

Міністерство освіти і науки України
Державний університет "Житомирська політехніка"

Кваліфікаційна наукова
праця на правах рукопису

КОВАЛЕВСЬКИЙ В'ЯЧЕСЛАВ ВАЛЕРІЙОВИЧ

УДК [004.421+004.42]:[004.056.5:004.738.5:339.1]

ДИСЕРТАЦІЯ

**АЛГОРИТМІЧНЕ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ АНАЛІЗУ
ЕФЕКТИВНОСТІ СИСТЕМ ЗАХИСТУ СЕРВІСІВ ЕЛЕКТРОННОЇ
КОМЕРЦІЇ**

121 Інженерія програмного забезпечення

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

/Ковалевський В.В.

Науковий керівник: Вакалюк Тетяна Анатоліївна, доктор педагогічних наук, професор, завідувач кафедри інженерії програмного забезпечення Державного університету «Житомирська політехніка»

Житомир – 2026

АНОТАЦІЯ

Ковалевський В.В. Алгоритмічне та програмне забезпечення аналізу ефективності систем захисту сервісів електронної комерції. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 121 "Інженерія програмного забезпечення". – Державний університет "Житомирська політехніка". – Житомир, 2026.

Зміст анотації.

Сервіси електронної комерції є невід’ємною частиною сучасного світу. Створюючи комфортні умови для взаємодії з користувачами, сервіси електронної комерції знаходяться в постійному фокусі уваги злоумисників та потребують неперервного розвитку і вдосконалення механізмів захисту. Ця частина функціонування сервісів електронної комерції залишається непомітною для користувачів, але потребує розуміння всіх аспектів їх роботи задля забезпечення балансу між захистом та збереженням позитивного досвіду користувачів від користування сервісом електронної комерції. Окремо стоїть питання забезпечення бізнес-показників вплив на які має впровадження безпекових механізмів без належної адаптації під особливості та потреби сервісу електронної комерції.

В контексті даного дослідження було проведено роботу з аналізу наявних підходів для побудови систем захисту для сервісів електронної комерції, проаналізовано публікації присвячені безпековим аспектам роботи сервісів електронної комерції. Проведений аналіз показав, що наявні підходи до побудови та оцінюванні систем захисту сервісів електронної комерції в першу чергу сфокусовані на технічних метриках та показниках і не забезпечують цілісної картини функціонування систем захисту сервісів електронної комерції. Зокрема, вплив безпекових подій та відповідних реакцій на них систем захисту на бізнес-показники залишається практично поза аналізом функціонування систем захисту. Традиційні механізми захисту та системи оцінки їх ефективності не враховують вплив на конверсію, довіру користувачів, критичність певних

етапів взаємодії користувачів з сервісом електронної комерції. В свою чергу це виливається у невдалі зміни налаштувань механізмів захисту приводячи до погіршення ситуації в цілому та негативному впливі на ключові бізнес-показники сервісу електронної комерції.

Метою дисертаційної роботи є розробка алгоритмів та програмного забезпечення аналізу ефективності систем захисту сервісів електронної комерції.

Дисертаційне дослідження викладено у трьох розділах, в яких подано та обґрунтовано основні результати проведеного дослідження.

У вступі обґрунтовано актуальність теми дослідження, визначено мету, завдання, об'єкт та предмет дослідження, описано методи дослідження, які використовувались при отриманні результатів дисертаційного дослідження, представлена наукова новизна, теоретичне та практичне значення отриманих результатів, наведено кількість публікацій та апробація результатів дослідження.

У першому розділі дисертаційної роботи проведено аналіз методів, засобів та технологій оцінки ефективності роботи систем захисту вебсервісів. Виконана робота над аналізом сучасних публікацій пов'язаних з проблемою оцінки ефективності роботи систем захисту сервісів електронної комерції. Проведено оцінку стану досліджень у галузі розробки та функціонування систем захисту сервісів електронної комерції. Проаналізовано сучасні системи захисту сервісів електронної комерції, а також аспекти використання систем штучного інтелекту в контексті безпекових механізмів сервісів електронної комерції.

Другий розділ дисертаційного дослідження присвячений розробці методу оцінки ефективності роботи системи захисту сервісу електронної комерції. Було обґрунтовано обрану архітектуру методу. Визначено основні критерії та показники необхідні для проведення аналізу ефективності роботи систем захисту сервісів електронної комерції. Обґрунтовано та розраховано коефіцієнти критичності етапів взаємодії користувачів з сервісом електронної комерції, що необхідно для подальшого оцінювання впливу систем захисту на бізнес-показники сервісу електронної комерції. Запропоновано формалізований метод визначення коефіцієнтів критичності етапів взаємодії користувачів з сервісом

електронної комерції, що забезпечує процедуру їх отримання та створює можливості для адаптації та відтворюваного застосування методу оцінювання ефективності роботи систем захисту сервісів електронної комерції до інших сервісів електронної комерції враховуючи специфіку їх функціонування. В рамках другого розділу дисертаційного дослідження розроблено та обґрунтовано математичну складову роботи методу оцінки ефективності роботи системи захисту сервісу електронної комерції. Запропоновано схему основних компонентів системи, що реалізують функціональну складову методу аналізу ефективності роботи системи захисту сервісів електронної комерції.

У третьому розділі проведено розробку алгоритмів методу, програмну реалізацію та експериментальну перевірку методу аналізу ефективності системи захисту сервісів електронної комерції. Визначено вимоги до зовнішньої системи збору та агрегації даних і розроблено специфікацію стандартизованого інтерфейсу, що забезпечує незалежність аналітичного модуля від конкретних технологій збору даних. Побудовано алгоритми розрахунку чотирьох показників ефективності, інтегрального індексу ефективності захисту, контекстного індексу з урахуванням часового та бізнес-факторів, а також системи формування рекомендацій. Для кожного алгоритму розроблено блок-схеми, визначено вхідні та вихідні дані, описано правила обробки особливих випадків. Виконано програмну реалізацію аналітичного модуля мовою Python із застосуванням модульної архітектури та вебінтерфейсом для візуалізації результатів. Розроблено систему моделювання взаємодії користувачів з сервісом електронної комерції. Проведено серію експериментів на даних створених з використанням системи моделювання, які підтвердили незалежність показників ефективності, коректність контекстної адаптації оцінки, здатність методу розмежовувати бізнес-контекст та позаштатні ситуації, а також його працездатність на різних часових масштабах аналізу.

Наукова новизна та теоретичне значення отриманих результатів полягають у тому, що:

вперше: формалізовано модель взаємодії користувачів з сервісами електронної комерції у вигляді послідовності з семи етапів та визначено коефіцієнти критичності етапів взаємодії із застосуванням методу аналізу ієрархій за п'ятьма критеріями оцінювання, що забезпечує формалізацію та відтворюваність процесу розрахунку; обґрунтовано систему з чотирьох показників ефективності роботи систем захисту сервісів електронної комерції: виявлення загроз, взаємодія з користувачами, якість реагування, покриття захистом етапів взаємодії користувачів з сервісом електронної комерції, та визначено їх вагові коефіцієнти із застосуванням методу аналізу ієрархій; запропоновано розрахунок контекстного індексу ефективності захисту, що додатково враховує контекст функціонування сервісів електронної комерції через часовий фактор та бізнес-фактор за допомогою коефіцієнта контекстної чутливості; розроблено метод аналізу ефективності системи захисту сервісів електронної комерції, що на відміну від наявних підходів, які фокусуються переважно на технічних параметрах, забезпечує урахування бізнес-контексту на трьох рівнях: через коефіцієнти критичності етапів взаємодії користувачів з сервісами електронної комерції, через коефіцієнт контекстної чутливості при розрахунку контекстного індексу ефективності захисту та через розрахунок пріоритетів проблемних аспектів при роботі системи рекомендацій;

удосконалено систему формування рекомендацій на основі оцінювання ефективності роботи систем захисту, що дозволяє провести діагностику стану показників та визначити пріоритети виявлених проблемних аспектів із урахуванням контексту роботи сервісу електронної комерції;

набули подальшого розвитку теоретичні та методичні засади побудови адаптивних рішень у сфері захисту сервісів електронної комерції.

Практичне значення отриманих результатів полягає в тому, що:

- розроблено специфікацію стандартизованого JSON-інтерфейсу, що формалізує комунікацію між зовнішніми джерелами даних та аналітичною складовою методу, що дозволяє уникнути залежності від конкретних зовнішніх систем та розширити можливості інтеграції

аналітичної складової методу з різними платформами електронної комерції та системами захисту;

- виконано програмну реалізацію прототипу аналітичного модуля мовою програмування Python із застосуванням модульної архітектури, що складається з чотирьох обчислювальних компонентів для відображення та аналізу отриманих даних;
- розроблено ряд алгоритмів, що забезпечують повний цикл функціонування аналітичної складової методу від отримання та перевірки вхідних даних до формування структурованого звіту рекомендацій;
- розроблено систему моделювання взаємодії користувачів з сервісом електронної комерції, що підтримує чотири базові сценарії (штатний режим, чорна п'ятниця, розпродаж, DDoS-атака), кожен з яких визначає характерні шаблони трафіку, розподіл безпекових подій та контекстні параметри, що дозволяє створювати вхідні дані із заданою часовою деталізацією для верифікації методу на різних масштабах аналізу;
- проведено серію з дев'яти експериментів, результати яких підтвердили незалежність показників, контекстну кореляцію результатів роботи систем захисту, коректне розмежування впливу бізнес-контексту та позаштатних ситуацій, а також чутливість методу на різних часових масштабах даних, що підтверджує можливість його практичного застосування у різних режимах роботи.

Матеріали дослідження можуть бути використані організаціями, що здійснюють діяльність у сфері електронної комерції, для аналізу та підвищення ефективності функціонування їхніх систем захисту.

Ключові слова: алгоритми, методи, показники ефективності, коефіцієнт ефективності, моделювання, система, прийняття рішень, метод аналізу ієрархій, електронна комерція, інформаційна безпека, інформаційна система, надійність, система підтримки прийняття рішень, класифікація даних, виявлення, архітектура системи, потік даних, структуризація багатовимірних даних.

ABSTRACT

Kovalevskyi V. V. Algorithmic and Software Solutions for Analyzing the Effectiveness of Security Systems of E-Commerce Services. – Qualification scientific work submitted as a manuscript.

Dissertation for the degree of Doctor of Philosophy (PhD) in specialty 121 “Software Engineering”. – Zhytomyr Polytechnic State University. – Zhytomyr, 2026.

Abstract content

E-commerce services are an integral part of the modern world. By creating a user-friendly environment for customer interaction, e-commerce services are constantly targeted by cybercriminals and require continuous development and improvement of their security mechanisms. This aspect of how e-commerce services operate remains invisible to users. However, it requires an understanding of all their functions to ensure a balance between security and a positive user experience. A separate issue is the impact on business performance metrics caused by the implementation of security mechanisms without proper adaptation to the specific features and needs of the e-commerce service.

In the context of this study, work was carried out to analyse existing approaches to building security systems for e-commerce services and to analyse publications dedicated to the security aspects of e-commerce services. The analysis revealed that existing approaches to the design and evaluation of security systems for e-commerce services primarily focus on technical metrics and indicators and do not provide a comprehensive picture of their functioning. In particular, the impact of security incidents and the corresponding responses by security systems on business metrics remains largely outside the scope of analysis of security system operations. Traditional security mechanisms and systems for assessing their effectiveness do not account for the impact on conversion rates, user trust, or the criticality of specific stages of user interaction with the e-commerce service. In turn, this results in unsuccessful changes to security mechanism settings, leading to a deterioration of the overall situation and a negative impact on the key business indicators of the e-commerce service.

This thesis aims to develop algorithms and software for analysing the effectiveness of security systems for e-commerce services.

The dissertation research is organised into three chapters, each of which presents and substantiates the main results of the study.

The introduction justifies the relevance of the research topic, defines the aim, objectives, object and subject of the research, describes the research methods used to obtain the results of the dissertation, presents the scientific novelty, theoretical and practical significance of the results obtained, and lists the number of publications and the validation of the research results.

The first chapter of the thesis analyses the methods, tools and technologies for assessing the effectiveness of web service security systems. An analysis has been conducted of contemporary publications on assessing the effectiveness of e-commerce service security systems. An assessment of the state of research in e-commerce service security system development and operation has been conducted. Modern e-commerce service protection systems were analysed, as well as aspects of the use of artificial intelligence systems in the context of e-commerce service security mechanisms.

The second chapter of the thesis is devoted to developing a method for assessing the effectiveness of e-commerce service protection systems. The chosen method architecture was justified. The main criteria and indicators necessary for analysing the effectiveness of e-commerce service protection systems have been identified. The criticality coefficients for the stages of user interaction with the e-commerce service have been justified and calculated, which are necessary for further assessment of the impact of protection systems on the e-commerce service's business indicators. A formalised method for determining the criticality coefficients of the stages of user interaction with an e-commerce service is proposed, which provides a procedure for their derivation and creates opportunities for the adaptation and reproducible application of the method for assessing the effectiveness of e-commerce service security systems to other e-commerce services, taking into account the specifics of their operation. In the second chapter of the dissertation, the mathematical component of the method for evaluating the effectiveness of an e-commerce service protection system

has been developed and justified. A diagram of the main components of the system that implement the method's functional component for analysing the effectiveness of an e-commerce service protection system is proposed.

In the third chapter, the algorithms of the method, the software implementation, and the experimental verification of the method for analysing the effectiveness of the e-commerce service protection system are presented. Requirements for an external data collection and aggregation system are defined, and a specification for a standardised interface is developed, ensuring the analytical module's independence from specific data collection technologies. Algorithms have been developed to calculate four performance indicators: an integrated protection effectiveness index, a contextual index that accounts for temporal and business factors, and a recommendation generation system. Block diagrams were developed for each algorithm, input and output data were defined, and rules for handling special cases were described. The analytical module was implemented in Python using a modular architecture and a web interface for visualising results. A system for modelling user interaction with an e-commerce service was developed. A series of experiments was conducted on data generated by the modelling system, which confirmed the independence of the performance indicators, the correctness of the contextual adaptation of the evaluation, the method's ability to distinguish between business context and exceptional situations, and its performance across different time scales of analysis.

Scientific novelty and theoretical significance of the results obtained lie in the fact that:

for the first time: a model of user interaction with e-commerce services has been formalised as a sequence of seven stages, and the criticality coefficients of the interaction stages have been determined using the hierarchical analysis method based on five evaluation criteria, ensuring the formalisation and reproducibility of the calculation process; a system of four performance indicators for e-commerce service protection systems has been substantiated: threat detection, interaction with users, quality of response, and protection coverage of the stages of user interaction with the e-commerce service; their weighting coefficients have been determined using the

hierarchical analysis method; a method for calculating a contextual protection effectiveness index has been proposed, which additionally accounts for the operational context of e-commerce services via a time factor and a business factor using a contextual sensitivity coefficient; a method has been developed for analysing the effectiveness of e-commerce service protection systems which, unlike existing approaches that focus primarily on technical parameters, ensures that the business context is taken into account at three levels: through the criticality coefficients of the stages of user interaction with e-commerce services, through the context sensitivity coefficient when calculating the contextual protection effectiveness index, and through the calculation of priorities for problematic aspects in the operation of the recommendation system;

improved the recommendation generation system based on the evaluation of the effectiveness of protection systems, which allows for the diagnosis of indicator status and the prioritisation of identified problematic aspects, taking into account the operational context of the e-commerce service;

further developed the theoretical and methodological foundations for building adaptive solutions in the field of e-commerce service protection.

The practical significance of the results obtained lies in the fact that:

- a specification for a standardised JSON interface has been developed, formalising communication between external data sources and the analytical component of the method, which allows avoiding dependence on specific external systems and expands the possibilities for integrating the analytical component of the method with various e-commerce platforms and security systems.

- a software implementation of the analytical module prototype has been carried out in the Python programming language using a modular architecture consisting of four computational components for displaying and analysing the data obtained;

- Several algorithms have been developed to ensure the full operational cycle of the analytical component of the method, from receiving and verifying input data to generating a structured report of recommendations.

- a system has been developed to model user interaction with an e-commerce service, supporting four basic scenarios (normal mode, Black Friday, sale, DDoS attack), each of which defines characteristic traffic patterns, the distribution of security events and contextual parameters, allowing input data to be generated with a specified temporal granularity for verifying the method at various scales of analysis;

- a series of eight experiments was conducted, the results of which confirmed the independence of indicators, the contextual correlation of security system performance, the correct differentiation between the influence of business context and abnormal situations, as well as the sensitivity of the method across different time scales of data, confirming its practical applicability in various operating modes.

The research materials can be used by organisations operating in e-commerce to analyse and improve the effectiveness of their security systems.

Keywords: algorithms, methods, performance indicators, efficiency coefficient, modelling, system, decision-making, hierarchical analysis method, e-commerce, information security, information system, reliability, decision support system, data classification, detection, system architecture, data flow, structuring of multidimensional data.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Публікації в наукових фахових виданнях України

1. Москалик Д.О., Антонюк Д.С., Вакалюк Т.А., Огінський Є.В., Ковалевський В. В. Огляд застосувань теорії графів у розробці та обслуговуванні програмних систем. *Computer Science and Applied Mathematics*. Запоріжжя: Видавничий дім «Гельветика», 2022. № 1. С. 75-82. DOI: [10.26661/2413-6549-2022-1-09](https://doi.org/10.26661/2413-6549-2022-1-09)
2. Ковалевський В.В., Вакалюк Т.А. Стан досліджень у галузі розробки та функціонуванні систем захисту сервісів електронної комерції. *Вчені записки Таврійського національного університету імені В.І. Вернадського. Серія: Технічні науки*, 2022. Том 33 (72), № 6. С. 92-98. DOI: [10.32782/2663-5941/2022.6/16](https://doi.org/10.32782/2663-5941/2022.6/16)
3. Ковалевський В.В., Вакалюк Т.А. Огляд наявних методів оцінки ефективності роботи систем захисту сервісів електронної комерції. *Вісник Херсонського національного технічного університету*, 2023. №3 (86). С. 102-110. DOI: [10.35546/kntu2078-4481.2023.3.13](https://doi.org/10.35546/kntu2078-4481.2023.3.13)
4. Ковалевський В.В., Вакалюк Т.А. Огляд сучасних систем захисту електронних сервісів. *Вісник Хмельницького національного університету. Серія: Технічні науки*, 2024. Том 337, №3(2). С. 176-182. DOI: [10.31891/2307-5732-2024-337-3-26](https://doi.org/10.31891/2307-5732-2024-337-3-26)
5. Ковалевський В., Вакалюк Т. Використання штучного інтелекту у системах захисту сервісів електронної комерції. *Інформаційні технології та суспільство*, 2025. №3 (18). С. 72-76. DOI: [10.32689/maup.it.2025.3.9](https://doi.org/10.32689/maup.it.2025.3.9)

Наукові праці, що засвідчують апробацію матеріалів дисертації

6. Ковалевський В.В., Вакалюк Т.А. Виклики у сфері захисту сервісів електронної комерції. *Наука, технології, інновації: світові тенденції та регіональний аспект : Матеріали VII Міжнародної науково-практичної конференції (м. Одеса, 27–28 вересня 2024 р.)* / ГО «Інститут інноваційної освіти»; Науково-навчальний центр прикладної інформатики НАН України. Одеса; Запоріжжя : АА Тандем, 2024. С. 62-64. <https://novaosvita.com/wp->

<content/uploads/2024/10/ScTechInn-Odesa-Sept2024.pdf>

7. Ковалевський В.В., Вакалюк Т.А., Необхідність розробки алгоритмічного та програмного забезпечення аналізу ефективності систем захисту сервісів електронної комерції. *Матеріали V Всеукраїнської науково-практичної інтернет-конференції студентів, аспірантів та молодих вчених за тематикою «Сучасні комп'ютерні системи та мережі в управлінні»*: збірка наукових праць /під редакцією А.А. Григорової. Херсон: Видавництво ФОП Вишемирський В. С., 2022. С. 22-23. <https://kntu.net.ua/ukr/content/download/99376/566912/file/CICT2022.pdf>

8. Ковалевський В.В. Безпекові виклики у сфері електронної комерції пов'язані з розвитком технологій штучного інтелекту. *Глобальні виклики та інновації: шляхи розвитку сучасної науки: збірник наукових праць з матеріалами IV Міжнародної наукової конференції, м. Львів, 11 липня, 2025 р.* Львів, 2025. С. 145-148. DOI: [10.62731/mcnd-11.07.2025.005](https://doi.org/10.62731/mcnd-11.07.2025.005)

ЗМІСТ

Перелік умовних скорочень	16
Вступ	17
РОЗДІЛ 1. Аналіз методів, засобів та технологій оцінки ефективності роботи систем захисту вебсервісів.....	25
1.1. Стан досліджень у галузі розробки та функціонуванні систем захисту сервісів електронної комерції	25
1.2. Огляд наявних методів оцінки ефективності роботи систем захисту сервісів електронної комерції	35
1.3. Огляд сучасних систем захисту електронних сервісів	46
1.4. Використання штучного інтелекту у системах захисту сервісів електронної комерції.....	57
Висновки до першого розділу	66
РОЗДІЛ 2. Метод оцінки ефективності роботи систем захисту сервісів електронної комерції.....	68
2.1. Проблеми оцінки ефективності захисту сервісів електронної комерції	68
2.2. Загальна архітектура методу аналізу ефективності системи захисту сервісів електронної комерції.	74
2.3. Коефіцієнти критичності етапів взаємодії користувача з сервісом електронної комерції.....	88
2.4. Аналітична складова методу аналізу ефективності системи захисту сервісів електронної комерції	114
Висновки до другого розділу.....	137
РОЗДІЛ 3. Алгоритми, та програмна реалізація методу аналізу ефективності системи захисту сервісів електронної комерції.....	139
3.1. Алгоритмічне забезпечення методу аналізу ефективності системи захисту сервісів електронної комерції	139
3.2. Програмна реалізація методу аналізу ефективності системи захисту сервісів електронної комерції та системи моделювання	163

3.3. Експериментальні дослідження методу аналізу ефективності системи захисту сервісів електронної комерції	181
Висновки до третього розділу	196
Висновки	199
Література.....	203
Додатки.....	220
Додаток А.....	220
Лістинги програмного коду.....	220
Додаток Б	252
Список публікацій здобувача за темою дисертації.....	252
Додаток В.....	252
Відомості про апробацію результатів дисертації.....	254
Додаток Г	255
Довідки про впровадження результатів дисертації	255
Додаток Д.....	258
Звіт подібності дисертації.....	258

Перелік умовних скорочень

Скорочення, термін, позначення	Пояснення
CSES	Cyberspace Security Econometrics System
CSF	критичних факторів успіху
CVE, NVD	відкриті бази даних вразливостей
CVSS	Common Vulnerability Scoring System
GNN	Graph Neural Networks
IDS/IPS	системи виявлення та запобігання вторгненням
KPI	ключових показників ефективності
LLM	Large Language Models
MFC	Mean Failure Cost – вартість відмови системи
NGFW	Next Generation Firewall
NIST CSF	National Institute of Standards and Technology's cybersecurity framework
SIEM	Security Information and Event Management
SOC	Security Operations Center
SSH	Протокол захищеного з'єднання
SSL	Протокол захищеної комунікації
TLS	захист на транспортному рівні
VPN	Virtual Private Network
WAF	Web Application Firewall,
ZTA	Zero Trust Architecture
БФ	Бізнес-фактор
ІЕЗ	індекс ефективності захисту
ІЕЗ _к	контекстний індекс ефективності захисту
ІПР	індекс пріоритету рекомендації
ККЧ	коефіцієнт контекстної чутливості
ЧФ	часовий фактор

Вступ

Актуальність дослідження. Різноманітні онлайн сервіси та додатки стали невід’ємною частиною сучасного життя. Величезна кількість конфіденційної інформації, зокрема й персональні та фінансові дані, передаються та обробляються під час користувацької активності в мережі Інтернет. Особливо це стосується сервісів електронної комерції, актуальність створення та використання яких збільшилась за останні роки, враховуючи обмеження, введені у зв’язку з пандемією. Надання послуг електронної комерції підвищує вимоги щодо забезпечення надійної обробки та збереження даних користувачів. Компанії постійно розвивають та вдосконалюють системи захисту сервісів, які вони надають, адже несанкціонований доступ несе не лише фінансові, а й репутаційні ризики, що можуть повністю знищити бізнес, який будувався роками.

Наразі наявна велика кількість різноманітних систем, що забезпечують захист та аналіз наявності потенційних загроз на різних рівнях функціонування сервісів та оточуючого їх середовища, починаючи з етапів розробки і закінчуючи безпосереднім впровадженням сервісу у роботу.

До систем захисту кінцевих продуктів, де відбувається взаємодія з користувачами, можна віднести системи ідентифікації користувачів, шифрування користувацького трафіку з використанням сучасних протоколів та шифрів, системи моніторингу та аналізу вхідних запитів користувачів.

Серед вчених, що займалися вивченням та розробкою теоретичних методів оцінювання захищеності та ефективності роботи систем захисту інформації можна відмітити В.О. Хорошко, Р.В. Гришук, О.Г. Корченко, І.Ю. Субач, О.Г. Оксіюк, О.К. Юдін, В.А. Савченко, К.В. Молодецька, С.В. Казмірчук, К.Д. Жук, Є.Г. Левченко, В.Л. Шевченко, Л. Гордона та інших.

Варто зазначити, що велику увагу даному питанню приділяли також закордонні вчені. Зокрема, Хеннес Холм (Hannes Holm) та Матіас Екстедт (Mathias Ekstedt) досліджували ефективність використання web application firewall для захисту від цілеспрямованих атак на вебсервіси [64]. Станіслав Даков

(Stanislav Dakov) та Анна Малинова (Anna Malinova) проводили аналіз актуальних загроз та засобів їх усунення для систем електронної комерції [50]. Ю. Вен (Yuanqiao Wen) та Ч. Жоу (Chunhui Zhou) та ін. опублікували статтю, у якій проводять аналіз безпекових загроз відносно систем електронної комерції [125]. А. І. Антон (Annie I. Antón) і Ю. Б. Ірп (Julia B. Earp) вивчали стратегії розробки політик та вимог для забезпечення захищеності сервісів електронної комерції [23].

Однак, проаналізувавши ці роботи, можна побачити, що є необхідність в розробці практичних алгоритмів та програмного забезпечення, які допоможуть проводити оцінку та оптимізацію функціонування систем захисту інформації.

Сучасні підходи до захисту сервісів електронної комерції являють собою багат шарову структуру, частини якої відповідають за різні аспекти роботи сервісу. Забезпечення захисту має бути на всіх етапах роботи з сервісом та гарантувати збереження і цілісність конфіденційних даних користувачів.

Найпоширенішим методом компрометації роботи сервісу електронної комерції є експлуатація наявних вразливостей платформи, на якій він побудований. До них можна віднести вразливості операційної системи серверної частини, застарілі протоколи шифрування, використання програмних вразливостей сервісу для віддаленого виконання шкідливих команд. Для запобігання цьому необхідно впроваджувати комплекс організаційних та технічних заходів, що забезпечують відповідність сучасним безпековим стандартам і надають можливість оперативно виявляти потенційні загрози. Одним з таких технічних заходів являється аналіз даних, що надходять до системи електронної комерції від користувачів та супутніх сервісів. Частково це може бути реалізовано безпосередньо на рівні самого сервісу електронної комерції, але більш надійним є використання безпекових систем, що спеціалізуються на аналізі вхідних користувацьких запитів.

Основною задачею сучасних систем, що безпосередньо займаються аналізом вхідних користувацьких запитів з подальшою передачею їх до цільового вебсервісу, є обробка вхідних даних, відповідно до попередньо

налаштованих правил та сигнатур, для виявлення потенційно небезпечних елементів. Більшість сучасних WAF систем (Web Application Firewall – брандмауер вебдодатків) використовує машинне навчання для побудови більш точної та гнучкої конфігурації, що враховує особливості роботи сервісу, який потребує захисту. На цьому етапі постає актуальна задача оцінки коректності та ефективності створеної конфігурації WAF. Особливо це затребуване завдання в контексті вебсервісів, що мають складну та розгалужену структуру.

Окремо слід зазначити, що традиційні методи оцінки рівня захищеності сервісів електронної комерції переважно використовують технічні метрики для оцінювання їх функціонування. Такий підхід не враховує наслідки безпекових інцидентів для бізнесу [63, 70]. В контексті роботи сервісів електронної комерції ця складова є ключовою, так як вплив безпекових систем на бізнес-показники може нанести безпосередню шкоду як фінансову так і репутаційну. Необхідність враховувати наслідки для бізнесу при оцінюванні ризиків в контексті систем захисту, що взаємодіють з сервісами електронної комерції знаходить відображення у роботах таких дослідників як Д. Бехбехані (D. Behbehani), Н. Комнінос (N. Komninos), К. Аль-Бегейн (K. Al-Begain) [28].

Істотна частина наявних методів оцінювання захищеності інформаційних систем ґрунтується на статичному представленні їхнього стану. Такий підхід не дає змоги повною мірою врахувати динаміку функціонування сервісів електронної комерції та зміни у характері загроз інформаційній безпеці. Це підкреслюють інші автори, які пропонують використовувати часові характеристики мережевих конфігурацій і вразливостей як основу для подальшого оцінювання ризиків [25].

Важливою технічною проблемою наявних підходів є інтегрування метрик різного походження та типу в єдину кількісну оцінку ефективності роботи системи захисту. У дослідженні групи авторів на чолі з У. Бансал (U. Bansal) продемонстровано, що кількісне оцінювання великих наборів вразливостей потребує додаткового застосування аналізу витрат і вигоди. Автори наголошують, що проста лінійна агрегація навіть однотипних безпекових метрик

не охоплює всю множину можливих шляхів атак і обсяг зусиль, необхідних для їх реалізації. Як наслідок, отримані оцінки можуть не повною мірою відображати фактичний стан захищеності системи [26].

Виходячи із вище зазначеного, актуальною є науково-технічна задача з розробки алгоритмів та програмного забезпечення, що надає можливість проводити аналіз ефективності роботи систем захисту сервісів електронної комерції.

Зв'язок роботи з науковими програмами, планами та темами. Тема дисертації затверджена Вченою радою Державного університету "Житомирська політехніка" (протокол № 9 від 31.08.2022 р.).

Дисертаційне дослідження виконувалось відповідно до НДР "Аналіз і моделювання процесу розробки програмних рішень в галузі електронної комерції" (12.01НДР-34-2023) кафедри інженерії програмного забезпечення Державного університету "Житомирська політехніка" (2023-2024 р.).

Мета дослідження – розробка алгоритмів та програмного забезпечення аналізу ефективності систем захисту сервісів електронної комерції.

Визначена мета досягається шляхом вирішення таких **завдань**:

1. Проаналізувати закордонний та вітчизняний досвід з окресленої проблематики.
2. Здійснити аналіз наявних методів, засобів та технологій оцінки ефективності роботи систем захисту сервісів електронної комерції та проблеми їх функціонування.
3. Обґрунтувати основні показники ефективності систем захисту сервісів електронної комерції в залежності від складності їх структури.
4. Розробити алгоритм та метод аналізу ефективності функціонування систем захисту сервісів електронної комерції.
5. Розробити прототип експериментального програмного забезпечення, що реалізує авторський метод аналізу ефективності систем захисту сервісів електронної комерції та його протестувати.

Об’єктом дослідження є процеси аналізу ефективності систем захисту сервісів електронної комерції.

Предмет дослідження – методи, алгоритми та програмне забезпечення аналізу ефективності систем захисту сервісів електронної комерції.

Для вирішення визначених завдань використовувалась низка **методів**, зокрема *теоретичні*: аналіз і узагальнення для дослідження існуючих підходів до оцінювання ефективності систем захисту сервісів електронної комерції, системний аналіз – для розгляду системи захисту як багаторівневої системи, структурна декомпозиція – для виділення основних функціональних складових запропонованого методу, формалізація – для побудови математичного апарату і опису процедур аналізу; *емпіричні* – моделювання для відтворення процесів функціонування системи захисту та оцінювання її ефективності, метод аналізу ієрархій – для визначення коефіцієнтів критичності етапів взаємодії користувача із сервісом та ваги показників ефективності, обчислювальний експеримент – для перевірки працездатності розробленого методу, аналіз історичних даних – для апробації методу на ретроспективних даних, проєктування та програмна реалізація – для розроблення програмного засобу реалізації методу аналізу ефективності систем захисту.

Використання технологій штучного інтелекту. У процесі виконання дисертаційного дослідження технології штучного інтелекту використовувались як допоміжний інструмент візуалізації для кращого представлення окремих розроблених схем за власним описом.

Формування наукових положень, постановка мети і завдань дослідження, проведення експериментів, обробка результатів та формулювання висновків виконані автором самостійно. Технології штучного інтелекту не використовувались для генерування тексту дисертації чи формулювання наукових результатів.

Наукова новизна та теоретичне значення отриманих результатів полягають у тому, що:

вперше: формалізовано модель взаємодії користувачів з сервісами електронної комерції у вигляді послідовності з семи етапів та визначено коефіцієнти критичності етапів взаємодії із застосуванням методу аналізу ієрархій за п'ятьма критеріями оцінювання, що забезпечує формалізацію та відтворюваність процесу розрахунку; обґрунтовано систему з чотирьох показників ефективності роботи систем захисту сервісів електронної комерції: виявлення загроз, взаємодія з користувачами, якість реагування, покриття захистом етапів взаємодії користувачів з сервісом електронної комерції, та визначено їх вагові коефіцієнти із застосуванням методу аналізу ієрархій; запропоновано розрахунок контекстного індексу ефективності захисту, що додатково враховує контекст функціонування сервісів електронної комерції через часовий фактор та бізнес-фактор за допомогою коефіцієнта контекстної чутливості; розроблено метод аналізу ефективності системи захисту сервісів електронної комерції, що на відміну від наявних підходів, які фокусуються переважно на технічних параметрах, забезпечує урахування бізнес-контексту на трьох рівнях: через коефіцієнти критичності етапів взаємодії користувачів з сервісами електронної комерції, через коефіцієнт контекстної чутливості при розрахунку контекстного індексу ефективності захисту та через розрахунок пріоритетів проблемних аспектів при роботі системи рекомендацій;

удосконалено: систему формування рекомендацій на основі оцінювання ефективності роботи систем захисту, що дозволяє провести діагностику стану показників та визначити пріоритети виявлених проблемних аспектів із урахуванням контексту роботи сервісу електронної комерції;

набули подальшого розвитку: теоретичні та методичні засади побудови адаптивних рішень у сфері захисту сервісів електронної комерції.

Практичне значення отриманих результатів полягає в тому, що:

- розроблено специфікацію стандартизованого JSON-інтерфейсу, що формалізує комунікацію між зовнішніми джерелами даних та аналітичною складовою методу, що дозволяє уникнути залежності від конкретних зовнішніх систем та розширити можливості інтеграції аналітичної

складової методу з різними платформами електронної комерції та системами захисту;

- виконано програмну реалізацію прототипу аналітичного модуля мовою програмування Python із застосуванням модульної архітектури, що складається з чотирьох обчислювальних компонентів для відображення та аналізу отриманих даних;
- розроблено ряд алгоритмів, що забезпечують повний цикл функціонування аналітичної складової методу від отримання та перевірки вхідних даних до формування структурованого звіту рекомендацій;
- розроблено систему моделювання взаємодії користувачів з сервісом електронної комерції, що підтримує чотири базові сценарії (штатний режим, чорна п'ятниця, розпродаж, DDoS-атака), кожен з яких визначає характерні шаблони трафіку, розподіл безпекових подій та контекстні параметри, що дозволяє створювати вхідні дані із заданою часовою деталізацією для верифікації методу на різних масштабах аналізу;
- проведено серію з дев'яти експериментів, результати яких підтвердили незалежність показників, контекстну кореляцію результатів роботи систем захисту, коректне розмежування впливу бізнес-контексту та позаштатних ситуацій, а також чутливість методу на різних часових масштабах даних, що підтверджує можливість його практичного застосування у різних режимах роботи.

Матеріали дослідження можуть бути використані організаціями, що здійснюють діяльність у сфері електронної комерції, для аналізу та підвищення ефективності функціонування їхніх систем захисту.

Впровадження результатів дослідження в практику підтверджується довідками ТОВ "САНА КОМЕРС УКРАЇНА" та ТОВ "Візевен Європа" (довідки додаються).

Особистий внесок здобувача. Усі основні результати дисертаційного дослідження, які представлені до захисту, одержані автором особисто (звіт подібності сформований за допомогою програми StrikePlagiarism додається).

У працях, опублікованих у співавторстві, автору належать: описано окремі виклики у сфері захисту сервісів електронної комерції [3]; проведено огляд окремих сучасних систем захисту електронних сервісів [5]; досліджено стан доробку у галузі розробки та функціонуванні систем захисту сервісів електронної комерції [6]; обґрунтовано необхідність розробки алгоритмічного та програмного забезпечення аналізу ефективності систем захисту сервісів електронної комерції [7]; описано окремі аспекти використання штучного інтелекту у системах захисту сервісів електронної комерції [1]; описано окремі аспекти практичного застосування теорії графів у розробці та обслуговуванні програмних систем [9]; описано окремі методи оцінки ефективності роботи систем захисту сервісів електронної комерції [4].

Апробація результатів дисертації. Основні результати наукових досліджень неодноразово доповідалися на ряді міжнародних та Всеукраїнських наукових конференціях та семінарах, зокрема: VII Міжнародній науково-практичній конференції (м. Одеса, 27–28 вересня 2024 р.), V Всеукраїнській науково-практичній інтернет-конференції студентів, аспірантів та молодих вчених за тематикою «Сучасні комп'ютерні системи та мережі в управлінні» (Херсон, 2022 р), IV Міжнародній науковій конференції (м. Львів, 11 липня, 2025 р.).

Публікації. Результати дослідження було опубліковано у 8 наукових працях, з них 5 статей у фахових наукових виданнях України категорії «Б» та 3 у матеріалах наукових конференцій.

Структура та обсяг дисертації. Дисертаційна робота складається з анотації, вступу, трьох розділів, висновків до кожного розділу, висновків, списку використаних джерел (136 найменування, з них 124 іноземною мовою), 5 додатків. Загальний обсяг дисертації – 261 сторінка, з них 186 сторінок основного тексту, у якому міститься 68 таблиць та 72 рисунка.

РОЗДІЛ 1. Аналіз методів, засобів та технологій оцінки ефективності роботи систем захисту вебсервісів

1.1. Стан досліджень у галузі розробки та функціонування систем захисту сервісів електронної комерції

Проблема захисту як вебдодатків загалом, так і сервісів електронної комерції зокрема, є актуальним питанням, увага до якого не згасає, так як з розвитком систем захисту покращуються та адаптуються методи їх компрометації. Постійно проводиться робота над дотриманням балансу доцільного зменшення потенційних безпекових ризиків та збереженням комфортного середовища для кінцевих користувачів.

Забезпечення захисту сервісів електронної комерції поділяється на дві основні категорії – технічну та організаційну. До технічних заходів забезпечення захисту можна віднести різноманітні автоматизовані системи аналізу користувацького трафіку, організацію безпечних умов обробки і зберігання інформації якою оперує сервіс електронної комерції, своєчасне оновлення програмного забезпечення для запобігання використанню зловмисниками наявних вразливостей, проведення планових тестувань систем захисту сервісів електронної комерції незалежними експертами. У свою чергу, організаційні заходи включають у себе проведення планових аудитів систем захисту на відповідність встановленим вимогам, інформування користувачів щодо потенційних загроз, сертифікацію в межах наявних міжнародних безпекових стандартів.

Клер Лейбатс (Claire Laybats) та Люк Тредіннік (Luke Tredinnick) у своїй роботі розглядають сучасні виклики інформаційній безпеці [78]. Згідно їх аналізу, незважаючи на стрімкий розвиток інформаційних технологій та збільшення цінної інформації, якою оперують різні системи, світ не спостерігає бурхливого зростання кількості кібер-злочинів. Автори вважають, що це пояснюється тим, що по мірі розповсюдження різноманітних інформаційних систем за останні десятиліття, паралельно зростала і зазнала змін та розвитку

сфера їх захисту. Також вони роблять висновки, що основним напрямком забезпечення захисту інформаційних систем в першу чергу має бути розуміння та управління ризиками, а не усунення загроз та їх наслідків. Незважаючи на розвиток технологій, головним безпековим ризиком будь-якої інформаційної системи є людський фактор і зменшення його впливу на вразливість системи має бути частиною безпекових заходів [78].

У контексті організаційних заходів велика увага приділяється захисту, обробці та зберіганню персональних даних користувачів сервісів електронної комерції, що відображено у нормативно-правових актах, прийнятих у різних країнах. О. Мервінський проводить аналіз основних законодавчих вимог щодо захисту персональних даних у сфері електронної комерції, наголошуючи на важливості їх врахування при використанні технічних засобів забезпечення захисту сервісів електронної комерції [8].

Б. Тригубець у своєму дослідженні акцентує увагу на важливості захищеності обробки фінансової та персональної інформації користувачів, якою оперують системи електронної комерції [12]. Розглядаючи основні види шахрайських дій, направлених на неправомірне використання користувацьких даних, науковець виділяє дві складові захисту сервісів електронної комерції: програмну та організаційну, вказуючи на необхідність постійного вдосконалення методів захисту для своєчасного запобігання наявним загрозам.

М. Бенц (M. Benz) та Д. Чаттерджі (D. Chatterjee) розглянули інформаційні безпекові ризики, що стосуються малого і середнього бізнесу та запропонували методологію аналізу стану захищеності інформаційної системи [31]. Автори зазначають, що не зважаючи на вже наявні фреймворки управління інформаційною безпекою, такі як ISO, CIS, PCI DSS, COBIT, для невеликих компаній вони можуть бути занадто складними та високовартісними для впровадження. Запропонована методологія базується на фреймворку NIST CSF (National Institute of Standards and Technology's cybersecurity framework), що дозволяє використовувати його систему оцінки та рекомендацій (рис. 1.1) [31]. Розробники методології проаналізували роботу фреймворку, використовуючи

власний досвід та, враховуючи потреби цільової аудиторії, адаптували необхідні параметри фреймворку для створення набору вхідних даних для подальшого аналізу.

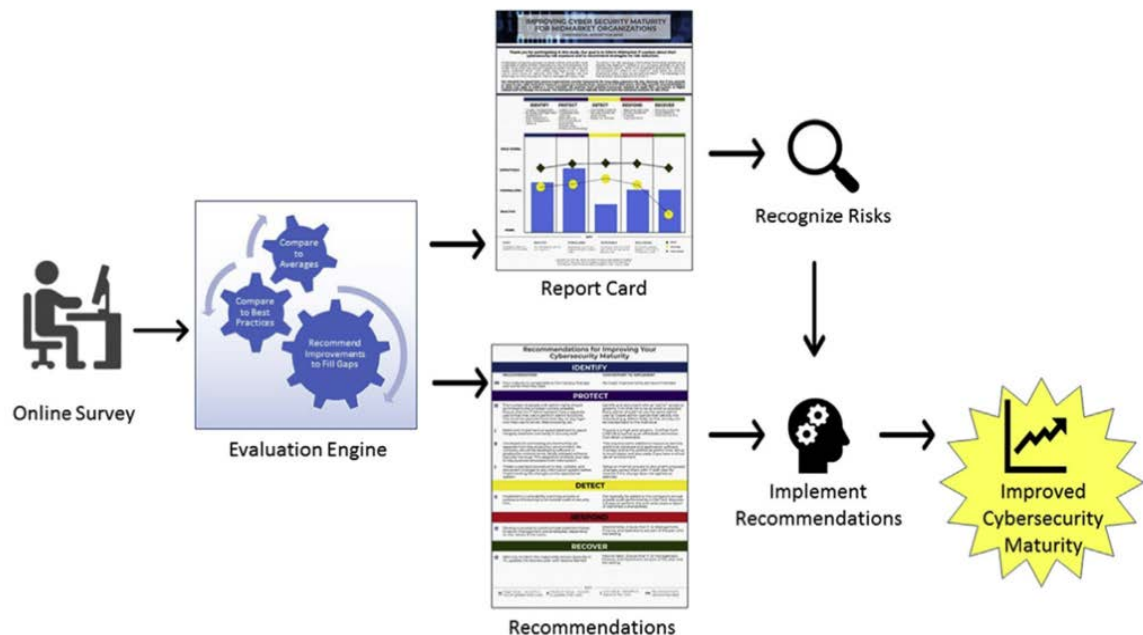


Рис. 1.1. Робота фреймворку NIST CSF (за Бенц М. (Benz M.) та Чаттерджі Д. (Chatterjee D.)) [31].

Результатом обробки даних є рекомендації щодо можливих змін та покращень для підвищення рівня захисту інформаційної системи, що аналізується. Також надається приблизна оцінка вартості необхідних заходів з фінансової точки зору та необхідних людських ресурсів для її впровадження. Розроблена методологія дозволяє ідентифікувати найбільш вразливі місця інформаційної системи, оцінити її відповідність наявним стандартам та визначити найбільш ефективні заходи для покращення її захисту [31].

Колективом авторів Ідіано д'Адамо (Idiano D'Adamo), Росіо Гонсалес-Санчес (Rocío González-Sánchez), Марія Соня Медіна-Сальгадо (Maria Sonia Medina-Salgado), Давід Сеттембре-Блундо (Davide Settembre-Blundo) було проаналізовано тенденції розвитку сервісів електронної комерції в останні роки, зважаючи на їх бурхливий розвиток через пандемію COVID-19 [49]. Автори

використовували дані з відкритих джерел, серед яких можна виділити Eurostat та Salesforce Shopping Index, а також залучали незалежних експертів для проведення опитувань згідно теми дослідження. Для аналізу отриманих даних використовувались MCDA метод та метод оцінювання за шкалою Лайкерта (Likert Scale Survey).

Отримані результати дозволяють стверджувати, що одним із вагомих факторів, що впливають на стале зростання та розвиток сервісів електронної комерції, є забезпечення надійної та безпечної обробки і зберігання фінансової інформації користувачів та їх персональних даних. Автори зазначають про необхідність планування інвестицій в інформаційну безпеку та системний підхід до управління ризиками захисту інформації громадян та підприємств, що збирається та обробляється через цифрові канали [49].

Групою авторів запропоновано методологію моделювання взаємодії антагоністичних агентів у системах кібербезпеки [88]. У запропонованій методології традиційні методи і інструменти моделювання не протиставляються один одному, а розглядаються в сукупності, формуючи тим самим єдину методологічну базу моделювання поведінки антагоністичних агентів. Автори зазначають, що системи захисту інформаційних систем функціонують в умовах невизначеності, що характеризується браком інформації для формалізації процесів, з якими вони взаємодіють. Це, в свою чергу, підвищує суб'єктивний вплив особи, що приймає рішення на роботу системи захисту. Таким чином, побудова формальної моделі прийняття рішень дозволяє знизити вплив суб'єктивних факторів на функціонування системи захисту інформаційної системи і, як результат, підвищити ефективність її роботи. Враховуючи складність і різноманітність процесів та об'єктів, з якими взаємодіє система захисту, досить складно використовувати уніфікований метод моделювання, який дозволить отримати необхідний рівень абстракції, тому автори пропонують використовувати інтеграцію різноманітних методів моделювання для побудови загальної моделі взаємодії антагоністичних агентів (рис. 1.2). Така методика дозволяє сукупне використання всієї множини моделей та координацію їх

застосування, що дозволяє підвищити якість моделювання за рахунок компенсації недоліків одних моделей перевагами інших. Саме ця особливість запропонованої методології виділяє її на тлі інших [88].

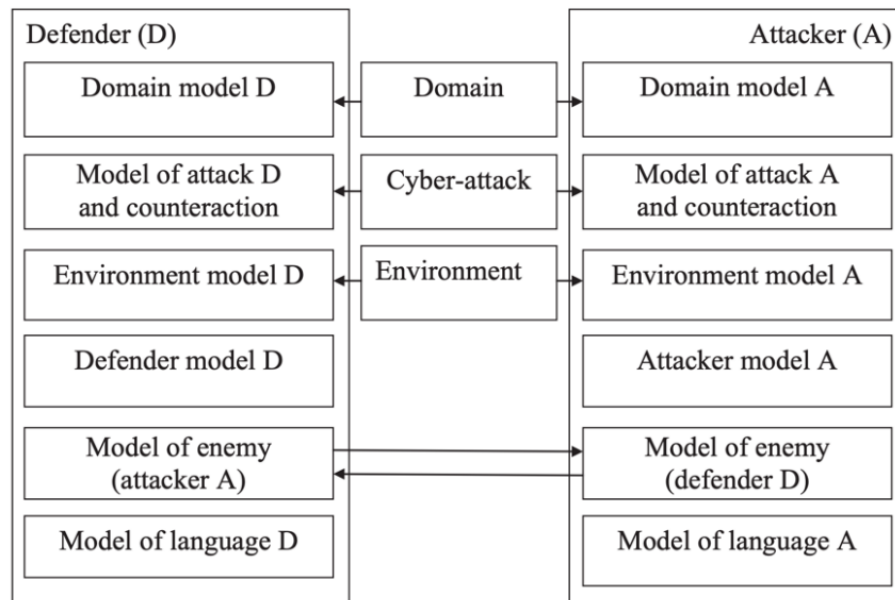


Рис. 1.2. Схема взаємозв'язку моделей компонентів антагоністичної взаємодії (згідно з колективом авторів [88]).

Необхідно зазначити, що автори вказують на наявні обмеження розробленої моделі, що, в свою чергу, залишає простір для майбутніх досліджень та розширення інструментів моделювання, таких як використання нейронних мереж, глибинного аналізу даних, застосування генетичних алгоритмів тощо [88].

Х. Матбулі (H. Matbouli) та К. Гао (Q. Gao) провели дослідження безпекових ризиків, що мають вплив на розвиток та розповсюдження сервісів електронної комерції [86]. Автори зазначають, що недостатня захищеність сервісів електронної комерції призводить до значних фінансових втрат як через дії зловмисників, так і через побоювання користувачів щодо захищеності їх фінансових даних при проведенні електронних платежів. Як приклад, автори наводять статистику компанії McAfee, однієї з найбільших компаній, що спеціалізується на розробці систем захисту інформаційних систем. У

відповідності до цих даних, 63% споживачів переривали процес оформлення онлайн купівлі, не отримуючи підтверджень тому, що сервіс електронної комерції, яким вони вирішили скористуватись, відповідає необхідним безпековим стандартам [86].

Згідно проведеного аналізу, основними безпековими загрозами для сервісів електронної комерції являються викрадення конфіденційної та фінансової інформації користувачів. Запобігання цьому потребує комплексного підходу, що охоплює весь процес електронної комерції, починаючи з підвищення безпекової обізнаності користувача і закінчуючи підтримкою інфраструктури сервісу електронної комерції (сервери, канали передачі інформації, платіжні системи тощо) на належному рівні, що відповідає сучасним безпековим стандартам [86].

