	Maximum size of packet in backward direction
10.	Bwd Pkt Len Min	Minimum size of packet in backward direction
11.	Bwd Pkt Len Mean	Mean size of packet in backward direction
12.	Bwd Pkt Len Std	Standard deviation size of packet in backward direction
13.	Flow Byts/s	flow byte rate that is number of packets transferred per second
14.	Flow Pkts/s	flow packets rate that is number of packets transferred per second
15.	Flow IAT Mean	Average time between two flows
16.	Flow IAT Std	Standard deviation time two flows
17.	Flow IAT Max	Maximum time between two flows
18.	Flow IAT Min	Minimum time between two flows

19.	Fwd IAT Tot	Total time between two packets sent in the forward direction
20.	Fwd IAT Mean	Mean time between two packets sent in the forward direction
21.	Fwd IAT Std	Standard deviation time between two packets sent in the forward direction
22.	Fwd IAT Max	Maximum time between two packets sent in the forward direction
23.	Fwd IAT Min	Minimum time between two packets sent in the forward direction
24.	Bwd IAT Tot	Total time between two packets sent in the backward direction
25.	Bwd IAT Mean	Mean time between two packets sent in the backward direction
26.	Bwd IAT Std	Standard deviation time between two packets sent in the backward direction
27.	Bwd IAT Max	Maximum time between two packets sent in the backward direction
28.	Bwd IAT Min	Minimum time between two packets sent in the backward direction
29.	Fwd PSH Flags	Number of times the PSH flag was set in packets travelling in the forward direction (0 for UDP)
30.	Bwd PSH Flags	Number of times the PSH flag was set in packets travelling in the backward direction (0 for UDP)
31.	Fwd URG Flags	Number of times the URG flag was set in packets travelling in the forward direction (0 for UDP)
32.	Bwd URG Flags	Number of times the URG flag was set in packets travelling in the backward direction (0 for UDP)
33.	Fwd Header Len	Total bytes used for headers in the forward direction
34.	Bwd Header Len	Total bytes used for headers in the forward direction
35.	Fwd Pkts/s	Number of forward packets per second
36.	Bwd Pkts/s	Number of backward packets per second
37.	Pkt Len Min	Minimum length of a flow
38.	Pkt Len Max	Maximum length of a flow

39.	Pkt Len Mean	Mean length of a flow
40.	Pkt Len Std	Standard deviation length of a flow
41.	Pkt Len Var	Minimum inter-arrival time of packet
42.	FIN Flag Cnt	Number of packets with FIN
43.	SYN Flag Cnt	Number of packets with SYN
44.	RST Flag Cnt	Number of packets with RST
45.	PSH Flag Cnt	Number of packets with PUSH
46.	ACK Flag Cnt	Number of packets with ACK
47.	URG Flag Cnt	Number of packets with URG
48.	CWE Flag Count	Number of packets with CWE
49.	ECE Flag Cnt	Number of packets with ECE
50.	Down/Up Ratio	Download and upload ratio
51.	Pkt Size Avg	Average size of packet
52.	Fwd Seg Size Avg	Average size observed in the forward direction
53.	Bwd Seg Size Avg	Average size observed in the backward direction
54.	Fwd Byts/b Avg	Average number of bytes bulk rate in the forward direction
55.	Fwd Pkts/b Avg	Average number of packets bulk rate in the forward direction
56.	Fwd Blk Rate Avg	Average number of bulk rate in the forward direction
57.	Bwd Byts/b Avg	Average number of bytes bulk rate in the backward direction
58.	Bwd Pkts/b Avg	Average number of packets bulk rate in the backward direction
59.	Bwd Blk Rate Avg	Average number of bulk rate in the backward direction
60.	Subflow Fwd Pkts	The average number of packets in a sub flow in the forward direction
61.	Subflow Fwd Byts	The average number of bytes in a sub flow in the forward direction
62.	Subflow Bwd Pkts	The average number of packets in a sub flow in the backward direction
63.	Subflow Bwd Byts	The average number of bytes in a sub flow in the backward direction
64.	Init Fwd Win Byts	Number of bytes sent in initial window in the forward direction

65.	Init Bwd Win Byts	# of bytes sent in initial window in the backward direction
66.	Fwd Act Data Pkts	# of packets with at least 1 byte of TCP data payload in the forward direction
67.	Fwd Seg Size Min	Minimum segment size observed in the forward direction
68.	Active Mean	Mean time a flow was active before becoming idle
69.	Active Std	Standard deviation time a flow was active before becoming idle
70.	Active Max	Maximum time a flow was active before becoming idle
71.	Active Min	Minimum time a flow was active before becoming idle
72.	Idle Mean	Mean time a flow was idle before becoming active
73.	Idle Std	Standard deviation time a flow was idle before becoming active
74.	Idle Max	Maximum time a flow was idle before becoming active
75.	Idle Min	Minimum time a flow was idle before becoming active