Науковці пропонують перелік організаційних стратегій та технологічних рішень, направлених на покращення захисту сервісів електронної комерції.

Яцзюань Чжан (Yajuan Zhang), Сінъян Денг (Xinyang Deng), Дайцзюнь Вей (Daijun Wei) та Йонг Денг (Yong Deng) пропонують модель оцінювання захищеності сервісу електронної комерції, що має на меті покращити та спростити цей процес [134]. Автори зазначають, що запропонована модель оцінювання охоплює більшість основних безпекових параметрів функціонування сервісу електронної комерції. В основу розробленої моделі покладено метод аналізу ієрархій у поєднанні з теорією Демпстера-Шафера [134].

Запропонована модель складається з п'яти основних етапів:

- розбиття поставленої задачі на основні компоненти;
- присвоєння оціночної ваги кожному з компонентів;
- дисконтування кожного компоненту;
- об'єднання отриманих коефіцієнтів;
- визначення оцінки компоненту [134].

До перших двох етапів застосовується метод аналізу ієрархій, останні три використовують теорію Демпстера-Шафера (рис. 1.3).

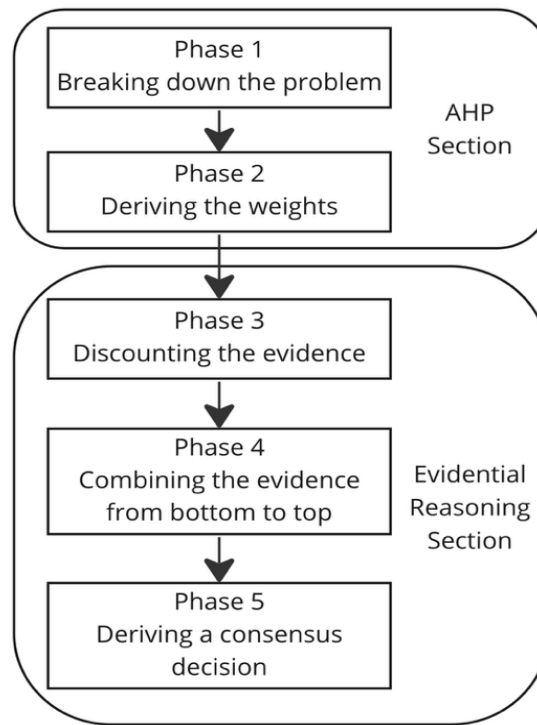


Рис. 1.3. Етапи роботи моделі [134].

Автори провели порівняння роботи розробленого алгоритму з аналогічними дослідженнями. Проаналізувавши отримані дані, вони дійшли висновку, що запропонований ними підхід дає більш точні результати оцінювання і є простішим у реалізації [134].

Колектив дослідників Лука Деметріо (Luca Demetrio), Габріеле Коста (Gabriele Costa), Андреа Валенса (Andrea Valenza), Джованні Лагоріо (Giovanni Lagorio)) провели аналіз функціонування WAF та розробили інструмент, який дозволяє проводити симуляцію атаки на інформаційну систему, захищену WAF [52].

Метою їх дослідження була спроба компрометації роботи WAF, що використовує машинне навчання для виявлення аномалій у вхідному трафіку. Слід зазначити, що WAF у комбінації з алгоритмами машинного навчання є сучасним підходом до забезпечення захисту інформаційних систем. Такі системи захисту здатні завчасно виявляти потенційні загрози, використовуючи попередньо накопичені дані щодо нормальної роботи інформаційної системи, і, керуючись закладеними у них політиками обробки трафіку, блокувати

потенційно небезпечні активності [52].

Дослідники скористались особливостями обробки даних алгоритмами машинного навчання для створення запитів, які не будуть розцінені як потенційно небезпечні (рис. 1.4).

```

1  admin' OR 1=1#
2  admin' OR 0X1=1 or 0x726!=0x726 OR 0x1Dd
   not IN/*(seleCt 0X0)>c^Bj>N]*/ ((SeLeCT
      476),(SELECT (SElEct 477)),0X1de) oR
      8308 noT lIkE 8308\x0c AnD truE OR '
      FZ6/q' LiKE 'fz6/qI' anD TRUE anD '>U'
      != '>uz'#t'%'03;Nd

```

Рис. 1.4. Семантично еквівалентні запити [52].

Методологія, використана авторами, належить до класу підходів керованого мутаційного тестування. Її ідея полягає в тому, що тестування починається з невдалої спроби, вхідні дані якої поступово трансформуються через випадкове застосування попередньо визначених операторів мутації. Модифіковані тести виконуються, порівнюються і впорядковуються згідно заданим критеріям. Процес повторюється для тестів, які показали найкращі результати, доки не буде знайдено успішний тест (рис. 1.5) [52].

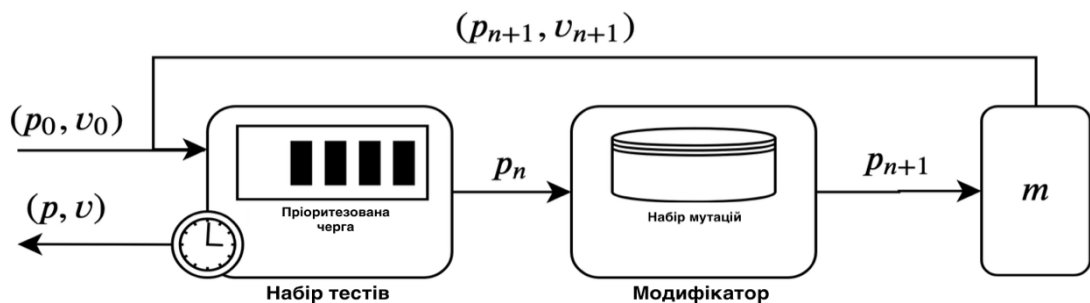


Рис. 1.5. Принцип роботи алгоритму [52].

Таким чином, дослідникам вдалося обійти захисні алгоритми WAF та скомпрометувати систему захисту. Дослідження проводились з використанням популярних WAF систем, що доступні на ринку [52].

Цю Ліронг (Qiu Lirong) та Лі Цзе (Li Jie), вивчаючи проблему захисту сервісів електронної комерції, запропонували комплексну систему аналізу

захищеності інформаційної системи, що включає в себе моніторинг, аналіз даних, оцінювання ризиків та інформування у разі виявлення потенційної загрози [99].

Автори пропонують представити систему електронної комерції у вигляді неорієнованого графу, де кожен компонент системи електронної комерції є його вершиною, а ребра – зв'язки між цими компонентами. Таким чином, система моніторингу отримує відомості про всі зв'язки компоненту, який підключений до неї. Це дозволяє автоматизувати оптимізацію масштабування системи моніторингу для більш раціонального використання ресурсів. Автори пропонують наступний алгоритм для реалізації масштабування системи моніторингу (рис. 1.6). Де G – система електронної комерції, $\Phi = \{T_1, \dots, T_n\}$ – множина компонентів, S – мінімальне необхідне покриття моніторингу [99].

```

(1)  $\Phi = \emptyset; S = \emptyset;$ 
(2) while  $G$  has more edges do
(3)   if  $S = \emptyset$  then
(4)     Pick an edge  $(u, v)$  such that  $d(u) + d(v)$  is the largest;
(5)   else
(6)     Pick an edge  $(u, v)$  such that  $v \in S$  and  $d(u) + d(v)$  is the largest;
(7)    $T_v \leftarrow$  the ME rooted at  $v$ ;
(8)   Add  $T_v$  into  $\Phi$ ;
(9)    $S \leftarrow S \cup \text{neighbor}(v)$ ;
(10)  Remove edges in  $T_v$  from  $G$ ;
(11)  if  $d(u) > 0$  then
(12)     $T_u \leftarrow$  the ME rooted at  $u$ ;
(13)    Add  $T_u$  into  $\Phi$ ;
(14)    Remove edges in  $T_u$  from  $G$ ;
(15)     $S \leftarrow S \cup \text{neighbor}(u)$ ;
(16)  Remove  $u$  and  $v$  and all nodes with degree 0 from  $G$ ;
(17) Return  $\Phi$ 

```

Рис. 1.6. Запропонований алгоритм оптимізації системи моніторингу [99].

Система моніторингу збирає дані з підключених до неї компонентів системи електронної комерції і проводить їх аналіз, керуючись заданими правилами та інформацією про наявні вразливості. При виявленні аномалій генеруються попередження про наявну загрозу. Автори зазначають, що запропонована система не охоплює всі аспекти функціонування системи електронної комерції та має функціональні обмеження. Запропоновані авторами алгоритми також потребують подальшого вдосконалення та оптимізації [99].

Серед підходів до захисту сервісів електронної комерції увагу дослідників привертає концепція архітектури нульової довіри (Zero Trust Architecture, ZTA). Так, згідно стандарту NIST SP 800-207, що був розроблений дослідниками С. Роз (S. Rose), О. Борхерт (O. Borchert), С. Мітчелл (S. Mitchell) та С. Коннеллі (S. Connelly), ZTA визначається як сукупність підходів до побудови системи захисту за якими жоден користувач, пристрій чи мережеве з'єднання не вважаються довіреними за замовчуванням, а кожен запит до ресурсів системи, для якої побудовано захист, має пройти верифікацію та авторизацію незалежно від того, хто ініціював цей запит [103]. Для сервісів електронної комерції, що займаються обробкою великої кількості транзакцій від різноманітних клієнтів, зовнішніх сервісів та внутрішніх систем, принцип відсутності довіри до будь-кого є особливо актуальним. Основними складовими ZTA є механізми аутентифікації, сегментація мережевої інфраструктури, постійний моніторинг та контроль доступу на основі атрибутів ідентифікації та вивчення контексту клієнтських сесій. Впровадження принципів ZTA суттєво ускладнює можливості злоумисників безперешкодно пересуватись між функціональними компонентами сервісу електронної комерції у разі компрометації одного з них, що є критично важливим, зважаючи на популярність використання мікросервісної архітектури при побудові сучасних сервісів електронної комерції.

Дослідники К. Бак (C. Buck), К. Оленбергер (C. Olenberger), А. Швайцер (A. Schweizer), Ф. Фельтер (F. Völter) та Т. Ейманн (T. Eymann) провели комплексний аналіз наявних публікацій щодо теоретичних підходів та практичного застосування архітектури нульової довіри [37]. Проведене дослідження виявило суттєві прогалини між загальною концепцією ZTA та практичним досвідом її впровадження. У результаті проведеної роботи автори визначили ключові фактори успішного впровадження ZTA, а саме – чітке визначення області, що потребує захисту, деталізація та документування потоків транзакцій між компонентами системи, визначення та інтеграція відповідних безпекових політик. Дослідники наголошують, що перехід до ZTA слід розглядати як поступовий процес, що не передбачає одномоментної перебудови

всієї наявної інфраструктури. Впровадження ZTA реалізується через послідовне розширення охоплення принципами ZTA від найбільш критичних елементів системи до менш значущих. У контексті сервісів електронної комерції це дозволяє узгодити всі потреби та вимоги до безпекових систем сервісу з урахуванням специфіки роботи сервісу електронної комерції та з найменшим впливом на безперервну доступність сервісу електронної комерції користувачам.

1.2. Огляд наявних методів оцінки ефективності роботи систем захисту сервісів електронної комерції

Оцінка ефективності роботи систем захисту сервісів електронної комерції це неперервний процес, який включає в себе аналіз поточного стану системи, виявлення потенційно вразливих елементів системи, постійне вдосконалення і розвиток системи захисту з урахуванням нових технологій та загроз.

Можна виділити наступні загальноприйняті підходи до організації оцінки ефективності роботи систем захисту сервісів електронної комерції:

1. Визначення та впровадження ключових показників ефективності роботи систем захисту.
2. Створення моделі безпекових ризиків сервісу електронної комерції. Таке моделювання дозволяє оцінити ефективність роботи системи захисту шляхом порівняння потенційних ризиків та наявних безпекових заходів.
3. Моделювання атак на систему в контрольованих умовах. Це допомагає оцінити ефективність роботи системи захисту та виявити можливі слабкі місця.

Визначення та впровадження ключових показників ефективності роботи систем захисту дозволяє вимірювати різні аспекти роботи системи захисту, кількість виявлених та виправлених вразливостей, швидкість виявлення вразливостей тощо. Це дає можливість візуалізувати та формалізувати актуальні дані, що, в свою чергу, полегшує подальший аналіз та автоматизацію прийняття рішень. Важливу роль відіграє визначення якісних метрик, що відображатимуть

реальний стан роботи системи захисту, матимуть максимальну користь та інформативність. Від цього напряму залежить на скільки оперативними та відповідними до ситуації будуть дії у разі виникнення безпекових інцидентів.

Дослідники Ігор Бернік (Igor Bernik) та Кайя Пріслан (Kaja Prislan) пропонують вимірювати ефективність роботи системи захисту використовуючи модель ISP 10x10M [32]. Даний підхід полягає у поєднанні десяти критичних факторів успіху (CSF), ста ключових показників ефективності (KPI), десяти для кожного з факторів успіху, та шести визначених рівнів ефективності роботи системи захисту. В свою чергу, для критичних факторів успіху та ключових показників ефективності визначаються вагові коефіцієнти. Крім визначення вагових коефіцієнтів, дослідники використовують статистичний аналіз для встановлення кореляцій між критичними факторами успіху та індивідуальними ключовими показниками ефективності. Процедура проводилась шляхом обчислення коефіцієнтів кореляції Пірсона між CSF та між KPI, включеними в індивідуальні CSF (рис. 1.7) [32].

Аналіз результатів та визначення важливості окремих елементів моделі ISP 10x10M також дає можливість графічно представити на скільки ефективною є система захисту в тих чи інших областях (рис. 1.8) [32]. Модель ISP 10x10M передбачає, що цілісна система захисту може бути досягнута лише шляхом забезпечення високого рівня результативності в десяти різних галузях. Однак абсолютна або 100% безпека не існує і не може бути досягнута на практиці, тому безпекові заходи лише частково успішні.

Біла область позначає абсолютну ефективність захисту, що складається з десяти факторів, яка є лише теоретично можливою. Темна область показує оптимальний рівень ефективності захисту, досягнутий при ефективному управлінні всіма областями. Сіра область представляє ситуацію, в якій жоден з показників не досягає очікуваних значень [32].

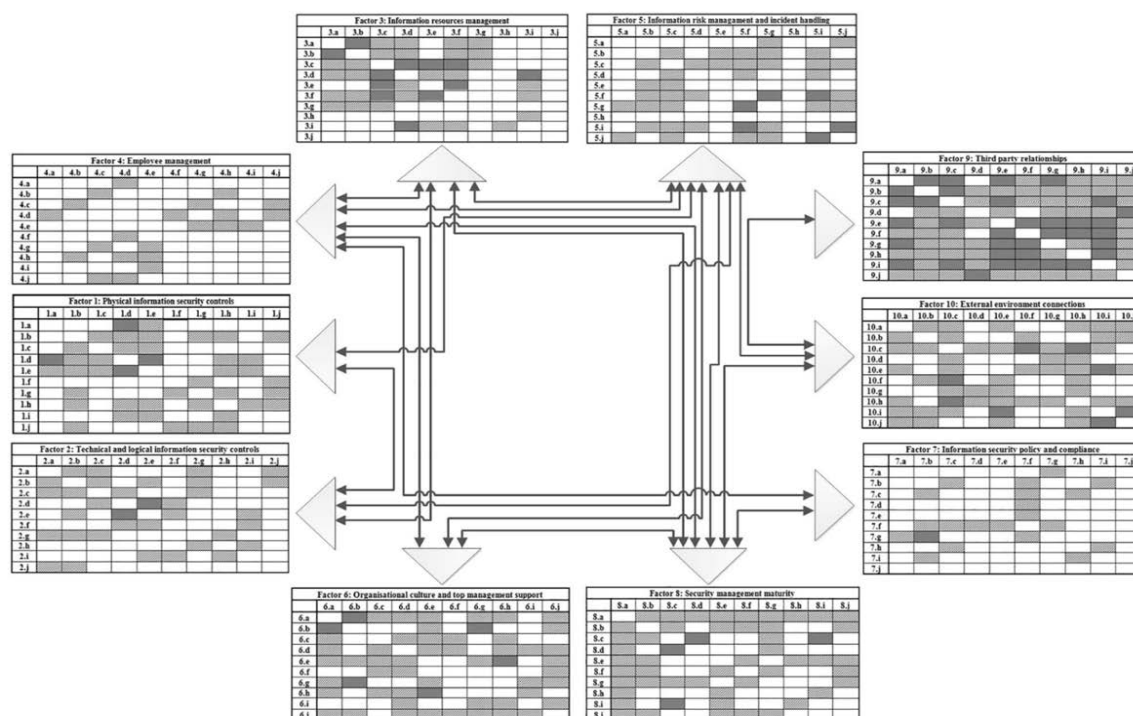


Рис.1.7. Модель кореляції між CSF та KPI [32].

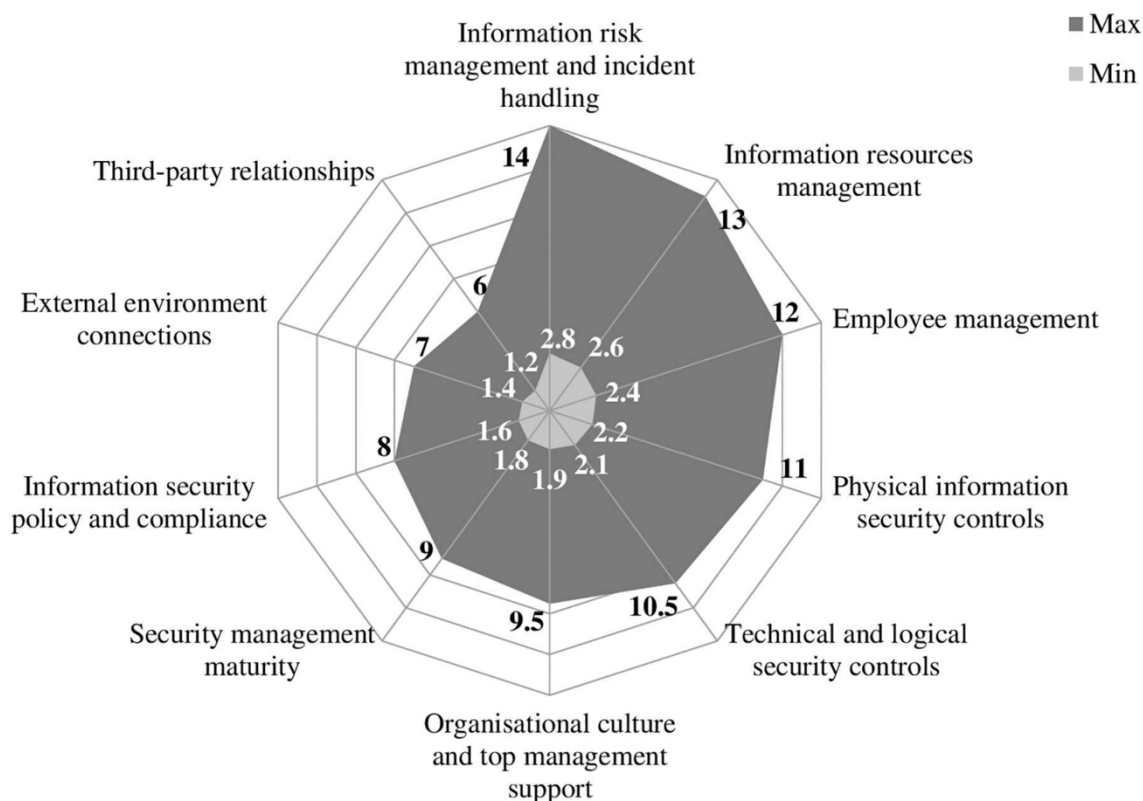


Рис.1.8. Графічне представлення аналізу ефективності системи захисту [32].

Результати отримані при використанні моделі ISP 10x10M надають можливість категоризувати ефективність роботи системи захисту, що, в свою

чергу, дозволяє визначити проблемні області та кроки необхідні для забезпечення бажаного рівня захисту[32].

Науковець Фредерік Шелдон (Frederick T. Sheldon) з групою співаторів пропонує використовувати систему економетрики кібербезпеки (Cyberspace Security Econometrics System - CSES) [112]. Цей підхід використовує кількісну оцінку надійності, продуктивності та ефективності системи захисту враховуючи критичність кожного елемента, який потребує захисту з точки зору економічних ризиків [112].

Для визначення середньої вартості відмови системи (Mean Failure Cost - MFC) автор пропонує зібрати наступну інформацію:

- перелік зацікавлених сторін, перелік специфікацій та вимог до системи захисту;
- для кожної з зацікавлених сторін та кожної з вимог до системи захисту визначити коефіцієнт втрат, ставку, які понесе зацікавлена сторона у разі відмови системи яку ми захищаємо;
- для кожного компонента вимог до системи захисту визначити ймовірність їх виконання [112].

Отримані дані дозволили побудувати автору наступну матрицю (рис. 1.9).

		Security Requirements				
		R1	R2	R3	...	Rn
Stakeholders	S1					
	S2					
	S3					
	...				FC_i^j	
	Sm					
		Probabilities of Security Requirements Delivery				
					P^j	

Рис.1.9. Матриця вартості відмови системи захисту [112].

Комірка матриці FC відображає втрати, які несе зацікавлена сторона S у випадку, якщо не виконуються вимоги, виставлені до системи захисту R.

Значення P відповідає визначеній ймовірності успішного виконання заданих вимог до системи захисту.

Враховуючи зазначене, середня вартість відмови системи визначається наступним чином (1.1) [112].

$$MFC_i = \sum_{j=1}^n FC_i^j \times (1 - P^j). \quad (1.1.)$$

Описаний спосіб оцінки ефективності системи захисту є гнучким та дозволяє використовувати широкий спектр показників, що можуть не завжди бути безпосередньо пов'язані з безпекою системи, для отримання кінцевої оцінки в контексті кожної із зацікавлених сторін.

Моделювання безпекових ризиків – це процес, що має на меті ідентифікацію, оцінку та пом'якшення загроз для системи, що потребує захисту (рис. 1.10) [121].

Цей процес дозволяє краще зрозуміти потенційні загрози та вжити заходів для їх запобігання. Базовий підхід до побудови моделі безпекових ризиків складається з чотирьох кроків [46, 19]:

1. Ідентифікація безпекових ризиків – на цьому етапі ідентифікують потенційні загрози для системи. Це можна зробити, провівши аналіз архітектури системи, бізнес-процесів, використання зовнішніх сервісів, тощо.
2. Оцінка безпекових ризиків – на цьому етапі проводиться оцінка ймовірності та впливу на систему кожної з визначених загроз. Це допомагає визначити, які загрози є найбільш серйозними.
3. Пом'якшення безпекових ризиків – на цьому етапі вживаються заходи для зменшення ризику виникнення загрози. Цього можна досягти впроваджуючи нові елементи системи захисту чи адаптуючи або оновлюючи вже наявні.

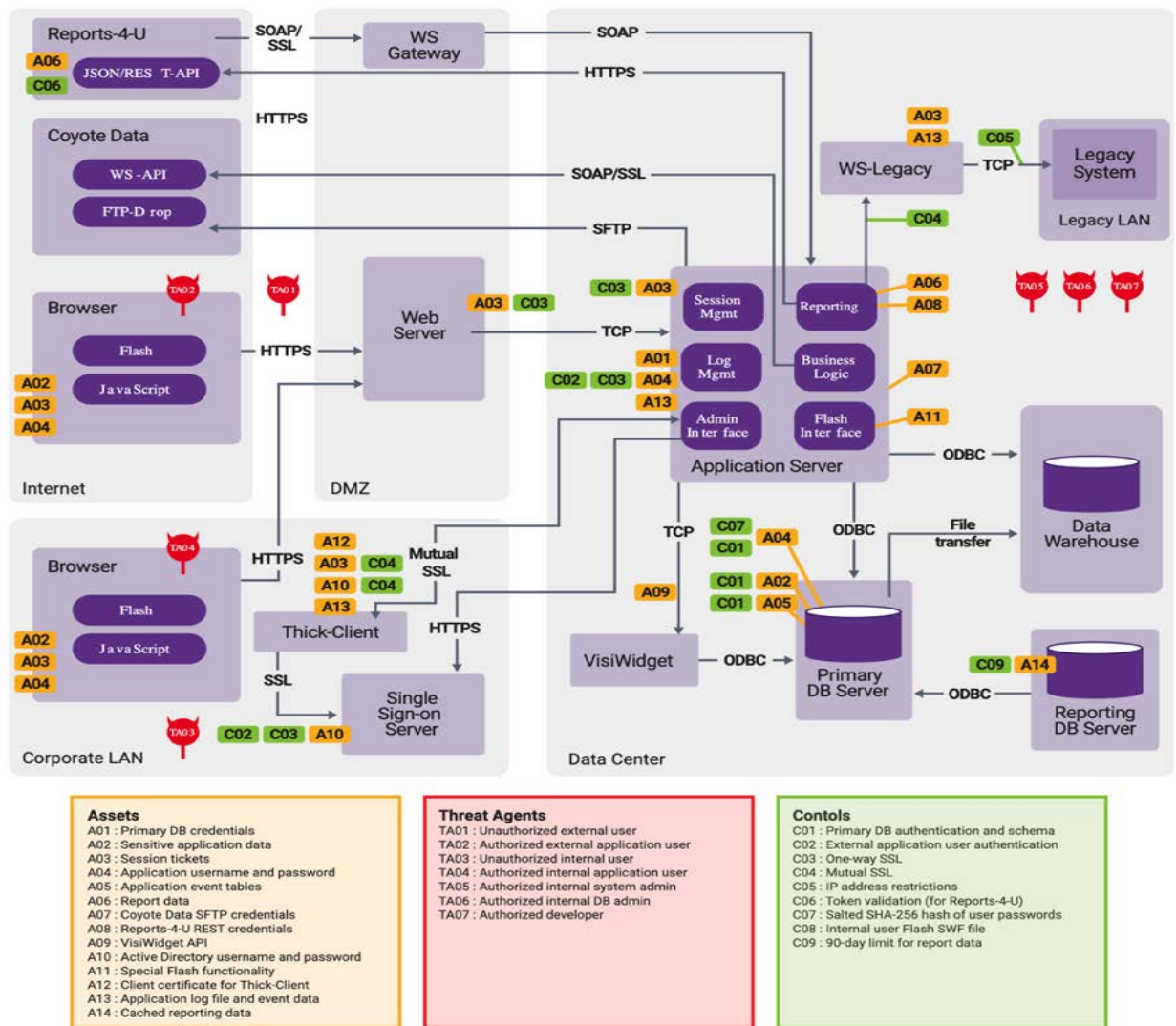


Рис. 1.10. Приклад моделювання безпекових ризиків [121].

4. Валідація – цей етап має на меті перевірку чи були вжиті всі необхідні заходи для пом'якшення кожної з визначених загроз.

Регулярне моделювання безпекових ризиків дозволяє отримати визначені та задокументовані кроки, необхідні для покращення роботи системи захисту. Окрім цього, такий підхід дозволяє виявляти потенційні проблеми в системі захисту заздалегідь; проводити оцінку нових видів загроз, які не були враховані при початковому проектуванні системи захисту; переглядати вимоги, що визначені до системи захисту; приділяти увагу безпековим ризикам, що є унікальними для сервісів, що потребують захисту; вчасно проводити

розподілення ресурсів необхідних для підтримки роботи системи захисту на належному рівні [121, 95].

Також виділяють наступні розповсюджені підходи до моделювання безпекових ризиків: STRIDE, PASTA, Bow-tie та CORAS. Метод STRIDE фокусується на шести найпоширеніших загрозах: підробленні ідентифікації, втручанні в обробку даних, неможливості притягнення до відповідальності, розкритті інформації, відмові в обслуговуванні та підвищенні привілеїв. Метод PASTA націлений на оцінку безпекових ризиків, що можуть вплинути на функціонування системи, і передбачає сім етапів моделювання безпекових ризиків. Метод Bow-tie дозволяє проілюструвати ризики системи у формі метелика (рис. 1.11), де загрози знаходяться зліва, наслідки – справа, а події – посередині [66].

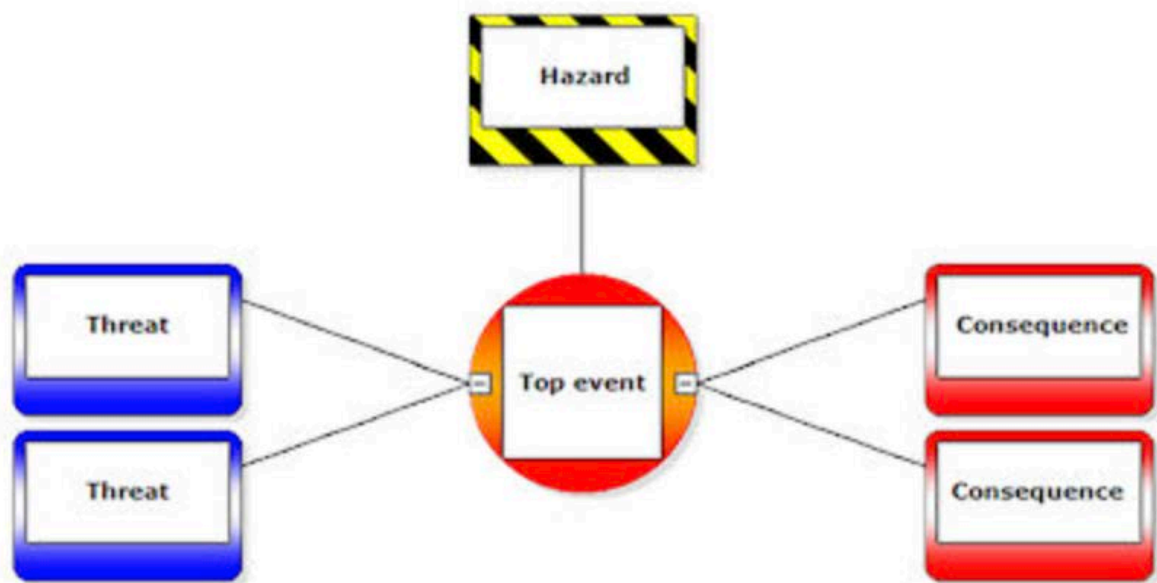


Рис. 1.11. Bow-tie метод моделювання безпекових ризиків [66].

Метод CORAS включає в себе 8 кроків (рис. 1.12), що дозволяють проаналізувати потенційні загрози та розробити заходи протидії [102].

Моделювання атак на систему захисту в контрольованих умовах є дієвим засобом оцінки ефективності її роботи, дозволяє в наближених до реальних умовах перевірити реакцію системи захисту на ті чи інші сценарії та сформулювати звіти щодо виявлених проблем та вразливостей. Регулярне проведення таких

тестувань допомагає підтримувати систему захисту на актуальному рівні в контексті потенційних загроз, що постійно змінюються [21].

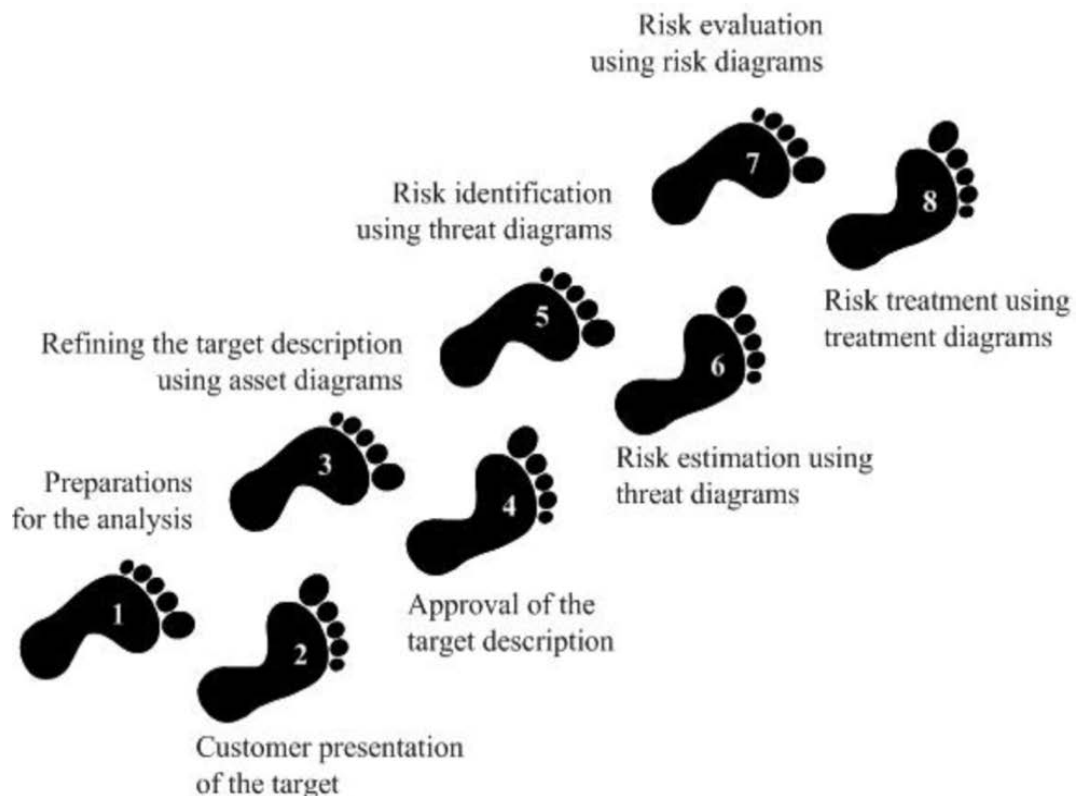


Рис. 1.12. Метод CORAS, який включає етапи аналізу безпекових ризиків [120].

Одним з поширених методів проведення моделювання атак на систему захисту є тестування на проникнення. Його суть полягає в тому, що спеціалісти з безпеки намагаються обійти систему захисту, використовуючи різноманітні техніки та засоби. Загалом, у тестуванні на проникнення можна виділити шість етапів (рис. 1.13) [74]:

1. Підготовка до тесту – на цьому етапі проводиться збір інформації про систему, де буде проводитись тестування, узгоджуються деталі тесту, включаючи затвердження методів і засобів, що будуть використані.
2. Створення плану тестування – цей етап включає в себе визначення потенційно вразливих елементів системи захисту та які саме безпекові перевірки мають бути застосовані щодо них.
3. Підготовка команди, що займатиметься тестуванням, узгодження деталей та сценаріїв, що мають бути відпрацьовані.

4. Визначення цілей, на які будуть направлені спроби проникнення. Окрім заздалегідь означених потенційно проблемних елементів системи захисту, спеціалісти визначають додаткові вектори атаки, які на їх думку будуть доцільними.
5. Проведення тесту на проникнення – на цьому етапі спеціалісти з безпеки безпосередньо намагаються обійти наявну систему захисту та задокументувати отримані результати.
6. Агрегація та аналіз отриманих даних – цей етап має на меті обробку отриманих результатів та створення звітів щодо знайдених вразливостей та рекомендацій для їх подальшого усунення.

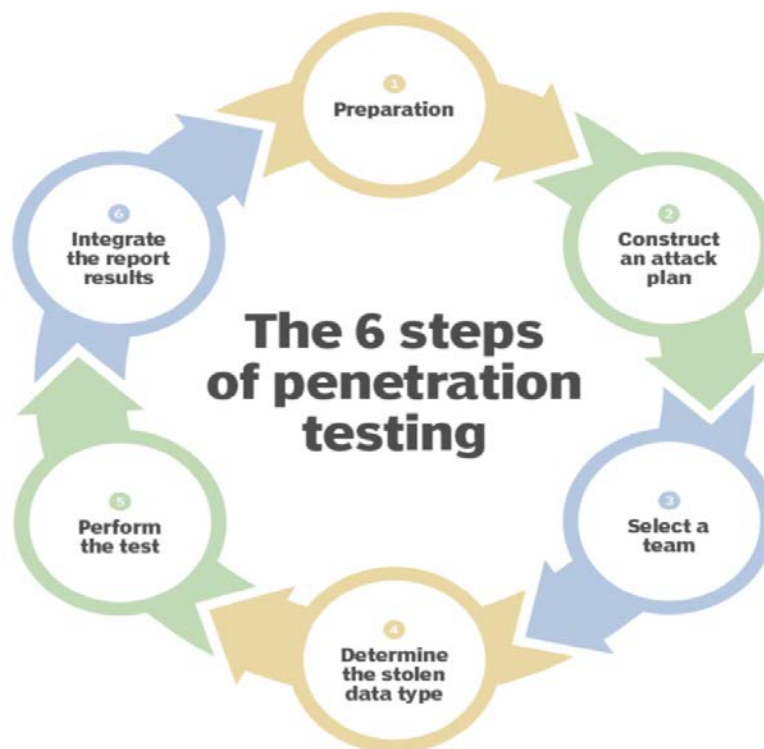


Рис. 1.13. Етапи тестування на проникнення [74].

Виділяють три загальні рівні проведення тестування на проникнення [74]:

1. Тестування методом "чорної скриньки" – під час проведення цього тесту, спеціалісти з безпеки не мають жодної інформації про систему, яку вони тестують, задача полягає в знаходженні вразливостей, що можуть бути використані.

2. Тестування методом "сірої скриньки" – у цьому випадку спеціалісти, що проводять тестування, отримують деяку інформацію про систему захисту, яку вони тестують. Ця інформація використовується для пошуку вразливостей, які не були виявлені при тестування методом «чорної скриньки».
3. Тестування методом "білої скриньки" – спеціалісти з безпеки, що проводять тестування, отримують повні дані про систему захисту. Задача полягає у виявленні вразливостей, які не були знайдені під час тестування методом «чорної скриньки» та тестування методом «сірої скриньки».

Також необхідно зазначити, що наявні різні стандарти та фреймворки для проведення тестування на проникнення. Це обумовлено варіативністю цілей тестування та відмінностями безпекових стандартів у різних галузях. До поширених у використанні стандартів і фреймворків можна віднести OSSTMM, OWASP, PTES, ISSAF, NIST, PCI DSS [91, 130]. Кожен з них надає можливість провести тестування необхідної складності та з урахуванням специфіки роботи системи, що перевіряється.

Перспективним напрямком у сфері оцінки ефективності систем захисту є концепція DevSecOps, що передбачає інтеграцію безпекових практик у безперервний процес розробки та впровадження програмного забезпечення. Р. Н. Раджапаксе (R. N. Rajapakse), М. Захеді (M. Zahedi), М. А. Бабар (M. A. Babar) та Г. Шен (H. Shen) провели систематичний огляд досліджень присвячених проблемам впровадження DevSecOps практик у реальних проектах [101]. Отримані результати демонструють, що зміщення відповідальності за безпекові рішення на ранні етапи циклу розробки дозволяє в середньому у шість разів скоротити витрати на усунення вразливостей порівняно з аналогічними діями, але вже на етапі експлуатації розробленого програмного забезпечення. Окремо дослідники визначають основні проблеми впровадження DevSecOps до яких відносять організаційні перешкоди між командами розробки та відповідальними за безпеку, відсутність стандартизованих метрик безперервної оцінки забезпечення захисту, обмежений перелік автоматизованих інструментів

для впровадження безпекових перевірок незалежно від стеку технологій, що застосовується при розробці. Для сервісів електронної комерції, де розробка та впровадження окремого функціоналу відбувається з високою частотою, інтеграція оцінювання безпекових ризиків в процеси CI/CD є необхідною умовою для підтримання задовільного рівня захисту.

Регулярне та автоматизоване тестування програмного забезпечення на відповідність безпековим стандартам в умовах використання CI/CD процесів суттєво скорочує час між виявленням вразливостей та їх усуненням, що є важливим показником ефективності систем захисту сервісів електронної комерції. Міжнародна організація OWASP розробляє та систематизує методики проведення автоматизованого тестування на різних рівнях архітектури інформаційних систем [94]. Розроблена документація охоплює понад дев'яносто різноманітних сценаріїв тестування, що відповідають різним типам вразливостей. У контексті роботи сервісів електронної комерції слід виділити наявність тестів для перевірки специфічним вимогам безпековим стандартам платіжних карток PCI DSS. Поєднання аналізу розробленого програмного коду на відповідність безпековим стандартам, динамічного тестування в процесі розробки та ручного тестування на етапах, де автоматизація відсутня, дозволяє створити середовище, що забезпечує високі стандарти захисту та вчасне виявлення потенційних проблем.

1.3. Огляд сучасних систем захисту електронних сервісів

Зважаючи на швидке поширення та розвиток різноманітних електронних сервісів, що торкаються практично всіх сфер життя сучасної людини, слід відзначити постійну увагу до розробки нових і вдосконалення наявних систем захисту електронних сервісів від загроз, що становлять небезпеку як для користувачів електронних сервісів (у контексті втрати персональних даних), так і для їх власників (матеріальні витрати, втрата бізнесу, репутаційні втрати). Сучасні системи захисту електронних сервісів у першу чергу націлені на проактивне запобігання ситуацій, які можуть становити безпекову загрозу, а також мінімізацію наслідків у випадку, коли зловмисники все ж змогли реалізувати свої наміри.

Серед сучасних систем захисту електронних сервісів, що широко використовуються, можна виділити наступні:

- брандмауери та брандмауери вебдодатків;
- системи виявлення та запобігання вторгненням (IDS/IPS);
- системи моніторингу та журналювання;
- системи шифрування користувацького трафіку та даних.

Слід зазначити, що у більшості випадків ці системи використовуються комплексно для забезпечення багатоварового захисту від потенційних атак.

Розглянемо ці системи більш детально. Системи виявлення і запобігання вторгненням проводять безперервний моніторинг трафіку, що передається в мережі організації, на предмет підозрілої діяльності (рис. 1.14). Системи IDS і IPS являють собою дві незалежні системи, але у більшості випадків вони використовуються разом, для отримання максимальних результатів їх роботи [65].

Система виявлення вторгнень проводить моніторинг трафіку в мережі, аналізує трафік на відповідність сигнатурам відомих атак і, у разі виявлення підозрілої активності, забезпечує інформування відповідальних осіб. Система IDS не перешкоджає атаці, що відбувається [65]. У свою чергу, система запобігання вторгненням також проводить моніторинг трафіку мережі, але у

випадку виявлення підозрілої активності, трафік блокується та лишається заблокованим до подальшого аналізу ситуації, що склалася і прийняття рішення щодо розблокування [65].

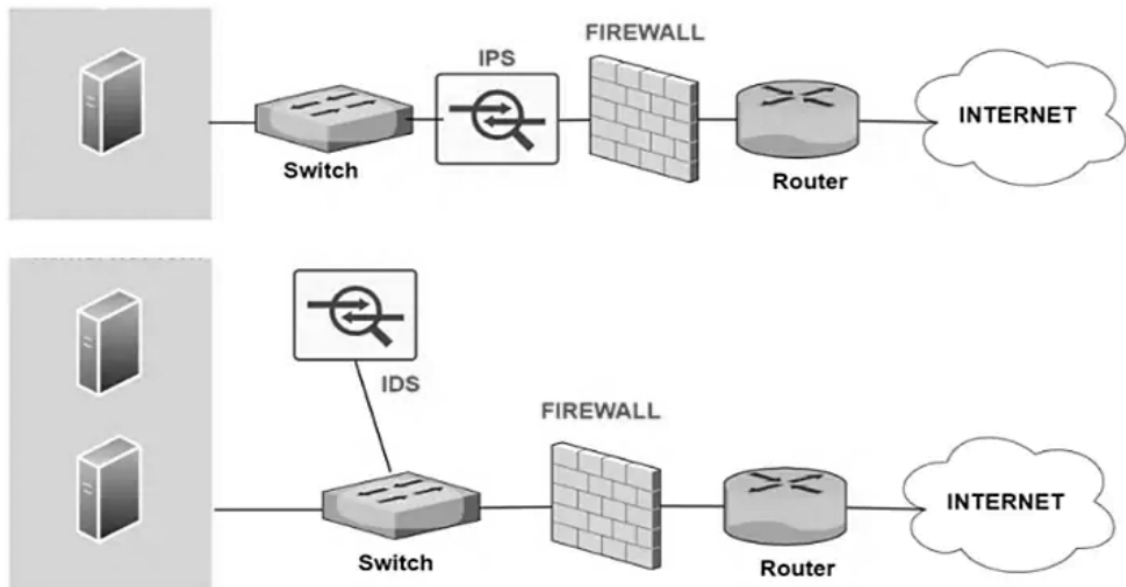


Рис. 1.14. Діаграма розміщення систем IPS та IDS у мережі [128].

Поєднане впровадження систем виявлення і запобігання вторгненням забезпечує багаторівневий захист мережі, зменшує кількість хибних спрацьовувань, підвищує ефективність управління мережею, що, в свою чергу, сприяє можливості організацій протистояти різноманітним кіберзагрозам.

Брандмауери та брандмауери вебдодатків покликані забезпечувати контроль доступу та захист від несанкціонованого доступу до елементів мережевої інфраструктури. Маючи спільну мету, вони функціонують на різних рівнях мережевої інфраструктури та зосереджені на різних безпекових аспектах.

Брандмауери – це мережеві безпекові системи, задачею яких є контроль вхідного і вихідного трафіку. Брандмауери слугують бар'єром між внутрішньою мережею організації та зовнішнім середовищем. Брандмауер проводить інспекцію вхідних і вихідних пакетів на відповідність заданим правилам проходження трафіку. У разі невідповідності – пакети блокуються [117].

Звичайні брандмауери оперують на мережевому та транспортному рівні моделі OSI, оперуючи трафіком на основі IP адрес та TCP/UDP портів (рис. 1.15).

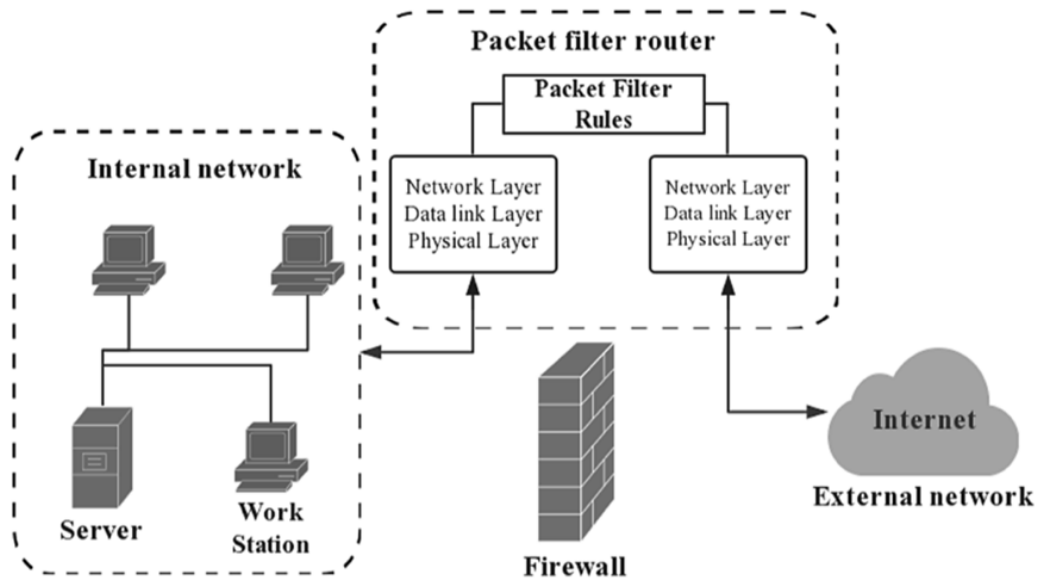


Рис. 1.15. Мережевий брандмауер [71].

Послідовним етапом розвитку мережевих брандмауерів є Next Generation Firewall (NGFW) – брандмауери наступного покоління, що охоплюють всі можливості традиційних брандмауерів, а також містять інтегровані механізми запобігання вторгнень, можливості контролю трафіку на прикладному рівні, отримують постійні оновлення щодо загальновідомих загроз, мають засоби та можливості для поширення інформації про аномалії для подальшого централізованого аналізу [126].

Розповсюдження і впровадження брандмауерів наступного покоління значно спрощує протидію наявним кіберзагрозам, оскільки обмін інформацією про відомі типи атак відбувається централізовано. У разі виявлення аномалій, що можуть бути індикаторами потенційно небезпечної активності, одним брандмауером, решта, через певний час, потрібний для аналізу, отримують інструкції щодо протидії. Це значно пришвидшує реакцію на загрози, та у багатьох випадках запобігає їх подальшому поширенню.

Набір доступного функціоналу серед наявних брандмауерів наступного покоління може відрізнатись залежно від виробника та обраного рівня

необхідного захисту. Узагальнені можливості, що можуть бути реалізовані за допомогою NGFW, представлені на рис. 1.16.

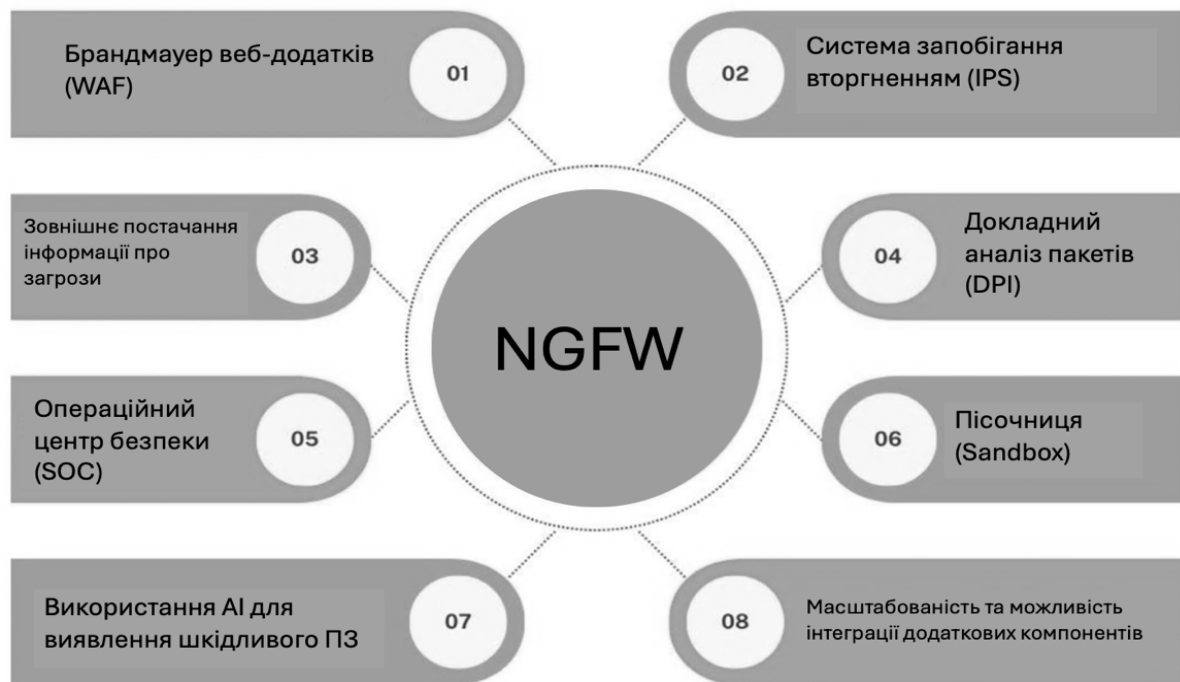


Рис. 1.16. Ключові можливості NGFW [129].

Незважаючи на широкі можливості брандмауерів наступного покоління, вони мають застосовуватись як частина загальної архітектури системи захисту в поєднанні з іншими технічними та організаційними заходами. Це дозволяє побудувати цілісну систему запобігання та контролю загроз, що покриває всі безпекові аспекти інформаційної системи [129].

На відміну від звичайних брандмауерів, брандмауери вебдодатків є вузькоспеціалізованими засобами забезпечення захисту вебдодатків, що зосереджуються на специфічних для них загрозах. До таких можна віднести SQL ін'єкції (SQL-injections), міжсайтовий скриптинг (XSS), неправомірне використання даних користувацьких сесій та форм, DDoS атаки. Також WAF використовується для захисту API інтерфейсів, захисту від атак мережеских ботів, брутфорс атак [100]. Брандмауери вебдодатків оперують на прикладному рівні моделі OSI.

Брандмауер вебдодатків працює як зворотній проксі, що убезпечує захищені ресурси від прямої комунікації з користувачами. Всі вхідні запити

користувачів проходять через WAF, де проводиться їх аналіз на відповідність заданим політикам і правилам (рис. 1.17). У своїй роботі WAF опирається на використання стратегій позитивної (Positive Security Model) та негативної (Negative Security Model) безпекових моделей [116]. Їх поєднання дозволяє отримати найкращі результати запобігання загрозам.

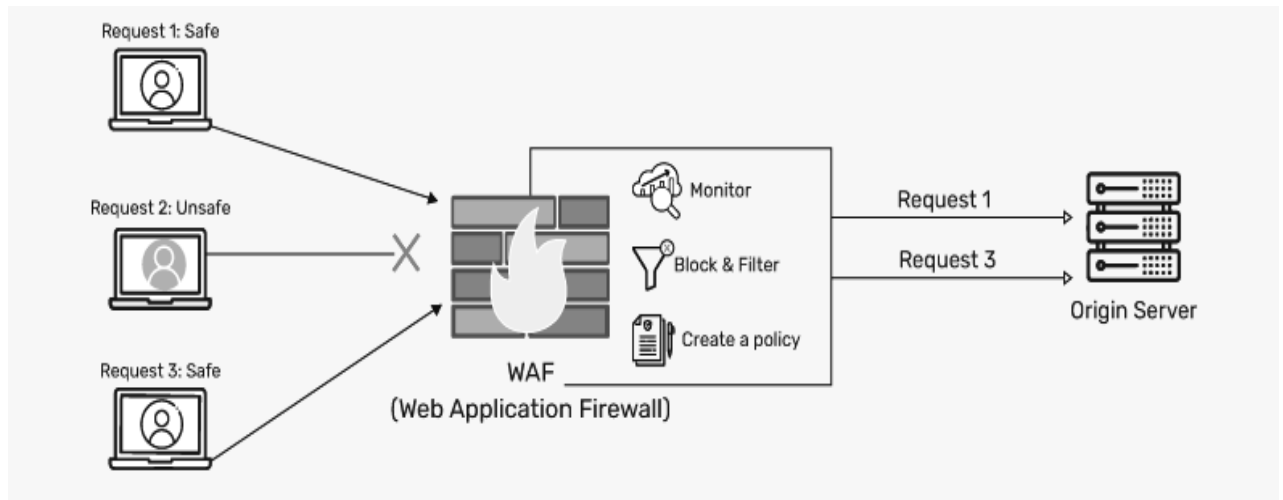


Рис. 1.17. Брандмауер вебдодатків [116].

Позитивна безпекова модель полягає у чіткому визначенні дозволених шаблонів та поведінки, дозволяючи лише легітимний трафік походження якого відоме та відхиляє все інше, що не збігається зі списком дозволеного [24].

У свою чергу, згідно з негативною безпековою моделлю, відбувається ідентифікація та блокування трафіку, що відповідає відомим шаблонам та сигнатурам, припускаючи, що будь-який трафік, який відповідає попередньо визначеним шаблонам атак є шкідливим [24].

Розвиток технологій штучного інтелекту дозволив значно розширити можливості WAF щодо виявлення та запобігання потенційних загроз. Це досягається шляхом навчання штучного інтелекту на базі атак, що відбуваються та, базуючись на отриманих даних, подальшій адаптації параметрів WAF для більш ефективної роботи [24]. Так, дослідники Іто Мічіакі (Ito Michiaki) та Іятомі Хітоші (Iyatomi Hitoshi), використовуючи брандмауер вебдодатків у поєднанні з машинним навчанням змогли досягнути точності 98.8% у виявленні шкідливих запитів, що надходили до тестового середовища [68].

Брандмауери вебдодатків відіграють ключову роль у забезпеченні стабільної роботи різноманітних електронних сервісів. Згідно з даними компанії Cloudflare, що являється одним зі світових лідерів у сфері захисту електронних сервісів, у четвертому кварталі 2023 року спостерігалось зростання загальної кількості DDoS атак на 117% в порівнянні з аналогічним періодом попереднього року (рис. 1.18) [132]. Використовуючи власні розроблені технології та кооперацію з іншими представниками галузі, компанії Cloudflare вдалося пом'якшити одну з найбільших DDoS атак, що складала 201 мільйон запитів на секунду [132].

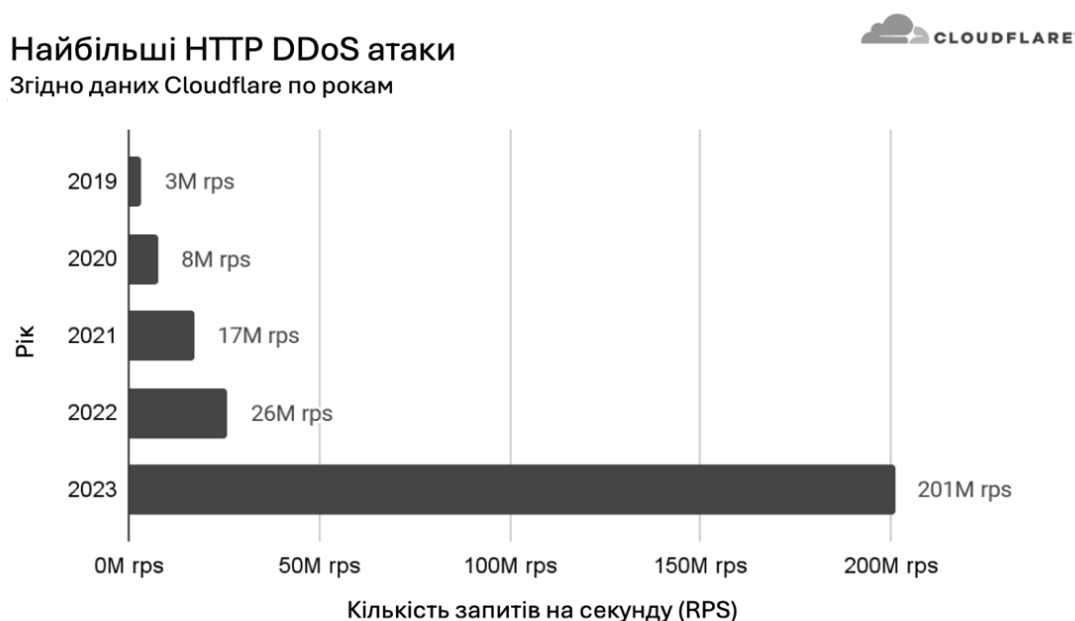


Рис. 1.18. Найбільші атаки HTTP DDoS за даними Cloudflare [132].

Системи моніторингу та журналювання являються невід'ємною частиною цілісної архітектури системи захисту. Моніторинг – це можливість мати інформацію, про певний момент у роботі інформаційної системи, а також історичний огляд попередніх станів системи, таких як продуктивність системи, цілісність даних, що обробляються інформаційною системою, доступність компонентів інформаційної системи [82]. Спостереження за цими станами дозволяє створити систему сповіщень, що буде інформувати відповідальних осіб у разі відхилень від заданих значень.

Журналювання – це процес агрегації записів про події, що відбуваються в інформаційній системі [82]. Вагомим фактором успішного впровадження систем журналювання, є визначення корисних даних для зберігання. Окрім цього, необхідно забезпечити надійне зберігання отриманої інформації, її конфіденційність та проводити періодичні перевірки правильності збору інформації згідно з заданими параметрами.

Часто недооцінені системи моніторингу та журналювання відіграють важливу роль, надаючи можливість вчасно виявляти проблеми та проводити аналіз подій, що відбулися, в розрізі певних проміжків часу. Так, організація OWASP, що є визнаним експертом в галузі кібербезпеки, визначає проблеми наявності систем моніторингу та журналювання чи правильності їх налаштування, як одну з десяти найпоширеніших безпекових загроз інформаційних систем [17].

Використання машинного навчання у поєднанні з системами моніторингу та журналювання значно покращує результати аналізу отриманих даних та виявлення аномалій і шаблонних дій, що могли бути непомітними для людини [90]. Як результат, вагомо підвищується швидкість та якість реагування на потенційні загрози, щодо інформаційної системи.

Науковці Цимін Цао (Qimin Cao), Іньюн Цяо (Yinrong Qiao), Чжун Лю (Zhong Lyu) у своєму дослідженні описують роботу системи виявлення аномалій з використанням машинного навчання для аналізу журналів роботи вебсервера [39]. Автори пропонують систему виявлення аномалій, що використовує дворівневий алгоритм машинного навчання (рис. 1.19). Модель дерева рішень класифікує нормальні та аномальні набори даних. Нормальний набір даних вручну перевіряється для створення кількох прихованих марковських моделей. Експериментальні дані надходили з журналів роботи реального вебсервера.

Отримані результати показали точність виявлення аномалій на рівні 93.54% та 4.09% хибнопозитивних результатів, в порівнянні з однорівневими алгоритмами машинного навчання. Автори зазначають, що будь-яка система виявлення аномалій з використанням машинного навчання, потребує постійного

оновлення, оскільки нові атаки змінюються, що, в свою чергу, знижує ефективність роботи системи виявлення. Тому автори планують додати до запропонованої системи модуль повторного навчання, який має оновлювати застарілі дані системи виявлення автоматично.

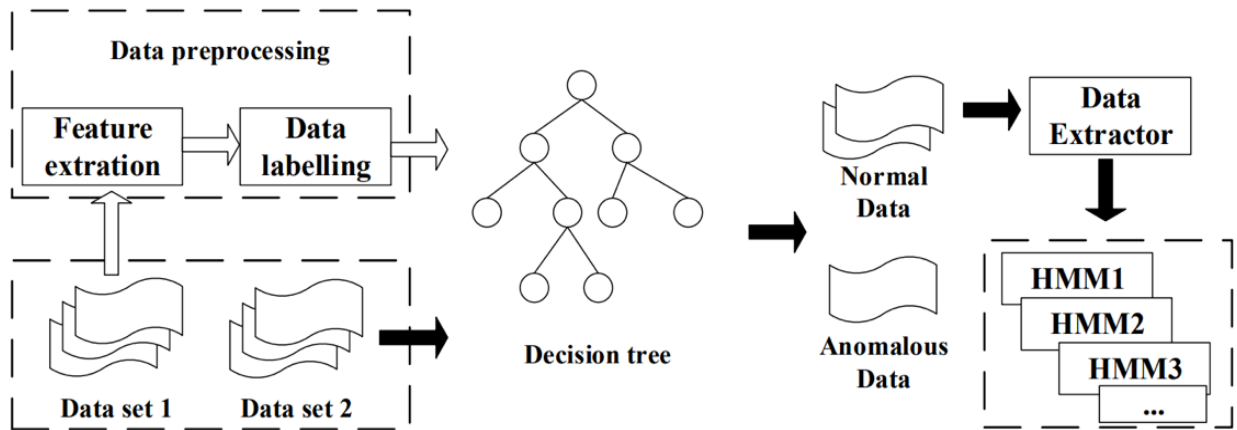


Рис. 1.19. Діаграма роботи запропонованої системи виявлення аномалій [39].

Важливим компонентом сучасної архітектури захисту електронних сервісів, що доповнює розглянуті системи моніторингу та журналювання, є системи управління інформацією та безпековими подіями (Security Information and Event Management, SIEM). На відміну від окремих систем моніторингу та журналювання, що аналізують події в межах одного компонента інформаційної системи, SIEM забезпечує централізований збір, нормалізацію та кореляцію безпекових подій з різномірних джерел, а саме – мережевих пристроїв, серверів, систем IDS/IPS, брандмауерів, WAF, баз даних тощо. Можливість виявляти складні багатоетапні атаки, ознаки яких розподілені між різними компонентами системи захисту та у часі, є принциповою перевагою SIEM перед ізольованими засобами моніторингу. М. Вільберт (M. Vielberth), Ф. Бем (F. Böhm), І. Фіхтінгер (I. Fichtinger) та Г. Пернул (G. Pernul) у систематичному дослідженні центрів безпекових операцій (Security Operations Center, SOC) розглянули SIEM як центральну технологічну платформу, що забезпечує роботу SOC [123]. Автори виявили, що ефективність SIEM суттєво залежить від якості правил кореляції та процедур реагування на інциденти, а основними відкритими викликами

залишаються висока кількість хибно-позитивних спрацьовувань та дефіцит кваліфікованих аналітиків для опрацювання потоку оповіщень. У контексті захисту сервісів електронної комерції SIEM дозволяє виявляти такі складні загрози, як повзучий брутфорс облікових даних, що розподіляється між численними IP-адресами для уникнення порогових обмежень, або аномалії у поведінці привілейованих облікових записів адміністраторів, що можуть свідчити про компрометацію або внутрішні загрози.

Системи шифрування користувацького трафіку та даних є однією з основних частин захисту інформаційної системи. Основною метою використання систем шифрування користувацького трафіку та даних є забезпечення цілісності та конфіденційності даних, унеможливлення втручання у процес передачі даних, забезпечення доступності даних для авторизованих користувачів (рис. 1.20) [115].



Рис. 1. 20. Основні вимоги до захисту мережі та комп'ютерних систем [115].

Одним з найрозповсюдженіших методів захисту користувацького трафіку від стороннього втручання, при роботі з електронними сервісами, є використання захисту на транспортному рівні (TLS). Це криптографічний протокол, що забезпечує безпечну передачу даних з використанням асиметричного шифрування та сертифікатів X.509 [115]. Протокол TLS є оновленою версією SSL, де усунули відомі вразливості. При комунікації з вебсерверами використання TLS реалізовується за допомогою протоколу HTTPS (HTTP, що передається через SSL або TLS). У цьому випадку шифруються

наступні елементи комунікації: адреса ресурсу з яким відбувається комунікація, дані що циркулюють між клієнтом і сервером (дані форм, cookies тощо), вміст HTTP заголовків [115].

Таким чином, сучасна комплексна система захисту електронного сервісу поєднує в собі засоби захисту мережевого периметра (брандмауери, IDS/IPS), захист на рівні застосунків (WAF), централізований збір та кореляцію безпекових подій (SIEM), шифрування трафіку та даних, а також організаційні заходи протидії соціальній інженерії. Кожен з перелічених компонентів покриває певний аспект безпекового периметру, а їх ефективна взаємодія формує багаторівневий захист, стійкий до різноманітних загроз. Ефективна інтеграція цих компонентів у єдину узгоджену архітектуру є ключовим чинником забезпечення надійного захисту сучасних сервісів електронної комерції та потребує системного підходу як на етапі проектування, так і під час їх промислової експлуатації.

Також, для гарантування безпечної передачі даних, широко використовуються протокол SSH (Secure Shell) та технологія побудови приватних тунелів VPN (Virtual Private Network). Протокол SSH реалізує можливості захищеного доступу до віддалених серверів, обміну файлами та поштовими повідомленнями. В свою чергу, технологія VPN дозволяє будувати захищені комунікаційні тунелі між віддаленими вузлами мережі. Дані в такому тунелі передаються у зашифрованому вигляді та повністю виключають зовнішнє втручання при обміні трафіком [127].

Для гарантування цілісності та конфіденційності даних, що зберігаються в середині інформаційної системи, використовуються алгоритми шифрування даних, серед розповсюджених можна виділити такі як AES, Triple DES, RSA, Blowfish, Twofish [108]. Шифрування даних може бути реалізовано як на апаратному рівні, так і на рівні операційної системи, що використовується. Важливо приділити увагу вибору методу шифрування, оскільки при великих об'ємах даних можливі проблеми з продуктивністю інформаційної системи, де відбувається робота з зашифрованими даними.

Згідно з доповіддю "Global Cybersecurity Outlook 2024", що була представлена на Всесвітньому економічному форумі, протистояння кіберзагрозам залишається актуальною проблемою для більшості компаній та організацій у всьому світі. Автори доповіді зазначають, що стрімкий розвиток та розповсюдження технологій разом з браком кваліфікованих кадрів у сфері кібербезпеки, є глобальним викликом на шляху до побудови безпечного середовища для функціонування інформаційних систем різних рівнів. Тільки 15% з опитаних організацій зазначили, що володіють необхідними ресурсами, щоб забезпечити значне покращення своєї кібербезпеки у наступні два роки. 52% з опитаних організацій відмічають брак ресурсів та досвідчених спеціалістів для побудови захищених інформаційних систем, що відповідають сучасним вимогам [59].

Серед можливих наслідків кібератак, найбільше занепокоєння опитаних організацій та компаній викликають можливість порушення операційної діяльності, фінансові і репутаційні втрати, втрата доступу до важливих товарів та сервісів (рис. 1.21) [59].

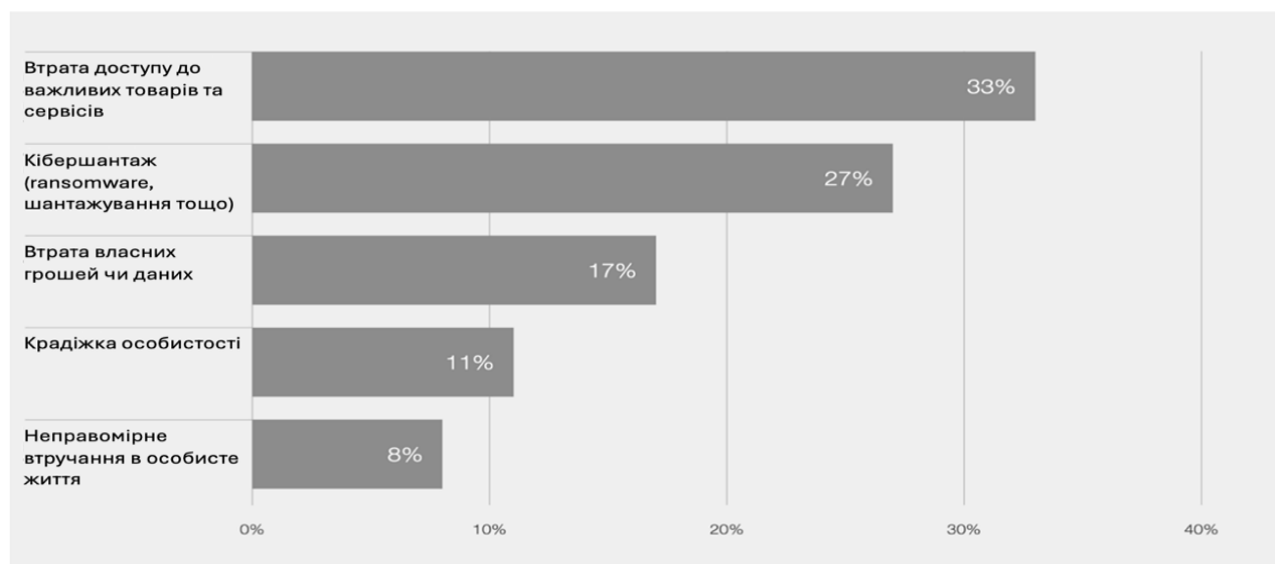


Рис. 1.21. Опитування «Global Cybersecurity Outlook 2024» [59].

1.4. Використання штучного інтелекту у системах захисту сервісів електронної комерції

Класичні методи захисту, що використовують статичні правила та ручний моніторинг, все частіше проявляють недостатню ефективність, коли з'являються складні та швидко еволюціонуючі шахрайські схеми. Подібні виклики збільшують потребу у використанні технологій штучного інтелекту, які у режимі реального часу здатні проводити аналіз великих обсягів даних, виявляти та реагувати на загрози [22].

За даними компанії Mastercard, втрати від шахрайської діяльності у сфері електронної комерції перевищують 40 мільярдів доларів [54]. У своєму щорічному звіті, присвяченому використанню платіжних систем у сфері електронної комерції, компанія Visa зазначає відчутне зростання кількості шахрайських дій, що спричиняють фінансові збитки, підривають довіру споживачів, а також спонукають компанії витрачати значні ресурси на боротьбу з діями шахраїв. Автори звіту оцінюють втрати компаній у 3% річного доходу [14].

Впровадження та використання систем штучного інтелекту у якості складової системи захисту сервісів електронної комерції розширює можливості для автоматизації процесів захисту, підвищує точність виявлення аномалій, збільшує швидкість реагування та адаптації до нових видів атак. Використання машинного навчання, поведінкового аналізу дій користувачів та постійне вдосконалення методів використання систем штучного інтелекту у системах захисту сервісів електронної комерції забезпечують проактивний, гнучкий та ефективний захист.

Таким чином, можна стверджувати, що застосування систем штучного інтелекту для забезпечення захисту сервісів електронної комерції є не лише сучасною тенденцією, а й умовою збереження довіри користувачів, підтримки фінансової стабільності бізнесу та готовності до новітніх безпекових викликів [10].

Поєднання системи захисту сервісів електронної комерції з системами

машинного навчання надає можливості з побудови моделей, що використовуються для аналізу історичних даних про транзакції та визначенні потенційно небезпечних або небажаних операцій. Виявлення аномалій у поведінці користувачів та обробка великих обсягів даних про транзакції відбувається у режимі реального часу з подальшим використанням отриманих результатів для вдосконалення механізмів захисту, що підвищує загальний рівень захищеності сервісів електронної комерції.

Група дослідників, у своїй роботі, присвяченій алгоритмам автоматизованого машинного навчання для виявлення шахрайських дій у цифрових платіжних системах, демонструє, що впровадження подібних систем має значні перспективи для підвищення точності визначення недоброчесних операцій [75].

Пропонується використовувати алгоритми з використанням Баєсівської оптимізації та генетичних алгоритмів для автоматизації вибору архітектури моделі, гіперпараметрів для налаштування моделі та визначення найважливіших змінних з наявних. Наступним кроком є створення ансамблів моделей для підвищення точності та надійності обробки даних.

У результаті проведених експериментів із використанням алгоритмів автоматизованого навчання, автор прийшов до висновку, що використані алгоритми автоматизації дозволяють за короткий час розглянути велику кількість варіантів моделей та складу вхідних даних. Побудований ансамбль моделей дозволив виявити до 85.7% шахрайських транзакцій. Водночас точність виявлення шахрайських транзакцій перебувала у діапазоні 79-85% [75].

Серед сучасних загроз сервісам електронної комерції окремо виділяють створення і використання підробних акаунтів користувачів. Дане явище стає значним безпековим ризиком, оскільки підробні профілі користувачів часто використовуються для проведення небажаних чи відверто шахрайських операцій, маніпуляцій з бонусними програмами, а також для атак на інфраструктуру компаній. Підробні акаунти активно використовують для маніпуляцій з рейтингами та відгуками, спотворення результатів пошуку та

рекомендаційних систем.

Під час пікових періодів бот-мережі створюють тисячі акаунтів для скуповування популярних товарів, що призводить до дефіциту для реальних покупців. У звіті компанії Radware, що є постачальником продуктів для кібербезпеки, вказується, що у сезон святкових розпродажів 2024 року понад 57% трафіку сервісів електронної комерції генерували саме боти [36].

Досліджуючи подібну проблему, Рауль Деко (Raoul Dekou) з групою співаторів пропонує об'єднане використання декількох моделей машинного навчання для отримання кращої продуктивності та точності результатів [51]. Об'єднана модель продемонструвала F1-міру зі значенням 0.73, що виявилось найвищим показником серед протестованих моделей (таблиця 1.1).

Незважаючи на високу точність визначення шахрайських акаунтів, ця проблема залишається актуальною та вимагає постійного оновлення моделей машинного навчання. Окрім цього, присутня загроза помилкового блокування легальних користувачів, особливо новостворених, де відсутня довга історія використання.

Таблиця 1.1

Порівняльна таблиця продуктивності протестованих моделей машинного навчання [51].

Модель	F1	Точність	Повнота	AUC
AutoML	0.7293	0.7206	0.7833	0.9850
Xgb	0.7134	0.7104	0.7165	0.9794
Catboost	0.7127	0.7375	0.6895	0.9809
RF	0.6810	0.7274	0.6401	0.9786

Окремо можна виділити перспективний напрямок з використання систем штучного інтелекту для впровадження поведінкової біометрії з безперервною аутентифікацією користувача. Це є суттєвим вдосконаленням систем захисту сервісів електронної комерції.

Концепція даного підходу полягає у неперервній оцінці унікальних шаблонів поведінки користувача та оцінки рівня довіри до нього. До унікальних

поведінкових шаблонів користувача можна віднести характер рухів миші, динаміку набору тексту, швидкість переходів між сторінками тощо. Ці параметри можуть бути поєднані з біометричними даними, такими як розпізнавання обличчя, голосу, відбитків пальців. Таким чином, створюється унікальний профіль користувача, що значно спрощує виявлення аномалій у його діяльності.

У контексті використання поведінкової біометрії для ідентифікації користувачів дослідники Чанг Жанг (Chang Zhang), Ючен Жанг (Yuchen Zhang) та Фулін Лі (Fullin Li) пропонують метод побудови унікальних характеристик користувача на базі аналізу його шаблонів набору тексту [133].

Автори використовують мультіваріативний процес Хоукса (Multivariate Hawkes Process) з експоненційним ядром для аналізу послідовностей натискання клавіш користувачем. Кожне натискання клавіші розглядається як подія у часовому просторі, де інтенсивність подій залежить від попередніх взаємодій.

У своєму дослідженні для визначення процесу Хоукса автори обрали метод визначення через умовну функцію інтенсивності (1.2) [133].

$$\lambda_i(t) := \mu_i(t) + \sum_{j=1}^D \int_{-\infty}^t g_{ij}(t - \tau) dN_j(\tau) \quad (1.2)$$

Дана формула (1.2) базується на припущенні, що багатовимірний лічильний процес $\mathbf{N}(t) = \{N_i(t)\}_{i=1}^D$, де $N(0)=0$, його розмірність дорівнює D , умовна функція інтенсивності має вигляд $\lambda(t) = \{\lambda_i(t)\}_{i=1}^D$, μ_i – константа, що визначає інтенсивність виникнення подій типу i . $G(t) = [g_{ij}(t)]_{i,j=1}^D \in D \times D$ -вимірною матрицею ядра збудження, а функція збудження $g^{ij} \geq 0$ описує стимул подій, що відбулися в поточному j -му вимірі багатовимірного процесу Хоукса на інтенсивність події i -го виміру [133].

Дослідники роблять висновки, що процес Хоукса доцільно застосовувати для статистичного опису часових послідовностей натискання клавіш, оскільки його умовна інтенсивність $\lambda(t)$ відтворює самозбудження цієї активності – ймовірність настання події зростає одразу після попередньої та експоненціально

згасає з плином часу. Працюючи неперервно, модель зберігає інформаційний зміст інтервалів між подіями без необхідності їх дискретизації, що критично важливо для виявлення відхилень на коротких часових проміжках [133]. Використання процесу Хоукса поєднує точність, інтерпретованість та обчислювальну ефективність, що робить його корисним інструментом для підвищення безпекових параметрів сервісів електронної комерції.

Серед методів машинного навчання, що знаходять широке застосування у системах захисту сервісів електронної комерції, виділяють графові нейронні мережі (Graph Neural Networks, GNN). Специфіка роботи з ними полягає у здатності GNN якісно моделювати структурні зв'язки між елементами системи, що є важливим етапом виявлення складних шахрайських схем. Ю. Ду (Y. Dou), З. Лю (Z. Liu), Л. Сунь (L. Sun), Дж. Денг (J. Deng), Г. Пенг (H. Peng), П. С. Юй (P. S. Yu) запропонували підхід на основі GNN для виявлення шахрайства у наборах даних, де шахрайські дії суттєво поступаються кількістю легітимним, що є типовою характеристикою даних сервісів електронної комерції [53]. Автори ідентифікували ключову проблему – мала кількість шахрайських транзакцій суттєво ускладнює навчання класифікаторів через переважання «нормальних» прикладів у тренувальних наборах. Для подолання цього обмеження авторами запропоновано метод балансування графів через вибіркове дублювання ребер між шахрайськими вузлами, що дозволяє підвищити представленість цільового класу без введення синтетичних прикладів. Отримані результати продемонстрували суттєве підвищення F1-міри для класу шахрайських транзакцій порівняно з традиційними методами машинного навчання та базовими підходами на основі GNN. Особливістю застосування GNN у задачах виявлення шахрайства є можливість врахування не лише характеристик окремих транзакцій чи акаунтів, але й характеру їх взаємодії з іншими елементами графу. У своїй іншій роботі автори демонструють алгоритм виявлення шахрайства на основі гетерогенних графів, що дозволяє моделювати різнотипні відношення між акаунтами, транзакціями та пристроями [81]. Зокрема, запропонована модель враховує такі типи зав'язків: спільне використання пристроїв різними акаунтами,

транзакції між акаунтами, спільні адреси доставки та інші атрибути, що можуть свідчити про координовану шахрайську активність. Модель демонструє здатність виявляти скоординовані шахрайські схеми, в яких учасники свідомо розподіляють активність між різними акаунтами з метою уникнення спрацьовування систем захисту, що аналізують кожен акаунт ізольовано. Авторами також показано, що запропонований підхід є стійким до стратегії «маскування», коли зловмисники намагаються імітувати поведінку легітимних користувачів для обходу захисних механізмів.

Практичне впровадження GNN у системи захисту сервісів електронної комерції постають перед рядом технічних та організаційних викликів. По-перше, великі сервіси електронної комерції оперують графами, що можуть містити сотні мільйонів вузлів та мільярди ребер, що висуває серйозні вимоги до масштабованості алгоритмів навчання. По-друге, конфіденційність даних, необхідних для побудови графу транзакцій, вимагає особливої уваги до питань анонімізації та обмеження доступу. По-третє, динамічна природа шахрайських схем зумовлює необхідність регулярного перенавчання або онлайн-адаптації моделей для підтримання їх ефективності в умовах постійно змінюваних тактик зловмисників. Незважаючи на ці виклики, GNN є перспективним напрямком розвитку систем виявлення шахрайства та несанкціонованого доступу у сервісах електронної комерції завдяки здатності виявляти складні реляційні шаблони дій, що залишаються прихованими для традиційних алгоритмів класифікації.

Широке впровадження методів машинного навчання у системи захисту сервісів електронної комерції створює нові загрози, пов'язані з можливістю цілеспрямованого маніпулювання цими системами з боку зловмисників. М. Голдблум (M. Goldblum), Д. Ціпрас (D. Tsipras), К. Ксе (C. Xie), К. Чен (X. Chen), А. Шварцшильд (A. Schwarzschild), Д. Сонг (D. Song), А. Мадрі (A. Madry), Б. Лі (B. Li), Т. Голдштейн (T. Goldstein) у своєму дослідженні безпеки наборів даних та систем машинного навчання класифікують атаки, спрямовані проти систем на основі штучного інтелекту, за двома основними категоріями – атаки на стадії навчання, відомих як «отруєння даних», та атаки на стадії взаємодії з системою

штучного інтелекту (обхід обмежень моделі) [61]. Атаки типу «отруєння даних» передбачають цілеспрямоване введення злоякісних прикладів до тренувального набору системи виявлення шахрайства з метою деградації її точності або формування специфічних сліпих зон, що залишають певні типи шахрайських транзакцій невиявленими. Для сервісів електронної комерції, де використовуються онлайн помічники з функцією неперервного навчання, коли модель адаптується на основі потоку нових запитів від користувачів, цей тип атак є особливо небезпечним.

Атаки під час взаємодії з системою штучного інтелекту полягають у цілеспрямованій модифікації вхідних даних шахрайських транзакцій чи поведінки акаунтів таким чином, що вони класифікуються захисною системою як легітимні. Принципова вразливість систем машинного навчання до таких атак пов'язана з дискретністю границь рішень навчених класифікаторів у просторі ознак. Зловмисник, що має доступ до зворотного зв'язку від системи захисту, наприклад, результатів блокування транзакцій, може систематично зондувати межі цих рішень, поступово адаптуючи шахрайські схеми до сліпих зон моделі. Для підвищення стійкості систем машинного навчання до атак такого типу дослідники пропонують декілька взаємодоповнюючих стратегій. По-перше, включення до тренувального набору синтезованих прикладів, що направлені на підвищення якості роботи моделі на межах рішення. По-друге, застосування ансамблевих методів з випадковими підпросторами ознак суттєво ускладнює перенесення атак між різними компонентами ансамблю. По-третє, впровадження перевірки узгодженості вхідних даних та детекторів розподілу поза тренувальним простором, це дозволяє виявляти нетипові запити до системи до їх передачі на класифікацію. Розробники систем захисту сервісів електронної комерції повинні розглядати стійкість до такого роду атак як окрему вимогу до якості системи, що регулярно перевіряється в рамках тестування на проникнення.

Великі мовні моделі (Large Language Models, LLM) відкривають принципово нові можливості для автоматизації процесів аналізу загроз та

реагування на безпекові інциденти, що виникають під час роботи сервісів електронної комерції. М. А. Ферраг (M. A. Ferrag), М. Ндхлову (M. Ndhlovu), Н. Тіханьї (N. Tihanyi), Л. К. Кордейро (L. C. Cordeiro), М. Деббах (M. Debbah), Т. Лестабль (T. Lestable), Н. Шендеб Тарабіа (N. Chendeb Tarabia) у своєму огляді досліджень у галузі застосування LLM для виявлення кіберзагроз аналізують широку вибірку сценаріїв, де генеративний штучний інтелект здатний суттєво підвищити ефективність та швидкість роботи аналітиків безпеки[56]. Зокрема, автори виділяють такі ключові напрямки застосування, як автоматичне опрацювання та структурування звітів вразливостей з відкритих баз даних (CVE, NVD) для оперативного оновлення систем захисту, генерація правил виявлення для систем IDS/IPS, SIEM та WAF на основі описів нових типів атак природною мовою, автоматизована пріоритизація потоку безпекових оповіщень для зниження навантаження на аналітиків безпеки. Для сервісів електронної комерції LLM також можуть застосовуватися для семантичного аналізу відгуків, повідомлень підтримки та контенту, що завантажуються користувачами, з метою виявлення ознак фішингових кампаній, соціальної інженерії або координованих зловживань платформою.

Напрямок застосування LLM, де їх можливості проявляються найкраще, є аналіз журналів безпекових подій. Традиційні підходи до аналізу журналів ґрунтуються на пошуку відповідності регулярним виразам та заздалегідь визначеним сигнатурам, що не дозволяє виявляти нові або ретельно замасковані атаки. Застосування LLM для цієї задачі дозволяє аналізувати послідовності подій у журналах на рівні їх змістового значення, а не лише формального синтаксису, що відкриває можливість виявлення аномальних шаблонів дій без їх попереднього опису. Крім того, LLM здатні виявляти зв'язки між подіями, розподіленими у часі та між різними компонентами системи, що є складним процесом для традиційних засобів аналізу журналів. Автори підкреслюють, що ефективне застосування LLM у кібербезпеці потребує їх спеціалізованого тонкого налаштування з використанням репрезентативних наборів даних,

включаючи бази вразливостей, звіти про інциденти та журнали безпечних систем [56].

Незважаючи на значний потенціал, застосування LLM у системах захисту сервісів електронної комерції вимагає зваженого підходу та аналізу можливих ризиків. Зокрема, атаки типу «ін'єкція підказки» дозволяють зловмиснику маніпулювати обробкою вхідних даних LLM складовою системи захисту, потенційно обходячи захисні механізми або отримуючи несанкціоновану інформацію. Крім того, LLM можуть генерувати хибні висновки або «галюцинації» при аналізі безпекових даних, що може призвести до пропуску реальних загроз або блокування легітимних операцій. Автори рекомендують застосовувати LLM у ролі допоміжного інструменту підтримки прийняття рішень, а не як автономний інструмент [56]. Таким чином, інтеграція LLM у системи захисту сервісів електронної комерції є перспективним напрямком, що потребує збалансованого підходу, поєднуючи переваги генеративного штучного інтелекту з необхідним рівнем передбачуваності та аналізу прийнятих рішень.

Незважаючи на всі переваги використання систем штучного інтелекту у системах захисту сервісів електронної комерції, слід зазначити, що їх інтеграція у робочі процеси потребує виваженого аналізу та додаткових перевірок на дотримання вимог безпечної обробки даних. Некоректна конфігурація таких систем, недостатній контроль за доступом до навчальних даних або відсутність механізмів аудиту можуть призвести не лише до витоку даних, а й до порушення вимог чинного законодавства у сфері захисту персональних даних, наприклад загальноєвропейський регламент захисту даних GDPR. Усе це свідчить про те, що впровадження штучного інтелекту у системи захисту сервісів електронної комерції має супроводжуватись не лише технічними, а й організаційними та правовими дослідженнями. Це у своїй роботі також підкреслює дослідник Алок Джаккула (Alok Jakkula), у якій вказує про важливість застосування надійних безпекових заходів при залученні систем штучного інтелекту для опрацювання даних, що використовуються системами електронної комерції, що мають бути поєднані з чіткими та прозорими правилами контролю їх виконання [69].

Висновки до першого розділу

У першому розділі – "Аналіз методів, засобів та технологій оцінки ефективності роботи систем захисту вебсервісів" було вивчено стан досліджень у галузі розробки та функціонування систем захисту сервісів електронної комерції; проведено огляд наявних методів оцінки ефективності роботи систем захисту сервісів електронної комерції; проведено огляд сучасних систем захисту електронних сервісів, досліджено можливості використання штучного інтелекту у системах захисту сервісів електронної комерції.

Проведений комплексний аналіз стану досліджень у галузі розробки та функціонування систем захисту сервісів електронної комерції дозволяє стверджувати, що на сьогоднішній день єдиного, уніфікованого підходу до вирішення питань захисту не існує. Дана проблема залишається актуальною, оскільки сфера кіберзагроз постійно еволюціонує. У відповідь на ці виклики дослідницька спільнота продовжує активну роботу над створенням нових алгоритмів та методик, спрямованих на поглиблення аналізу систем захисту сервісів електронної комерції та загальне підвищення рівня їхньої захищеності.

Огляд наявних методів оцінки ефективності роботи систем захисту демонструє сталий науковий інтерес до цієї проблематики. Проте динамічний розвиток технологій вимагає не лише вдосконалення вже наявних підходів, але й розробки принципово нових інструментів.

Впровадження та широке розповсюдження сучасних систем захисту електронних сервісів відіграє критичну роль у побудові цілісного периметра захисту інформаційних систем. В умовах постійного розширення поля кібератак, організації, що нехтують використанням актуальних засобів захисту, наражаються на значні фінансові та репутаційні ризики. Аналіз інформаційних джерел щодо цієї тематики свідчить про те, що розвиток галузі зосереджено не лише на посиленні захисних механізмів, а й на пошуку підходів для безшовної інтеграції нових рішень з вже працюючими інформаційними системами.

Якісно новим етапом розвитку є перехід до адаптивних рішень, здатних функціонувати в режимі реального часу. Інтеграція наявних безпекових рішень

з системами штучного інтелекту відкриває широкі можливості для аналізу подій та поведінкових особливостей користувачів. Використання систем штучного інтелекту дозволяє значно підвищити ефективність виявлення аномалій та загроз, знизити частку хибних спрацювань, що є критичним для безперебійної роботи бізнесу, і, завдяки прозорій побудові моделей, полегшує аудит рішень, прийнятих системою захисту та дотримання нормативних вимог.

Результати досліджень представлені в наукових публікаціях здобувача [2; 3; 4; 5; 6].

РОЗДІЛ 2. Метод оцінки ефективності роботи систем захисту сервісів електронної комерції

2.1. Проблеми оцінки ефективності захисту сервісів електронної комерції

Проведений аналіз наявних методів та засобів оцінки ефективності роботи систем захисту сервісів електронної комерції дозволяє зробити висновок, що наявні підходи недостатньо враховують специфіку функціонування сервісів електронної комерції. У більшості випадків традиційні методи оцінки ефективності захисту інформаційних систем першочергово орієнтовані на оцінку захисту корпоративних мереж та супутньої інфраструктури.

Основним інструментом оцінки виявлених вразливостей є система Common Vulnerability Scoring System (CVSS), завданням якої є забезпечення стандартизованого методу класифікації безпекових ризиків за десятибальною шкалою [48]. Метод оцінки вразливостей з використанням CVSS є статичним та не враховує зміни середовища, що оцінюється, протягом певного відрізка часу. Окрім цього, оцінка CVSS може відрізнятись у залежності від того, хто проводив оцінювання [131]. Таке неузгодження має вплив на оцінювання ефективності роботи системи захисту в цілому. Автори Дж. Спрінг (J. Spring), Е. Хатлбек (E. Hatleback), А. Хаусхолдер (A. Householder), А. Меніон (A. Manion) та Д. Шік (D. Shick) у своїй роботі зазначають, що початково оцінка CVSS не призначалась для використання у якості методу оцінки безпекових ризиків, проте використовується саме таким чином [113].

Моделювання атак та тестування на проникнення спрямовані на імітацію реальних атак і дозволяють провести аналіз роботи систем захисту в динаміці. Ці методи допомагають виявляти невідповідності у конфігураціях різних елементів системи захисту, перевірити наявність недоліків у роботі програмного та апаратного забезпечення системи захисту, оцінити можливість експлуатації потенційних вразливостей. Однак зазначені методи переважно орієнтовані на бінарні підходи у своїй роботі, та рідко здатні побудувати складні взаємозв'язки функціонування різних складових захисту інформаційних систем. Цю

особливість використання зазначених методів підкреслюють у своєму дослідженні автори С. Хігаші (S. Higashi), П. Крайкрітаякул (P. Kraikritayakul), Ю. Лю (Y. Liu), М. Ікеда (M. Ikeda), К. Мацуо (K. Matsuo), Л. Бароллі (L. Barolli) [63]. Автори також пропонують методи для побудови градієнтної оцінки безпекових ризиків з використанням нечіткої логіки.

Значна частина традиційних методів оцінки ефективності роботи систем захисту має на меті перевірку на відповідність певним стандартам та законодавчим вимогам. До таких стандартів та вимог можна віднести PCI DSS, GDPR тощо. Перевагою такого підходу є систематичний та комплексний аналіз стану функціонування системи захисту, а також наявності відповідних безпекових процедур та політик внутрішнього та зовнішнього контролю. Проте відповідність стандартам не є гарантією захисту, а лише її складовою. Цей аспект зазначають автори Ф. Джалалванд (F. Jalalvand), М. Б. Чхетрі (M. B. Chhetri), С. Непал (S. Nepal) та К. Паріс (C. Paris) [70] у своїй роботі з оцінки роботи центрів обробки безпекових подій.

Одним з поширених підходів до оцінки безпекових ризиків є класифікація ресурсів, що потребують захисту, за важливістю з подальшою пріоритезацією на основі потенційного впливу компрометації ресурсу [30]. Згідно з дослідженням Д. Бехбехані (D. Behbehani), Н. Комнінос (N. Komninos), К. Аль-Бегейн (K. Al-Begain), більшість наявних моделей для оцінки ризиків не в повній мірі забезпечують можливість отримання кількісної оцінки поточних безпекових ризиків для подальшого прийняття рішень, що матимуть вплив на бізнес [28].

Основною відмінністю сервісів електронної комерції від звичних інформаційних систем, де основним аспектом роботи є захист даних у стані спокою (data at rest), постійна робота з фінансовими транзакціями [92, 80]. Кожен безпековий інцидент має вплив на конверсію, продажі та довіру клієнтів. Ефективний захист конфіденційних даних користувачів збільшує довіру до сервісів електронної комерції, що безпосередньо впливає на розвиток бізнесу загалом.

Кожен етап взаємодії користувача з сервісом електронної комерції містить різні ризики та вимоги до захисту. Наявні методи оцінки ефективності захисту інформаційних систем не виділяють ці етапи окремо.

Окремо слід виділити такі особливості сучасних систем електронної комерції, як багатоканальність взаємодії з кінцевими користувачами та сезонність навантажень. До каналів взаємодії з користувачами відносяться вебсайти, торговельні майданчики, додатки для мобільних телефонів, соціальні мережі тощо [79]. Таке різноманіття створює багатовимірні сценарії взаємодії з сервісами електронної комерції та значно розширює поле для потенційних дій зловмисників. В умовах екстремальних навантажень, характерних для періодів сезонних розпродажів, коли спостерігається одночасне зростання кількості легітимних користувачів, трафіку від різноманітних ботів та зловмисників, сервіси електронної комерції функціонують у режимі, що вимагає застосування принципово відмінного підходу до оцінювання ефективності механізмів захисту, порівняно з традиційними корпоративними інформаційними системами, яким притаманний стабільний та, як правило, прогнозований рівень навантаження.

Загальноприйняті безпекові метрики, такі як True Positive Rate (TPR), False Positive Rate (FPR), Mean Time to Detect (MTTD), Mean Time to Respond (MTTR) широко використовуються для оцінки ефективності систем виявлення вторгнень. Однак у контексті роботи систем електронної комерції перераховані метрики не дають комплексного уявлення про вплив безпекових подій на систему загалом [30]. Системи електронної комерції в процесі своєї роботи опрацьовують персональні дані користувачів, різноманітні платіжні дані, інтегруються із зовнішніми бізнес-процесами. Кожен з цих вимірів потребує захисту, але в той самий час оцінка захищеності кожного компоненту окремо не надає розуміння стану захисту системи загалом.

Традиційні безпекові метрики були створені і переважно використовуються для оцінювання технічної складової ефективності роботи безпекових механізмів інформаційних систем, але без урахування наслідків безпекових інцидентів для бізнесу [63, 70]. Ця компонента є ключовою для

якісної оцінки ефективності роботи системи захисту сервісів електронної комерції. Важливість врахування наслідків для бізнесу при оцінці безпекових ризиків для систем електронної комерції у своїх дослідженнях також підкреслено багатьма авторами [28, 92].

Більшість з наявних методів оцінки захищеності інформаційних систем забезпечують статичну оцінку їх стану. Такий підхід не враховує динамічну складову сервісів електронної комерції та загроз інформаційній безпеці. На цьому наголошують у своєму дослідженні автори [25] та пропонують використання часових характеристик мережевих конфігурацій та вразливостей для подальшої оцінки ризиків.

Використання Баєсівських мереж є поширеним інструментом для вирішення цієї проблеми. Вони дозволяють проводити моделювання причинно-наслідкових зв'язків між вразливостями та ймовірностями успішних атак, перетворюючи розрізнені дані про загрози на структуровані ймовірнісні моделі. Врахування фактору часу стає доступним при застосуванні динамічних Баєсівських мереж. Зокрема, група авторів пропонують підхід з використанням динамічних Баєсівських мереж для кількісної оцінки безпекових ризиків у реальному часі [77]. Проте, незважаючи на широкі можливості, що надає використання Баєсівських мереж для оцінки ризиків зокрема та роботи системи захисту в цілому, наявні моделі переважно орієнтовані на мережеву інфраструктуру і рідко враховують транзакційну динаміку та особливості бізнес-процесів систем електронної комерції.

Однією з ключових технічних проблем наявних підходів є агрегація метрик різного походження та типу у єдину кількісну оцінку ефективності роботи системи захисту. Так, група авторів на чолі з У. Бансал. (U. Bansal) у своїй роботі демонструють, що кількісна оцінка великих наборів вразливостей потребує додаткового застосування аналізу витрат та вигоди. Автори зазначають, що проста лінійна агрегація навіть однотипних безпекових метрик не враховує всю множину можливих шляхів атак та зусиль, необхідних для їх

реалізації. Як наслідок, отримані значення можуть не в повній мірі відображати реальний стан захищеності системи [26].

У контексті складності агрегації метрик можна зазначити наступні фактори: різнорідність метрик – метрики FPR чи TPR вимірюються у відсотках, часові метрики як MTTD та MTTR у секундах чи хвилинах, фінансові метрики потребують вираження у грошових одиницях. Приведення їх до єдиної шкали потребує застосування процедур нормалізації з обґрунтованим підходом, що враховує контекст використання метрик. Різна спрямованість метрик, коли для деяких метрик більше значення є кращим, а для інших навпаки, ускладнює об'єднання їх у єдину оцінку. Деякі метрики не мають лінійних залежностей, так, наприклад, значення метрики FPR за різних умов матиме різний практичний ефект для роботи системи в цілому. Врахування контексту метрик також несе вагоме практичне значення, так як важливість певних метрик може варіюватись у залежності від направленості та виду діяльності сервісу електронної комерції. Для систем електронної комерції, де є необхідність інтеграції технічних та бізнес-метрик, проблема якісної агрегації метрик постає особливо гостро.

Встановлені проблемні аспекти можуть бути згруповані за трьома основними напрямками: методологічний, технічний та контекстний. Кожна з трьох груп характеризує окремі аспекти обмежень наявних підходів щодо оцінки ефективності захисту сервісів електронної комерції. Використання такої класифікації забезпечує можливість структурованого аналізу та визначення ключових напрямків подальшого розвитку методів оцінювання.

На основі проведеного аналізу узагальнено інформацію щодо проблемних аспектів наявних методів оцінки ефективності роботи системи захисту сервісів електронної комерції, що представлена у таблиці 2.1.

Проведений аналіз демонструє, що наявні підходи до оцінки захищеності інформаційних систем не може бути безпосередньо застосований для оцінки ефективності системи захисту сервісів електронної комерції. Традиційні метрики надають часткову технічну оцінку без урахування бізнес-контексту.

Таблиця 2.1.

Огляд проблемних аспектів наявних методів оцінки ефективності роботи системи захисту

Напрямок	Проблемний аспект	Короткий опис	Наслідки для сервісів електронної комерції
Методологічний	Статичність оцінок	Методи не враховують динамічність сервісів електронної комерції та розвитку загроз	Невідповідні реакції систем захисту під час сезонних навантажень
	Фрагментарність оцінки	Метрики не враховують комбіновані вразливості	Неможливо отримати цілісну картину стану захисту системи
	Відсутність бізнес-контексту	Технічні метрики не враховують фінансової складових процесів	Відсутність врахування впливу безпекових інцидентів на довіру користувачів, конверсію, репутацію
Технічний	Проблема агрегації метрик	Метрики різної природи та походження потребують методів для їх об'єднання	Відсутність повноцінних зв'язків між технічними та бізнес-метриками
	Орієнтація на мережеву інфраструктуру	Наявні методи націлені на роботу з корпоративними мережами та інфраструктурою	Специфіка роботи сервісів електронної комерції та супутніх бізнес-процесів не врахована
Контекстний	Відсутність врахування специфіки роботи сервісів електронної комерції	Наявні методи не враховують транзакційну особливість сервісів електронної комерції, багатоканальність та сезонність	Неповна оцінка безпекових ризиків для різних етапів взаємодії користувача з сервісом електронної комерції
	Неврахування зручності користування сервісом у контексті роботи систем захисту	Зручність користування рідко враховується при оцінці захисту	Можлива втрата клієнтів через надмірні безпекові заходи чи навпаки через пріоритет зручного інтерфейсу над безпекою

Транзакційна специфіка сервісів електронної комерції має слабке відображення у наявних методах оцінки захисту. Традиційні багаторівневі підходи оцінки систем захисту в першу чергу орієнтовані на недопущення безпекових інцидентів, але не на аналіз ефективності їх роботи.

Динамічна оцінка ризиків для систем захисту залишається актуальною дослідницькою проблемою. На цьому наголошують П. Хеймонідіс (P. Cheimonidis) та К. Рантос (K. Rantos) у своєму дослідженні, присвяченому даній тематиці [40]. У контексті сервісів електронної комерції, де системи постійно змінюються, адаптуючись до вимог бізнесу, ці обмеження мають критичний характер.

Таким чином, можна зробити висновок, що існує об'єктивна потреба у розробці нового методу, що дозволить об'єднати переваги наявних підходів та усунути їх недоліки, створюючи можливості для проведення комплексної оцінки ефективності роботи систем захисту сервісів електронної комерції.

2.2. Загальна архітектура методу аналізу ефективності системи захисту сервісів електронної комерції.

В основу запропонованого методу покладено багаторівневу архітектуру оцінки ефективності системи захисту. Використання багаторівневого аналізу безпекових подій забезпечує умови для систематичної трансформації технічних метрик від нижчих рівнів до узагальненої оцінки ефективності роботи системи захисту.

У межах даного дослідження під *системою захисту сервісу електронної комерції* розглядається сукупність наявних безпекових механізмів, що мають вплив на роботу сервісу електронної комерції на різних рівнях роботи інформаційної системи, та дії якої можуть бути журнальовані та передані для подальшої обробки для класифікації та кореляції з іншими подіями за той самий проміжок часу.

Пропонується поетапний збір та нормалізація даних на кожному з рівнів, що має на меті розмежування задач аналізу, зменшення складності обробки даних та прозорість аудиту подій у системі при переходах між рівнями, що, в свою чергу, робить можливим оцінити внесок кожного з рівнів у формування загальної оцінки ефективності системи захисту сервісів електронної комерції. Для кожного з рівнів визначені його призначення, вхідні дані та очікуваний результат, який передається на наступний етап аналізу.

Використання багаторівневої архітектури при побудові методу аналізу ефективності системи захисту сервісів електронної комерції закладає основу для подальшої адаптації методу до конкретних потреб сервісів електронної комерції в залежності від наявних захисних механізмів та джерел безпекових подій. Такий підхід дозволяє уникати масштабних змін у методі в цілому та проводити коригування лише на відповідних рівнях аналізу з можливістю гнучкого масштабування.

Застосування багаторівневих підходів у сучасних безпекових рішеннях не є новим та широко використовується. Подібний підхід формалізовано у стандартах NIST [110] та ISO [67], відповідно до яких система захисту розглядається як сукупність взаємопов'язаних компонентів або рівнів. Автори Д. Рю (D. Ryu), С. Лі (S. Lee), С. Ян (S. Yang), Дж. Джон (J. Jeong), Ю. Лі (Y. Lee) та Д. Шін (D. Shin) у своєму дослідженні багаторівневого захисту інформаційних систем, пропонують п'ятирівневу архітектуру безпекового рішення, яка забезпечує специфічний тип захисту на кожному з рівнів [105]. Схожу концепцію у своєму дослідженні описують Е. Вай (E. Wai) та К. К. М. Лі (C. K. M. Lee), зазначаючи, що кожен з рівнів багаторівневої системи захисту забезпечує незалежний захист, водночас реалізуючи узгоджену стратегію захисту [124].

Однак аналіз наявних підходів виявляє, що фокус досліджень акцентовано на технічній спроможності запобігання безпековим інцидентам, в той час як оцінка ефективності цих заходів у контексті бізнесу залишається недостатньо вивченою. Як зазначають у своєму дослідженні Елені Філіппу (Eleni Philippou), Сільвен Фрей (Sylvain Frey) та Аваїс Рашид (Awais Rashid), більшості організацій

доводиться розв'язувати проблему розриву між технічними показниками безпекових метрик та їх реальним впливом на бізнес-процеси [97]. Маркус Пенделтон (Marcus Pendleton) з групою авторів у своїй роботі присвяченій безпековим метрикам наголошує, що більшість наявних фреймворків оцінювання захисту зосереджені на технічній ефективності контролю, водночас ігноруючи їх операційні та організаційні витрати [96].

Запропонована узагальнена архітектура методу аналізу ефективності системи захисту сервісів електронної комерції містить чотири рівні (рис. 2.1), що забезпечує покриття від технічних метрик до оцінки впливу на бізнес без надлишкової складності. Розглянемо детально кожен рівень.

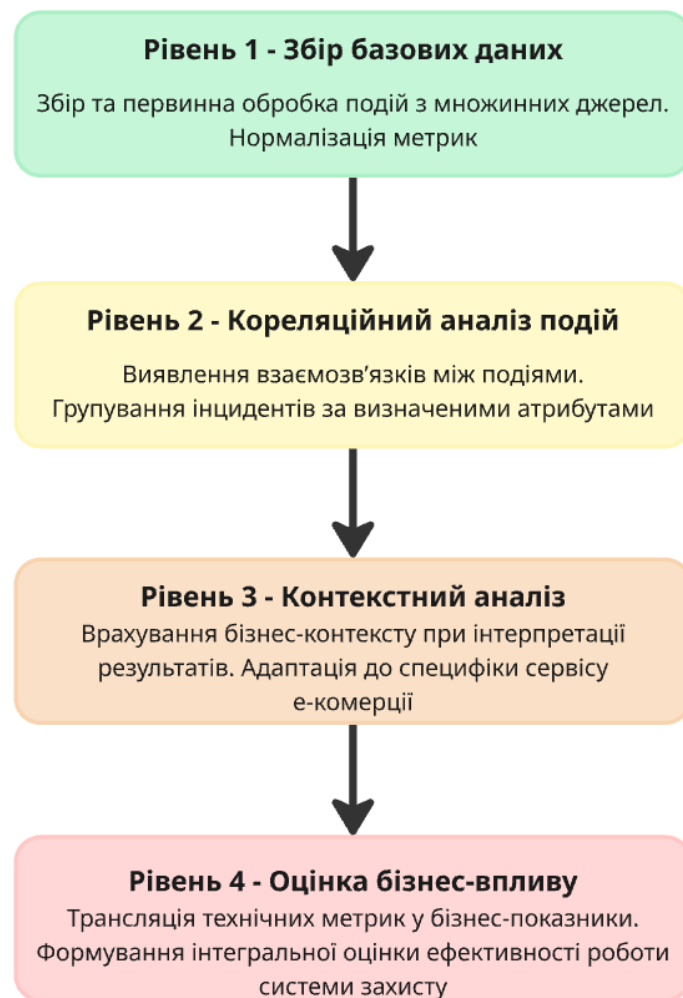


Рис. 2.1. Узагальнена архітектура методу

Рівень 1 – збір базових даних. Цей рівень забезпечує етап збору та первинної обробки сирих подій, пов'язаних з роботою сервісу електронної

комерції, що надходять з множинних джерел. До вхідних даних на цьому рівні відносяться безпекові події від систем виявлення вторгнень, SIEM систем, логи вебсерверів, результати сканування на вразливості, метрики брандмауерів вебдодатків (WAF), логи авторизації та аутентифікації, інформація про використання сертифікатів та шифрування, дані моніторингу доступності вебдодатку, дані про платіжні транзакції, метрики CDN тощо. Отримані дані приводяться до єдиного формату зі стандартизацією часових міток та уніфікацією форматів даних, класифікуються за типами загроз, збагачуються додатковою контекстною інформацією про етапи взаємодії користувача з сервісом електронної комерції.

Вихідними даними першого рівня є нормалізовані метрики у стандартизованому форматі, що містять необхідну для подальшого аналізу інформацію.

Рівень 2 – кореляційний аналіз подій. На даному етапі забезпечується виявлення взаємозв'язків між окремими безпековими подіями. Проводиться кореляція подій на основі подібності: порівняння атрибутів подій, ідентифікація джерел подій, групування за цільовим призначенням. Застосовується часова кореляція подій, що забезпечує виявлення послідовності подій у часі, визначення шаблонів виникнення подій, визначення часових проміжків інцидентів. Вхідними даними є нормалізовані метрики від першого рівня, з розширеною інформацією про етапи взаємодії користувачів з сервісом електронної комерції. Вихідними даними роботи другого етапу методу є скорельовані події, виявлені пов'язані події, метрики кореляції.

Рівень 3 – контекстний аналіз. Завдання третього рівня аналізу – врахування контексту роботи сервісів електронної комерції при інтерпретації результатів кореляції. На цьому рівні відбувається адаптація порогових значень та ваг метрик залежно від контексту. Специфіка роботи сервісів електронної комерції вимагає врахування унікальних контекстних факторів. До них відносяться: часовий контекст (сезонність); бізнес-контекст – акції, розпродажі, свята; врахування етапу взаємодії користувача з сервісом електронної комерції –

додавання до кошика покупок, перегляд товару, оформлення замовлення, оплата; сегмент користувача – новий, постійний; тип транзакцій – B2C, B2B, одноразові покупки. Вихідними даними третього рівня є оцінки безпекових подій у контексті етапів роботи сервісу електронної комерції, адаптовані порогові значення метрик, пріоритезовані безпекові події.

Рівень 4 – оцінка бізнес-впливу. Четвертий рівень методу аналізу ефективності системи захисту сервісів електронної комерції забезпечує трансляцію технічних метрик у бізнес-показники та формування оцінки ефективності роботи системи захисту. Вихідними даними цього етапу будуть фінансова оцінка безпекових подій, оцінка впливу на бізнес-метрики сервісу електронної комерції, оцінка ефективності системи захисту.

Для визначення оптимальної кількості рівнів архітектури методу аналізу ефективності системи захисту сервісів електронної комерції було сформульовано формальні критерії, яким повинен відповідати кожен з рівнів, що представлені у таблиці 2.2.

Таблиця 2.2.

Критерії формування рівня архітектури

	Критерій	Опис
1	Унікальність трансформації	Рівень забезпечує трансформацію вхідних даних, що не може бути проведена при об'єднанні з сусідніми рівнями без втрати інтерпретованості результату.
2	Визначеність вхідних та вихідних даних	Рівень має формально визначені дані, що приходять на цей рівень та виходять з нього у результаті обробки.
3	Незалежність	Рівень функціонально не залежить від інших та може бути реалізований окремо.
4	Наукова обґрунтованість	Наявність академічних робіт, що підтверджують необхідність даного рівня для окремого етапу аналізу.

Проведемо аналіз кожного рівня на відповідність кожного з рівнів запропонованої архітектури методу аналізу ефективності системи захисту сервісів електронної комерції. Таблиця 2.3 містить результати проведеного аналізу.

Таблиця 2.3

Аналіз відповідності критеріям формування рівнів архітектури методу

Рівень	Критерій	Обґрунтування відповідності
Перший рівень	Унікальність трансформації	Забезпечує перетворення подій з множинних джерел у стандартизовані метрики.
	Визначеність вхідних та вихідних даних	Вхідні дані: сирі безпекові події; вихідні дані: нормалізовані метрики, приведені до єдиного стандарту.
	Незалежність	Може бути реалізований як окремий додаток.
	Наукова обґрунтованість	Стандарт NIST визначає необхідність окремого етапу метричної оцінки систем захисту [110]. Мохамед Шираз (Muhammad Sheeraz) у своєму дослідженні ефективності безпекового моніторингу з використанням SIEM систем наголошує на необхідності нормалізації безпекових даних, отриманих з множинних джерел до проведення кореляції [111].
Другий рівень	Унікальність трансформації	Виявляє зв'язки між подіями, групує інциденти за визначеними атрибутами.
	Визначеність вхідних та вихідних даних	Вхідні дані: нормалізовані метрики; вихідні дані: скорельовані події та інформація про зв'язки між ними.
Другий рівень	Незалежність	Може бути реалізований як окремий додаток.
	Наукова обґрунтованість	У своїй роботі Герберт Маоса (Herbert Maosa) та Карім Озане (Karim Ouzzane) підкреслюють роль кореляції як окремого процесу [83]. Аналогічно Густаво Гонзалес-Гранадільйо (Gustavo González-Granadillo) у роботі присвяченій огляду SIEM систем зазначає, що кореляція є окремим етапом, процесом, що є окремою аналітичною стадією [62].

Третій рівень	Унікальність трансформації	Забезпечує врахування бізнес-контексту при інтерпретації отриманих результатів оцінки безпекових подій.
	Визначеність вхідних та вихідних даних	Вхідні дані: скорельовані події, доданий бізнес-контекст; вихідні дані: оцінка безпекових подій з урахуванням бізнес-контексту, пріоритезовані безпекові події, адаптовані порогові значення безпекових метрик.
Третій рівень	Незалежність	Може бути реалізований як окремий додаток.
	Наукова обґрунтованість	Необхідність врахування бізнес-контексту при аналізі безпекових метрик підтверджується сучасними дослідженнями, які демонструють залежність ефективності систем захисту від специфіки бізнес-процесів [96, 111, 83]. Врахування контексту роботи сервісів електронної комерції є ключовим для коректної оцінки їх захищеності.
Четвертий рівень	Унікальність трансформації	Транслює технічні метрики у бізнес-показники.
	Визначеність вхідних та вихідних даних	Вхідні дані: безпекові метрики, пріоритезовані безпекові інциденти; вихідні дані: оцінка бізнес-впливу, оцінка ефективності роботи системи захисту.
	Незалежність	Може бути реалізований як окремий додаток.
	Наукова обґрунтованість	Необхідність самостійного рівня аналізу бізнес-впливу безпекових подій у контексті роботи сервісів електронної комерції підтверджується в академічних роботах. Зокрема, автори демонструють, що технічні метрики не можуть нада-ти повну оцінку захищеності системи без урахування бізнес-процесів та економічних наслідків, оцінювання ефективності захисту має здійснюватися в контексті бізнес-цілей організацій [96, 89].

Розглянемо можливість зміни кількості рівнів методу аналізу ефективності системи захисту сервісів електронної комерції. У випадку скорочення кількості рівнів, суміжні рівні мають бути об'єднані. Об'єднання рівня 1 та рівня 2 порушує критерій унікальності трансформації та незалежності рівня. У свою чергу, при спробі об'єднання рівня 2 та рівня 3 буде порушено критерій визначеності вхідних та вихідних даних, а також критерій незалежності рівня. При спробі об'єднати рівень 3 та рівень 4 порушується критерій унікальності трансформації та визначеності вхідних та вихідних даних. Жоден варіант скорочення кількості рівнів не є прийнятним без порушення визначених формальних критеріїв, яким мають відповідати рівні методу. Скорочення кількості рівнів призводить до втрати функціональності або гнучкості системи. Таблиця 2.4 містить зведену інформацію щодо спроб об'єднання рівнів.

Таблиця 2.4.

Зведена інформація щодо спроб об'єднання рівнів

Варіант об'єднання	Порушені критерії	Проблеми об'єднання
Рівень 1 + Рівень 2	Унікальність трансформації, незалежність.	Різна природа операцій з даними.
Рівень 2 + Рівень 3	Визначеність вхідних та вихідних даних, незалежність.	Різні джерела даних.
Рівень 3 + Рівень 4	Унікальність трансформації, незалежність, визначеність вхідних та вихідних даних.	Вихідні дані призначені для різних кінцевих споживачів, невідповідність вимог щодо часових проміжків які застосовуються для аналізу.

Потенційними опціями для розширення кількості рівнів є впровадження рівня архітектури, що буде надавати можливості прогнозування на базі проведеного аналізу, або рівня, що реалізовуватиме функціонал з візуалізації та генерації звітності. Жоден з цих рівнів не відповідає попередньо сформованим критеріям відповідності рівнів архітектури. Означені рівні не є необхідними для

побудови архітектури методу аналізу ефективності системи захисту сервісів електронної комерції.

Проведений аналіз доводить, що чотирьохрівнева архітектура задовольняє вимоги для повного циклу трансформації даних (рис. 2.2) з подальшою оцінкою ефективності роботи систем захисту сервісів електронної комерції. Надмірна кількість рівнів призведе до ускладнення системи та збільшення часу, потрібного на обробку даних.

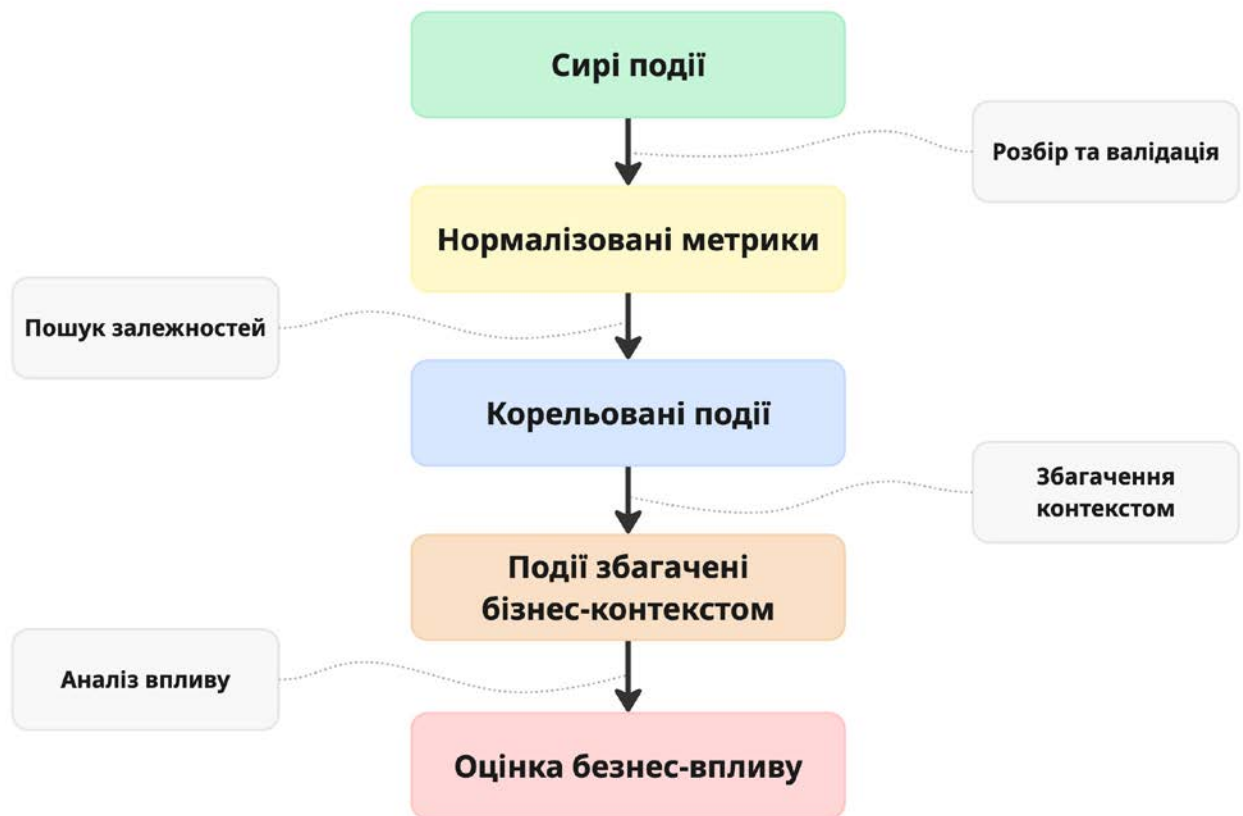


Рис. 2.2. Етапи циклу трансформації даних

Слід зазначити, що вказана архітектура методу описує основні етапи обробки даних, що необхідні для його реалізації. При практичній реалізації архітектури методу аналізу ефективності системи захисту сервісів електронної комерції вона поділяється на дві функціональні частини (рис. 2.3): 1) підготовка даних (рівень 1-2); 2) аналіз отриманих даних (рівень 3-4).



Рис. 2.3. Функціональний поділ архітектури методу.

Такий підхід має ряд переваг, а саме можливість інтеграції з наявною інфраструктурою захисту, використання стандартизованих функцій збору, нормалізації та кореляції безпекових подій, значно зменшує час впровадження рішення у роботу.

Запропонований метод аналізу ефективності систем захисту сервісів електронної комерції надає можливість враховувати специфічні вимоги сервісів електронної комерції, та на відміну від традиційних методів оцінки ефективності захищеності інформаційних систем, дозволяє отримати кількісну оцінку впливу безпекових інцидентів на роботу сервісу електронної комерції. Узагальнене порівняння методів наведено у таблиці 2.5.

Таблиця 2.5

Порівняння характеристик наявних методів оцінки ефективності захисту інформаційних систем

Критерій	NIST	FAIR	SIEM (кореляція подій)	Запропонований метод
Тип оцінки	Якісна	Кількісна (фінансова)	Кількісна (технічна)	Кількісна (об'єднана)
Режим роботи	Періодичний	Періодичний	У реальному часі	У реальному часі
Спеціалізація	Універсальний	Універсальний	Універсальний	Електронна комерція
Врахування специфіки сервісів електронної комерції	Ні	Ні	Ні	Так
Кількісна оцінка впливу на бізнес- процеси	Ні	Так	Ні	Так
Адаптивність та зворотній зв'язок	Ні	Ні	Ні	Так

Метод NIST використовує якісну оцінку, що надає опис ступенів формалізації процесів присутніх в інформаційній системі, але не визначає числової оцінки ефективності захисту інформаційної системи. Метод FAIR у першу чергу призначений для кількісної фінансової оцінки ризиків, але не враховує технічних метрик ефективності роботи системи захисту. SIEM системи покликані проводити аналіз, кореляцію та групування технічних метрик, але не виконують трансформації цих даних з урахуванням бізнес-контексту. Зазначені методи мають широке коло застосування без певної спеціалізації, тому врахування специфіки тих чи інших процесів не лежить у фокусі їх використання. Ще однією особливістю перерахованих методів є використання статичних порогів для оцінки подій, що виникають у системі. Такий підхід

ускладнює або робить неможливою корекцію режимів роботи систем аналізу в залежності від попередньо отриманих результатів. Перелічені обмеження враховані при розробці методу аналізу ефективності системи захисту сервісів електронної комерції.

Для визначення впливу безпекових подій та роботи системи захисту на функціонування сервісу електронної комерції необхідно встановити критичність впливу на бізнес-процеси кожного з етапів взаємодії користувача з сервісом електронної комерції.

Автори К. Н. Лемон (K. N. Lemon) та П. К. Верхоф (P. C. Verhoef), у своєму дослідженні з маркетингу та управління досвідом клієнтів, визначають класичну модель взаємодії клієнта в процесі прийняття рішення про покупку того чи іншого товару. Автори виділяють три основні стадії моделі: дослідження (вибір), оформлення покупки, дії після покупки (рис. 2.4). Ця модель залишається актуальною і для використання в контексті роботи сервісів електронної комерції, але потребує певної адаптації її етапів [79].

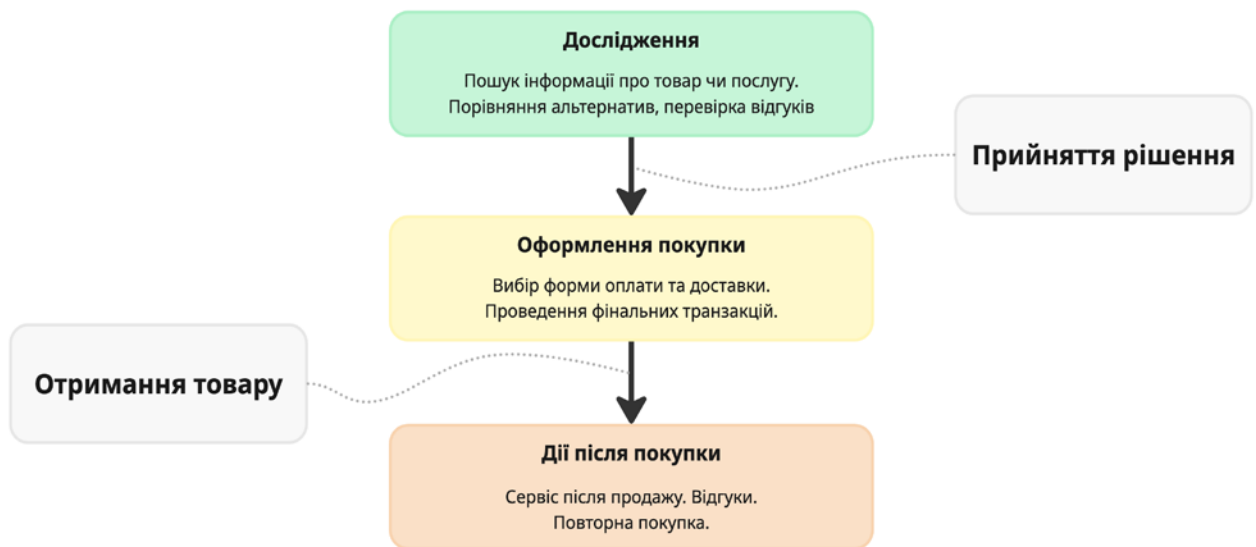


Рис. 2.4. Етапи класичної моделі взаємодії клієнта [79].

У межах даного дослідження класичну модель пропонується розширити до семи етапів (E_n) (рис. 2.5), що дозволить врахувати етапи взаємодії з користувачем, характерні для сервісів електронної комерції.



Рис. 2.5. Розширена модель етапів взаємодії користувача і сервісу електронної комерції.

Етап «Дослідження» включає в себе E_1 – стартову сторінку сервісу електронної комерції; E_2 – перегляд каталогу доступних товарів; E_3 – пошук потрібного товару; E_4 – перегляд обраного товару. Етап «Оформлення покупки» включає в себе E_5 – додавання товару до кошика; E_6 – оформлення замовлення; E_7 – оплата замовлення. Останній етап класичної моделі «Дії після покупки» не є необхідною частиною для аналізу ефективності систем захисту сервісів електронної комерції і не буде враховуватись в подальшому дослідженні.

Розглянемо кожен з етапів більш детально. Стартова сторінка сервісу електронної комерції (E_1) – це етап першої взаємодії користувачів з сервісом електронної комерції. На цьому етапі користувачі знайомляться з інтерфейсом сервісу, оцінюють його на відповідність своїм очікуванням та приймають рішення щодо подальшої взаємодії. У своєму дослідженні автори Н. М. Пуччінеллі (N. M. Puccinelli), Р. К. Гудстін (R. C. Goodstein), Д. Грювал (D. Grewal), Р. Прайс (R. Price), П. Рагубір (P. Raghuram) та Д. Стюарт (D. Stewart) підкреслюють, що початкове враження користувача від взаємодії з сервісом електронної комерції визначає успіх подальшої користувацької активності [98].

Перегляд каталогу доступних товарів (E_2) – на цьому етапі користувачі виконують пошук потрібної інформації, оцінюють альтернативи та зважують доступні варіанти. Пошук потрібного товару (E_3) – користувачі займаються

активним пошуком конкретного товару. Дослідження авторів Ю. Туанрат (Y. Tueanrat), С. Пападжаннідіс (S. Papagiannidis) та Е. Аламанос (E. Alamanos) виявило, що користувачі сервісів електронної комерції звертають особливу увагу на зручність використання пошуку конкретного товару або категорії товарів. Етапи E_2 та E_3 тісно пов'язані та відіграють вагомую роль у прийнятті рішення користувачами чи продовжувати подальшу взаємодію з сервісом електронної комерції [122].

Перегляд обраного товару (E_4) – є результатом взаємодії користувачів з сервісом електронної комерції на етапах E_2 та E_3 . На цьому етапі відбувається оцінка обраного товару, його ціни, відгуків та іншої доступної інформації, необхідної для прийняття рішення про покупку. Додавання товару до кошика (E_5) – є сигналом щодо наміру здійснити покупку. Етап додавання товару до кошика є унікальним для сервісів електронної комерції і представляє критичний перехідний момент зі стадії огляду до стадії вибору.

Оформлення замовлення (E_6) та оплата замовлення (E_7) – є фінальними етапами взаємодії користувачів з сервісом електронної комерції, які мають найбільший вплив на бізнес-показники сервісу електронної комерції. Досвід користувача, що формується на цьому етапі, визначає лояльність та намір повторно скористатись сервісом електронної комерції. Окремо слід зазначити, на цих етапах відбувається надання персональної та фінансової інформації користувачами, що є особливо критично з точки зору безпеки.

Додатковими факторами, які впливають на визначення критичності та формування кінцевої оцінки кожного з етапів взаємодії користувачів із сервісом електронної комерції, може виступати певна галузева приналежність, тип розміщених продуктів, контекст взаємодії з користувачами (роздрібні товари чи орієнтація на роботу з компаніями).

Для подальшого визначення коефіцієнтів критичності (K_E) для кожного з описаних етапів взаємодії користувача з сервісом електронної комерції, необхідно визначити критерії для оцінки критичності впливу на бізнес-процеси кожного з етапів взаємодії.

Слід зазначити, що коефіцієнти, розраховані в даній роботі, є демонстративними і мають на меті ілюстрацію роботи методу аналізу ефективності системи захисту сервісів електронної комерції, оскільки критерії не є статичними і потребують періодичного оновлення в контексті поточної роботи сервісу електронної комерції ситуації. При практичному застосуванні коефіцієнти критичності для кожного з етапів взаємодії користувача з сервісом електронної комерції мають бути актуалізовані в контексті роботи конкретного сервісу електронної комерції. Для цього в роботі запропонована формалізована та відтворювана методика розрахунку коефіцієнтів критичності для етапів взаємодії користувача з сервісом електронної комерції з використанням методу аналізу ієрархій.

2.3. Коефіцієнти критичності етапів взаємодії користувача з сервісом електронної комерції

Коефіцієнт критичності кожного з етапів взаємодії користувача з сервісом електронної комерції (K_E) відображає, в якій мірі безпековий інцидент або пов'язані з ним реакції систем захисту сервісу електронної комерції впливають на бізнес-результати роботи сервісу електронної комерції.

Для визначення коефіцієнту критичності етапу взаємодії користувача з сервісом електронної комерції пропонуються наступні критерії (C_n) (рис. 2.6.):

1. Вплив на конверсію (C_1).
2. Чутливість до збоїв (C_2).
3. Вплив захисних механізмів (C_3).
4. Вплив на подальшу лояльність (довіру) (C_4).
5. Платіжні ризики (C_5).

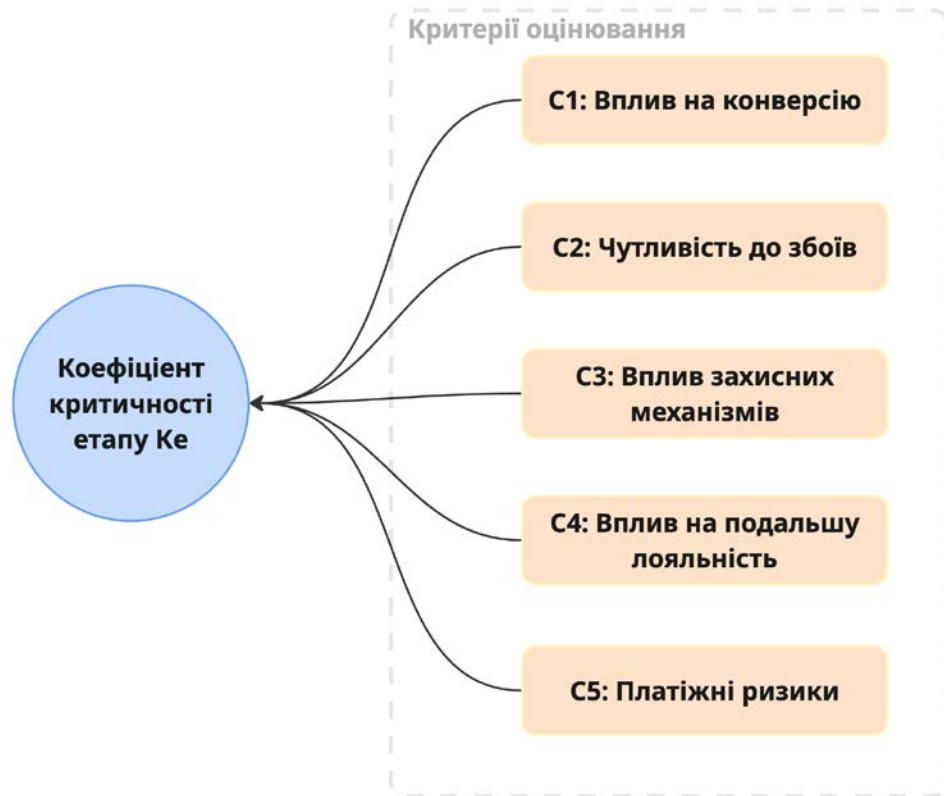


Рис. 2.6. Критерії визначення коефіцієнту критичності етапу.

Коефіцієнт критичності етапу (K_E) є результатом агрегації всього зазначеного набору критеріїв (C_n) (рис. 2.6), а безпекові інциденти на етапах з більшою критичністю мають більший внесок у формування загальної оцінки впливу роботи систем захисту на бізнес-процеси сервісу електронної комерції.

Розглянемо кожен з критеріїв більш детально. Вплив на конверсію (C_1) – характеризує, на скільки порушення роботи на певному етапі взаємодії користувача з сервісом електронної комерції підвищує ймовірність відмови від завершення сесії покупкою [34, 41]. Чутливість до збоїв (C_2) – цей критерій демонструє, на скільки етап вразливий до різноманітних технічних проблем, як недоступність, виникнення помилок, зниження продуктивності, затримки у завантаженні сторінки [109]. Дослідження демонструють зв'язок між часом завантаження сторінок та показниками конверсії сервісів електронної комерції [72]. Вплив захисних механізмів (C_3) – даний критерій оцінює вплив безпекових заходів, які використовує сервіс електронної комерції. Надмірні безпекові заходи можуть спричинити відмову від подальшого користування сервісом [114, 84].

Вплив на подальшу лояльність (C_4) – описує як події на певному етапі взаємодії користувача з сервісом електронної комерції впливають на намір повторного використання сервісу [27]. Платіжні ризики (C_5) – характерний для етапів, де виникають фінансові ризики. Безпечні онлайн транзакції є невід’ємною умовою функціонування сервісів електронної комерції [27].

Визначення коефіцієнтів критичності етапів взаємодії користувачів з сервісами електронної комерції належить до класу задач теорії прийняття рішень, так як передбачає формалізоване обґрунтування пріоритизації етапів взаємодії користувача з сервісами електронної комерції [73, 29].

За своєю постановкою ця задача є задачею багатокритеріального аналізу, оскільки критичність кожного етапу не може бути охарактеризована одним показником та потребує визначення на базі сукупності критеріїв, що відображають різні аспекти впливу на взаємодію користувача з сервісом електронної комерції. Для кожного з етапів необхідно отримати інтегральну оцінку, що об’єднує внесок кожного з критеріїв і на її основі провести ранжування етапів за коефіцієнтами критичності [104, 29].

Для вирішення поставленої задачі з визначення коефіцієнтів критичності етапів взаємодії користувачів з сервісами електронної комерції було обрано використання методу аналізу ієрархій [107]. Даний метод дозволяє структурувати складну задачу у вигляді ієрархій та розбити її на менш об’ємні кроки для визначення коефіцієнтів критичності. Узагальнюючи поставлену задачу можна представити у вигляді наступної ієрархії, де мета – це визначення критичності етапів взаємодії користувачів з сервісами електронної комерції, критерії – множина критеріїв для аналізу кожного з етапів $C = \{C_1, \dots, C_n\}$, об’єкти ранжування – етапи взаємодії користувача з сервісом електронної комерції, що представлені множиною $E = \{E_1, \dots, E_n\}$ (рис. 2.7).

Метод аналізу ієрархій використовує механізм попарних порівнянь, дозволяючи кількісно формалізувати відносну важливість об’єктів ранжування навіть за наявності критеріїв, що надають якісну оцінку.

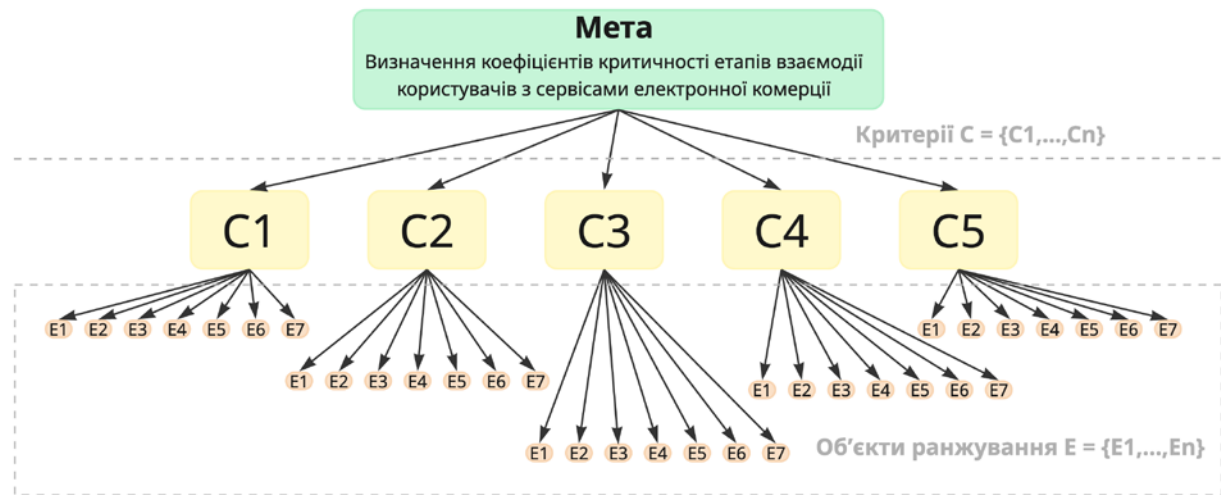


Рис. 2.7. Ієрархія задачі визначення коефіцієнтів критичності.

Для порівнянь використовується шкала інтенсивності переваг, яка дозволяє ставити у відповідності до ступеню переваги одного елементу перед іншим деяке число з діапазону від 1 до 9 та відповідні обернені значення. Якщо елемент оцінювання X порівняно з елементом оцінювання Y отримує значення Z , то елемент оцінювання Y порівняно з елементом оцінювання X отримує значення $1/Z$. У таблиці 2.6 наведено пояснення шкали попарних порівнянь, що використовується методом аналізу ієрархій [107].

Таблиця 2.6.

Значення шкали інтенсивності переваг з поясненнями [107].

Рівень переваги	Визначення	Пояснення
1	Однакова важливість	Обидва елементи дають однаковий внесок
3	Один елемент незначним чином важливіший за другий	Досвід дозволяє поставити один елемент трохи вище за другий
5	Суттєва перевага	Безумовна перевага одного елементу над іншим
7	Значна перевага	Один елемент настільки важливіший за інший, що є практично значимим
9	Абсолютна перевага одного елементу над іншим	Очевидність переваги підтверджується більшістю
2,4,6,8	Проміжні оцінки між сусідніми твердженнями	Компромісне рішення

Результати попарних порівнянь формують квадратну матрицю суджень A розмірністю $n \times n$, де a_{ij} – числова оцінка переваги (2.1). Якщо критеріїв N , а об'єктів ранжування M , то будується одна матриця розміром $N \times N$ для критеріїв та N матриць розміром $M \times M$ для порівняння альтернатив за кожним критерієм. Таким чином, метод аналізу ієрархій передбачає два типи попарних порівнянь – критеріїв між собою відносно мети для визначення ваг критеріїв, та об'єктів ранжування між собою відносно кожного з критеріїв для визначення локальних пріоритетів.

$$A = \begin{pmatrix} a_{\{11\}} & a_{\{12\}} & \cdots & a_{\{1n\}} \\ a_{\{21\}} & a_{\{22\}} & \cdots & a_{\{2n\}} \\ \vdots & \vdots & \ddots & \vdots \\ a_{\{n1\}} & a_{\{n2\}} & \cdots & a_{\{nn\}} \end{pmatrix} \quad (2.1)$$

Наступним кроком є обчислення локальних векторів пріоритетів для кожної з сформованих матриць. Пріоритети визначаються як нормований головний власний вектор w матриці A . Отриманий вектор $w = (w_1, w_2, \dots, w_n)$ є вектором локальних пріоритетів, компоненти вектору показують відносну важливість елементів у межах групи порівняння.

Обчислення вектору пріоритетів здійснюється у два етапи. Спочатку проводиться розрахунок суми елементів для кожного стовпця матриці порівнянь j , де $j = 1..n$, S_j – сума елементів j -го стовпця матриці A (2.2).

$$S_j = \sum_{i=1}^n a_{ij} \quad (2.2)$$

Далі проводиться нормалізація матриці порівняння, коли кожен елемент матриці a_{ij} ділиться на суму елементів відповідного стовпця S_j (2.3). Таким чином отримуємо нову матрицю $\bar{A}$, що містить нормалізовані елементи $\bar{a}_{ij}$. Сума елементів кожного стовпця матриці $\bar{A}$ дорівнює 1.

$$\bar{a}_{ij} = \frac{a_{ij}}{S_j} \quad (2.3)$$

Обчислення значень власного вектору, який i є вектором локальних пріоритетів виконується за допомогою розрахунку середнього арифметичного

значення елементів у кожному рядку нормалізованої матриці. Для i -го елемента його вага w_i визначається як (2.4):

$$w_i = \frac{1}{n} \sum_{j=1}^n \bar{a}_{ij} \quad (2.4)$$

В результаті отримуємо вектор локальних пріоритетів (2.5).

$$w = \begin{pmatrix} w_1 \\ w_2 \\ \dots \\ w_n \end{pmatrix} \quad (2.5)$$

Сума всіх компонентів отриманого вектору завжди дорівнює одиниці і відображає відносну значущість кожного з порівнюваних елементів.

Однією з основних переваг методу аналізу ієрархій є вбудований механізм перевірки узгодженості виставлених оцінок. Неузгодженість виникає при порушенні транзитивності суджень – якщо $X > Y$, а $Y > Z$, то має бути $X > Z$. Для оцінки якості виставлених оцінок розраховується відношення узгодженості (ВУ) (2.6).

$$ВУ = \frac{IY}{BIY} \quad (2.6)$$

Спочатку визначається індекс узгодженості (IY), де n – розмірність матриці (2.7).

$$IY = \frac{\lambda_{max} - n}{n - 1} \quad (2.7)$$

Отриманий індекс узгодженості порівнюється з випадковим індексом узгодженості (BIY) – емпіричною величиною, що відповідає середньому індексу узгодженості для випадково згенерованих матриць розмірністю n . Дані значення BIY наведені автором методу аналізу ієрархій Т. Л. Сааті (T. L. Saaty) [106] (таблиця 2.7). Згідно з цією методологією, якщо $ВУ \leq 0.10$, то узгодженість матриці вважається прийнятною. У випадку, коли узгодженість є недостатньою, оцінки, що містить матриця, підлягають перегляду до досягнення прийнятного відношення узгодженості.

Таблиця випадкових індексів узгодженості згідно Сааті Т. Л. [106].

п	1	2	3	4	5	6	7	8	9	10
ВІУ	0.00	0.00	0.52	0.89	1.11	1.25	1.35	1.40	1.45	1.49

Коли всі локальні пріоритети для всіх рівнів ієрархії обчислені, відбувається розрахунок глобальних пріоритетів для об'єктів ранжування. Визначення глобального пріоритету можна описати наступним чином (2.8) [106]:

$$P_j = \sum_{i=1}^c w_i * p_{ij} \quad (2.8)$$

де P_j – глобальний пріоритет об'єкту ранжування, w_i – вага критерію i , p_{ij} – локальний пріоритет об'єкту ранжування j відносно критерію i , c – кількість критеріїв.

Завершальним етапом використання методу аналізу ієрархій є інтерпретація отриманих результатів та формування фінального рейтингу об'єктів ранжування.

Використання методу аналізу ієрархій для знаходження коефіцієнтів критичності етапів взаємодії користувача з сервісом електронної комерції дозволяє формалізувати процедуру розрахунку коефіцієнтів критичності та забезпечити її відтворюваність у разі застосування до будь-якого сервісу електронної комерції. Окрім цього, метод аналізу ієрархій забезпечує контроль якості вхідних оцінок завдяки обрахування коефіцієнтів узгодженості в процесі застосування методу та їх корекції до прийнятного рівня у разі виявлення невідповідності.

Розрізняють індивідуальне та групове застосування методу аналізу ієрархій. У першому випадку попарні порівняння та пріоритети формує одна особа, що приймає рішення, в другому випадку використовуються оцінки кількох учасників, які агрегуються у групове рішення. Це знаходить підтвердження у публікаціях автора методу Т. Л. Сааті (T. L. Saaty) [107], а також інших роботах дослідників, що використовують даний метод у своїх роботах

[106, 85]. Процедура застосування методу аналізу ієрархій не висуває вимог щодо кількості експертів, задіяних у прийнятті рішення, а також забезпечує механізм перевірки узгодженості оцінок експертів, що дозволяє контролювати їх якість незалежно від кількості експертів.

Визначимо коефіцієнти критичності етапів взаємодії користувача з сервісом електронної комерції. Вхідні дані для даної задачі представлені в таблиці 2.8 та таблиці 2.9.

Таблиця 2.8.

Критерії для розрахунку коефіцієнтів критичності

Позначення	Критерій
C1	Вплив на конверсію
C2	Чутливість до збоїв
C3	Вплив захисних механізмів
C4	Вплив на подальшу лояльність
C5	Платіжні ризики

Таблиця 2.9

Об'єкти ранжування для розрахунку коефіцієнтів критичності

Позначення	Об'єкт ранжування (етап)
E1	Стартова сторінка
E2	Перегляд каталогу
E3	Пошук товару
E4	Перегляд обраного товару
E5	Додавання товару до кошика
E6	Оформлення замовлення
E7	Оплата замовлення

Проведемо порівняння критеріїв за пріоритетом (таблиця 2.10).

Таблиця 2.10

Попарні порівняння критеріїв.

	C1	C2	C3	C4	C5
C1	1	2	3	4	1/2
C2	1/2	1	2	3	1/3
C3	1/3	1/2	1	2	1/4
C4	1/4	1/3	1/2	1	1/5
C5	2	3	4	5	1

Розрахуємо вектор локальних пріоритетів критеріїв оцінювання. Для цього обчислимо суми кожного стовпця матриці порівняння (2.9):

$$\begin{aligned}
 S_{C_1} &= 1 + 0.5 + 0.333 + 0.25 + 2 = 4.083 \\
 S_{C_2} &= 2 + 1 + 0.5 + 0.33 + 3 = 6.833 \\
 S_{C_3} &= 3 + 2 + 1 + 0.5 + 4 = 10.5 \\
 S_{C_4} &= 4 + 3 + 2 + 1 + 5 = 15.0 \\
 S_{C_5} &= 0.5 + 0.333 + 0.25 + 0.2 + 1 = 2.283
 \end{aligned} \tag{2.9}$$

Наступним кроком проводимо нормалізацію стовпців матриці порівняння, для цього кожен з елемент матриці ділимо на розраховану суму стовпця, в якій він знаходиться (таблиця 2.11). Окремо проводимо контроль розрахунків – сума значень нормалізованого стовпця має дорівнювати одиниці.

Таблиця 2.11

Розрахунок нормалізованих значень стовпців матриці порівняння

	C1	C2	C3	C4	C5
C1	1/4.083	2/6.833	3/10.5	4/15.0	0.5/2.283
C2	0.5/4.083	1/6.833	2/10.5	3/15.0	0.333/2.283
C3	0.333/4.083	0.5/6.833	1/10.5	2/15.0	0.25/2.283
C4	0.25/4.083	0.333/6.833	0.5/10.5	1/15.0	0.2/2.283
C5	2/4.083	3/6.833	4/10.5	5/15.0	1/2.283

Отримані значення з контрольною сумою (таблиця 2.12):

Таблиця 2.12

Нормалізовані значення стовпців матриці порівняння

	C1	C2	C3	C4	C5
C1	0.245	0.293	0.286	0.267	0.219
C2	0.122	0.146	0.190	0.200	0.146
C3	0.082	0.073	0.095	0.133	0.110
C4	0.061	0.049	0.048	0.067	0.088
C5	0.490	0.439	0.381	0.333	0.438
Σ	1	1	1	1	1

Отримані значення використовуємо для обчислення вектору локальних пріоритетів, що є середнім арифметичним по рядках матриці порівняння (таблиця 2.13).

Таблиця 2.13

Вектор локальних пріоритетів

	W_{C1}	W_{C1}	W_{C1}	W_{C1}	W_{C1}	Σ
W	0.262	0.161	0.099	0.062	0.416	1

Далі проводиться перевірка узгодженості матриці порівняння. Для цього, використовуючи попередньо отримані значення локальних пріоритетів, обчислюємо вектор зважених сум (2.10).

$$S_1 = 1 * 0.262 + 2 * 0.161 + 3 * 0.099 + 4 * 0.062 + 0.5 * 0.416 = 1.337$$

$$S_2 = 0.5 * 0.262 + 1 * 0.161 + 2 * 0.099 + 3 * 0.062 + 0.333 * 0.416 = 0.815$$

$$S_3 = 0.333 * 0.262 + 0.5 * 0.161 + 1 * 0.099 + 2 * 0.062 + 0.25 * 0.416 = 0.495 \quad (2.10)$$

$$S_4 = 0.25 * 0.262 + 0.333 * 0.161 + 0.5 * 0.099 + 1 * 0.062 + 0.2 * 0.416 = 0.314$$

$$S_5 = 2 * 0.262 + 3 * 0.161 + 4 * 0.099 + 5 * 0.062 + 1 * 0.416 = 2.129$$

Зведена таблиця отриманих значень для кожного з критеріїв (таблиця 2.14):

Таблиця 2.14

Отримані значення для вектора зважених сум.

Критерій	S_i
C1	1.337
C2	0.815
C3	0.495
C4	0.314
C5	2.129

Наступним кроком проводимо обчислення вектору узгодженості для матриці порівнянь. Для цього використаємо розраховані значення вектору локальних пріоритетів та вектора зважених сум матриці порівнянь (2.11).

$$\begin{aligned}
 V_1 &= \frac{1.337}{0.262} = 5.103 \\
 V_2 &= \frac{0.815}{0.161} = 5.062 \\
 V_3 &= \frac{0.495}{0.099} = 5.000 \\
 V_4 &= \frac{0.314}{0.062} = 5.065 \\
 V_5 &= \frac{2.129}{0.416} = 5.118
 \end{aligned}
 \tag{2.11}$$

Отримані значення використовуємо для розрахунку максимального власного значення матриці порівнянь (2.12).

$$\lambda_{max} = \frac{(5.103+5.062+5.000+5.065+5.118)}{5} = 5.069 \tag{2.12}$$

Отримане максимальне власне значення для матриці порівнянь дозволяє провести обчислення індексу узгодженості (2.13).

$$IU = \frac{5.069 - 5}{5 - 1} = 0.017 \tag{2.13}$$

Обчислюємо відношення узгодженості (2.14). Для цього використовуємо табличне значення випадкового індексу узгодженості, яке для матриці розмірністю 5x5 становить 1.11 (таблиця 2.6).

$$BU = \frac{0.017}{1.11} = 0.016 \tag{2.14}$$

Отримане відношення узгодженості задовольняє вимоги методології та підтверджує узгодженість матриці порівнянь (2.15).

$$BU = 0.016 < 0.10 \tag{2.15}$$

Таким чином, було отримано та перевірено значення ваг для критеріїв визначення критичності етапів взаємодії користувача з сервісом електронної комерції (рис. 2.8).

Отримані значення дозволяють надати більшу вагу тим критеріям оцінювання етапів взаємодії користувача з сервісом електронної комерції, які мають найвищий вплив на бізнес-показники сервісу електронної комерції. Критерій С5, «Платіжні ризики», отримав найвищий пріоритет, так як фінансові втрати внаслідок недостатнього або надмірного захисту мають незворотній характер.

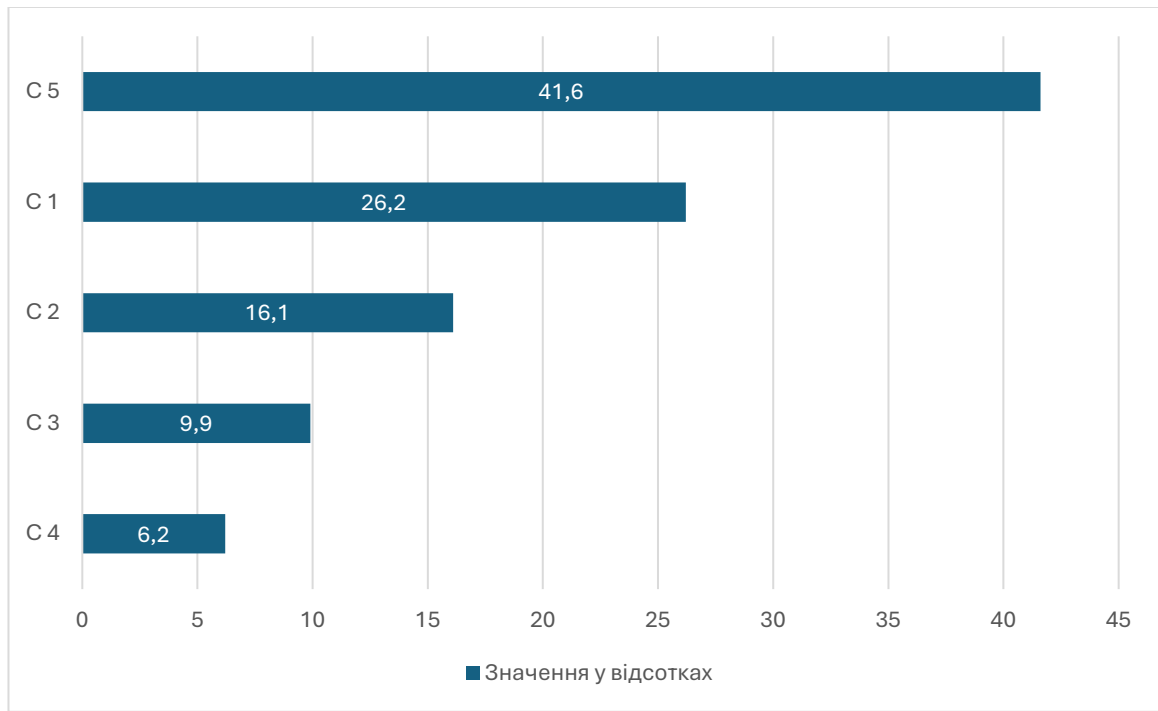


Рис. 2.8. Отримані значення ваги критеріїв порівняння.

Шахрайські транзакції чи витoki чутливої платіжної інформації призводять не тільки до фінансових, а й репутаційних та юридичних наслідків. Критерій C1, «Вплив на конверсію», отримав другий пріоритет. Показники конверсії є одним з ключових бізнес-показників роботи сервісу електронної комерції. Безпекові інциденти можуть спонукати користувача відмовитись від подальшої взаємодії з сервісом електронної комерції і відповідно не здійснити покупку товарів. Критерій C2, «Чутливість до збоїв», займає середню позицію. На ранніх етапах взаємодії з сервісом електронної комерції збої в роботі сервісу є менш критичними ніж на фінальних етапах, де користувач вже прийняв рішення про покупку і хоче здійснити оплату. Критерій C3, «Вплив захисних механізмів», отримав четверту позицію серед критеріїв оцінювання. Надмірні безпекові заходи можуть мати негативний вплив на конверсію, який зростає з просуванням користувача до фінальних етапів оформлення покупки. Останню позицію за впливом серед критеріїв оцінювання критичності етапів взаємодії користувача з сервісом електронної комерції займає критерій C4, «Вплив на подальшу лояльність», дана оцінка зумовлена відкладеним впливом на бізнес-

показники та не формується самостійно, а під впливом сукупності різних факторів.

Проведемо оцінювання етапів взаємодії користувача з сервісом електронної комерції за кожним з критеріїв. Розрахуємо оцінку за критерієм С1, «Вплив на конверсію». Першим етапом є попарне порівняння етапів відносно критерію С1, результати порівняння представлені в таблиці 2.15.

Таблиця 2.15.

Попарні порівняння етапів відносно критерію С1.

	E1	E2	E3	E4	E5	E6	E7
E1	1	1	2	1/2	1/3	1/5	1/5
E2	1	1	1	1/2	1/3	1/5	1/5
E3	1/2	1	1	1/2	1/3	1/4	1/4
E4	2	2	2	1	1/2	1/3	1/3
E5	3	3	3	2	1	1/2	1/2
E6	5	5	4	3	2	1	1
E7	5	5	4	3	2	1	1

Розрахуємо вектор локальних пріоритетів оцінювання етапів взаємодії користувача з сервісом електронної комерції відносно критерію С1. Для цього обчислимо суми кожного стовпця матриці порівняння (2.16):

$$S_{E_1} = 1 + 1 + 0.5 + 2 + 3 + 5 + 5 = 17.5$$

$$S_{E_2} = 1 + 1 + 1 + 2 + 3 + 5 + 5 = 18$$

$$S_{E_3} = 2 + 1 + 1 + 2 + 3 + 4 + 4 = 17$$

$$S_{E_4} = 0.5 + 0.5 + 0.5 + 1 + 2 + 3 + 3 = 10.5 \quad (2.16)$$

$$S_{E_5} = 0.333 + 0.333 + 0.333 + 0.5 + 1 + 2 + 2 = 6.499$$

$$S_{E_6} = 0.2 + 0.2 + 0.25 + 0.333 + 0.5 + 1 + 1 = 3.483$$

$$S_{E_7} = 0.2 + 0.2 + 0.25 + 0.333 + 0.5 + 1 + 1 = 3.483$$

Обчислюємо нормалізовані значення стовпців матриці порівняння (таблиця 2.16 та 2.17).

Використовуючи отримані значення, обчислюємо вектор локальних пріоритетів, що є середнім арифметичним по рядках матриці порівняння (таблиця 2.18).

Таблиця 2.16

Розрахунок нормалізованих значень стовпців матриці порівняння

	E1	E2	E3	E4	E5	E6	E7
E1	1/17.5	1/18	2/17	0.5/10.5	0.333/6.499	0.2/3.483	0.2/3.483
E2	1/17.5	1/18	1/17	0.5/10.5	0.333/6.499	0.2/3.483	0.2/3.483
E3	0.5/17.5	1/18	1/17	0.5/10.5	0.333/6.499	0.25/3.483	0.25/3.483
E4	2/17.5	2/18	2/17	1/10.5	0.5/6.499	0.333/3.483	0.333/3.483
E5	3/17.5	3/18	3/17	2/10.5	1/6.499	0.5/3.483	0.5/3.483
E6	5/17.5	5/18	4/17	3/10.5	2/6.499	1/3.483	1/3.483
E7	5/17.5	5/18	4/17	3/10.5	2/6.499	1/3.483	1/3.483

Таблиця 2.17

Нормалізовані значення стовпців матриці порівняння

	E1	E2	E3	E4	E5	E6	E7
E1	0.057	0.056	0.118	0.048	0.051	0.057	0.057
E2	0.057	0.056	0.059	0.048	0.051	0.057	0.057
E3	0.029	0.056	0.059	0.048	0.051	0.072	0.072
E4	0.114	0.111	0.118	0.095	0.077	0.096	0.096
E5	0.171	0.167	0.176	0.190	0.154	0.144	0.144
E6	0.286	0.278	0.235	0.286	0.308	0.287	0.287
E7	0.286	0.278	0.235	0.286	0.308	0.287	0.287
Σ	1.000	1.000	1.000	1.000	1.000	1.000	1.000

Таблиця 2.18

Вектор локальних пріоритетів

	W_{E1}	W_{E2}	W_{E3}	W_{E4}	W_{E5}	W_{E6}	W_{E7}	Σ
W_1	0.063	0.055	0.055	0.101	0.164	0.281	0.281	1.000

Проводимо перевірку узгодженості матриці порівняння. Для цього обчислюємо вектор зважених сум (2.17).

$$S_1 = 1 * 0.063 + 1 * 0.55 + 2 * 0.055 + 0.5 * 0.101 + 0.333 * 0.164 + 0.2 * 0.281 + 0.2 * 0.281 = 0.446$$

$$S_2 = 1 * 0.063 + 1 * 0.55 + 1 * 0.055 + 0.5 * 0.101 + 0.333 * 0.164 + 0.2 * 0.281 + 0.2 * 0.281 = 0.391$$

$$S_3 = 0.5 * 0.063 + 1 * 0.55 + 1 * 0.055 + 0.5 * 0.101 + 0.333 * 0.164 + 0.25 * 0.281 + 0.25 * 0.281 = 0.387$$

$$S_4 = 2 * 0.063 + 2 * 0.55 + 2 * 0.055 + 1 * 0.101 + 0.5 * 0.164 + 0.333 * 0.281 + 0.333 * 0.281 = 0.716$$

$$S_5 = 3 * 0.063 + 3 * 0.55 + 3 * 0.055 + 2 * 0.101 + 1 * 0.164 + 0.5 * 0.281 + 0.5 * 0.281 = 1.166$$

$$S_6 = 5 * 0.063 + 5 * 0.55 + 4 * 0.055 + 3 * 0.101 + 2 * 0.164 + 1 * 0.281 + 1 * 0.281 = 2.003 \quad (2.17)$$

$$S_7 = 5 * 0.063 + 5 * 0.55 + 4 * 0.055 + 3 * 0.101 + 2 * 0.164 + 1 * 0.281 + 1 * 0.281 = 2.003$$

Отримані значення вектора зважених сум наведені у таблиці 2.19.

Таблиця 2.19

Отримані значення для вектора зважених сум.

Етап	S _i
E1	0.446
E2	0.391
E3	0.387
E4	0.716
E5	1.166
E6	2.003
E7	2.003

Проводимо обчислення вектору узгодженості для матриці порівнянь (2.18).

$$\begin{aligned}
 V_1 &= \frac{0.446}{0.063} = 7.079 \\
 V_2 &= \frac{0.391}{0.055} = 7.109 \\
 V_3 &= \frac{0.387}{0.055} = 7.036 \\
 V_4 &= \frac{0.716}{0.101} = 7.089 \\
 V_5 &= \frac{1.166}{0.164} = 7.110 \\
 V_6 &= \frac{2.003}{0.281} = 7.128 \\
 V_7 &= \frac{2.003}{0.281} = 7.128
 \end{aligned} \tag{2.18}$$

Тепер розрахуємо максимальне власне значення матриці порівнянь (2.19).

$$\lambda_{max} = \frac{7.079+7.109+7.036+7.089+7.110+7.128+7.128}{7} = 7.097 \tag{2.19}$$

Далі обчислюємо індекс узгодженості (2.20).

$$IU = \frac{7.097 - 7}{7 - 1} = 0.016 \tag{2.20}$$

Наступним кроком обчислюємо відношення узгодженості (2.21). Значення випадкового індексу узгодженості, яке для матриці розмірністю 7x7 становить 1.35 (таблиця 2.6).

$$B_U = \frac{0.016}{1.35} = 0.012 \quad (2.21)$$

Отримане відношення узгодженості задовольняє вимоги методології та підтверджує узгодженість матриці порівнянь (2.22).

$$B_U = 0.012 < 0.10 \quad (2.22)$$

Розрахуємо оцінку етапів взаємодії користувача з сервісом електронної комерції за критерієм С2, «Чутливість до збоїв». У таблиці 2.20 приведені попарні порівняння етапів відносно критерію С2.

Таблиця 2.20.

Попарні порівняння етапів відносно критерію С2.

	E1	E2	E3	E4	E5	E6	E7
E1	1	1	1/2	1	1/3	1/5	1/6
E2	1	1	1/2	1	1/3	1/5	1/6
E3	2	2	1	2	1/2	1/3	1/4
E4	1	1	1/2	1	1/3	1/5	1/6
E5	3	3	2	3	1	1/2	1/3
E6	5	5	3	5	2	1	1/2
E7	6	6	4	6	3	2	1

Обчислені нормалізовані значення стовпців матриці порівняння критерію С2 наведені у таблиці 2.21

Таблиця 2.21

Нормалізовані значення таблиці порівняння відносно критерію С2.

	E1	E2	E3	E4	E5	E6	E7
E1	0.053	0.053	0.043	0.053	0.044	0.045	0.065
E2	0.053	0.053	0.043	0.053	0.044	0.045	0.065
E3	0.105	0.105	0.087	0.105	0.067	0.075	0.097
E4	0.053	0.053	0.043	0.053	0.044	0.045	0.065
E5	0.158	0.158	0.174	0.158	0.133	0.113	0.129
E6	0.263	0.263	0.261	0.263	0.267	0.226	0.194
E7	0.316	0.316	0.348	0.316	0.400	0.451	0.387
Σ	1.000	1.000	1.000	1.000	1.000	1.000	1.000

Розраховані значення локальних пріоритетів порівняння відносно критерію С2 наведені у таблиці 2.22.

Таблиця 2.22

Вектор локальних пріоритетів порівняння відносно критерію С2.

	W_{E1}	W_{E2}	W_{E3}	W_{E4}	W_{E5}	W_{E6}	W_{E7}	Σ
W_2	0.051	0.051	0.092	0.051	0.146	0.248	0.362	1.000

Отримані значення для вектора зважених сум наведені у таблиці 2.23.

Таблиця 2.23

Отримані значення для вектора зважених сум.

Етап	S_i
E1	0.357
E2	0.357
E3	0.642
E4	0.357
E5	1.031
E6	1.758
E7	2.577

Розрахуємо максимальне власне значення матриці порівнянь (2.23).

$$\lambda_{max} = \frac{7.026+7.026+7.013+7.026+7.057+7.088+7.120}{7} = 7.051 \quad (2.23)$$

Далі аналогічно обчислюємо індекс узгодженості (2.24).

$$IU = \frac{7.051-7}{7-1} = 0.009 \quad (2.24)$$

Також обчислюємо відношення узгодженості (2.25). Значення випадкового індексу узгодженості, яке, для матриці розмірністю 7x7, становить 1.35 (таблиця 2.6).

$$BU = \frac{0.009}{1.35} = 0.007 \quad (2.25)$$

Отримане відношення узгодженості задовольняє вимоги методології та підтверджує узгодженість матриці порівнянь (2.26).

$$BU = 0.007 < 0.10 \quad (2.26)$$

Розрахуємо оцінку етапів взаємодії користувача з сервісом електронної комерції за критерієм С3, «Вплив захисних механізмів». Значення попарних порівнянь етапів відносно критерію С3 наведені у таблиці 2.24.

Таблиця 2.24.

Попарні порівняння етапів відносно критерію С3.

	E1	E2	E3	E4	E5	E6	E7
E1	1	1	1	1	1/2	1/4	1/7
E2	1	1	1	1	1/2	1/4	1/7
E3	1	1	1	1	1/2	1/4	1/7
E4	1	1	1	1	1/2	1/4	1/7
E5	2	2	2	2	1	1/3	1/5
E6	4	4	4	4	3	1	1/3
E7	7	7	7	7	5	3	1

Нормалізовані значення попарних порівнянь етапів відносно критерію С3 наведені у таблиці 2.25.

Таблиця 2.25

Нормалізовані значення таблиці порівняння відносно критерію С3.

	E1	E2	E3	E4	E5	E6	E7
E1	0.059	0.059	0.059	0.059	0.045	0.047	0.068
E2	0.059	0.059	0.059	0.059	0.045	0.047	0.068
E3	0.059	0.059	0.059	0.059	0.045	0.047	0.068
E4	0.059	0.059	0.059	0.059	0.045	0.047	0.068
E5	0.118	0.118	0.118	0.118	0.091	0.062	0.095
E6	0.235	0.235	0.235	0.235	0.273	0.188	0.158
E7	0.412	0.412	0.412	0.412	0.455	0.563	0.475
Σ	1.000	1.000	1.000	1.000	1.000	1.000	1.000

Таблиця 2.26 містить значення локального вектору пріоритетів порівняння етапів відносно критерію С3.

Таблиця 2.26

Вектор локальних пріоритетів порівняння відносно критерію С3.

	W_{E1}	W_{E2}	W_{E3}	W_{E4}	W_{E5}	W_{E6}	W_{E7}	Σ
W_3	0.057	0.057	0.057	0.057	0.103	0.223	0.448	1.000

Отримані значення вектора зважених сум приведені у таблиці 2.27.

Таблиця 2.27

Отримані значення для вектора зважених сум.

Етап	E1	E2	E3	E4	E5	E6	E7
S _i	0.397	0.397	0.397	0.397	0.719	1.584	3.213

Розрахуємо максимальне власне значення матриці порівнянь (2.27).

$$\lambda_{max} = \frac{7.029+7.029+7.029+7.029+6.997+7.111+7.164}{7} = 7.056 \quad (2.27)$$

Знову обчислюємо індекс узгодженості (2.28).

$$IY = \frac{7.056 - 7}{7 - 1} = 0.009 \quad (2.28)$$

А також обчислюємо відношення узгодженості (2.29). Значення випадкового індексу узгодженості, яке для матриці розмірністю 7x7 становить 1.35 (таблиця 2.6).

$$BY = \frac{0.009}{1.35} = 0.007 \quad (2.29)$$

Отримане відношення узгодженості задовольняє вимоги методології та підтверджує узгодженість матриці порівнянь (2.30).

$$BY = 0.007 < 0.10 \quad (2.30)$$

Розрахуємо оцінку етапів взаємодії користувача з сервісом електронної комерції за критерієм С4, «Вплив на подальшу лояльність». Попарні порівняння етапів відносно критерію С4 приведені у таблиці 2.28.

Таблиця 2.28.

Попарні порівняння етапів відносно критерію С4.

	E1	E2	E3	E4	E5	E6	E7
E1	1	2	2	1/2	2	1/3	1/4
E2	1/2	1	1	1/3	1	1/4	1/5
E3	1/2	1	1	1/3	1	1/4	1/5
E4	2	3	3	1	3	1/2	1/3
E5	1/2	1	1	1/3	1	1/4	1/5
E6	3	4	4	2	4	1	1/2
E7	4	5	5	3	5	2	1

Нормалізовані значення попарних порівнянь етапів відносно критерію С4

наведені у таблиці 2.29.

Таблиця 2.29

Нормалізовані значення таблиці порівняння відносно критерію С4.

	E1	E2	E3	E4	E5	E6	E7
E1	0.087	0.118	0.118	0.067	0.118	0.073	0.093
E2	0.043	0.059	0.059	0.044	0.059	0.055	0.075
E3	0.043	0.059	0.059	0.044	0.059	0.055	0.075
E4	0.174	0.176	0.176	0.133	0.176	0.109	0.124
E5	0.043	0.059	0.059	0.044	0.059	0.055	0.075
E6	0.261	0.235	0.235	0.267	0.235	0.218	0.186
E7	0.348	0.294	0.294	0.400	0.294	0.436	0.373
Σ	1.000	1.000	1.000	1.000	1.000	1.000	1.000

Таблиця 2.30 містить значення локального вектору пріоритетів порівняння етапів відносно критерію С4.

Таблиця 2.30

Вектор локальних пріоритетів порівняння відносно критерію С4.

	W_{E1}	W_{E2}	W_{E3}	W_{E4}	W_{E5}	W_{E6}	W_{E7}	Σ
W_4	0.096	0.056	0.056	0.153	0.056	0.234	0.348	1.000

Отримані значення вектора зважених сум приведені у таблиці 2.31.

Таблиця 2.31

Отримані значення для вектора зважених сум.

Етап	E1	E2	E3	E4	E5	E6	E7
S_i	0.675	0.396	0.396	1.084	0.396	1.677	2.502

Розрахуємо максимальне власне значення матриці порівнянь (2.31).

$$\lambda_{max} = \frac{7.024+7.041+7.041+7.091+7.041+7.165+7.181}{7} = 7.083 \quad (2.31)$$

Обчислюємо аналогічно індекс узгодженості (2.32).

$$IU = \frac{7.083 - 7}{7 - 1} = 0.012 \quad (2.32)$$

Обчислюємо відношення узгодженості (2.33). Значення випадкового

Таблиця 2.34 містить значення локального вектору пріоритетів порівняння етапів відносно критерію С5.

Таблиця 2.34

Вектор локальних пріоритетів порівняння відносно критерію С5.

	W_{E1}	W_{E2}	W_{E3}	W_{E4}	W_{E5}	W_{E6}	W_{E7}	Σ
W_5	0.045	0.045	0.045	0.045	0.083	0.258	0.478	1.000

Отримані значення вектора зважених сум приведені у таблиці 2.35

Таблиця 2.35

Отримані значення для вектора зважених сум.

Етап	S_i
E1	0.319
E2	0.319
E3	0.319
E4	0.319
E5	0.579
E6	1.837
E7	3.464

Розрахуємо максимальне власне значення матриці порівнянь (2.35).

$$\lambda_{max} = \frac{7.025+7.025+7.025+7.025+7.012+7.124+7.250}{7} = 7.069 \quad (2.35)$$

Обчислюємо індекс узгодженості (2.36).

$$IU = \frac{7.069-7}{7-1} = 0.012 \quad (2.36)$$

Обчислюємо відношення узгодженості (2.37). Значення випадкового індексу узгодженості, яке для матриці розмірністю 7х7 становить 1.35 (таблиця 2.6).

$$BU = \frac{0.012}{1.35} = 0.009 \quad (2.37)$$

Отримане відношення узгодженості задовольняє вимоги методології та підтверджує узгодженість матриці порівнянь (2.38).

$$BU = 0.009 < 0.10 \quad (2.38)$$

Наступним кроком використання методу аналізу ієрархій є розрахунок глобальних пріоритетів використовуючи значення локальних пріоритетів

обчислених для кожного з об'єктів ранжування та ваги критеріїв оцінювання (таблиця 2.12). Нижче наведена зведена таблиця отриманих значень локальних пріоритетів для кожного з об'єктів ранжування відносно критеріїв оцінювання (таблиця 2.36).

Таблиця 2.36

Зведена таблиця значень локальних пріоритетів.

Об'єкт ранжування	Критерій оцінювання				
	C1	C2	C3	C4	C5
E1	0.063	0.051	0.057	0.096	0.045
E2	0.055	0.051	0.057	0.056	0.045
E3	0.055	0.092	0.057	0.056	0.045
E4	0.101	0.051	0.057	0.153	0.045
E5	0.164	0.146	0.103	0.056	0.083
E6	0.281	0.248	0.223	0.234	0.258
E7	0.281	0.362	0.448	0.348	0.478

Використовуючи формулу 2.7 проведемо розрахунок глобального пріоритету для кожного з об'єктів ранжування. Результати розрахунку для об'єкту ранжування E1 приведені у таблиці 2.37.

Таблиця 2.37

**Розрахунок значення глобального пріоритету для об'єкту ранжування E1
(Стартова сторінка)**

Критерій оцінювання	Вага критерію	Локальний пріоритет об'єкту ранжування	Розраховане значення
C1	0.262	0.063	0.017
C2	0.161	0.051	0.008
C3	0.099	0.057	0.006
C4	0.062	0.096	0.006
C5	0.416	0.045	0.019
Σ			0.055

Результати розрахунку для об'єкту ранжування E2 приведені у таблиці 2.38.

Таблиця 2.38

**Розрахунок значення глобального пріоритету для об'єкту ранжування Е2
(Перегляд каталогу товарів)**

Критерій оцінювання	Вага критерію	Локальний пріоритет об'єкту ранжування	Розраховане значення
C1	0.262	0.055	0.014
C2	0.161	0.051	0.008
C3	0.099	0.057	0.006
C4	0.062	0.056	0.003
C5	0.416	0.045	0.019
Σ			0.050

Результати розрахунку для об'єкту ранжування Е3 приведені у таблиці 2.39.

Таблиця 2.39

**Розрахунок значення глобального пріоритету для об'єкту ранжування Е3
(Пошук товару)**

Критерій оцінювання	Вага критерію	Локальний пріоритет об'єкту ранжування	Розраховане значення
C1	0.262	0.055	0.014
C2	0.161	0.092	0.015
C3	0.099	0.057	0.006
C4	0.062	0.056	0.003
C5	0.416	0.045	0.019
Σ			0.057

Результати розрахунку для об'єкту ранжування Е4 приведені у таблиці 2.40.

Таблиця 2.40

**Розрахунок значення глобального пріоритету для об'єкту ранжування Е4
(Перегляд товару)**

Критерій оцінювання	Вага критерію	Локальний пріоритет об'єкту ранжування	Розраховане значення
C1	0.262	0.101	0.026
C2	0.161	0.051	0.008
C3	0.099	0.057	0.006

продовж. табл. 2.40

Критерій оцінювання	Вага критерію	Локальний пріоритет об'єкту ранжування	Розраховане значення
C4	0.062	0.153	0.009
C5	0.416	0.045	0.019
Σ			0.069

Результати розрахунку для об'єкту ранжування E5 приведені у таблиці 2.41.

Таблиця 2.41

**Розрахунок значення глобального пріоритету для об'єкту ранжування E5
(Додавання до кошика)**

Критерій оцінювання	Вага критерію	Локальний пріоритет об'єкту ранжування	Розраховане значення
C1	0.262	0.164	0.043
C2	0.161	0.146	0.024
C3	0.099	0.103	0.010
C4	0.062	0.056	0.003
C5	0.416	0.083	0.035
Σ			0.115

Результати розрахунку для об'єкту ранжування E6 приведені у таблиці 2.42.

Таблиця 2.42

**Розрахунок значення глобального пріоритету для об'єкту ранжування E6
(Оформлення замовлення)**

Критерій оцінювання	Вага критерію	Локальний пріоритет об'єкту ранжування	Розраховане значення
C1	0.262	0.281	0.074
C2	0.161	0.248	0.040
C3	0.099	0.223	0.022
C4	0.062	0.234	0.015
C5	0.416	0.258	0.107
Σ			0.257

Результати розрахунку для об'єкту ранжування E1 приведені у таблиці 2.43.

Таблиця 2.43

**Розрахунок значення глобального пріоритету для об'єкту ранжування E7
(Оплата замовлення)**

Критерій оцінювання	Вага критерію	Локальний пріоритет об'єкту ранжування	Розраховане значення
C1	0.262	0.281	0.074
C2	0.161	0.362	0.058
C3	0.099	0.448	0.044
C4	0.062	0.348	0.022
C5	0.416	0.478	0.199
Σ			0.397

Отримані значення глобальних пріоритетів об'єктів ранжування, а саме етапів взаємодії користувача з сервісом електронної комерції, визначають критичність кожного з них (коефіцієнт критичності, K_E) та потенційний вплив на бізнес-показники сервісу електронної комерції (таблиця 2.44 та рис. 2.9).

Таблиця 2.44

Коефіцієнти критичності етапів взаємодії користувача з сервісом електронної комерції

№	Етап	Коефіцієнт критичності		Значення у відсотках %
1	E7 (Оплата замовлення)	K_7	0.397	39.7%
2	E6 (Оформлення замовлення)	K_6	0.257	25.7%
3	E5 (Додавання до кошика)	K_5	0.115	11.5%
4	E4 (Перегляд товару)	K_4	0.069	6.9%
5	E3 (Пошук товару)	K_3	0.057	5.7%
6	E1 (Стартова сторінка)	K_1	0.055	5.5%
7	E2 (Перегляд каталогу)	K_2	0.050	5.0%
	Σ		1.000	100.0%

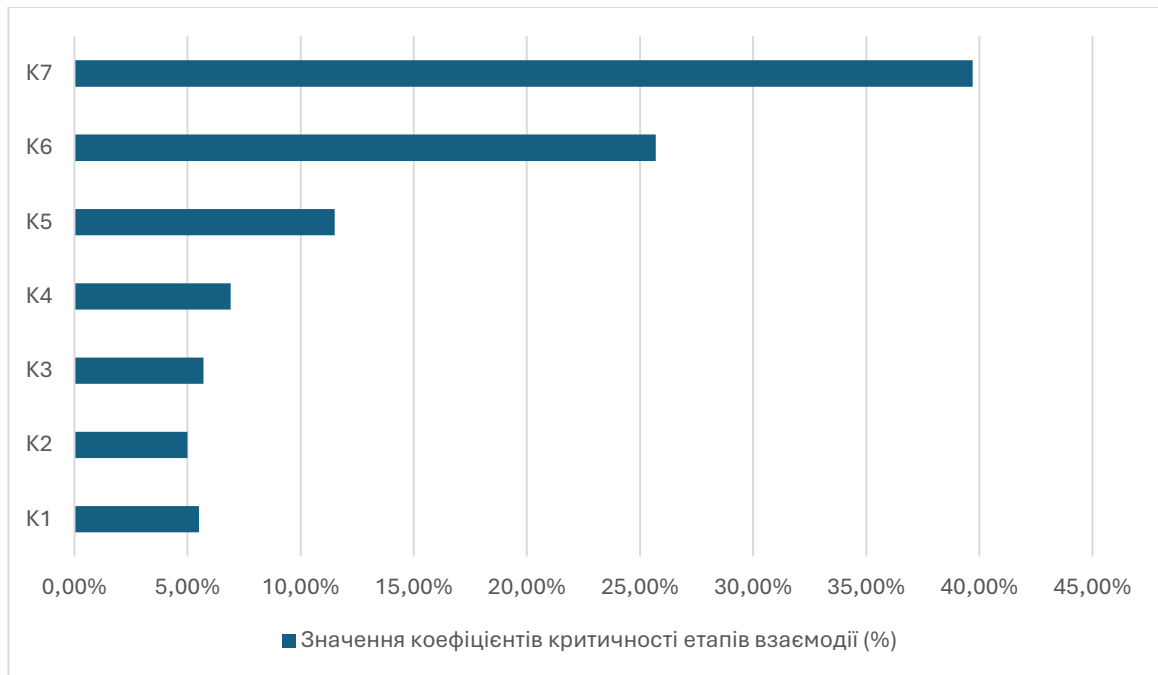


Рис. 2.9. Порівняння коефіцієнтів критичності етапів взаємодії.

Отримані коефіцієнти критичності взаємодії користувача з сервісом електронної комерції демонструють, що згідно проведеного оцінювання, найкритичнішими етапами взаємодії з сервісом електронної комерції в контексті можливого впливу систем захисту на бізнес-показники сервісу електронної комерції є E7 (Оплата замовлення, 39.7%) та E6 (Оформлення замовлення 25.7%). Решта етапів мають менший безпосередній вплив на бізнес-показники, але в цілому не мають бути проігноровані при оцінці впливу систем захисту на роботу сервісу електронної комерції, для забезпечення цілісної роботи сервісу електронної комерції та формування позитивного досвіду у користувачів.

2.4. Аналітична складова методу аналізу ефективності системи захисту сервісів електронної комерції

Як було зазначено раніше, практична реалізація архітектури методу аналізу ефективності системи захисту сервісів електронної комерції поділяється на дві функціональні складові – збір даних та аналіз даних. Функції складової, що

відповідає за збір даних (рівні архітектури 1 та 2) є стандартними та не потребують розробки в рамках даної роботи.

Основною задачею аналітичної складової методу є оцінка впливу систем захисту на взаємодію користувача з сервісом електронної комерції. Вхідними даними аналітичної складової є (рис. 2.10):

- Множина безпекових подій, що надійшли від систем захисту за період, що аналізується.
- Вектор коефіцієнтів критичності етапів взаємодії користувача $K=(K_1, K_2 \dots K_7)$, розрахований з використанням методу аналізу ієрархій.
- Дані про загальну кількість сесій користувачів сервісу електронної комерції на кожному з етапів взаємодії користувача з сервісом електронної комерції за період, що аналізується.

Застосування методу має на меті отримання наступних результатів (рис. 2.10):

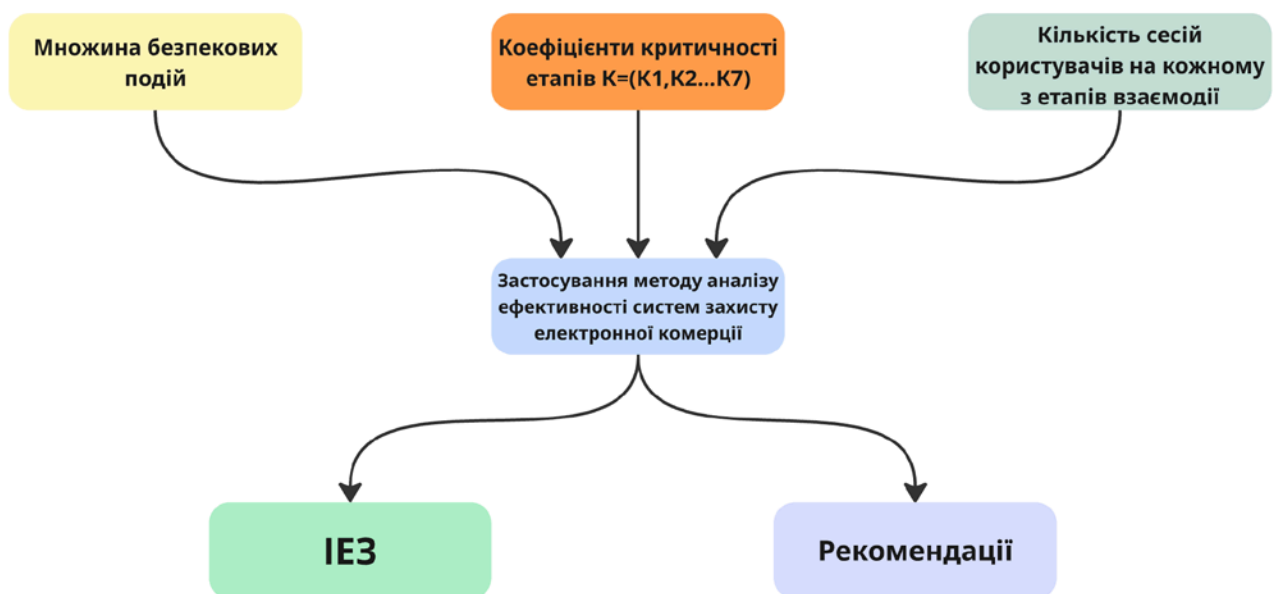


Рис. 2.10. Вхідні та вихідні дані методу.

- Індексу ефективності захисту (ІЕЗ), де $ІЕЗ \in [0,1]$ – інтегральна оцінка, що характеризує загальну ефективність роботи системи захисту в контексті специфіки сервісу електронної комерції.

- Рекомендації щодо змін налаштувань систем захисту в контексті поточного аналізу з урахуванням контексту роботи сервісу електронної комерції.

Попередньо було визначено та обґрунтовано етапи взаємодії користувача з сервісом електронної комерції, їх можна представити у вигляді множини (2.39):

$$E = \{E_1, E_2, E_3, E_4, E_5, E_6, E_7\} \quad (2.39)$$

Інформація про безпекові події містить дві складові, множину дій системи захисту (2.40) та множину результатів класифікації безпекових подій (2.41). Розглянемо їх більш детально. Множина дій системи захисту містить елементи, що визначають конкретні реакції системи захисту у відповідь на дії користувача.

$$A = \{block, allow, flag, challenge\} \quad (2.40)$$

Дія «block» – це повне блокування запитів користувача та припинення його сесії на відповідному етапі взаємодії з сервісом електронної комерції. Дія «allow» - запити користувача пройшли без втручання, подія зафіксована у журналі подій. «Flag» - дана реакція має на меті позначити запити користувача для подальшого вивчення, система захисту розпізнала їх як підозрілі, але ще не застосовує механізми блокування. Дія «challenge» - користувачу було запропоновано пройти додаткову перевірку, після успішного проходження якої користувач може продовжити взаємодію з сервісом електронної комерції.

Множина результатів класифікації безпекових подій (2.41) представляє собою дані, що отримані аналітичним шляхом на базі ретроспективного огляду реакції систем захисту на дії користувача.

$$R = \{TP, FP, TN, FN\} \quad (2.41)$$

де TP (true positive) – правильне спрацювання системи захисту, загроза була заблокована; FP (false positive) – хибне спрацювання, система захисту заблокувала доброчесні дії користувача; TN (true negative) – правильне розпізнавання запитів, що не містять загрози і відповідна відсутність реакції систем захисту на них; FN (false negative) – система захисту пропустила безпековий інцидент і він пройшов непоміченим.

У якості індивідуального екземпляру аналізу, з яким працює даний метод, виступає сесія користувача на відповідному етапі взаємодії користувача з сервісом електронної комерції. Вибір сесії користувача як одиниці аналізу базується на тому, що це є зв'язана у часі послідовність дій одного користувача, що відбувається в контексті однієї безперервної взаємодії з сервісом електронної комерції. Сесія користувача має важливе значення для бізнес-показників сервісу електронної комерції, так як кожна сесія потенційно може завершитись покупкою, а також саме на рівні сесії можна отримати цілісну оцінку впливу систем захисту на взаємодію з сервісом електронної комерції конкретного користувача.

У контексті однієї сесії користувача, якщо відбулося декілька реагувань системи захисту різного типу на одному етапі взаємодії користувача з сервісом електронної комерції, тип дії системи захисту визначається найжорсткішою дією з множини A (2.37). Одна сесія може мати декілька різних реакцій систем захисту на різних етапах взаємодії користувача з сервісом електронної комерції, в такому випадку кожна реакція визначається та опрацьовується як окрема на відповідному етапі. Результат взаємодії користувача з сервісом електронної комерції в межах однієї сесії визначається за фактичним наслідком цієї взаємодії та може бути описаний множиною H (2.42).

$$H = \{purchase, abandoned, support, incident, unknown\} \quad (2.42)$$

Іє purchase (покупка) – сесія завершилась покупкою, abandoned (покинута) – сесія була перервана, support (служба підтримки) – користувач звернувся до служби підтримки, incident (безпековий інцидент) – підтверджений безпековий інцидент, unknown (невідомий) – наслідки невідомі.

На попередніх етапах дослідження було визначено коефіцієнти критичності етапів взаємодії користувача з сервісами електронної комерції (таблиця 2.43). Для розрахунку коефіцієнтів критичності було використано метод аналізу ієрархій. Отримані коефіцієнти критичності можуть бути представлені у вигляді вектору коефіцієнтів критичності етапів взаємодії (2.43).

$$K = (K_1, K_2, K_3, K_4, K_5, K_6, K_7) \quad (2.43)$$

Коефіцієнти критичності відображають відносну частку критичності кожного етапу взаємодії користувача з сервісом електронної комерції у загальній критичності всього процесу взаємодії. Розподіл критичності етапів взаємодії демонструє, що два останні етапи (E_6 та E_7) разом становлять 65,4% загальної критичності всього процесу взаємодії, що відображає їх виключну важливість для бізнес-показників (див. таблиця 2.44). У той самий час, три ранніх етапи взаємодії користувача (E_1 , E_2 , E_3) разом складають лише 16,2% від загальної критичності процесу взаємодії з сервісом електронної комерції (див. таблиця 2.44). Відповідно вплив систем захисту на сесію користувача має різні наслідки в залежності від етапу взаємодії на якому він відбувся.

Таким чином, кожна безпекова подія (P), що надходить до подальшої обробки та аналізу представлена набором атрибутів (2.44):

$$P = (t, S, A, E_n, H) \quad (2.44)$$

де t – це час виникнення безпекової події, S – вказівник системи захисту, що зробила запис про безпекову подію. Системи захисту описуються окремо для конкретного сервісу електронної комерції при первинному налаштуванні системи аналізу. A – тип дії, що була застосована системою захисту, E_n – етап взаємодії користувача з сервісом електронної комерції, H – результат взаємодії користувача з сервісом електронної комерції.

Значення параметрів TP , FP , FN та TN не є складовою частиною безпекової події, даний метод визначає ці параметри на базі історичних даних роботи систем захисту та сервісу електронної комерції. Такий підхід обрано тому, що більшість наслідків безпекових подій не проявляються миттєво, класифікація подій потребує додаткового аналізу та зіставлення подій з різних джерел. Також у межах даної роботи, використання історичних даних роботи систем захисту та сервісу електронної комерції для класифікації безпекових подій дозволяє задавати значення параметрів при генерації вхідних даних, що забезпечує відтворюваність та можливість верифікації отриманих результатів.

Як зазначалось раніше, у якості одиниці для аналізу використовується сесія користувача при роботі з сервісом електронної комерції. Загальна кількість сесій

користувачів (N) за період, що аналізується, отримується з записів журналів вебсерверу, використовуючи підрахунок унікальних ідентифікаторів сесій з подальшим розбиттям на групи, що відповідають етапам взаємодії користувача з сервісом електронної комерції.

Етапи взаємодії користувачів з сервісом електронної комерції визначаються за допомогою налаштування відповідності між шаблонами URL запитів та етапами взаємодії (E_n). Ці налаштування задаються для конкретного сервісу електронної комерції при початковому розгортанні системи.

Часовий період, що аналізується, визначається наступними параметрами: t – час початку аналізу отриманих даних, W – величина періоду вибірки даних для аналізу. Таким чином, інтервал аналізу можна визначити як $[t-W, t]$ і відповідно всі дані для аналізу беруться за цей період. Вибір величини вибірки даних (W) впливає на якість оцінки, при зменшенні періоду вибірки даних, окремі події можуть мати більшу вагу при формуванні кінцевих результатів. У той самий час, менший період вибірки дозволяє швидше виявляти погіршення роботи систем захисту. Відповідно величина вибірки даних для опрацювання має підбиратись для виконання конкретної задачі в рамках допустимих коливань кінцевих результатів, що визначається для кожного сервісу електронної комерції окремо.

Для оцінки ефективності роботи систем захисту в контексті взаємодії користувачів з сервісом електронної комерції даним методом пропонується розрахунок інтегрального показника ефективності роботи систем захисту ІЕЗ (індекс ефективності захисту) (2.45) (рис. 2.11).

$$IEZ(t, W) = \sum_{i=1}^4 w_i * \Pi_i \quad (2.45)$$

де w_i – вагові коефіцієнти показників оцінки ефективності Π_i , t – час початку аналізу отриманих даних, W – період вибірки даних для аналізу.

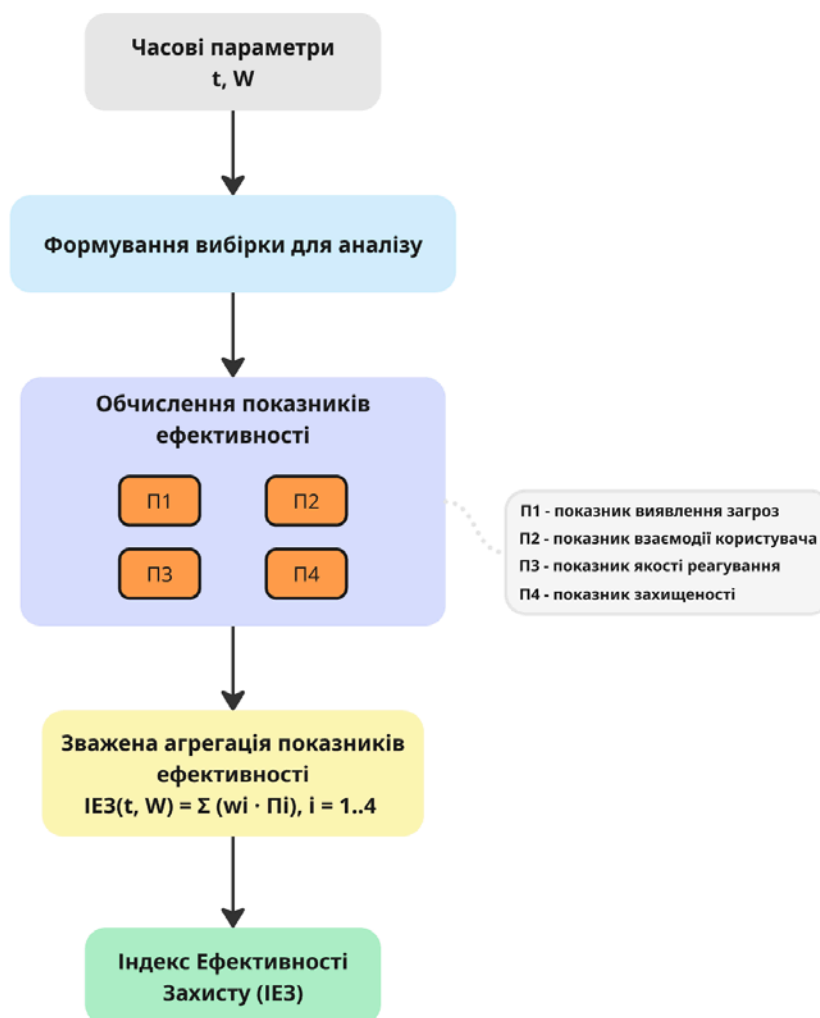


Рис. 2.11. Схема формування інтегральної оцінки ІЕЗ.

Показниками оцінки ефективності роботи системи захисту було визначено наступні: P_1 – показник виявлення загроз системами захисту, P_2 – показник взаємодії користувача з сервісом електронної комерції, P_3 – показник якості реагування систем захисту, P_4 – показник захищеності етапів взаємодії з сервісом електронної комерції. Зведена інформація про показники оцінки ефективності наведена у таблиці 2.45.

Таблиця 2.45

Зведена таблиці показників індексу ефективності захисту.

Показник	Скорочена назва	Призначення	Врахування коефіцієнту критичності K_i	Походження даних для розрахунку
Показник виявлення загроз	P_1	Відображає частку виявлених безпекових інцидентів	Ні	Потребує даних класифікації безпекових подій
Показник взаємодії користувача	P_2	Кількість хибних спрацювань систем захисту	Так	Потребує даних класифікації безпекових подій
Показник якості реагування систем захисту	P_3	Демонструє якість роботи систем захисту	Так	Базується на первинних даних
Показник захищеності етапів	P_4	Наявність захисту на етапах взаємодії	Так	Базується на первинних даних

Кількість показників для оцінки ефективності роботи систем захисту визначена кількістю незалежних аспектів, що характеризують роботу системи захисту.

Кожен з означених аспектів оцінки роботи системи захисту є необхідним, оскільки виключення будь-якого з них призведе до неповної оцінки ефективності роботи системи захисту. Кожен з перелічених аспектів роботи системи захисту є незалежним та відображає різні типи проблем у налаштуванні системи захисту.

Визначені чотири показники дозволяють провести оцінювання ефективності роботи системи захисту. Додаткові показники можуть бути додані до процесу аналізу, якщо цього потребує специфіка роботи конкретного сервісу електронної комерції.

Розглянемо кожен з показників більш детально. Π_1 (показник виявлення загроз) – демонструє здатність системи захисту виявляти та блокувати реальні загрози. Π_1 є однією з базових технічних метрик систем захисту (2.46), а саме TPR (true positive rate) [35].

$$\Pi_1 = \frac{TP}{TP+FN} \quad (2.46)$$

де TP (true positive) – загальна кількість правильно виявлених загроз, FN – загальна кількість пропущених загроз. Π_1 обраховується для всього періоду аналізу, без розбиття на етапи взаємодії користувача з сервісом електронної комерції та без урахування коефіцієнтів критичності K_i . Діапазон значень Π_1 полягає між 0 та 1, де 0 – жодна загроза не була ідентифікована, а 1 – всі загрози були виявлені.

Π_2 (показник взаємодії користувача) – надає оцінку впливу роботи систем захисту на взаємодію користувача з сервісом електронної комерції. Даний показник враховує коефіцієнт критичності етапів взаємодії користувача з сервісом електронної комерції і може бути представлений наступним чином (2.47):

$$\Pi_2 = \sum_{i=1}^7 K_i * (1 - FPR_i) \quad (2.47)$$

де K_i – коефіцієнт критичності етапу E_i , FPR_i – частка хибних спрацювань (false positive rate) на етапі E_i . FPR_i розраховується як (2.48) [35]:

$$FPR_i = \frac{FP_i}{FP_i + TN_i} \quad (2.48)$$

Параметр TN_i , кількість правильних виявлень відсутності загрози, розраховується як (2.49):

$$TN_i = N_i - TP_i - FP_i - FN_i \quad (2.49)$$

де N_i – кількість сесій на етапі взаємодії, TP_i – кількість правильних спрацювань систем захисту на етапі взаємодії, FP_i – кількість хибних спрацювань систем захисту на етапі взаємодії, FN_i – кількість хибних неспрацювань систем захисту на етапі взаємодії.

Оскільки $\sum K_i = 1$, то значення Π_2 лежить в межах від 0 до 1. Таким чином, якщо значення $FPR_i = 0$ на всіх етапах взаємодії користувача з сервісом електронної комерції, то показник Π_2 має ідеальне значення – 1. У випадку якщо $FPR_i = 1$ на всіх етапах взаємодії, то показник Π_2 отримує найгірше можливе значення – 0. Використання коефіцієнтів критичності K_i для розрахунку показника Π_2 дозволяє врахувати вплив роботи систем захисту сервісів електронної комерції на бізнес-показники.

Π_3 (показник якості реагування систем захисту) – демонструє на скільки дії системи захисту сервісу електронної комерції відповідають критичності етапу взаємодії користувача з сервісом електронної комерції (2.50).

$$\Pi_3 = \sum_{i=1}^7 K_i * M_i \quad (2.50)$$

де M_i – показник якості дій систем захисту на етапі E_i . У випадку, якщо на етапі E_i були спрацювання систем захисту, M_i розраховується як (2.51):

$$M_i = 1 - \frac{w_i - w_{min}}{w_{max} - w_{min}}, i = 1..7$$

$$w_i = \frac{w_a * N_{a_i}}{N_{all_i}}, i = 1..7 \quad (2.51)$$

де w_a – коефіцієнт впливу дії, N_{a_i} – кількість дій a на етапі E_i , N_{all_i} – кількість всіх спрацювань систем захисту всіх типів на етапі E_i . Варіанти спрацювань систем захисту визначені множиною A (2.41). $w_{min} = 1$, коефіцієнт впливу дії allow, $w_{max} = 4$, коефіцієнт впливу дії block. w_i – середньозважений коефіцієнт впливу дій систем захисту на етапі E_i .

У випадку, якщо на етапі E_i не було зафіксовано жодної реакції безпекових систем, то $M_i = 1$, що означає відсутність впливу систем захисту на взаємодію користувача з сервісом електронної комерції. Якщо ж всі дії систем захисту на етапі E_i відносились до типу block, то $M_i = 0$.

Показник Π_3 дозволяє врахувати, який вплив ті чи інші дії систем захисту мають на бізнес-показники сервісу електронної комерції. Так, на ранніх етапах взаємодії користувача з сервісом електронної комерції вплив систем захисту на

бізнес-показники мінімальний. У той самий час, на пізніх етапах, де користувач вже має чіткі наміри здійснити покупку, невдале втручання систем захисту несе більш відчутний вплив на бізнес-показники сервісу електронної комерції.

Застосований для розрахунку показника якості дії системи захисту M_i коефіцієнт впливу безпекових дій w_a приймає значення від 1 до 4, що відображає міру впливу кожної з безпекових дій на взаємодію користувача з сервісом електронної комерції (таблиця 2.46). Дія allow не вносить жодних змін у процес взаємодії, значення $w_a = 1$. Дія flag несе суто внутрішній вплив, але в подальшому може стати причиною більш жорстких дій відносно користувача, $w_a = 2$. Дія challenge змушує користувача проходити етапи додаткової верифікації, що може призвести до відмови подальшої взаємодії з сервісом електронної комерції, $w_a = 3$. Дія block повністю блокує подальші дії користувача і відповідно має максимальний вплив на взаємодію з сервісом електронної комерції, $w_a = 4$.

Таблиця 2.46

Значення коефіцієнту впливу безпекових подій.

Тип безпекової дії	Значення коефіцієнта w_a	Пояснення
block	4	Повне блокування, подальша взаємодія користувача з сервісом електронної комерції припиняється.
allow	1	Дії користувача визнані безпечними, система захисту на взаємодію користувача з сервісом електронної комерції не впливає.
flag	2	Дії користувача позначені для вивчення, доступ дозволено. Можливі мінімальні технічні затримки через додаткову обробку.
challenge	3	Дії користувача потребують його додаткової верифікації.

P_4 (показник захищеності етапів) – оцінює повноту захисту етапів взаємодії користувача з сервісом електронної комерції. Показник P_4 може бути описаний наступним чином (2.52):

$$P_4 = \sum_{i=1}^7 K_i * G_i \quad (2.52)$$

де G_i приймає значення 0 або 1, та є показником наявності активного захисту на етапі взаємодії E_i . Значення показника P_4 лежить в межах від 0 до 1, якщо захист присутній на всіх етапах взаємодії користувача з сервісом електронної комерції P_4 набуває значення 1. У випадку відсутності активних систем захисту на всіх етапах взаємодії – $P_4 = 0$. Використання коефіцієнтів критичності K_i для розрахунку показника P_4 надає можливість змінювати вплив різних етапів взаємодії на значення P_4 .

Показники P_1 та P_2 потребують додаткової класифікації отриманих даних для визначення класу безпекових подій. Показники P_3 та P_4 базуються виключно на первинних даних і можуть бути обчислені без додаткових етапів обробки даних. Це дозволяє проводити розрахунок значень індексу ефективності захисту навіть маючи обмежені відомості щодо роботи систем захисту сервісу електронної комерції.

Визначення коефіцієнтів критичності етапів взаємодії k_i є ключовим елементом методу аналізу ефективності системи захисту сервісів електронної комерції. Їх подальше використання при розрахунку індексу ефективності захисту робить можливим послідовне врахування специфіки роботи сервісів електронної комерції та впливу на бізнес-показники спрацювання систем захисту на різних етапах взаємодії користувача з сервісом електронної комерції.

Розрахунок індексу ефективності захисту сервісу електронної комерції потребує визначення вагових коефіцієнтів кожного з показників P_i . Для їх обчислення було застосовано метод аналізу ієрархій, описаний і застосований раніше для визначення коефіцієнтів критичності етапів взаємодії користувача з сервісом електронної комерції. Показники порівнюються між собою для визначення їх ваги відносно визначеної мети. Такий підхід забезпечує узгоджений та обґрунтований розподіл ваг показників оцінки ефективності систем захисту сервісів електронної комерції. Визначення ваги кожного з показників P_i дає відповіді на наступні питання: ваговий коефіцієнт P_1 – на

скільки важливо виявляти всі безпекові інциденти; ваговий коефіцієнт P_2 – наскільки важливо не блокувати легітимні запити користувачів; ваговий коефіцієнт P_3 – наскільки важливо мати відповідність між реакцією систем захисту та критичністю етапу взаємодії користувача з сервісом електронної комерції; ваговий коефіцієнт P_4 – наскільки важливе покриття захистом всіх етапів взаємодії користувача з сервісом електронної комерції. Визначення вагових коефіцієнтів показників P_i відносно один одного представляє собою дворівневу ієрархію зображену нижче (рис. 2.12).



Рис. 2.12. Ієрархія визначення вагових коефіцієнтів показників P_i .

Проведемо попарні порівняння показників P_i , результати порівняння представленні у таблиці 2.47.

Таблиця 2.47

Попарні порівняння показників P_i

	P_1	P_2	P_3	P_4
P_1	1	3	5	2
P_2	1/3	1	3	1/2
P_3	1/5	1/3	1	1/3
P_4	1/2	2	3	1

Таблиця 2.48 містить нормалізовані значення попарних порівняння показників P_i .

Таблиця 2.48

Нормалізовані значення таблиці порівняння показників Π_i

	Π_1	Π_2	Π_3	Π_4
Π_1	0.492	0.474	0.417	0.522
Π_2	0.164	0.158	0.250	0.130
Π_3	0.098	0.053	0.083	0.087
Π_4	0.246	0.316	0.250	0.261
Σ	1.000	1.000	1.000	1.000

Отримані значення розрахунку вектора локальних пріоритетів порівняння показників Π_i наведені у таблиці 2.49.

Таблиця 2.49

Вектор локальних пріоритетів порівняння показників Π_i .

	$W_{\Pi 1}$	$W_{\Pi 2}$	$W_{\Pi 3}$	$W_{\Pi 4}$	Σ
W	0.476	0.176	0.080	0.268	1.000

Розраховані значення вектора зважених сум приведені у таблиці 2.50.

Таблиця 2.50

Отримані значення для вектора зважених сум.

Етап	S_i
Π_1	1.941
Π_2	0.709
Π_3	0.323
Π_4	1.098

Проведемо обчислення вектору узгодженості для матриці порівнянь (2.53).

$$\begin{aligned}
 V_1 &= \frac{1.941}{0.476} = 4.077 \\
 V_2 &= \frac{0.709}{0.176} = 4.028 \\
 V_3 &= \frac{0.323}{0.080} = 4.038 \\
 V_4 &= \frac{1.098}{0.268} = 4.097
 \end{aligned}
 \tag{2.53}$$

Використовуючи отримані значення, розрахуємо максимальне власне значення матриці порівнянь показників Π_i (2.54).

$$\lambda_{max} = \frac{4.077+4.028+4.038+4.097}{4} = 4.060 \quad (2.54)$$

Обчислюємо індекс узгодженості (2.55).

$$IU = \frac{4.060-4}{4-1} = 0.020 \quad (2.55)$$

Обчислюємо відношення узгодженості (2.56). Значення випадкового індексу узгодженості, яке для матриці розмірністю 4x4 становить 0.89 (таблиця 2.6).

$$BU = \frac{0.020}{0.89} = 0.022 \quad (2.56)$$

Отримане відношення узгодженості задовольняє вимоги методології та підтверджує узгодженість матриці порівнянь (2.57).

$$BU = 0.022 < 0.10 \quad (2.57)$$

Таким чином, було отримано та перевірено значення ваг для показників Π_i (рис. 2.13).

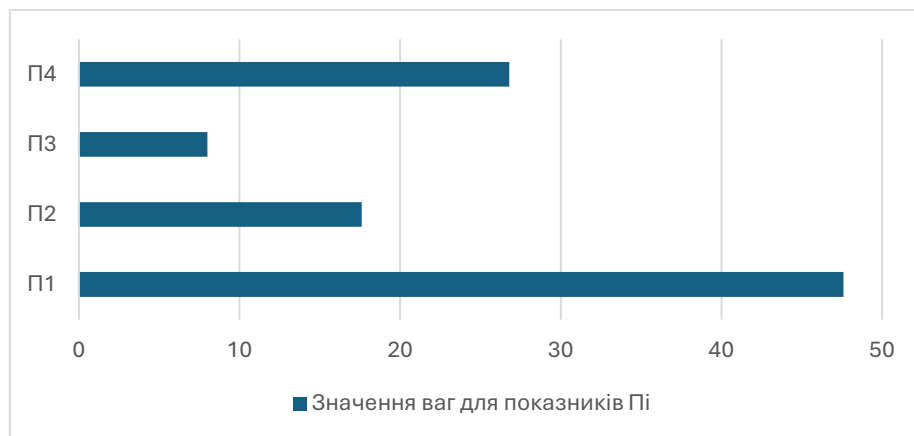


Рис. 2.13. Порівняння значення ваг показників Π_i

Значення вагових коефіцієнтів показників Π_i наведені у таблиці 2.51.

Таблиця 2.51

Вагові коефіцієнти показників Π_i

Показник	Ваговий коефіцієнти
Π_1	0.476
Π_2	0.176
Π_3	0.080
Π_4	0.268

Згідно проведеного оцінювання показників P_i , майже половина загальної ваги (47.6%) показників P_i зосереджена за показником P_1 – показником виявлення загроз системами захисту. Такий результат є цілком обґрунтованим, оскільки виявлення загроз є першою ланкою функціонування систем захисту, без своєчасного виявлення безпекових загроз решта захисних механізмів не буде активована. Другим за значимістю, в результаті оцінювання ваг показників P_i , є показник P_4 – показник захищеності етапів взаємодії користувача з сервісом електронної комерції. Його вага становить 26.8% від загальної ваги. Цей результат відображає специфіку роботи сервісів електронної комерції, так як безпекові інциденти на будь-якому з етапів взаємодії користувача з сервісом електронної комерції можуть мати наслідки у вигляді витоку персональної або фінансової інформації. Показник P_2 – показник взаємодії користувача з сервісом електронної комерції, отримав вагу 17.6%. Це відповідає концепції проєктування систем захисту, де безпека і зручність мають збалансовані, але у випадку конфлікту пріоритетів перевага надається захисту системи. Найменшу вагу отримав показник P_3 – показник якості реагування систем захисту. Відносно низьке його значення не означає, що він є неважливим, а демонструє його залежність від показників P_1 та P_4 , так як якість реагування залежить від якісного та своєчасного виявлення безпекових інцидентів.

Для більш збалансованого оцінювання в контексті конкретного сервісу електронної комерції необхідно залучати фахівців, що відповідають за різні аспекти функціонування сервісу електронної комерції. Це дозволить охопити всі проблемні області та отримати оцінку, що буде відображати актуальний стан та бажані результати на поточний момент для конкретного сервісу електронної комерції.

Результатом розрахунку індексу ефективності захисту є отримання загальної оцінки ефективності роботи систем захисту електронної комерції. Індекс ефективності захисту приймає значення в межах від 0 до 1. Для інтерпретації отриманих значень пропонується використовувати шкалу, що має п'ять рівнів. Такий спосіб категоризації забезпечує достатню деталізацію та

зручність тлумачення отриманих результатів. Зазначений спосіб оцінювання також застосовується для інтерпретації отриманих значень показників ефективності захисту Π_i . В рамках даної роботи використана наступна шкала інтерпретації отриманих результатів (таблиця 2.52).

Таблиця 2.52

Запропонована шкала інтерпретації значення ІЕЗ

Значенні ІЕЗ	Узагальнена оцінка	Інтерпретація
≥ 0.90	Відмінно	Захист та якість взаємодії збалансовані
0.80 – 0.90	Добре	Певні показники вимагають незначного покращення
0.70 – 0.80	Задовільно	Відчутний вплив на взаємодію з користувачами
0.60 – 0.70	Незадовільно	Система захисту потребує перегляду налаштувань
< 0.60	Критично	Система захисту перешкоджає нормальній взаємодії з сервісом електронної комерції

Межі використані для узагальненої оцінки можуть бути адаптовані під потреби конкретного сервісу електронної комерції з урахуванням специфіки його роботи та вимог до рівня захищеності.

Індекс ефективності захисту є стабільною метрикою, що надає можливість порівнювати отримані результати за різні періоди аналізу. Проте однакові значення індексу ефективності відображають різний вплив на бізнес-показники в залежності від контексту роботи сервісу електронної комерції.

Зважаючи на потребу враховувати контекст роботи сервісу електронної комерції, для кількісного відображення цієї залежності додатково розраховується контекстний індекс ефективності захисту (ІЕЗ_k). Для кількісної оцінки впливу контексту роботи сервісу електронної комерції на бізнес-показники залежні від ефективності роботи систем захисту використано коефіцієнт контекстної чутливості (ККЧ) (2.58).

$$\text{ККЧ}(W) = \text{ЧФ}(W) * \text{БФ}(W) \quad (2.58)$$

де $\text{ЧФ}(W)$ – це середнє значення часового фактору за період аналізу W , $\text{БФ}(W)$ – середнє значення бізнес-фактору за період аналізу W . $\text{ККЧ}(W)$ – розрахований коефіцієнт, що визначає ступінь впливу контексту на оцінку ефективності захисту сервісу електронної комерції.

Часовий фактор (ЧФ) відображає частку очікуваного користувацького трафіку відносно пікового рівня. Зокрема, вночі користувачів менше, в обідній час та ближче до кінця робочого дня кількість користувачів може зростати. Значення $\text{ЧФ}(W) = 1$ відповідає максимальному рівню трафіку користувачів. Можливі інші шаблони взаємодії користувачів із сервісом електронної комерції, ці параметри визначаються в контексті специфіки конкретного сервісу електронної комерції та на основі аналізу історичних даних про трафік.

Бізнес-фактор (БФ) – це відображення очікуваного зростання трафіку користувачів внаслідок запланованих бізнес-подій. До таких подій можна віднести розпродажі, святкові дні та інші події, що несуть системний характер та планування. Відповідно системи захисту повинні враховувати очікуване зростання кількості користувачів, так як їх вплив на взаємодію користувачів з сервісом електронної комерції має більший вплив на бізнес-показники. Значення $\text{БФ}(W) = 1$ відповідає нормальному режиму роботи. Конфігурація параметрів для визначення бізнес-фактору відбувається на основі історичних даних про роботу сервісу, аналізу маркетингових очікувань тощо. Ці параметри визначаються в контексті роботи конкретного сервісу електронної комерції.

Для розрахунку контекстного індексу ефективності захисту необхідно визначити дефіцит ефективності захисту $\Delta(t, W)$ (2.59)

$$\Delta(t, W) = 1 - \text{IE3}(t, W) \quad (2.59)$$

де $\text{IE3}(t, W)$ – базовий індекс ефективності захисту. Значення $\Delta(t, W)$ лежить в межах від 0 до 1, де $\Delta(t, W) = 0$ – це ідеальний захист, $\Delta(t, W) = 1$ – захист системи повністю неефективний.

Використовуючи отримане значення $\Delta(t, W)$, можемо розрахувати контекстний індекс ефективності захисту (2.60).

$$IEZ_K = 1 - KKЧ(W) * \Delta(t, W) \quad (2.60)$$

де $KKЧ(W)$ – коефіцієнт контекстної чутливості, $\Delta(t, W)$ – дефіцит ефективності захисту.

Значення IEZ_K інтерпретується за шкалою з п'яти рівнів, що була представлена вище (див. табл. 2.52).

Базовий IEZ та контекстний IEZ_K не є заміниками один одного, оскільки вони виконують різні функції в методі аналізу ефективності систем захисту сервісів електронної комерції. IEZ дозволяє на постійній основі проводити порівняння між різними періодами аналізу, відстежувати прогрес оптимізації роботи систем захисту та виконання встановлених показників. IEZ_K у свою чергу залежить від контексту роботи сервісу електронної комерції на період аналізу та дозволяє оцінити і пріоритезувати необхідні дії для підготовки систем захисту до бізнес-подій.

Результатом застосування методу аналізу ефективності системи захисту сервісів електронної комерції є отримання індексу ефективності захисту, що формується на базі чотирьох показників ефективності (Π_1 - Π_4), та контекстного індексу ефективності захисту, який додатково враховує специфіку функціонування сервісів електронної комерції, а саме часовий фактор та бізнес-фактор.

Метод аналізу ефективності систем захисту сервісів електронної комерції працює з агрегованими даними про роботу систем захисту та взаємодію користувачів з сервісом електронної комерції, відповідно опрацювання та зберігання деталізованої інформації про конкретні безпекові події залишається на рівні журналів подій систем захисту. Метою застосування даного методу є отримання загального розуміння про стан взаємодії систем захисту в контексті роботи сервісу електронної комерції. У зв'язку з цим, метод не передбачає точного визначення конкретних причин проблем, що були ідентифіковані, але здатний точно вказати напрямок, у якому необхідно рухатись для локалізації проблеми та оптимізації відповідних налаштувань.

Зважаючи на це, система рекомендацій методу аналізу ефективності системи захисту сервісів електронної комерції виконує діагностичну функцію, але не передбачає рекомендацій щодо конкретний дій. Пошук конкретних причин виникнення тих чи інших проблем проводиться на подальших етапах поглибленого вивчення операційних журналів систем захисту та сервісу електронної комерції, що лежить поза межами аналізу ефективності роботи систем захисту.

Система рекомендацій методу аналізу ефективності системи захисту сервісів електронної комерції складається з трьох етапів (рис. 2.14).

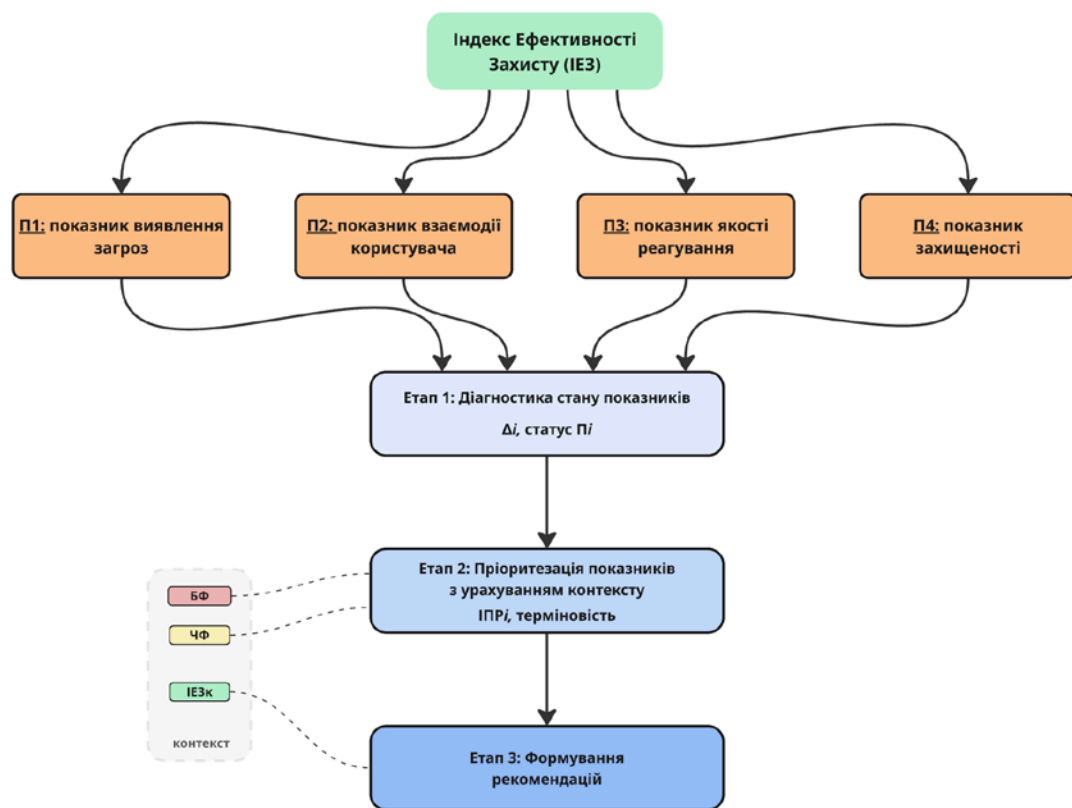


Рис. 2.14. Робота системи рекомендацій.

На першому етапі для кожного з чотирьох показників ефективності системи захисту визначається його належність до однієї з п'яти узагальнених оцінок шкали інтерпретації значень (таблиця 2.52) та обчислюється значення відхилення від цільового рівня.

Значення відхилення від цільового показника Δ_i розраховується як різниця між цільовим та фактичним значенням (2.61).

$$\Delta_i = P_{i_{\text{цільове}}} - P_{i_{\text{фактичне}}} \quad (2.61)$$

де $P_{i_{\text{цільове}}} = 0.90$ – нижня межа узагальненої оцінки «Відмінно», що приймається за цільовий рівень значення показника P_i . У випадку, якщо $P_i \geq 0.90$, то $\Delta_i = 0$ і показник P_i не потребує подальшого опрацювання системою рекомендацій. Класифікація стану показників та відповідного опрацювання системою рекомендацій приведено у таблиці 2.53.

Таблиця 2.53

Класифікація стану показників ефективності системи захисту

Фактичне значення показника P_i	Визначений статус показника P_i	Реакція системи рекомендацій
≥ 0.90	Відмінно	Рекомендації відсутні, показник в нормі
$0.80 - 0.90$	Добре	Рекомендація звернути увагу на показник при наступному циклі оцінювання
$0.70 - 0.80$	Задовільно	Рекомендація провести аналіз причин низького значення показника та планування покращень
$0.60 - 0.70$	Незадовільно	Рекомендація цілеспрямованого аналізу журналів подій та перегляд заданих конфігурацій
< 0.60	Критично	Рекомендація термінової перевірки та втручання у процеси реагування систем захисту

Результатом першого етапу роботи системи рекомендацій є перелік показників P_i з вказаним відхиленням від цільового показника Δ_i , кожен з яких має визначений статус.

Другий етап роботи системи рекомендацій виконує пріоритезацію показників P_i з урахуванням значень часового фактору та бізнес-фактору. Для цього для всіх P_i з $\Delta_i > 0$ розраховується індекс пріоритету рекомендації (ІПР)

$$\text{ІПР}_i = \Delta_i * \text{БФ} * \text{ЧФ} \quad (2.62)$$

Індекс пріоритету рекомендації дозволяє врахувати вплив відхилення від цільового значення показника $П_i$ та встановити рекомендовану пріоритетність реагування на недоліки у роботі систем захисту.

Рекомендаційна система методу аналізу ефективності системи захисту сервісів електронної комерції передбачає класифікацію отриманих значень $ІПР_i$ за чотирма рівнями пріоритету (таблиця 2.54). Порогові значення, використані для визначення рівнів пріоритету є параметром, що визначається для потреб конкретного сервісу електронної комерції виходячи зі специфіки його роботи та вимог до захисту. В якості порогових значень рівнів класифікації ІПР у межах даної роботи прийнято пороги 0.10, 0.20 та 0.30 з рівномірним кроком 0.10. Обрані значення відповідають різниці між рівнями оцінювання представленими у таблиці 2.53 і демонструють віддалення від нижньої межі найвищої оцінки в бік погіршення.

У якості рівнів пріоритету показників $П_i$ пропонується використовувати загальноприйнятну класифікацію, що широко використовуються у ризик-менеджменті та системах управління проєктами [57]. Дана класифікація передбачає визначення декількох рівнів пріоритету, в залежності від потреб, де Р1 позначає найвищий пріоритет.

Таблиця 2.54

Значення рівнів пріоритету рекомендацій

Рівень пріоритету	Значення $ІПР_i$	Скорочене позначення
Низький	≤ 0.10	Р4
Помірний	0.10 – 0.20	Р3
Високий	0.20 – 0.30	Р2
Критичний	> 0.30	Р1

Результатом другого етапу є впорядкований за ІПР перелік показників $П_i$, що мають визначений клас терміновості та потребують уваги.

Третій етап роботи системи рекомендацій об'єднує результати діагностики та пріоритезації у структурований перелік рекомендацій. Для кожного показника

P_i формуються рекомендації, що поєднують значення отримані на першому та другому етапі роботи системи рекомендацій:

- показник (P_i) – вказує, яка саме частина роботи системи захисту потребує уваги: виявлення загроз (P_1), взаємодія з користувачами (P_2), якість реагування (P_3), покриття захистом (P_4).
- статус показника – вказує визначений статус показника та рекомендацію щодо подальших дій згідно визначень у таблиці 2.51.
- рівень пріоритету – вказує визначений пріоритет рекомендованих дій з урахуванням поточних умов роботи сервісу електронної комерції.

Загальний стан роботи системи захисту, з врахуванням поточного контексту роботи сервісу електронної комерції, визначається значенням контекстного індексу ефективності захисту (IEZ_K), інтерпретація якого надається згідно таблиці 2.52. Деталізація загальної оцінки на рівні окремих показників P_i здійснюється з використанням індексу пріоритету рекомендацій (ІПР), який репрезентує внесок кожного з показників P_i у відхилення від бажаного значення. Таким чином, IEZ_K та ІПР являються двома рівнями деталізації одного механізму оцінки роботи систем захисту.

Розроблений метод аналізу ефективності систем захисту сервісів електронної комерції (рис. 2.15) формує три рівня врахування бізнес-контексту сервісів електронної комерції при оцінці ефективності роботи систем захисту.

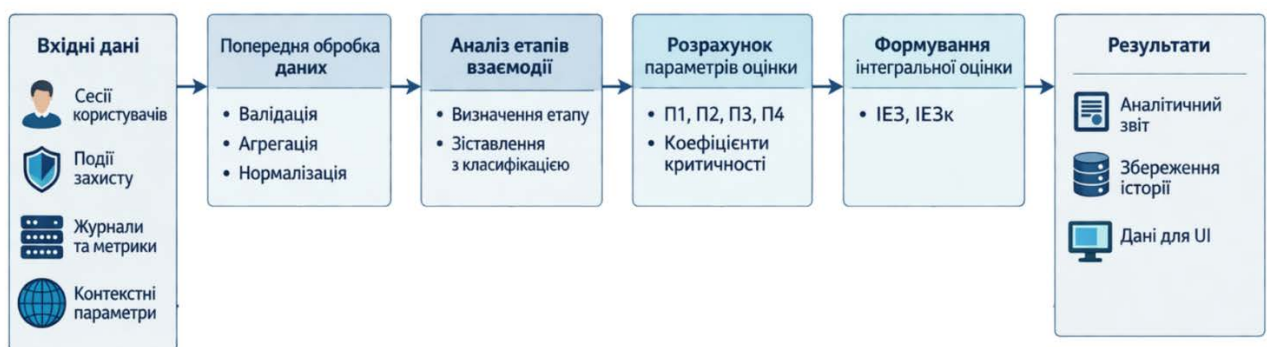


Рис. 2.15. Загальна схема функціонування методу.

Перший рівень – це використання коефіцієнтів критичності етапів взаємодії користувачів з сервісом електронної комерції K_E . Другий рівень – це

коефіцієнт контекстної чутливості (ККЧ), що відображає динамічну природу роботи сервісів електронної комерції та дозволяє оцінити технічний рівень захисту в залежності від поточного контексту функціонування сервісу електронної комерції. Третій рівень – формування рекомендацій, де контекст роботи сервісу електронної комерції безпосередньо впливає на пріоритизацію тих чи інших дій, визначених у процесі діагностики стану показників Π_i .

Висновки до другого розділу

У другому розділі "Метод оцінки ефективності роботи систем захисту сервісів електронної комерції" досліджено проблеми оцінки ефективності захисту сервісів електронної комерції; запропонована загальна архітектура методу аналізу ефективності системи захисту сервісів електронної комерції; визначено коефіцієнти критичності етапів взаємодії користувача з сервісом електронної комерції; наведена аналітична складова методу аналізу ефективності системи захисту сервісів електронної комерції.

Визначено, що наявні підходи першочергово фокусуються на оцінці роботи систем захисту за технічними параметрами, не враховуючи вплив захисних механізмів на взаємодію користувачів із сервісами електронної комерції та бізнес-показники сервісів електронної комерції.

Розроблено чотирирівневу архітектуру методу аналізу ефективності системи захисту сервісів електронної комерції, що забезпечує повний цикл аналізу від збору метрик до формування бізнес-оцінки. Формалізовано модель взаємодії користувачів з сервісами електронної комерції у вигляді послідовності з семи етапів.

Визначено коефіцієнти критичності етапів взаємодії користувачів з сервісами електронної комерції K_E . Для цього було використано метод аналізу ієрархій та визначено п'ять критеріїв оцінювання. Узгодженість отриманих результатів було перевірено за допомогою розрахунку індексу узгодженості. Застосована методологія забезпечує формалізацію та відтворюваність процесу

розрахунку коефіцієнтів критичності етапів взаємодії користувачів із сервісами електронної комерції.

Розроблено аналітичну складову методу аналізу ефективності системи захисту сервісів електронної комерції, що дозволяє розрахувати інтегральний індекс ефективності захисту на основі розрахунку чотирьох показників ефективності роботи систем захисту: виявлення загроз (P_1), взаємодія з користувачами (P_2), якість реагування (P_3), покриття захистом (P_4). Обґрунтовано важливість використання чотирьох показників для оцінки роботи системи захисту сервісів електронної комерції. Для визначення вагових коефіцієнтів показників P_i використано метод аналізу ієрархій. Запропоновано розрахунок контекстного індексу ефективності захисту, що додатково враховує контекст функціонування сервісів електронної комерції, а саме часовий фактор та бізнес-фактор через коефіцієнт контекстної чутливості.

Запропоновано систему формування рекомендацій на основі оцінювання ефективності роботи систем захисту сервісів електронної комерції. Система формування рекомендацій дозволяє провести діагностику стану показників P_i та визначити пріоритети виявлених проблемних аспектів із урахуванням контексту роботи сервісу електронної комерції.

Розроблений метод аналізу ефективності системи захисту сервісів електронної комерції забезпечує урахування бізнес-контексту сервісів електронної комерції на трьох рівнях: через коефіцієнти критичності етапів взаємодії користувачів з сервісами електронної комерції; через коефіцієнт контекстної чутливості при розрахунку контекстного індексу ефективності захисту; через розрахунок пріоритетів проблемних аспектів при роботі системи рекомендацій.

Результати досліджень представлені в наукових публікаціях здобувача [1, 4, 7].

РОЗДІЛ 3. Алгоритми, та програмна реалізація методу аналізу ефективності системи захисту сервісів електронної комерції

3.1. Алгоритмічне забезпечення методу аналізу ефективності системи захисту сервісів електронної комерції

Метод аналізу ефективності системи захисту сервісів електронної комерції має чітке розмежування функціональних рівнів обробки даних. Відповідно до запропонованої архітектури методу (рис. 2.1), рівні 1 та 2, збір базових даних та кореляційний аналіз подій, відповідають за підготовку даних, у той час, як рівні 3 та 4, контекстний аналіз та оцінка бізнес-впливу, є аналітичною складовою методу. Дане розмежування робить можливим забезпечення модульності методу аналізу системи захисту сервісів електронної комерції та уникнути залежності від конкретних систем збору та підготовки даних.

Система збору та підготовки даних виступає у ролі постачальника даних для подальшого аналізу аналітичною складовою методу. Задачею зовнішньої системи збору та підготовки даних є агрегація та трансформація різнорідних потоків даних з багатьох джерел у єдиний стандартизований формат, що є придатним для аналізу з використанням методу аналізу ефективності системи захисту сервісів електронної комерції. Розробка зовнішньої системи збору та підготовки даних не є частиною цього дослідження, однак дана робота визначає перелік вимог до такої системи, що має на меті забезпечити коректну роботу аналітичної складової методу аналізу ефективності системи захисту сервісів електронної комерції.

Система збору та підготовки даних повинна забезпечувати агрегацію даних з декількох джерел, кожне з яких необхідне для формування вхідного набору даних для подальшого аналізу. До таких джерел відносяться журнали подій вебсервера, журнали подій систем захисту, метрики сервісу електронної комерції. Окремо від цього, система збору та підготовки даних має забезпечувати наскрізну ідентифікацію сесій користувачів серед усіх подій, що надходять. Ідентифікатор сесій є атрибутом, що робить можливим об'єднання подій з різних

джерел між собою та формування повного ланцюга подій, пов'язаних між собою. Зважаючи на різноманітність джерел, забезпечення нормалізації формату ідентифікаторів є однією з вимог до системи збору та підготовки даних.

На етапі збору даних, зовнішня система, що забезпечує його реалізацію, повинна містити конфігурацію відповідності запитів до певних етапів взаємодії користувача з сервісом електронної комерції. Дана класифікація реалізується з допомогою використання URL-шаблонів запитів або інших атрибутів запиту, що роблять можливим віднести його до одного з множини етапів $E = \{E_1, E_2, E_3, E_4, E_5, E_6, E_7\}$. Налаштування відповідності запитів етапам відбуваються в контексті конкретного сервісу електронної комерції з урахуванням особливостей його роботи.

Окремо на зовнішньому етапі підготовки даних необхідно проводити класифікацію безпекових подій за категоріями TP, FP, TN, FN. Дана класифікація виконується на базі співставлення спостережуваних дій систем захисту та їх наслідків для взаємодій користувача з сервісом. Ця частина є опціональною та за відсутності достатньої інформації для проведення класифікації допускає відсутність даних.

Система збору та підготовки даних має виконувати підрахунок агрегованих метрик для кожного етапу взаємодії користувача з сервісом електронної комерції за період аналізу W . До цих метрик відносяться: загальна кількість сесій N , за наявності – кількість подій за категоріями безпекових подій, кількість дій за типами реакції системи захисту.

Результатом роботи зовнішньої системи збору та підготовки даних є формування вихідного документу у форматі JSON, що відповідає специфікації вхідного інтерфейсу аналітичної складової методу, яку наведено нижче.

Всі сім етапів взаємодії користувача з сервісом електронної комерції мають бути представлені у вхідному JSON документі. У випадку відсутності подій значення мають відповідати нульовим. Це є необхідною вимогою для коректного врахування коефіцієнтів критичності етапів взаємодії користувача.

Існує багато систем, що здатні забезпечити реалізацію вимог до зовнішньої системи збору та підготовки даних. До них належать такі рішення, як ELK Stack, SIEM системи, що мають вбудовані механізми кореляції та агрегації, потокові платформи обробки даних, як Apache Kafka, а також внутрішні розробки на базі скриптів. Вибір конкретного технологічного рішення та необхідні адаптації залежать від наявної інфраструктури сервісу електронної комерції, обсягів даних тощо. Аналітична складова методу аналізу ефективності системи захисту сервісів електронної комерції не залежить від технології реалізації зовнішньої системи збору та підготовки даних за умови дотримання специфікації вхідних даних.

Стандартизований інтерфейс обміну даними, що використовує JSON документи, є комунікаційною ланкою між рівнем збору даних та аналітичною складовою методу аналізу ефективності системи захисту сервісів електронної комерції. Вхідний JSON документ складається з двох основних секцій: `period` (часовий інтервал аналізу), `stages` (агреговані дані по етапах взаємодії користувача з сервісом електронної комерції). Окремі фрагменти документу JSON наведено нижче.

```
{
  "period": {
    "start": "<timestamp>",
    "end": "<timestamp>"
  },
```

Секція `period` містить часовий інтервал, за який відбувається збір та обробка даних. Дана секція містить два поля: «`start`» – визначає початок періоду вибірки даних для аналізу, «`end`» – визначає кінцеву часову мітку вибірки даних для аналізу. Вибір періоду для аналізу впливає на точність отриманих результатів та має узгоджуватись відносно поставленої задачі, що вимагає проведення аналізу.

Секція `stages` є основною секцією JSON документа та містить агреговані дані для кожного з семи етапів взаємодії користувача з сервісом електронної комерції.

```

"stages": {
  "e1_landing": {
    "N": "<int>",
    "TP": "<int>",
    "FP": "<int>",
    "FN": "<int>",
    "actions": {
      "block": "<int>",
      "challenge": "<int>",
      "flag": "<int>",
      "allow": "<int>"
    }
  },
  "e2_catalog": {...},
  "e3_search": {...},
  "e4_product": {...},
  "e5_cart": {...},
  "e6_checkout": {...},
  "e7_payment": {...}
}

```

Кожен з етапів взаємодії E_j представлений окремим блоком з фіксованим форматом. Поле «N» – містить загальну кількість унікальних сесій користувачів на даному етапі взаємодії, поле «TP» – кількість подій класифікованих як True Positive, «FP» – кількість подій класифікованих як False Positive, поле «FN» – кількість подій класифікованих як False Negative. Відсутність поля TN зумовлена тим, що значення даного параметру не передається явно, а розраховується під час аналізу та визначається як кількість сесій, де система захисту приймала вірні рішення не втручатись у дії користувача (2.49).

Підсекція actions містить дані про розподіл спрацювань систем захисту за типами дій, відображає кількість дій певного типу на даному етапі взаємодії E_j . Сума цих значень є загальною кількістю спрацювань системи на даному етапі взаємодії E_j і відповідає параметру N_{all} .

Якщо на етапі взаємодії E_j не було жодного спрацювання системи захисту, всі поля actions приймають значення 0. Поля TP, FP, FN також приймають значення 0.

Додатково до вхідних даних, що поступають зовні, аналітична складова методу використовує набір параметрів, що були визначені заздалегідь. До них відносяться: K_i – коефіцієнти критичності етапів взаємодії користувачів з сервісом електронної комерції (таблиця 2.44), W_{Π} – вагові коефіцієнти

показників оцінки ефективності Π_i (таблиця 2.51), w_a – коефіцієнт впливу безпекових подій (таблиця 2.46). Контекстні параметри ЧФ (f_T) та БФ (t_B) задаються при виконанні аналізу даних за обраний період. Конфігурація зберігається у JSON форматі, що забезпечує читабельність та простоту редагування.

```
{
  "stage_weights": {
    "k": [0.055, 0.050, 0.057, 0.069, 0.115, 0.257, 0.397],
    "labels": ["e1_landing", "e2_catalog", "e3_search",
              "e4_product", "e5_cart", "e6_checkout",
              "e7_payment"]
  },
  "pokaznyk_weights": {
    "w": [0.476, 0.176, 0.080, 0.268],
    "labels": ["P1_detection", "P2_interaction",
              "P3_response", "P4_coverage"]
  },
  "security_action_cost": {
    "block": 4,
    "challenge": 3,
    "flag": 2,
    "allow": 1
  },
  "context": {
    "f_T": 0.3,
    "f_B": 1.0,
    "context_label": "normal"
  }
}
```

Конфігурація має періодично переглядатись та оновлюватись відповідно до змін у параметрах функціонування сервісу електронної комерції, структури етапів взаємодії користувачів із сервісом електронної комерції, розуміння пріоритетів та потенційних загроз.

Аналітична складова методу аналізу ефективності системи захисту сервісів електронної комерції реалізує послідовну обробку вхідних даних, обчислення показників ефективності роботи системи захисту сервісів електронної комерції (IE_3 , IE_{3K}) та формування рекомендацій, базуючись на отриманих значеннях. Процес починається з отримання та перевірки даних від зовнішньої системи збору і підготовки даних. Окрім цього, завантажуються та перевіряються конфігураційні параметри системи (рис. 3.1).

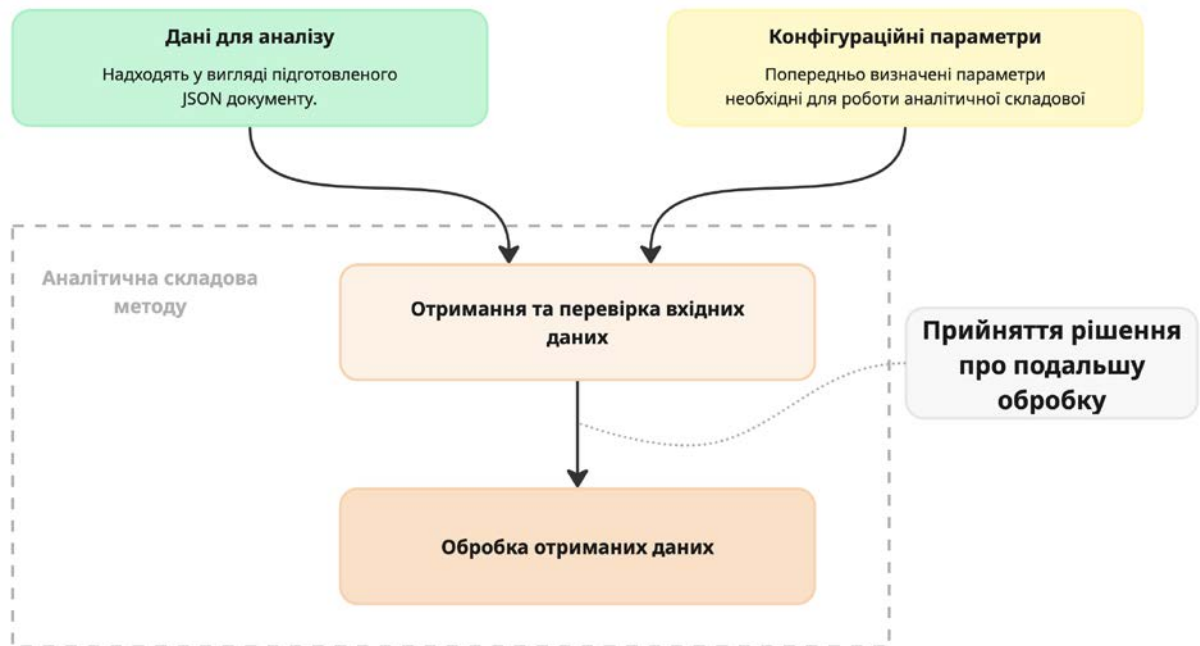


Рис. 3.1. Вхідні дані аналітичної складової методу.

Алгоритм отримання та перевірки вхідних даних забезпечує раннє виявлення помилок у вхідних даних, що дозволяє уникнути проблем з подальшими розрахунками, а також забезпечити інформування користувача про наявні проблеми. У разі виявлення критичних помилок у вхідних документах, обробка переривається з формуванням відповідного повідомлення і запису до системи журналювання.

На першому етапі виконується отримання та обробка вхідного JSON документу з даними для аналізу. Перевіряється відсутність синтаксичних помилок та відповідність формату JSON. Наступним кроком виконується перевірка структури отриманого JSON документу на наявність обов'язкових секцій «period», «stages» та полів, що вони містять. Відсутність будь-якого з обов'язкових елементів є критичною помилкою. Після завершення перевірки записів для всіх етапів взаємодії, описаних в секції «stages», виконується перевірка наявності помилок хоча б в одному з описів етапів взаємодії, і якщо такі присутні, то алгоритм ініціює запис повідомлення про виявлені проблеми та завершує роботу. Блок-схема алгоритму представлена на рис. 3.2.

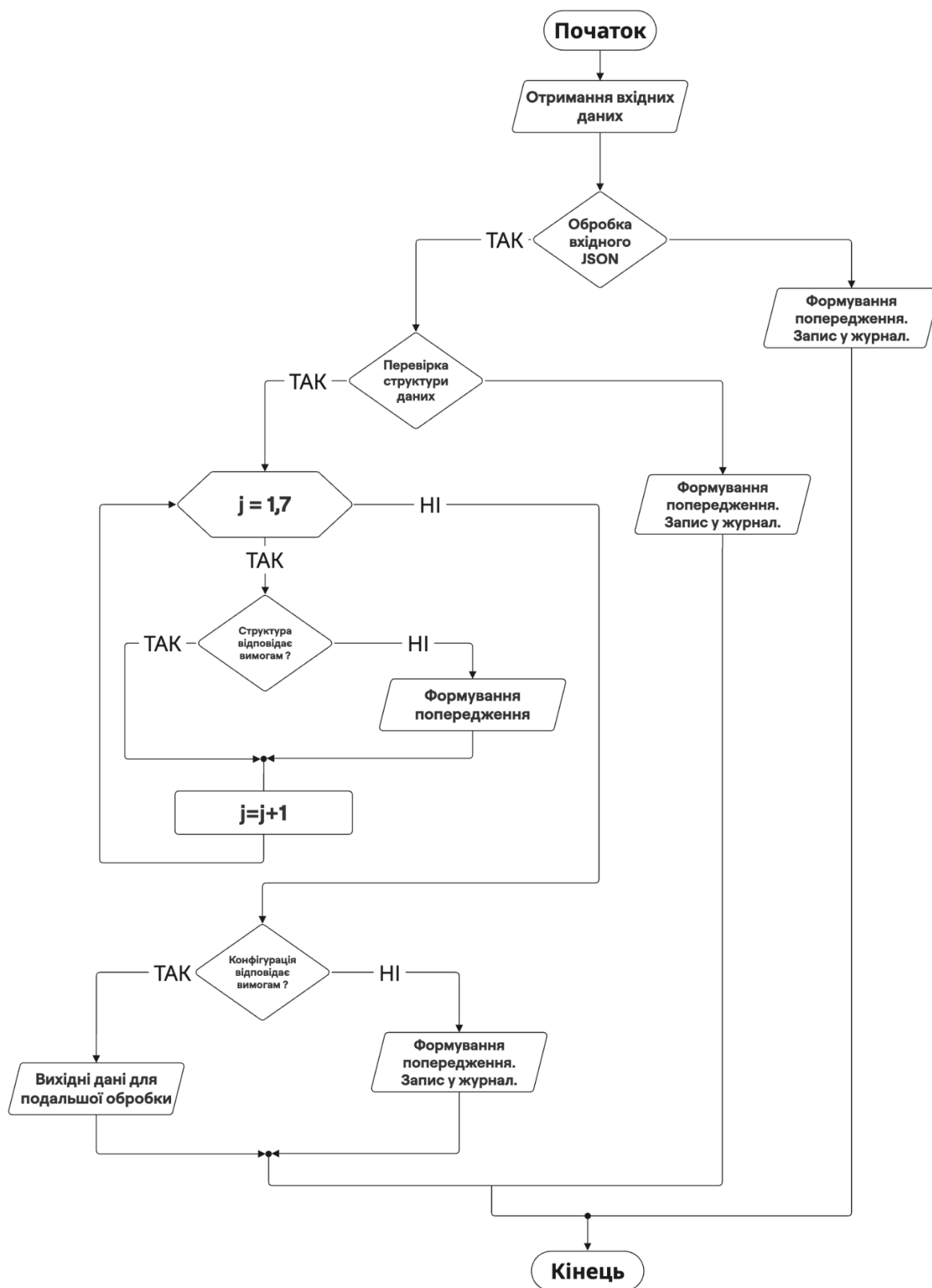


Рис. 3.2. Алгоритм отримання та перевірки вхідних даних

Якщо помилок структури опису етапів взаємодії у секції «stages» не виявлено, то виконується перевірка отриманої конфігурації, що містить попередньо розраховані коефіцієнти критичності K_i , вагові коефіцієнти w_i параметрів оцінки Π_i , коефіцієнти впливу дій систем захисту w_a . У разі виявлення помилок алгоритм робить відповідний запис та завершує роботу. Якщо всі перевірки пройшли успішно, то формується підсумкова структура даних, що передається до наступних етапів обробки даних.

Наступним кроком обробки отриманих даних є визначення показників ефективності захисту, що необхідні для розрахунку індексу ефективності захисту. Запропонований метод аналізу ефективності системи захисту сервісів електронної комерції передбачає використання чотирьох показників ефективності захисту. Розглянемо алгоритми для визначення кожного з них.

Показник Π_1 – показник виявлення загроз системами захисту. Розрахунок показника визначено формулою 2.46. Вхідними даними алгоритму є перевірена структура даних отримана після обробки алгоритмом отримання та перевірки вхідних даних. Результатом роботи алгоритму є отримання значення показника Π_1 у діапазоні від 0 до 1.

Розрахунок показника Π_1 потребує визначення загальної кількості правильно виявлених загроз на всіх етапах взаємодії та загальну кількість загроз, що не були виявлені. Для цього першому кроці роботи алгоритму визначаються змінні (TP_{all} , FN_{all}), що будуть використані у якості лічильників означених подій для всіх етапів взаємодії користувача з сервісом електронної комерції та присвоюємо їм нульові значення. Після цього проводиться підрахунок всіх подій даного типу для всіх етапів E_j , значення визначених змінних збільшуються на відповідну величину для поточного етапу. По завершенні збору даних про події для кожного з етапів, виконується перевірка отриманих значень, чи сума TP_{all} та FN_{all} дорівнює 0. Якщо умова істинна, це означає, що за період аналізу не було зареєстровано жодних спрацювань систем захисту, Π_1 набуває значення 1 і алгоритм завершує свою роботу, окремо генерується повідомлення користувачу звернути увагу та перевірити чи це не свідчить про проблеми виявлення загалом.

У випадку, якщо сума TP_{all} та FN_{all} більше нуля, то відбувається розрахунок показника Π_1 за формулою 2.46. Після розрахунку алгоритм повертає значення показника Π_1 і завершує роботу. Блок-схема алгоритму представлена на рис. 3.3.

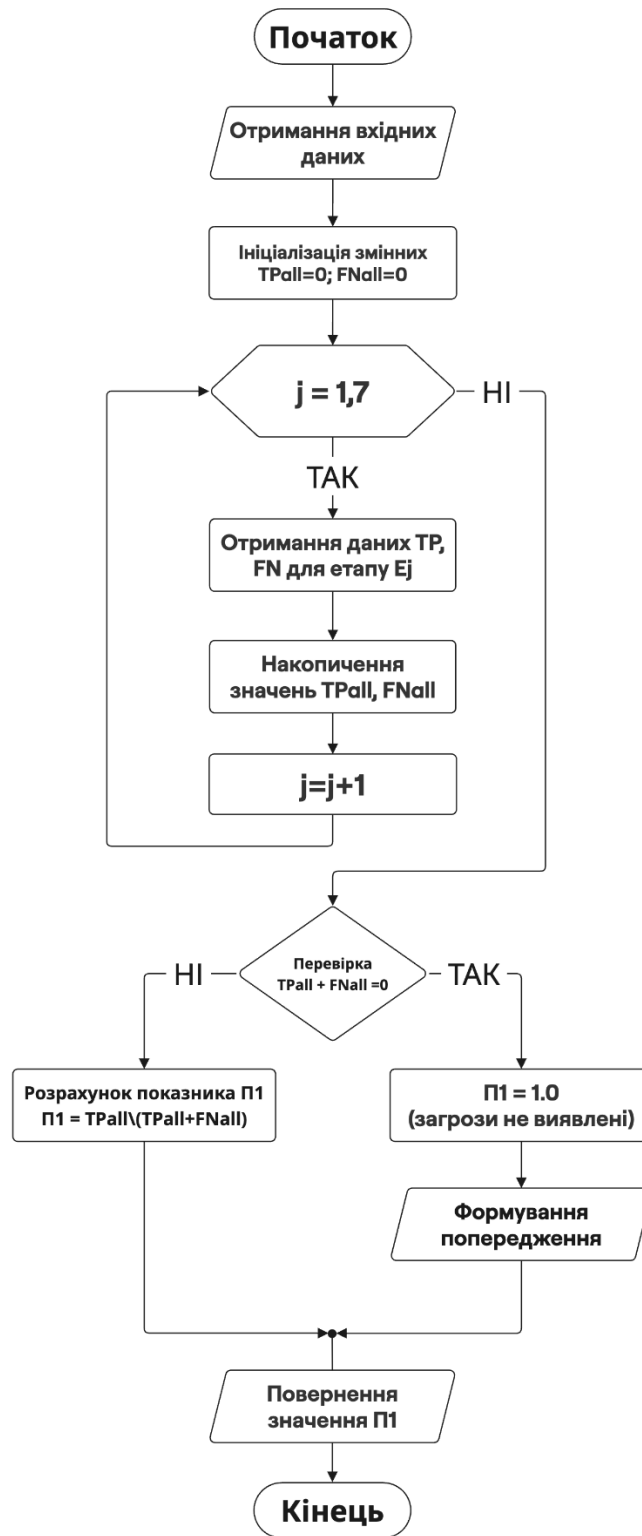


Рис. 3.3. Розрахунок показника Π_1 .

Показник P_2 характеризує вплив систем захисту на взаємодію користувачів з сервісом електронної комерції. Він враховує частоту помилкових спрацювань систем захисту (FPR) (2.48) на кожному з етапів взаємодії користувача з сервісом електронної комерції з урахуванням коефіцієнту критичності етапу. На вході алгоритм отримує перевірені дані від зовнішніх систем та перелік значень коефіцієнтів критичності K_j для кожного з етапів взаємодії користувача з сервісом електронної комерції. Значення K_j є частиною конфігураційних параметрів системи і визначаються заздалегідь (таблиця 2.44). Показник P_2 розраховується за формулою 2.47. Результатом роботи алгоритму є отримання значення показника P_2 у діапазоні від 0 до 1, де 1 означає відсутність негативного впливу систем захисту на взаємодію користувачів з сервісом електронної комерції.

Робота алгоритму починається з визначення змінної P_2 та присвоєння їй нульового значення. Після цього проводиться циклічна обробка даних по кожному етапу E_j . Спочатку отримуються дані поточного етапу, а саме значення для параметрів N_j , TP_j , FP_j , FN_j . Отримані значення дозволяють розрахувати TN_j , використовуючи формулу 2.49. Виконується перевірка, якщо $TN < 0$, то вхідні дані містять помилку, значення TN встановлюється рівним 0 та генерується попередження користувачу.

Використовуючи отримані дані, наступним кроком алгоритму є розрахунок значення FPR_j . Спочатку виконується перевірка чи сума FP та TN дорівнює 0. Якщо це твердження істинне, то FPR_j набуває значення 0. У іншому випадку значення FPR_j розраховується за формулою 2.48. Отримавши значення FPR , використовуючи коефіцієнт критичності для поточного етапу K_j розраховується значення P_2 для поточного етапу за формулою 2.47. Результат розрахунку додається до загального результату розрахунку P_2 , що міститься у змінній P_2 . По завершенню циклу обробки всіх етапів взаємодії користувачів з сервісом електронної комерції алгоритм повертає значення P_2 , що є значенням змінної P_2 . Блок-схема алгоритму представлена на рис. 3.4.

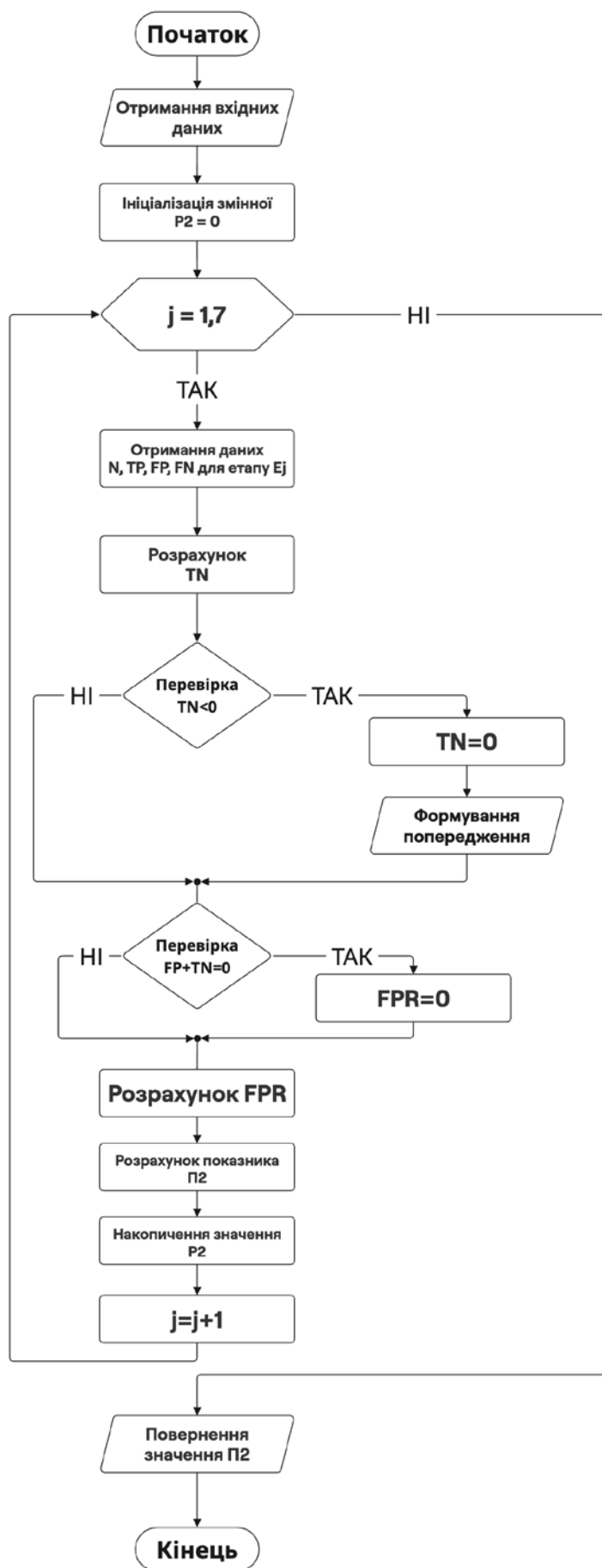


Рис. 3.4. Алгоритм розрахунку показника P_2 .

Показник P_3 характеризує якість роботи системи захисту сервісу електронної комерції. Для розрахунку показника P_3 застосовується формула 2.50. Розрахунок відбувається на базі значень коефіцієнту критичності етапу взаємодії K_j (таблиця 2.44), показника M_j , що демонструє якість дій систем захисту на етапі E_j (2.51). M_j , у свою чергу, враховує тип дії застосованої системою захисту (таблиця 2.46).

Вхідними даними алгоритму розрахунку показника P_3 є структуровані дані від зовнішньої системи збору даних, що пройшли перевірку алгоритмом отримання та перевірки вхідних даних, значення коефіцієнтів K_j (таблиця 2.44), значення коефіцієнтів впливу дій системи захисту (таблиця 2.46). Результатом роботи алгоритму є отримання значення показника P_3 , що лежить у діапазоні від 0 до 1. Блок-схема алгоритму представлена на рис. 3.5.

На першому етапі роботи алгоритму проводиться оголошення змінної P_3 та присвоєння їй нульового значення. Змінна P_3 міститиме кінцевий результат розрахунку значення показника P_3 . Окремо визначаються граничні значення коефіцієнту впливу дій системи захисту $w_{\min}=1$ та $w_{\max}=4$. Після цього проводиться циклічна обробка даних по кожному з етапів взаємодії E_j . Спочатку отримуються дані по кількості дій системи захисту кожного типу на поточному етапі N_{block} , $N_{\text{challenge}}$, N_{flag} , N_{allow} . Використовуючи отримані значення, проводиться розрахунок загальної кількості дій системи захисту на даному етапі взаємодії N_{total} , що є сумою N_{block} , $N_{\text{challenge}}$, N_{flag} та N_{allow} . Після цього виконується перевірка, чи $N_{\text{total}} = 0$, і якщо це твердження істинне, то це означає відсутність будь-яких дій з боку системи захисту на даному етапі E_j і показник M_j встановлюється рівним 1 і алгоритм переходить до розрахунку показника P_3 . У випадку, якщо значення $N_{\text{total}} > 0$, виконується розрахунок середньозваженого коефіцієнту впливу дій систем захисту w_{avg} на етапі E_j та показника якості дій системи захисту M_j (2.51).

На наступному кроці отримані значення показника M_j разом зі значеннями коефіцієнта критичності етапу взаємодії використовуються для розрахунку показника P_3 . Отримане значення додається до загального результату значення

показника Π_3 , що належить змінній P_3 . Алгоритм переходить до розрахунків значень наступного етапу E_j . Після завершення обробки даних для всіх етапів E_j алгоритм повертає отримане значення показника Π_3 , що міститься у змінній P_3 .

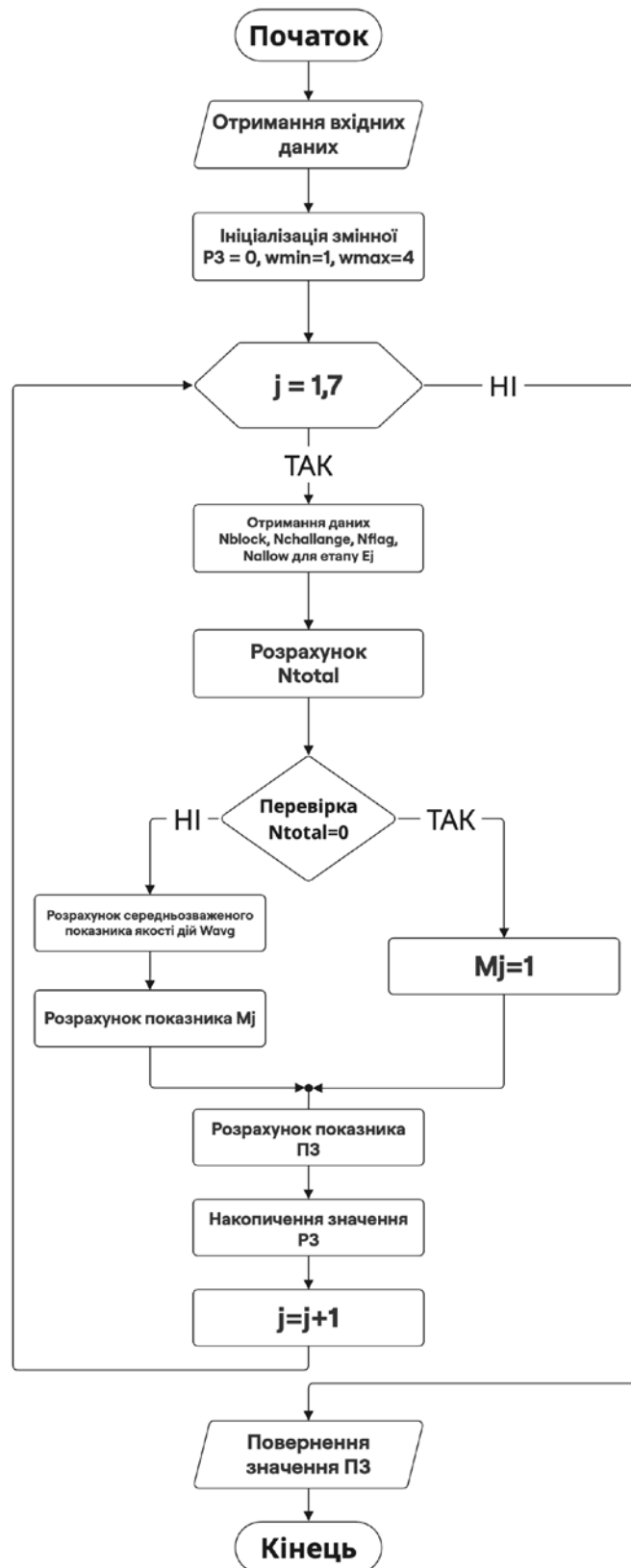


Рис. 3.5. Алгоритм розрахунку показника Π_3 .

Останнім показником, що потребує розрахунку для визначення ІЕЗ є показник захищеності етапів взаємодії користувача з сервісом електронної комерції P_4 . Він демонструє, які етапи взаємодії охоплені покриттям системи захисту сервісу електронної комерції. Слід зазначити, що розрахунок показника P_4 базується на наявності активних дій з боку системи захисту, у випадку їх відсутності, що може вказувати як на відсутність загроз за період аналізу, так і про відсутність покриття системою захисту, він слугує додатковим індикатором необхідності перевірки коректності налаштувань та роботи системи захисту загалом. Для точнішої оцінки необхідно проводити додатковий аналіз даних системи захисту, а також провести порівняння значень показника P_4 за декілька часових проміжків.

На вхід алгоритму розрахунку показника P_4 поступають структуровані дані від зовнішніх систем збору даних, що пройшли перевірку алгоритмом отримання та перевірки вхідних даних та значення коефіцієнтів K_j (таблиця 2.44). Для розрахунку показника P_4 використовується формула 2.52. Окремо визначається бінарний показник G_j , що приймає значення 0, якщо на етапі E_j не зафіксовано жодної активної дії системи захисту, та значення 1 у випадку, якщо такі дії мали місце. Результатом роботи алгоритму є отримання значення показника P_4 , що лежить у діапазоні від 0 до 1.

Першим кроком алгоритму є оголошення змінної P_4 та присвоєння їй нульового значення. Дана змінна використовується для накопичення значення P_4 при розрахунку для кожного з етапів взаємодії E_j . Після цього виконується циклічна обробка даних для кожного етапу взаємодії E_j . Спочатку отримуються дані по кількості дій системи захисту кожного типу на поточному етапі N_{block} , $N_{challenge}$, N_{flag} та N_{allow} . Отримані значення використовуються для розрахунку загальної кількості дій системи захисту на даному етапі взаємодії N_{total} , що є сумою N_{block} , $N_{challenge}$, N_{flag} та N_{allow} . Після цього виконується перевірка чи $N_{total} = 0$, якщо це твердження істинне, показник G_j набуває значення 0, і формується попередження користувачу. Якщо $N_{total} > 0$, то G_j отримує значення 1. Отримавши значення показника G_j проводиться обчислення значення P_4 для поточного

етапу. Значення додається до змінної P4. Алгоритм переходить до опрацювання даних наступного етапу. Після завершення обробки даних для всіх наявних етапів взаємодії, алгоритм повертає значення показника П₄. Блок-схема алгоритму представлена на рис. 3.6.

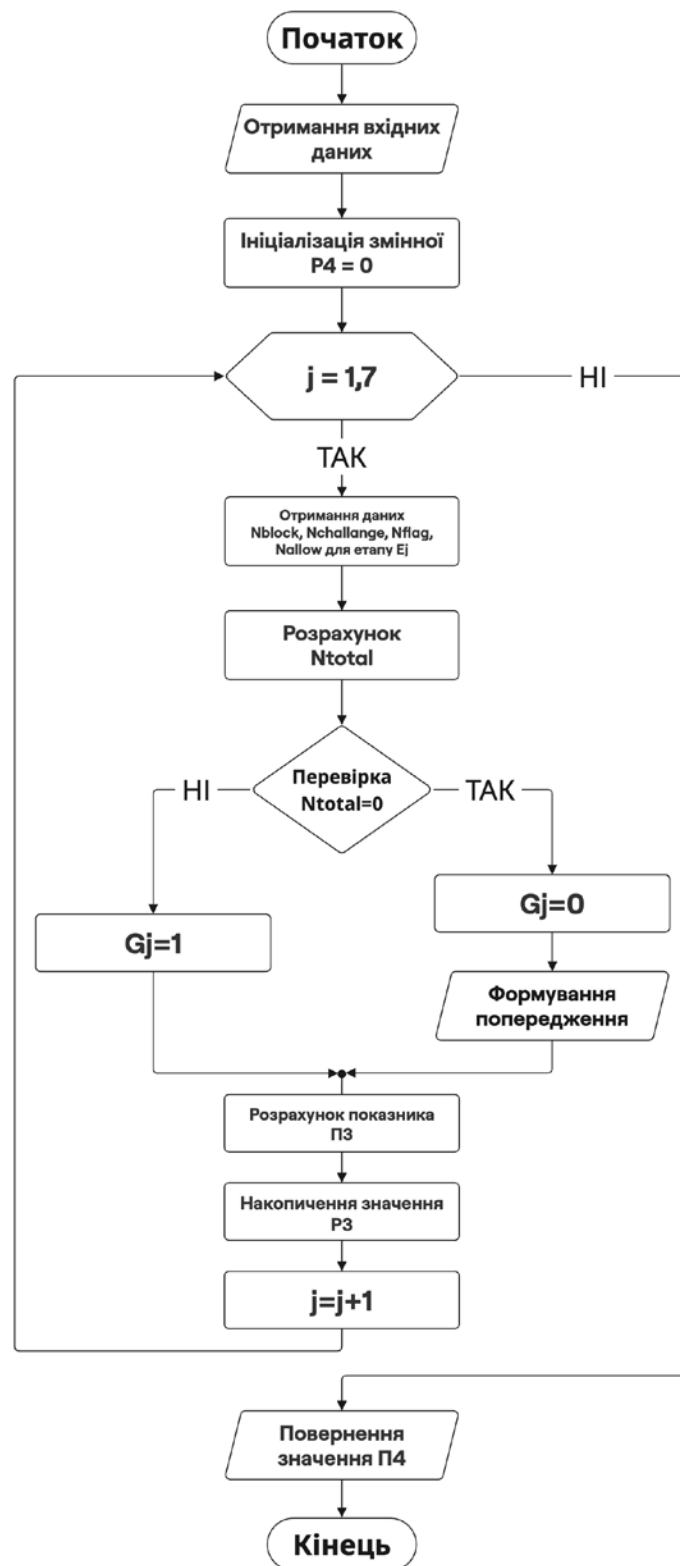


Рис. 3.6. Алгоритм розрахунку показника П₄.

Після розрахунку чотирьох показників ефективності роботи системи захисту сервісу електронної комерції (P_1, P_2, P_3, P_4), виконується їх інтеграція у загальний показник ефективності роботи системи захисту ІЕЗ. Індекс ефективності захисту є зваженою сумою чотирьох показників ефективності роботи системи захисту, де вагові коефіцієнти W_{Pi} (таблиця 2.51) відображають пріоритетність кожного з визначених аспектів захисту для конкретного сервісу електронної комерції.

Для обчислення індексу ефективності захисту використовується формула 2.45. Алгоритм розрахунку ІЕЗ у якості вхідних даних отримує розраховані значення показників P_1, P_2, P_3, P_4 та перелік відповідних вагових коефіцієнтів $W_{P1}, W_{P2}, W_{P3}, W_{P4}$. Результатом роботи алгоритму є отримання значення ІЕЗ, що лежить у діапазоні від 0 до 1.

Після отримання даних проводиться їх перевірка, всі значення показників мають знаходитись у діапазоні від 0 до 1. У випадку, якщо будь-який з показників виходить за межі визначеного діапазону, генерується повідомлення про помилку та алгоритм завершує свою роботу. Інакше наступним кроком визначається змінна ІЕЗ, якій присвоюється нульове значення. Далі алгоритм виконує циклічну обробку показників, для кожного показника P_i обчислюється добуток вагового коефіцієнта W_{Pi} та значення показника P_i . Отримане значення додається до змінної ІЕЗ. Алгоритм переходить до обробки наступного показника. Після завершення обробки всіх показників алгоритм повертає отримане значення показника ІЕЗ та завершує роботу. Блок-схема алгоритму представлена на рис. 3.7.

Отримане значення ІЕЗ інтерпретується згідно з таблицею 2.52. Важливо зазначити, що при аналізі отриманих результатів слід враховувати не тільки загальний показник ІЕЗ, а також значення окремих показників, це забезпечить більш цілісну картину стану роботи системи захисту сервісу електронної комерції.

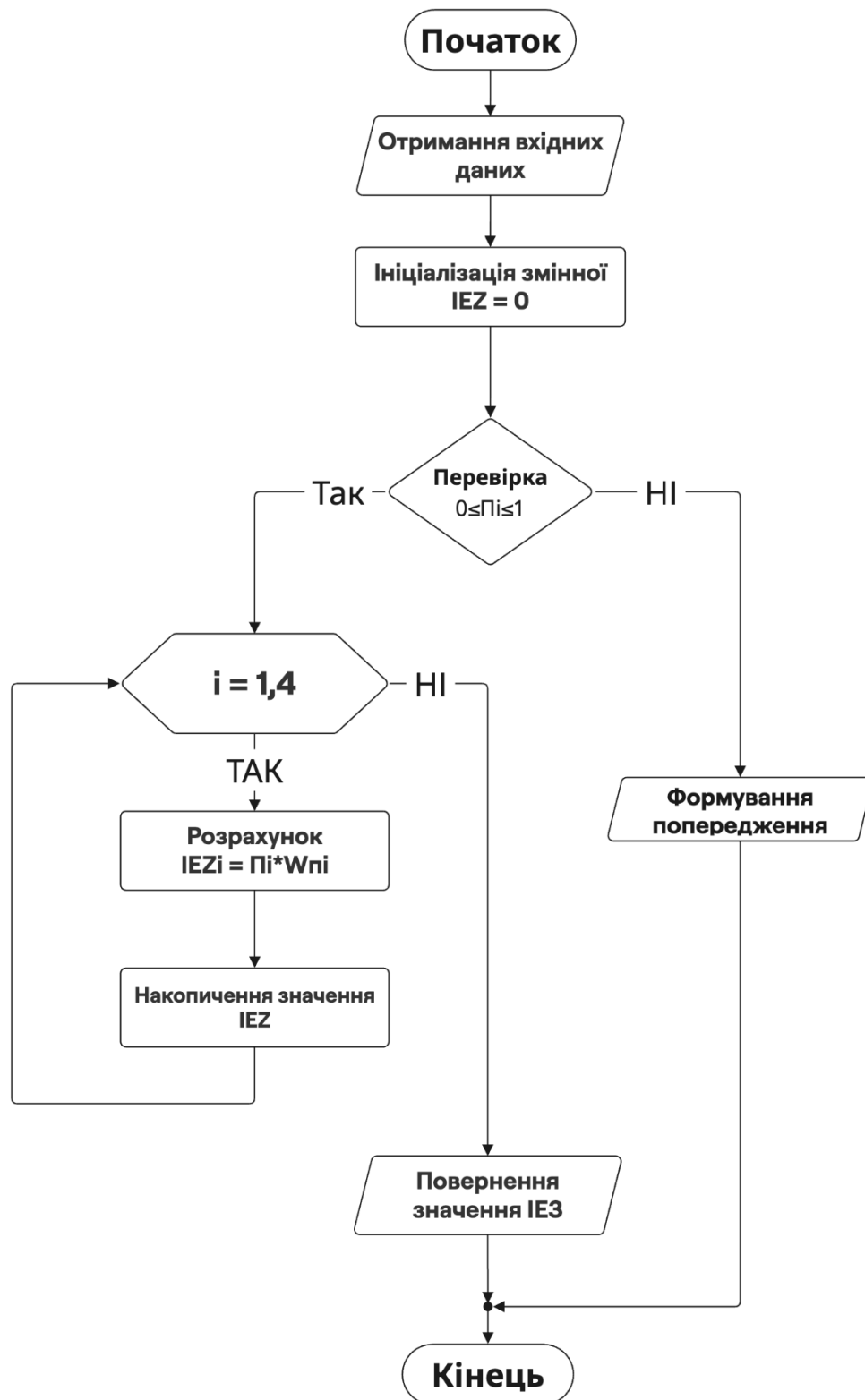


Рис. 3.7. Алгоритм розрахунку індексу ефективності захисту ІЕЗ

Отримання значення ІЕЗ робить можливим розрахувати контекстний індекс ефективності захисту ІЕЗ_к, що враховує часовий фактор та бізнес-фактор.

ІЕЗк забезпечує оцінку ефективності роботи системи захисту адаптовану до умов функціонування сервісу електронної комерції.

ІЕЗк розраховується за формулою 2.60. Допоміжними параметрами для розрахунку ІЕЗк є коефіцієнт контекстної чутливості ККЧ (2.58) та показник дефіциту ефективності захисту Δ (2.59).

Робота алгоритму з розрахунку ІЕЗк починається з отримання вхідних даних, а саме значення ІЕЗ, ЧФ та БФ. Наступним кроком виконується перевірка значення ІЕЗ на відповідність допустимому діапазону від 0 до 1. У випадку якщо значення показника виходить за межі визначеного діапазону, генерується повідомлення про помилку та алгоритм завершує свою роботу. Якщо значення знаходиться у допустимому діапазоні, то наступним кроком виконується розрахунок ККЧ згідно формули 2.58. Далі визначається дефіцит ефективності захисту за формулою 2.59. Отримані значення використовуються для розрахунку ІЕЗк згідно формули 2.60. Алгоритм повертає отримане значення та завершує роботу. Блок-схема алгоритму представлена на рис. 3.8.

Система рекомендацій є останній етапом обробки даних аналітичної складової методу аналізу ефективності роботи системи захисту сервісів електронної комерції. Дана система рекомендацій забезпечує агрегацію даних отриманих на всіх етапах роботи аналітичної складової методу аналізу ефективності роботи системи захисту сервісів електронної комерції, визначає статус показників ефективності роботи системи захисту P_i . У залежності від відхилення значень показників від цільового рівня система рекомендацій визначає проблемні аспекти функціонування системи захисту та пріоритезує їх в залежності від поточного контексту роботи сервісу електронної комерції, а також надає загальні рекомендації щодо подальших дій користувача.

Обробка даних системою рекомендацій відбувається у три етапи: визначення статусу отриманих показників ефективності роботи системи захисту P_i та відхилення від цільового рівня, пріоритезація показників P_i з урахуванням контекстних факторів БФ та ЧФ, формування переліку рекомендацій.

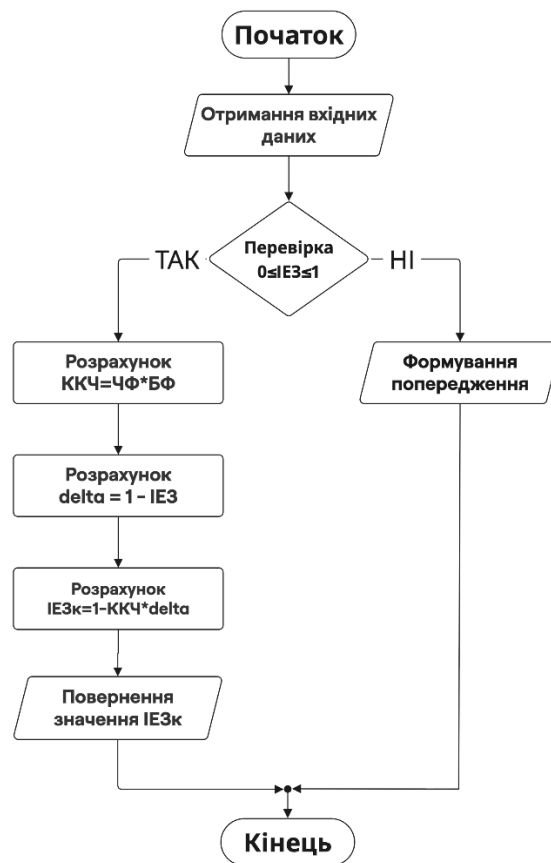


Рис. 3.8. Алгоритм розрахунку контекстного індексу ефективності захисту $IE3_k$.

Вхідними даними алгоритму визначення статусу показників P_i є розраховані значення показників P_i . Результатом роботи алгоритму є визначений статус кожного з показників, значення відхилення від цільового рівня Δ та текст базової рекомендації.

На першому етапі своєї роботи алгоритм циклічно опрацьовує всі показники P_i . Спочатку виконується визначення статусу показника P_i згідно таблиці 2.53. Після визначення статусу проводиться перевірка чи значення показника менше цільового рівня 0.90 (таблиця 2.53). Якщо значення показника $P_i \geq 0.90$ відхилення показника Δ_i встановлюється рівним 0. Якщо значення показника менше цільового рівня, то проводиться розрахунок відхилення значення показника P_i від цільового рівня Δ_i за формулою 2.61. На основі отриманого значення формується текст базової рекомендації відповідно до

шкали інтерпретації значень показників Π_i (таблиця 2.53). Результати обробки поточного показника зберігаються, алгоритм переходить до обробки наступного показника.

Другим кроком роботи алгоритму є формування переліку всіх показників з $\Delta_i > 0$, що потребують подальшої обробки. Алгоритм повертає отримані дані та завершує свою роботу. Блок-схема алгоритму представлена на рис. 3.9.

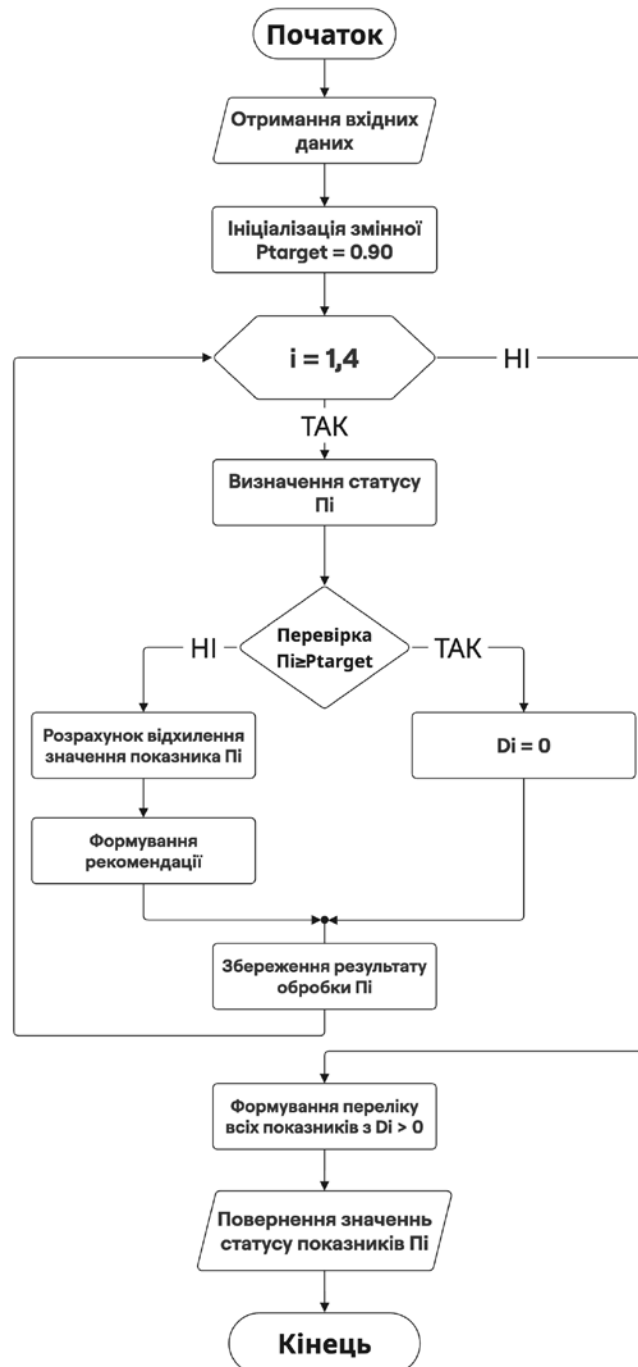


Рис. 3.9. Алгоритм визначення статусу показників Π_i .

Другий етап роботи системи рекомендації виконує пріоритезацію рекомендацій показників Π_i , розраховуючи індекс пріоритету рекомендацій ІПР (2.62), що мають відхилення від цільового рівня. Вхідними даними роботи алгоритму пріоритезації рекомендацій показників Π_i є перелік показників Π_i чиє значення $\Delta_i > 0$, значення відхилення Δ_i , значення ЧФ, значення БФ. Результатом роботи алгоритму є впорядкований за ІПР перелік показників з визначеним рівнем пріоритету (таблиця 2.54). Блок-схема алгоритму представлена на рис. 3.10.

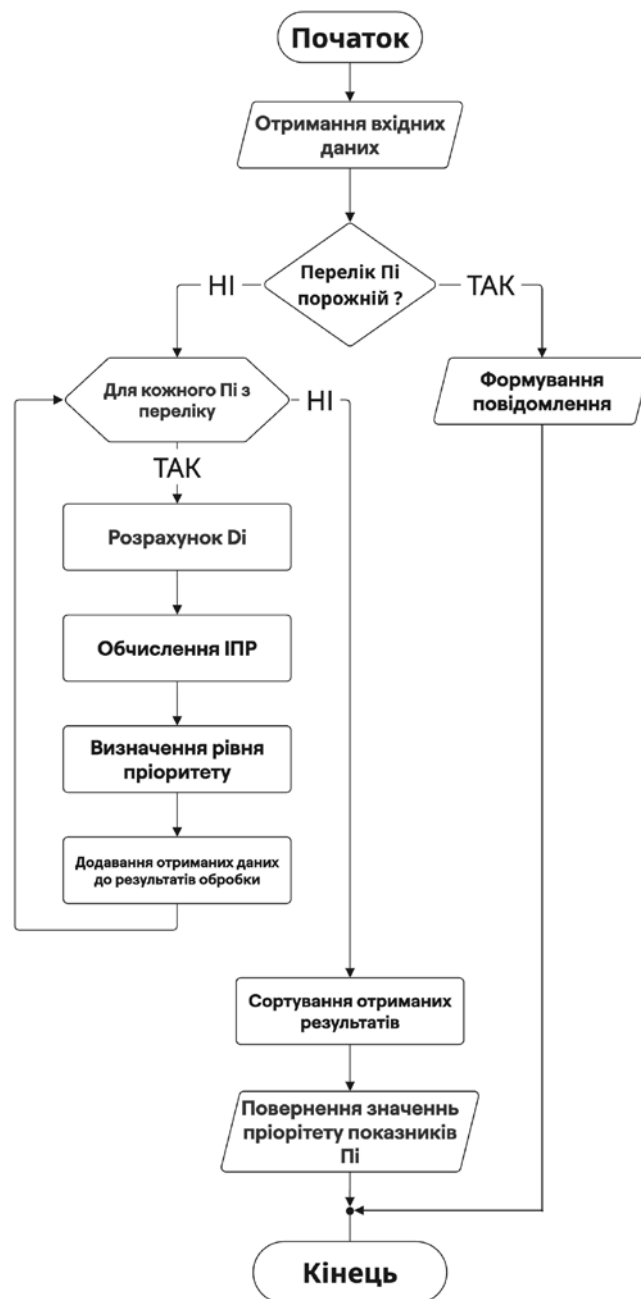


Рис. 3.10. Алгоритм пріоритезації рекомендацій Π_i .

Алгоритм розпочинає свою роботу з перевірки наявності показників для опрацювання, якщо перелік порожній, тобто значення всіх показників $P_i \geq 0.90$, алгоритм формує повідомлення про відсутність даних для обробки та завершує роботу. У випадку, якщо перелік не порожній, то виконується циклічна обробка наявних показників P_i . Для поточного показника P_i отримується значення відхилення Δ_i . Далі виконується обчислення ІПР за формулою 2.62. Після обчислення ІПР алгоритм визначає значення рівня пріоритету згідно таблиці 2.54. Отримані результати додаються до переліку з пріоритетами показників P_i , алгоритм переходить до обробки даних наступного показника.

Коли всі отримані показники P_i пройшли цикл обробки, виконується сортування переліку пріоритетів показників за значенням ІПР. Показники з найвищим пріоритетом розміщуються на початку переліку. Алгоритм повертає впорядкований перелік та завершує роботу.

Фінальним етапом роботи системи рекомендацій є об'єднання результатів роботи попередніх двох етапів у перелік рекомендацій та формування звіту. Для кожного показника P_i формуються рекомендації, що містить три складові: назва та тип показника (таблиця 2.45), статус показника та базова рекомендація (таблиця 2.53), рівень пріоритету рекомендованих дій (таблиця 2.54).

Вхідними даними алгоритму є результати першого і другого етапу роботи системи рекомендацій. Результатом роботи алгоритму є звіт з переліком рекомендацій.

Першим кроком алгоритм перевіряє наявність показників P_i , що потребують рекомендацій. Якщо всі показники P_i досягли цільового рівня та отримали статус «Відмінно» (таблиця 2.53), формується висновок про відсутність виявлених проблем, і алгоритм переходить до формування підсумкової частини звіту. За наявності показників, що потребують рекомендацій, виконується циклічна обробка отриманих значень для показників P_i . Для кожного з показників P_i формується текст рекомендації, що містить назву та тип показника, статус показника, інформація про пріоритет. Сформований текст рекомендації додається до переліку рекомендацій у звіті. Алгоритм

переходить до обробки даних наступного показника P_i . Блок-схема алгоритму представлена на рис. 3.11.

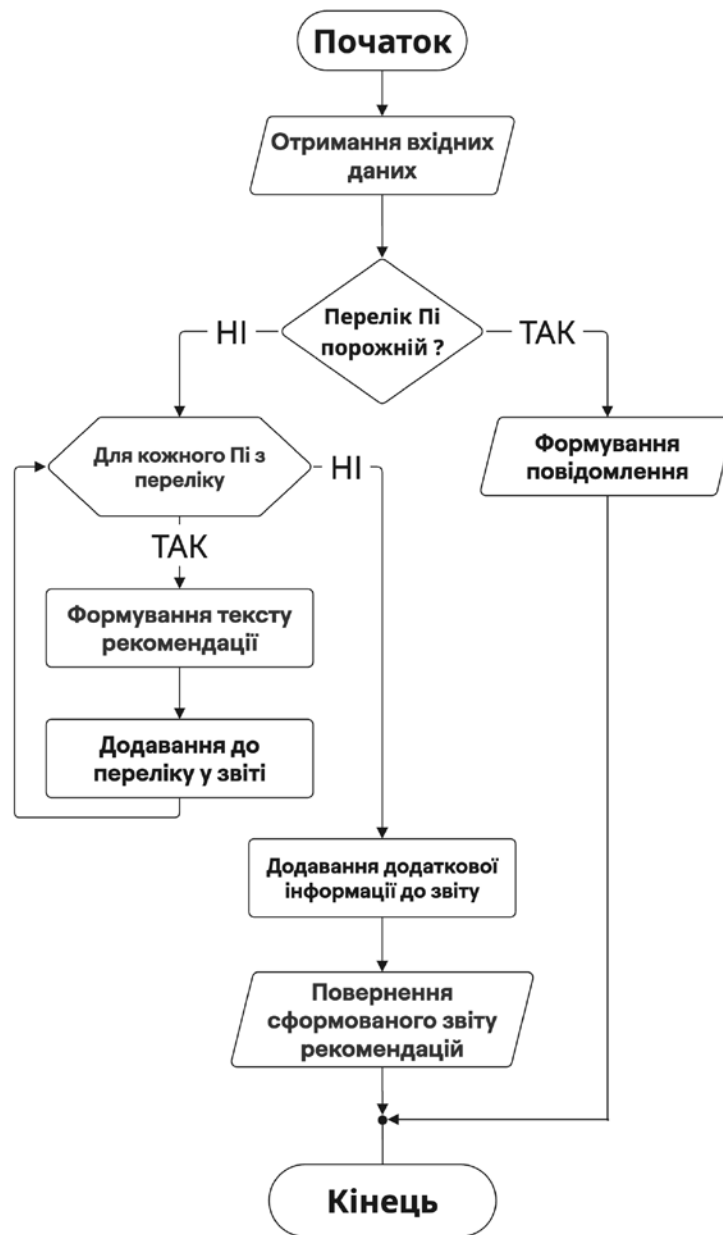


Рис. 3.11. Алгоритм формування звіту рекомендацій P_i .

Після завершення обробки наявних даних показників P_i , алгоритм додає загальний перелік рівнів пріоритетів та загальну кількість показників, що потребують уваги. Алгоритм повертає сформований звіт та завершує роботу. Отриманий звіт може використовуватись для інформування користувачів про виявлені проблеми, документування стану роботи системи захисту сервісу електронної комерції, планування заходів щодо вдосконалення роботи системи захисту сервісів електронної комерції.

Проведемо аналіз часової складності запропонованих алгоритмів. У таблиці 3.1 наведено перелік запропонованих алгоритмів, що реалізують аналітичну складову методу.

Таблиця 3.1

Перелік запропонованих алгоритмів

Умовне позначення	Назва
A_1	Алгоритм отримання та перевірки вхідних даних
A_2	Алгоритм розрахунку показника P_1
A_3	Алгоритм розрахунку показника P_2
A_4	Алгоритм розрахунку показника P_3
A_5	Алгоритм розрахунку показника P_4
A_6	Алгоритм розрахунку індексу ефективності захисту ІЕЗ
A_7	Алгоритм розрахунку контекстного індексу ефективності захисту ІЕЗ _к
A_8	Алгоритм визначення статусу показників P_i
A_9	Алгоритм пріоритезацій рекомендацій P_i
A_{10}	Алгоритм формування звіту рекомендацій P_i

Алгоритм A_1 проводить перевірку отриманих даних з фіксованою та заздалегідь визначеною кількістю вхідних параметрів. Кількість кроків, необхідних для проведення перевірки не залежить від кількості вхідних даних. Таким чином часова складність даного алгоритму визначається як $O(1)$.

Алгоритми $A_2 - A_5$ виконують розрахунок показників $P_1 - P_4$. Для розрахунку використовується сталий набір даних – попередньо розраховані коефіцієнти та вхідні дані отримані з JSON файлу. Кількість етапів обробки вхідних даних є фіксовано. Виходячи з цього, часова складність даних алгоритмів визначається як $O(1)$.

Алгоритми A_6 та A_7 реалізують обчислення ІЕЗ та ІЕЗ_к. Для отримання обох індексів використовується сталий набір даних, розрахованих на попередніх етапах роботи аналітичної складової методу. Відповідно часова складність обох алгоритмів A_6 та A_7 визначається як $O(1)$.

Фінальним етапом роботи аналітичної складової методу аналізу ефективності системи захисту сервісів електронної комерції є формування

рекомендацій. Алгоритми $A_8 - A_{10}$ відповідають за реалізацію системи рекомендацій. Зазначені алгоритми опрацьовують структуровані дані, отримані в результаті обробки на попередніх етапах роботи аналітичної складової методу. Кількість вхідних даних є сталою. Для формування рекомендацій використовуються заздалегідь обраховані коефіцієнти. Таким чином, часова складність алгоритмів $A_8 - A_{10}$ визначається як $O(1)$.

Аналітична складова методу аналізу ефективності системи захисту сервісів електронної комерції виконує послідовну обробку вхідних даних використовуючи зазначені алгоритми. Вхідний JSON документ містить визначений набір параметрів кількість яких не змінюється. Всі десять алгоритмів виконуються послідовно, кожен обробляє сталу кількість вхідних даних. Оскільки обсяг даних, що надходять для обробки, не залежить від жодного змінного параметра, часова складність кожного з алгоритмів становить $O(1)$. Відповідно загальна часова складність аналітичної складової методу розраховується як сума часових складностей всіх алгоритмів (3.1):

$$O(1) + O(1) + O(1) + O(1) + O(1) + O(1) + O(1) + O(1) + O(1) + O(1) = O(1) \quad (3.1)$$

Таким чином, загальна часова складність аналітичної складової методу становить $O(1)$.

3.2. Програмна реалізація методу аналізу ефективності системи захисту сервісів електронної комерції та системи моделювання

Аналітична складова методу аналізу ефективності системи захисту сервісів електронної комерції, що розробляється у межах даної роботи реалізована з використанням мови Python. Було застосовано модульний підхід при реалізації даного програмного забезпечення, де кожен модуль реалізує окрему функціональну задачу та може бути модифікований незалежно від інших компонентів системи.

Вибір мови програмування Python обумовлений наступними факторами: стандартні бібліотеки Python містять все необхідне для реалізації

обчислювальної логіки методу, наявність підтримки формату JSON через стандартний модуль `json` спрощує роботу з вхідними даними та конфігураційними файлами. Наявність можливості інтегрувати легкий вебфреймворк для реалізації графічного інтерфейсу без додаткових залежностей. Широке застосування мови Python полегшує інтеграцію аналітичної складової в інфраструктуру сервісу електронної комерції.

Для реалізації графічного інтерфейсу було обрано фреймворк Flask. Він забезпечує швидке розгортання, простоту розробки та відсутність зовнішніх залежностей. Flask має достатній функціонал для відображення результатів аналізу, роботи з HTML-шаблонами, створенню навігації між сторінками.

Для побудови графіків та діаграм була використана бібліотека Plotly, що забезпечує створення інтерактивних візуалізацій з можливістю масштабування та перегляду деталей. Plotly дозволяє вбудовувати графіки безпосередньо у HTML сторінки без необхідності використання додаткових бібліотек. Для побудови графіка достатньо передати Flask списки значень та параметри відображення, що спрощує інтеграцію візуалізацій роботи аналітичної складової у графічний інтерфейс.

Кожен функціональний компонент програми реалізовано як окремий модуль, що імпортується та виконується з головного файлу програми `main.py`. Модулі обмінюються даними використовуючи словники Python, що є стандартним способом передачі структурованих даних між функціями. Такий підхід забезпечує можливість незалежної розробки та тестування кожного модуля, зміни чи видалення окремих компонентів без впливу на інші модулі, спрощене розширення функціональності.

Кореневий каталог проєкту містить головний файл програми, каталог модулів, конфігураційні файли та допоміжні ресурси (рис. 3.12).

— config/	# Конфігурація ваг та порогів
— settings.json	# Ваги етапів (к), показників (w), безпекових дій
— thresholds.json	# Порогові значення статусів та пріоритетів
— data/	
— input/	# Вхідні дані (JSON-файли з метриками захисту)
— output/	# Останній результат аналізу
— history/	# Архів усіх результатів
— modules/	# Аналітичне ядро
— validation.py	# Валідація вхідних даних та конфігурації
— indicators.py	# Розрахунок показників P_1 – P_4
— index.py	# Розрахунок індексів ІЕЗ та ІЕЗк
— recommendations.py	# Статуси, пріоритезація, рекомендації
— web/	# Веб-інтерфейс
— app.py	# Flask-застосунок (маршрути, побудова графіків)
— static/style.css	# Стили
— templates/	# HTML-шаблони (dashboard, details, history)
— main.py	# Головний файл програми

Рис. 3.12. Структура проєкту програмної реалізації аналітичної складової методу.

Головний файл програми (main.py) є точкою входу та забезпечує координацію роботи всіх модулів. Він виконує ініціалізацію системи, завантаження конфігурації, послідовний виклик модулів обробки даних та запуск вебінтерфейсу. Модулі взаємодіють через визначені інтерфейси передаючи дані у вигляді словників Python.

Каталог modules містить функціональні модулі системи, а саме: validation.py – модуль отримання та перевірки вхідних даних (рис.3.2); indicators.py – модуль розрахунку показників ефективності P_i (рис.3.3, рис.3.4, рис.3.5, рис.3.6); index.py – модуль розрахунку ІЕЗ та ІЕЗк (рис.3.7, рис.3.8); recommendations.py – модуль формування рекомендацій (рис.3.9, рис.3.10, рис.3.11).

Каталог web містить компоненти графічного інтерфейсу: app.py – відповідає за ініціалізацію сервера Flask; templates – містить шаблони HTML сторінок; static – містить статичні ресурси такі як таблиці стилів.

Каталог config містить конфігураційні файли системи: settings.json – відповідає за зберігання статичних параметрів методу (K_i , W_{Pi} , ваги дій системи

захисту) та даних про контекст для поточного запуску (ЧФ, БФ); thresholds.json – містить порогові значення для системи рекомендацій.

Каталог data містить вхідні та вихідні дані: input – зберігає вхідні JSON файли з даними від зовнішніх систем; output – каталог для зберігання результатів аналізу; history – каталог для зберігання історичних даних попередніх запусків системи аналізу у вигляді JSON файлів.

Програма реалізує наступну послідовність обробки даних: головний модуль програми завантажує конфігурацію з config/settings.json, модуль validation.py отримує вхідний файл JSON та повертає перевірену структуру даних, модуль indicators.py отримує перевірені дані, розраховує показники P_i та повертає отримані значення, модуль index.py отримує дані від модуля indicators.py та контекстні параметри з конфігурації, розраховує IEЗ та IEЗк, та передає отримані результати далі. Модуль recommendations.py отримує всі розраховані результати, формує звіт рекомендацій. Головний модуль програми отримує сформовані дані від всіх модулів та зберігає у data/output та data/history після чого виконує запуск підсистеми графічного інтерфейсу (рис. 3.13).

Графічний інтерфейс забезпечує відображення результатів аналізу та побудову графіків. Графічний інтерфейс реалізований у вигляді вебдодатку на базі фреймворку Flask, що запускається на локальному сервері під час запуску програми аналітичної складової.

Вебдодаток складається з серверної частини app.py, що реалізовує маршрутизацію запитів, отримання результатів та передачу результатів до HTML шаблонів за допомогою механізму шаблонізації Jinja2, що є частиною фреймворку Flask. Відображення даних відбувається у вигляді таблиць та графіків, створених з використанням бібліотеки Plotly.

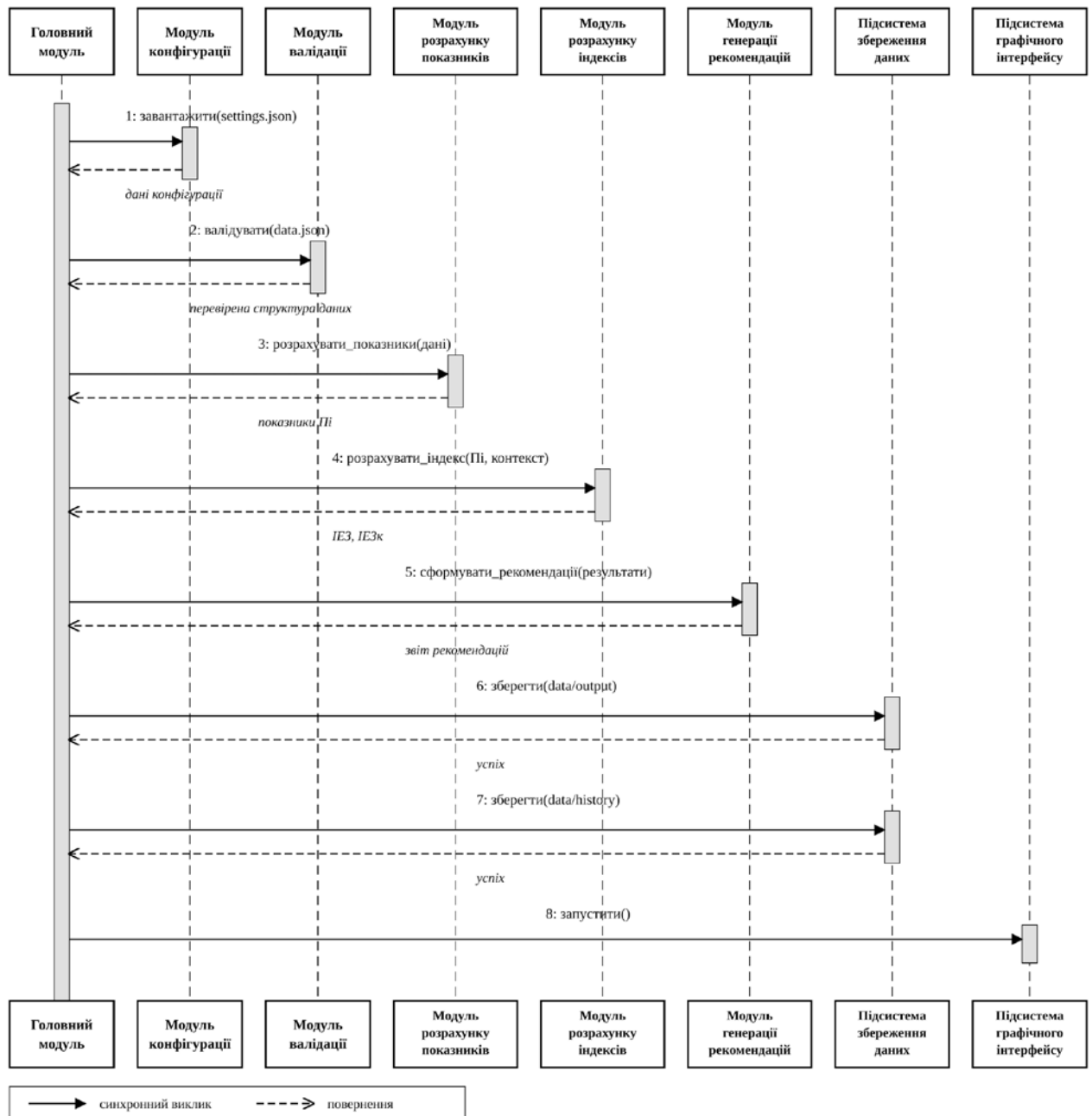


Рис. 3.13. Послідовність обробки даних програмою аналітичної складової методу.

Головна сторінка графічного інтерфейсу відображає зведену інформацію про результати аналізу на одному екрані (див. рис. 3.14). Сторінка містить наступні інформаційні блоки: інформацію про період аналізу, кількість унікальних сесій користувачів, що були використані для формування вхідних даних від зовнішніх систем збору даних, інтерпретацію контексту для періоду аналізу, значення ЧФ та БФ, що були використані в даному аналізі.

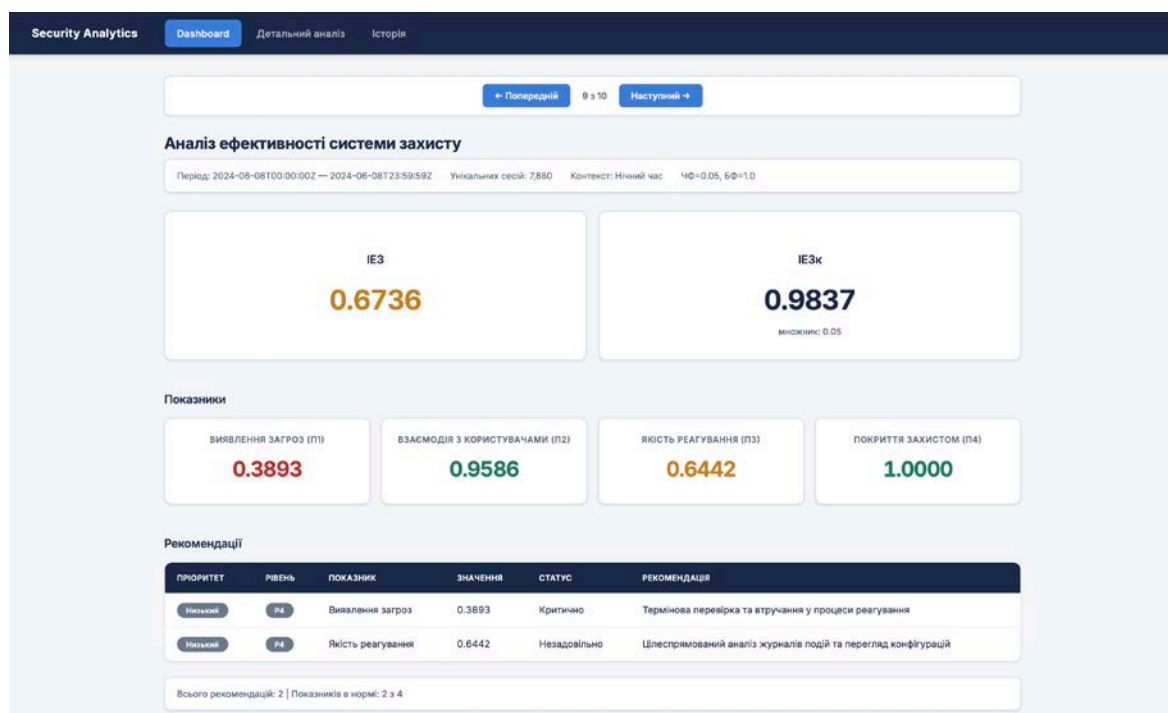


Рис. 3.14. Головна сторінка графічного інтерфейсу.

Блок відображення інформації про отримані значення ІЕЗ та ІЕЗк з кольоровою індикацією загального стану системи: зелений для значень у нормі, жовтий для значень, що потребують уваги, червоний для критичних значень. Далі розташовано блок відображення значень показників P_1 , P_2 , P_3 , P_4 з відповідною кольоровою індикацією їх статусу. Блок рекомендацій відображає перелік сформованих рекомендацій для поточного аналізу впорядкованих за рівнем пріоритету. Для кожної рекомендації зазначено назву показника, статус та текст базових рекомендацій. Якщо всі рекомендації мають статус «Відмінно», то блок відображає повідомлення про відсутність рекомендацій. Під блоком рекомендацій розміщена загальна інформація про кількість рекомендацій.

Сторінка детального аналізу надає розширену інформацію про кожен показник ефективності з використанням графіків, а також інформацію про значення кожного з показників на кожному з етапів взаємодії користувача з сервісом електронної комерції, що дає змогу детально оцінити вплив роботи системи захисту (рис. 3.15). На графіку також зазначені коефіцієнти критичності етапів K_i для покращення візуального аналізу отриманих даних.



Рис. 3.15. Сторінка детального аналізу.

На сторінці історії забезпечено перегляд результатів попередньо проведених аналізів ефективності роботи систем захисту сервісів електронної

комерції (рис. 3.16). При кожному виконанні процедури аналізу вхідних даних результати зберігаються у каталозі data/history у вигляді окремого JSON файлу. Дані зчитуються та відображаються на сторінці історії у вигляді таблиці. Таблиця містить дані про дату виконання аналізу, контекстне пояснення, значенні ІЕЗ та ІЕЗ_к, значення показників Π_i .

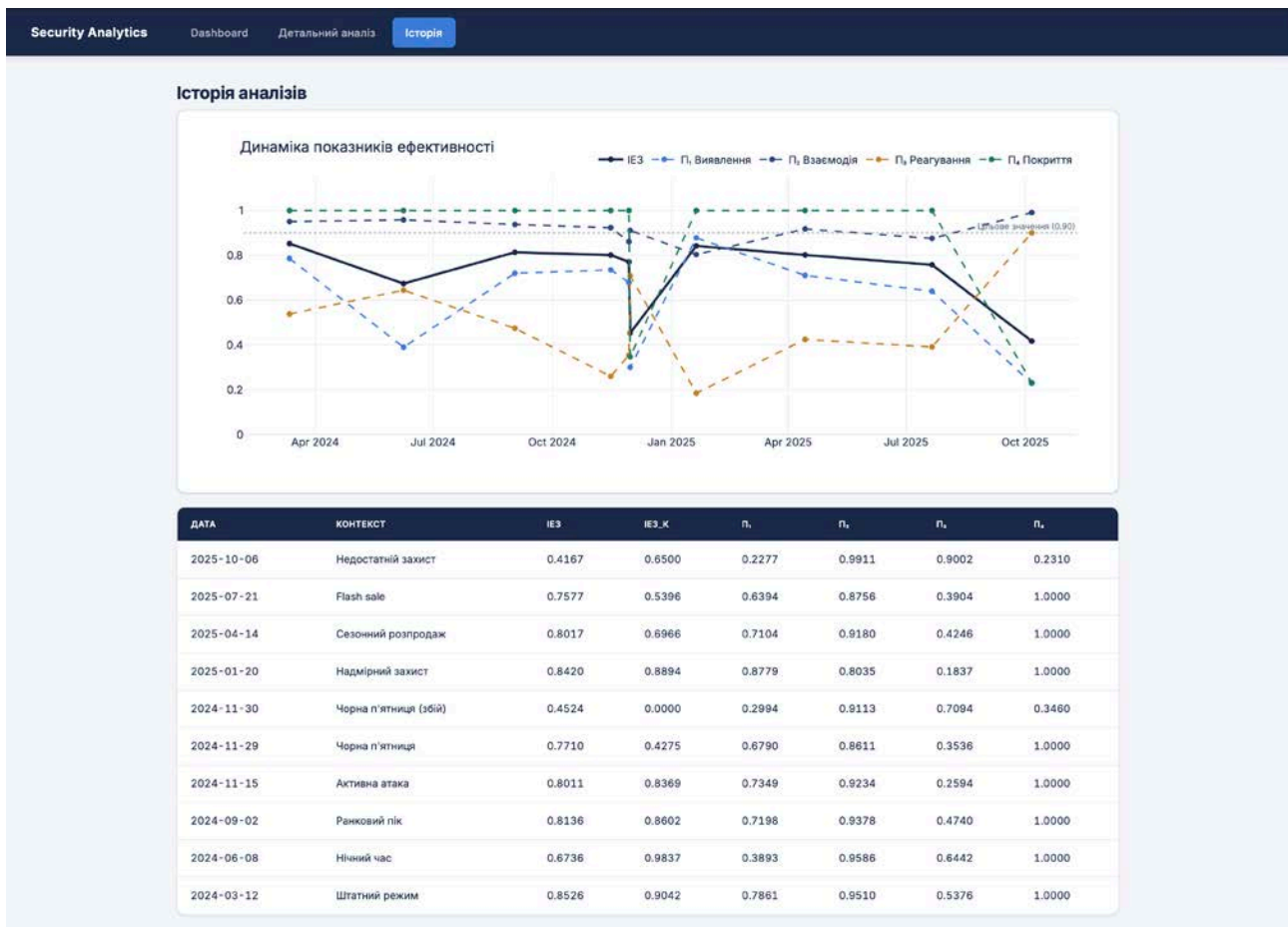


Рис. 3.16. Сторінка історії аналізу.

При наявності достатньої кількості записів (два або більше) на сторінці відображається лінійний графік Plotly, що демонструє динаміку зміни значень ІЕЗ та показників Π_i у часі. Графік дозволяє візуально виявляти тенденції до покращення або погіршення роботи системи захисту сервісу електронної комерції.

Для проведення експериментального дослідження методу аналізу ефективності системи захисту сервісів електронної комерції було розроблено систему моделювання, що створює синтетичні набори даних, які імітують

користувацький трафік та відповідну роботу систем захисту сервісу електронної комерції у різних умовах функціонування.

Серед обмежень щодо використання реальних даних працюючого сервісу електронної комерції можна віднести: дані про спрацювання систем захисту містять конфіденційну інформацію про вразливості, налаштування правил захисту та шаблони атак, так за даними звіту від компанії Verizon за 2025 рік було зафіксовано понад 12000 підтверджених витоків даних, що посилює безпекові вимоги щодо надання доступу до чутливої інформації [15].

Другим обмеженням є те, що доступ до класифікації спрацювань системи захисту (TP, FP, TN, FN) може бути обмеженим на різних вибірках даних та завжди вимагає ретроспективного аналізу кожного інциденту. Третім обмеженням є те, що використання реальних даних унеможливорює контрольований експеримент, так як неможливо повторити одну й ту саму бізнес-подію з різними налаштуваннями систем захисту для порівнянь результатів.

Моделювання процесів обробки користувацького трафіку системами захисту усуває зазначені обмеження та надає додаткові переваги, а саме контрольованість параметрів – можливість змін окремих характеристик, залишаючи інші без змін, що дозволяє виявляти причинно-наслідкові зв'язки між заданими параметрами та результатом аналізу; відтворюваність; масштабованість сценаріїв – можливість генерації даних за довільний період та довільними бізнес-факторами; наявність повної класифікації безпекових подій для всебічної перевірки методу аналізу.

Якість синтетичних даних забезпечується тим, що параметри моделі базуються на галузевих дослідженнях Baymard Institute, Statista, звітах OWASP, Open-Appsec та Verizon DBIR, статистичні характеристики згенерованих наборів перевіряються відносно опублікованих порівняльних тестів [33, 16]. Аналогічний підхід із використанням синтетичних даних на основі галузевих порівняльних тестів застосовується у дослідженнях з кібербезпеки електронної комерції [18].

Система моделювання реалізована також мовою Python з використанням стандартних бібліотек. Архітектура системи складається з трьох функціональних компонентів: модуля сценаріїв, модуля генерації даних та модуля верифікації. Загальну архітектуру системи генерації наведено на рис. 3.17.

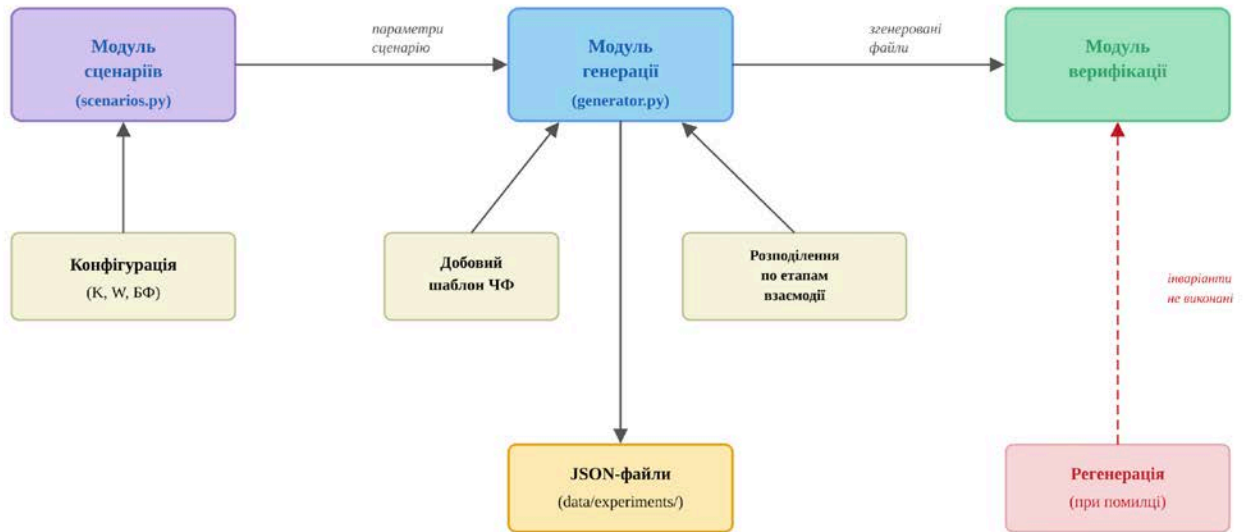


Рис. 3.17. Загальна архітектура системи генерації даних.

Модуль сценаріїв `scenarios.py` містить параметричні описи умов функціонування сервісу електронної комерції. Кожен сценарій визначає: базовий обсяг трафіку, добовий шаблон розподілу навантаження (ЧФ), значення БФ, безпековий профіль (відсоткові ставки TP, FP, FN від загальної кількості сесій на кожному етапі) та розподіл типів дій системи захисту.

Модуль генерації `generator.py` отримує на вхід сценарій, період генерації та параметри деталізації, після чого створює набір JSON-файлів, кожен з яких представляє один атомарний часовий зріз. Алгоритм генерації одного файлу наведено на рис. 3.18.

У якості вхідних даних алгоритм отримує сценарій за яким необхідно згенерувати події. Виходячи з цього сценарію, алгоритм визначає необхідний часовий проміжок та підбирає відповідне значення ЧФ; робить розрахунок кількості сесій на першому етапі взаємодії E_1 з урахуванням добового шаблону

та базового трафіку сценарію; проводить розрахунок кількості сесій на решті етапів взаємодії E_i .

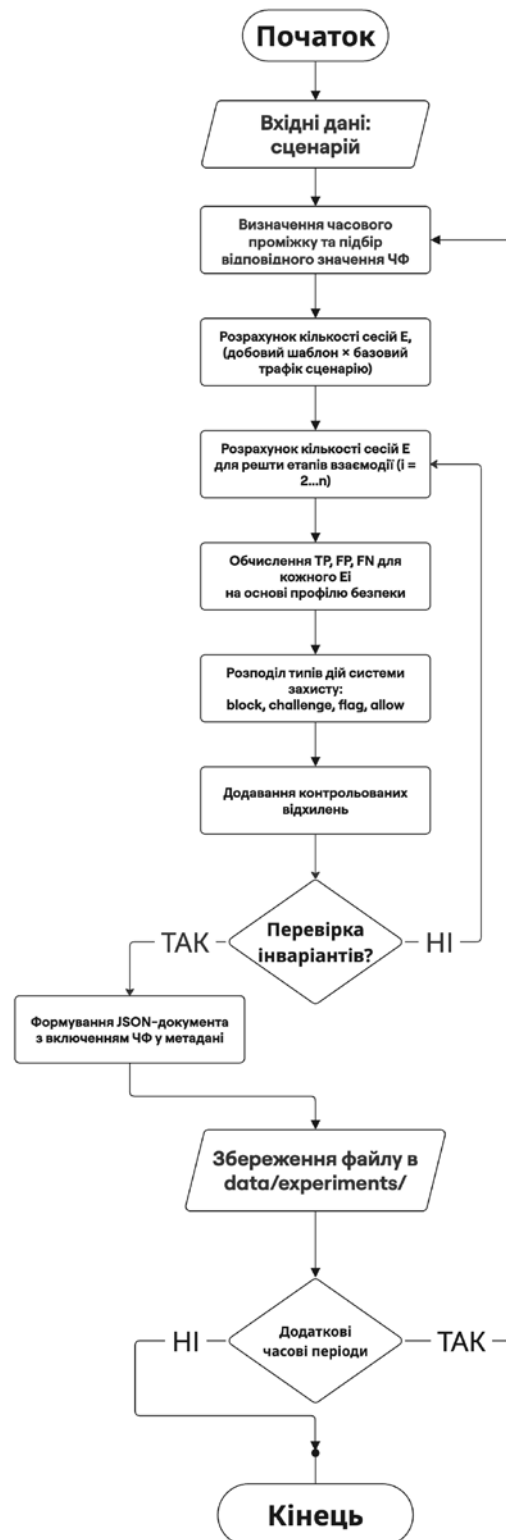


Рис. 3.18. Алгоритм генерації файлів даних.

Далі виконується обчислення TP, FP, FN для кожного етапу взаємодії E_i на основі безпекового профілю; проводить розподіл типів дій (block, challenge, flag,

allow); виконує додавання контрольованих відхилень; виконує перевірку інваріантів; формує JSON документ з включенням значення часового фактору у метадані.

Модуль верифікації перевіряє кожен згенерований файл на дотримання обов'язкових інваріантів (таблиця 3.2). Порушення будь-якого інваріанту призводить до регенерації файлу. Рівень деталізації генерації визначається періодом аналізу (таблиця 3.3).

Таблиця 3.2

Визначені інваріанти для системи моделювання.

Інваріант	Формальний запис	Пояснення
Обмеження класифікації	$TP + FP + FN \leq N$	Класифіковані події не перевищують загальну кількість сесій
Розподілення сесій по етапам взаємодії E_i	$N(E_i) \geq N(E_i + 1)$	Кількість сесій не зростає на наступних етапах
Невід'ємність	$TP, FP, FN, N \geq 0$	Всі числові значення невід'ємні
Мінімальність	$N(E_1) \geq 1$	На першому етапі є хоча б одна сесія

Таблиця 3.3

Рівні деталізації системи моделювання.

Період аналізу	Рівень деталізації файлу	Кількість файлів
1 рік	1 день	365
1 місяць	1 день	28–31
1 день	1 година	24
3 години	15 хвилин	12
1 година	5 хвилин	12

Для системи моделювання були визначені базові параметри, на основі яких генеруються синтетичні дані. До них відносяться: розподілення сесій по етапам

взаємодії користувачів з сервісом електронної комерції, добовий шаблон трафіку та безпекові профілі. Розподіл користувацьких сесій по етапах взаємодії базується на дослідженнях Baymard Institute та Statista щодо середніх показників електронної комерції.

За даними Baymard Institute, середній показник покинутих кошиків становить 70.19%, що означає: лише близько 30% користувачів, які додали товар до кошика, завершують покупку [16, 58]. За даними Statista, середня конверсія сервісів електронної комерції у третьому кварталі 2025 року становила 1.6% [58]. Пропорції етапів взаємодії користувачів системи моделювання наведено у таблиці 3.4.

Таблиця 3.4

Розподілення сесій користувачів по етапам взаємодії.

Етап	Позначення	Частка від E_1
Стартова сторінка	E_1	100%
Каталог	E_2	84%
Пошук	E_3	70%
Перегляд товару	E_4	56%
Кошик	E_5	30%
Оформлення	E_6	16%
Оплата	E_7	10%

Базова кількість сесій використана у системі моделювання для нормального робочого дня складає 50 000 на першому етапі. Конверсія моделі (E_1 - $E_7 = 10\%$) перевищує середньогалузевий показник (1.65-1.8% за даними IRP Commerce та Statista), що є свідомим спрощенням для забезпечення достатньої кількості безпекових подій на етапі оплати [55, 58]. Це спрощення не впливає на коректність оцінки ефективності, оскільки показники Π_i розраховуються як відносні величини.

Часовий фактор визначає частку очікуваного трафіку для кожної години доби відносно пікового рівня. Значення ЧФ = 1.0 відповідає піковій годині (16:00) (таблиця 3.5). Шаблон базується на дослідженнях поведінки онлайн-покупців та враховує типовий розподіл активності: мінімум у нічні години

(03:00-05:00, ЧФ = 0.04-0.05), поступове зростання протягом ранку, максимум у другій половині дня (рис. 3.19) [20].

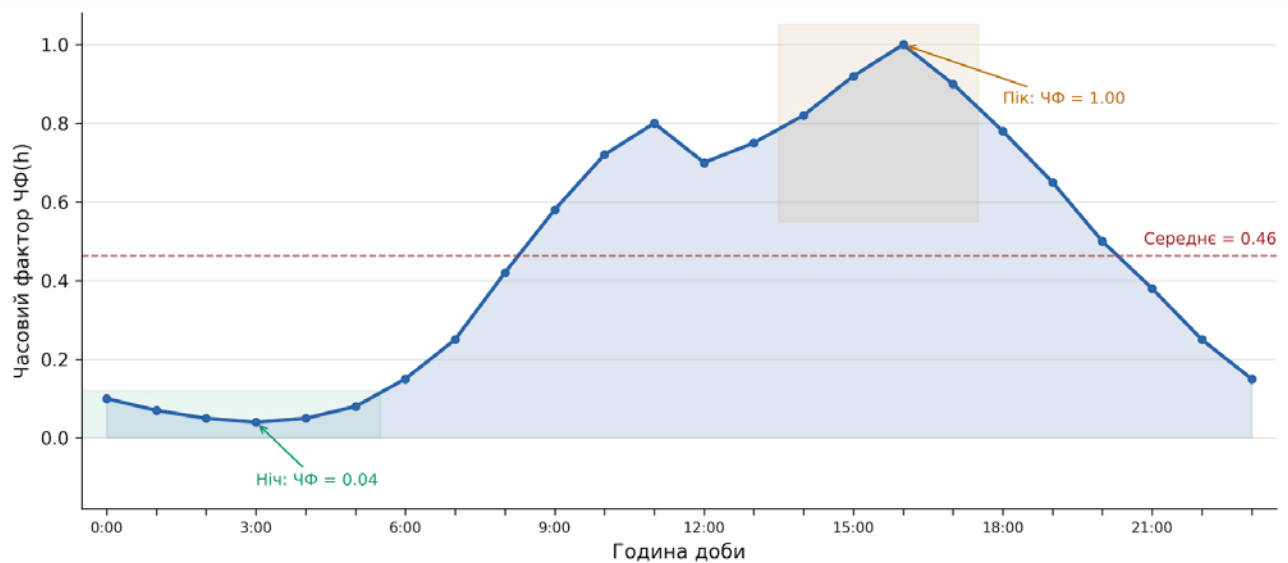


Рис. 3.19. Розподілення часового фактору.

Середнє значення ЧФ за добу становить 0.46. Для ночі (00:00-05:00) середнє ЧФ = 0.07, для робочих годин (09:00-18:00) - 0.77, для пікового блоку (14:00-17:00) - 0.91.

Таблиця 3.5

Значення ЧФ для часу доби у системі моделювання

Година	ЧФ	Година	ЧФ	Година	ЧФ	Година	ЧФ
00:00	0.10	06:00	0.15	12:00	0.70	18:00	0.78
01:00	0.07	07:00	0.25	13:00	0.75	19:00	0.65
02:00	0.05	08:00	0.42	14:00	0.82	20:00	0.50
03:00	0.04	09:00	0.58	15:00	0.92	21:00	0.38
04:00	0.05	10:00	0.72	16:00	1.00	22:00	0.25
05:00	0.08	11:00	0.80	17:00	0.90	23:00	0.15

Для кожного сценарію визначено безпековий профіль, що задає відсоткові значення TP та FP від загальної кількості сесій на кожному етапі, а також розподіл дій системи захисту. Значення параметрів базового сценарію (C1 звичайний день) обрано з урахуванням порядку величин характерних для сучасних WAF-систем [33]. Окремо слід зазначити, що консалтингова компанія

SecureIQLab, яка регулярно проводить порівняльні тестування систем захисту відомих компаній таких, як Microsoft, Akama, AWS, Cloudflare тощо, у своїх звітах демонструє, що кількість помилкових блокувань може сягати 8% [43, 45, 44]. Значення параметру FP для базового сценарію обрані у діапазоні 0.09-0.16% від кількості сесій на відповідному етапі, що має на меті продемонструвати чутливість методу.

Система підтримує чотири базових сценарії (таблиця 3.6), що покривають типові умови функціонування.

Таблиця 3.6

Характеристики сценаріїв системи моделювання

Параметр	C1: Звичайний день	C2: Чорна п'ятниця	C3: Розпродаж	C4: DDoS-атака
Базовий трафік (E_1 /день)	50 000	250 000	15 000/год	50 000
Бізнес-фактор (БФ)	1.0	2.5	2.0	1.0
FP на E_7 (% від N)	0.16%	0.90%	0.95%	0.25%
TP на E_7 (% від N)	0.50%	0.70%	0.65%	0.50%
Переважаюча дія на E_7	block 35%	block 50%	block 55%	block 70%
Тривалість	24 год	24 год	3 год	24 год (атака 2 год)
Відхилення ($\pm\%$)	5%	10%	15%	5%

Метою експериментів є демонстрація роботи методу, тому значення параметрів не відіграють важливої ролі допоки залишаються в межах галузевих показників. Розглянемо приклади обраних параметрів для кожного сценарію.

Для надання сценарію C1(звичайний день) більшої реалістичності, нижня межа діапазону параметру FP на ранніх етапах взаємодії відповідає значенню

0.09%. На початкових етапах взаємодії з сервісом електронної комерції дії користувачів є типовими та рідше спричиняють хибні спрацювання систем захисту. Верхня межа параметру FP , зі значенням 0.16%, відповідає етапу оплати товару (E_7). На даному етапі більш складна взаємодія користувачів з сервісом електронної комерції підвищує ймовірність хибних спрацювань систем захисту. Значення параметра TP на етапі взаємодії E_7 визначено як 0.50%. Значення навмисно обрано невеликим для демонстрації чутливості роботи методу – навіть при низькій частці зловмисних сесій метод має коректно оцінювати стан роботи системи захисту, але в той же час одиночні події не матимуть надмірного впливу на розрахунок показників ефективності захисту. Згідно даного сценарію система захисту уникає агресивних дій щодо користувачів, та працює збалансовано, збільшуючи кількість блокувань підозрілих дій на етапі оплати до 35%. До кожного параметра при генерації додається випадкове відхилення, щоб запобігти створенню файлів з однаковими параметрами. Для базового сценарію $S1$ відхилення мінімальне і становить $\pm 5\%$.

Сценарій $S2$ (чорна п'ятниця) моделює період пікового розпродажу з суттєвим зростанням трафіку. За даними Queue-it, трафік під час чорної п'ятниці 2025 року зріс удвічі порівняно зі звичайним днем [13]. Водночас у роботі прийнято множник кількості трафіку $\times 5$ як параметр сценарію моделювання підвищеного навантаження на системи захисту. Слід зазначити, що навантаження окремих систем електронної комерції у періоди розпродажів можуть суттєво перевищувати подвійне зростання. Параметр FP на етапі E_7 збільшено до 0.90%, під час масових розпродажів користувачі поведуться нетипово, така поведінка провокує зростання хибних спрацювань системи захисту. Параметр TP на етапі взаємодії E_7 отримує незначний приріст до 0.70%, більшість користувачів легітимні, але в той самий час кількість зловмисного трафіку також зростає. За даними Queue-it, зловмисний бот-трафік та трафік з дата-центрів складав 36% усього роздрібного трафіку під час святкового сезону 2024 року, що на 24% більше ніж попереднього року [13]. Зважаючи, що чорна п'ятниця є запланованою подією з очікувано високим трафіком, система захисту

заздалегідь налаштована працювати в посиленому режимі, на останньому етапі взаємодії частка блокувань становить 50%. Параметр відхилення для даного сценарію задано у $\pm 10\%$ так як під час масового розпродажу трафік менш передбачуваний.

Сценарій С3 (Розпродаж) моделює короткострокову акцію з розпродажу товарів тривалістю 3 години з різким сплеском трафіку на початку та поступовим спадом. Характерною особливістю сценарію є зростання кількості трафіку більш ніж у 7 разів відносно того ж проміжку часу за нормальних умов. Система захисту не встигає адаптуватись, відповідно стрімко зростає кількість хибних спрацювань, тому параметр FP визначено як 0.95% на етапі E₇. Параметр TP для етапу E₇ визначено у 0.65%, кількість коректного виявлення загроз також зростає, але через короткий період розпродажу значення TP зростає повільно. Значення блокувань на етапі E₇ сягає 55%, система захисту діє агресивно через різкий сплеск активності та відсутність часу для адаптації. Параметр відхилення для даного сценарію є найвищим, що відповідає різким змінам характеристик трафіку з яким взаємодіє система захисту, і становить $\pm 15\%$.

Сценарій С4 (DDoS-атака) принципово відрізняється від сценаріїв розпродажу: бізнес-фактор залишається 1.0, оскільки DDoS-атака не є запланованою бізнес-подією. Це дозволяє продемонструвати, що метод розрізняє ситуації очікуваного (розпродаж) та неочікуваного (атака) зростання трафіку. Для С4 наведено значення під час атаки у проміжку між 14:00-16:00 годиною. Під час атаки трафік зростає у вісім разів відносно базового (у таблиці 3.5 приведені значення очікуваного трафіку і відповідні значення інших параметрів, що відповідають сценарію С1). Згідно даного сценарію система захисту розпізнає DDoS атаку і активно блокує трафік на етапі E₁, через це значення FP на етапі E₇ має незначний приріст відносно базового сценарію С1, так як робота системи захисту у посиленому режимі більш вірогідно спричинятиме хибні спрацювання. Значення TP на етапі E₇ залишається незмінним відносно сценарію С1, так як зазвичай DDoS трафік блокується та не доходить до фінальних етапів взаємодії користувачів з сервісом електронної

комерції. Відповідно до сценарію, система захисту перебуває у режимі блокування для забезпечення доступності сервісу, тому поводить себе агресивно і на пізніх етапах взаємодії, відповідно кількість блокувань на етапі E_7 має значення 70%. Сценарій С3 передбачає, що DDoS атака генерує велику кількість трафіку, але він однотипний, тому відхилення залишається на рівні $\pm 5\%$.

Для річного набору даних базовий трафік додатково модифікується трьома детермінованими факторами: тижневим циклом (субота - множник 0.85, неділя - 0.75, що відповідає зниженню активності онлайн-покупців у вихідні), місячною сезонністю (серпень – 0.82, грудень – 1.25, що відображає сезонну динаміку сервісів електронної комерції) та загальним трендом зростання (+1% щомісяця, що відповідає середньорічним темпам зростання сервісів електронної комерції) [58].

Конверсія у системі моделювання (10%) перевищує середньогалузевий показник. Це обумовлено необхідністю забезпечити достатню кількість безпекових подій на етапах оформлення та оплати (E_6 , E_7) при базовому трафіку 50 000 сесій. При конверсії 1.8% кількість сесій на E_7 складає 900, з яких лише $\sim 4-5$ були б ТР, цього недостатньо для значущих даних аналізу. Спрощення не впливає на коректність оцінки, оскільки показники P_i розраховуються як відносні величини від кількості сесій на відповідному етапі.

Для кожного сценарію після генерації даних перевіряються: середнє та стандартне відхилення N по етапах взаємодії; співвідношення FP/TP по етапах взаємодії (значення має зростати від E_1 до E_7); розподіл дій (частка block має зростати до критичних етапів), відповідність інваріантів (таблиця 3.1).

3.3. Експериментальні дослідження методу аналізу ефективності системи захисту сервісів електронної комерції

Для проведення серії з дев'яти експериментів було згенеровано набори даних, перелік яких наведено у таблиці 3.7. Таблиця демонструє унікальні вхідні файли без урахування перевикористання між експериментами. Повні дані доступні за посиланням: <https://doi.org/10.5281/zenodo.20331397>.

Таблиця 3.7

Перелік наборів даних для експериментів

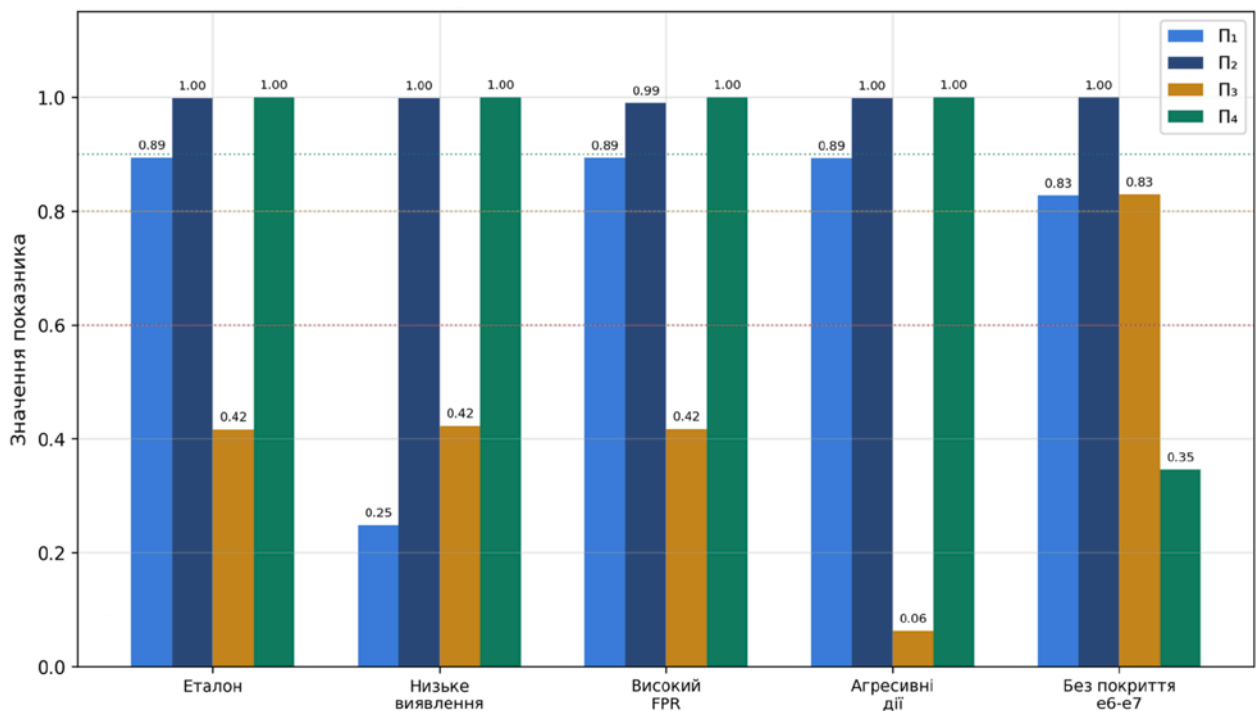
Категорія	Кількість файлів	Призначення
Діагностичні набори для параметрів P_i	4	Верифікація незалежності показників P_i
Добові набори	108	Погодинний аналіз
Набір ізольованого ЧФ	3	Демонстрація ефекту ЧФ при фіксованих даних
Набори без класифікації	24	Аналіз без TP/FP/FN
Набори після коригування	24	Порівняння до та після покращення
Річний зріз	365	Щоденні динаміка за рік
Місячний зріз	30	Деталізація одного місяця
Конфігураційні файли	27	Параметри аналізу для різних режимів
Усього	585	

Здійснимо експеримент 1 "Верифікація незалежності показників P_1 - P_4 " (E01), метою цього експерименту є підтвердити, реакцію кожного показника P_1 - P_4 виключно на свій тип проблеми, що не залежить від інших. Для цього створено 5 наборів даних – 1 еталонний (сценарій С1, нормальний день) та 4 діагностичних, кожен з яких цілеспрямовано деградує один конкретний показник. Аналіз проводиться без контекстної корекції. Отримані значення показників P_1 - P_4 наведені у таблиці 3.8 та на рис. 3.20.

Таблиця 3.8

Отримані значенні показників для E01

Набір	Π_1	Π_2	Π_3	Π_4	ІЕЗ
Еталон (C1)	0.8940	0.9988	0.4170	1.0000	0.9027
Низьке виявлення	0.2484	0.9988	0.4225	1.0000	0.5958
Високий FPR	0.8937	0.9899	0.4173	1.0000	0.9010
Агресивні дії	0.8929	0.9987	0.0628	1.0000	0.8738
Без покриття E_6 - E_7	0.8272	0.9997	0.8296	0.3460	0.7288

Рис. 3.20. Верифікація незалежності показників Π_1 - Π_4 .

Результати підтверджують незалежність показників. Зниження TPR впливає виключно на Π_1 (значення 0.2484 та еталонне 0.8940), тоді як $\Pi_2=0.9988$, $\Pi_3=0.4225$, $\Pi_4=1$ не змінюються. Аналогічно, підвищений FPR знижує лише Π_2 (0.9899 і 0.9988). Агресивні дії впливають лише на Π_3 (0.0628 і 0.4170). Відсутність покриття етапів E_6 - E_7 впливає насамперед на Π_4 (0.3460 і 1).

Додатково перевірено вплив вагових коефіцієнтів на ІЕЗ. На тих самих еталонних даних ІЕЗ обчислено з п'ятьма конфігураціями: розраховані коефіцієнти K_i та W_{Π_i} (ІЕЗ = 0.9027), рівномірні K_i (ІЕЗ = 0.9073), екстремальні K_i з домінуванням E_7 (ІЕЗ = 0.8984), рівномірні W_{Π_i} (ІЕЗ = 0.8275), екстремальні

W_{Π} з домінуванням Π_1 ($IE3 = 0.8871$). $IE3$ малочутливий до зміни ваг етапів K_i (різниця $< 1\%$), оскільки ефективність системи захисту розподілена відносно рівномірно по етапах. Водночас $IE3$ суттєво чутливий до ваг показників W_{Π} (різниця до 8%), що обумовлено структурно низьким значенням $\Pi_3 = 0.42$: при рівномірних вагах цей показник отримує вагу 0.25 замість 0.08 і непропорційно знижує інтегральну оцінку.

Показники Π_1 – Π_4 є незалежними індикаторами різних аспектів ефективності системи захисту. $IE3$ малочутливий до варіації ваг етапів K_i та чутливий до ваг показників W_{Π} , що підтверджує необхідність обґрунтованого вибору вагових коефіцієнтів.

Проведемо експеримент 2 "Штатний режим – базовий з добовою динамікою" (E02). Метою даного експерименту є підтвердити, що у нормальному режимі роботи $IE3_k$ відображає добову динаміку без суттєвих спотворень, та продемонструвати ізольований ефект часового фактору (ЧФ). Для цього здійснювався аналіз 24-х погодинних файлів сценарію С1 (звичайний день). Аналіз виконано у двох режимах: без контекстної корекції та з контекстною корекцією ($БФ = 1$) (рис. 3.21).

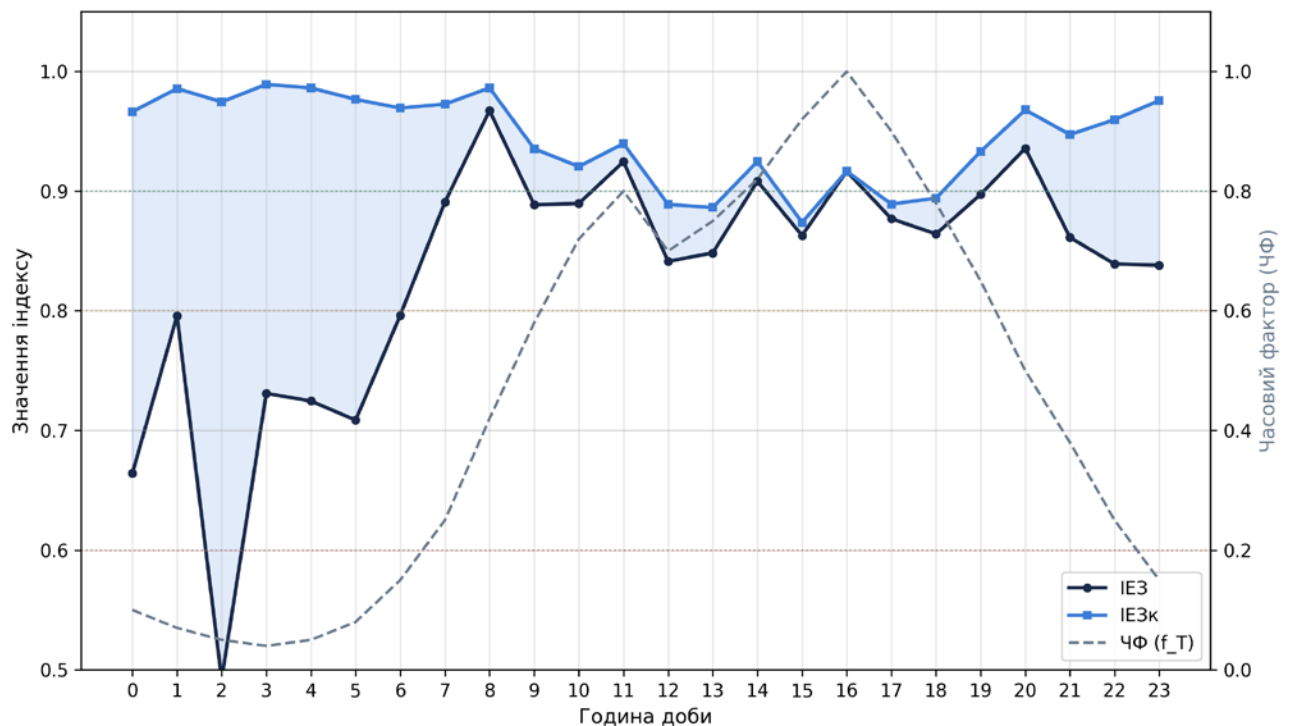


Рис. 3.21. Вплив ЧФ на $IE3$ та $IE3_k$

У штатному режимі ($БФ = 1.0$) ІЕЗ коливається протягом доби від ~ 0.50 у нічні години до ~ 0.95 вдень. Ці коливання зумовлені статистичним шумом: у нічні години ($ЧФ < 0.10$) кількість сесій на окремих етапах взаємодії мала і поодинокі спрацювання ТР/ФР мають непропорційний вплив на показники. ІЕЗк демонструє згладжену динаміку: при низькому ЧФ контекстна корекція зменшує вплив нічних відхилень ($ККЧ < 0.30$), що відповідає нижчій бізнес-критичності нічних інцидентів. У пікові години ($ЧФ = 1.0$) ІЕЗк наближається до ІЕЗ ($ККЧ = 1.0$). Середнє значення ІЕЗ за добу – 0.8318, ІЕЗк – 0.9442. Різниця 11.24% обумовлена тим, що середній $ККЧ = 0.46 < 1.0$.

Додатково перевірено ефект впливу часового фактору. Створено 3 файли з ідентичним вмістом (ті самі N, ТР, ФР, FN, безпекові дії), але різним значенням ЧФ: 0.05 (ніч), 0.42 (ранок), 1.00 (пік). Результати наведено у таблиці 3.9.

Таблиця 3.9

Вплив часового фактору на ІЕЗ та ІЕЗк

Часовий проміжок	ЧФ	ККЧ	ІЕЗ	ІЕЗк	Δ
Ніч (03:00)	0.05	0.05	0.8789	0.9939	0.1150
Ранок (08:00)	0.42	0.42	0.8789	0.9491	0.0702
Пік (16:00)	1.00	1.00	0.8789	0.8789	0.0000

На ідентичних даних ІЕЗ залишається незмінним (0.8789). ІЕЗк демонструє залежність від часового фактору: вночі ($ЧФ = 0.05$) $ІЕЗк = 0.9939$, у пік ($ЧФ = 1.0$) $ІЕЗк = 0.8789$ (рис. 3.22). Різниця Δ зростає пропорційно ЧФ (таблиця 3.9).

У базовому режимі роботи ІЕЗк згладжує статистичний шум при малих обсягах трафіку. Часовий фактор самостійно впливає на ІЕЗк пропорційно та передбачувано.

Проведемо експеримент 3 "Чорна п'ятниця – спільний ефект впливу ЧФ та БФ" (Е03), метою якого є підтвердити, що під час бізнес-подій ІЕЗк суттєво відрізняється від ІЕЗ, і ця різниця обґрунтована підвищеним бізнес-впливом. Для цього проведемо аналіз 24 погодинних файли сценарію С2 (чорна п'ятниця), де базовий трафік взято $\times 5$ (250 000 сесій), $БФ = 2.5$. Аналіз виконано у двох режимах: з та без контекстної корекції.

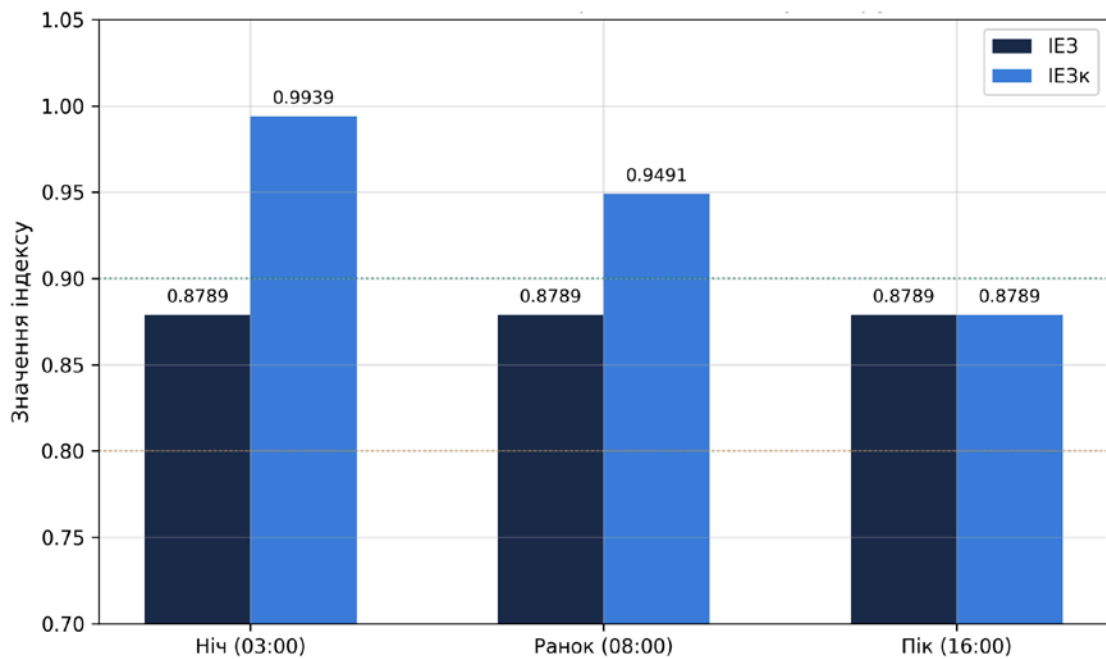


Рис. 3.22. Ефект впливу часового фактору

Під час чорної п'ятниці ІЕЗ становить в середньому 0.8726, відображаючи технічну ефективність. ІЕЗк з урахуванням ККЧ = ЧФ * БФ (середнє ККЧ = 1.49) становить 0.8125 – нижче за ІЕЗ, оскільки при ККЧ > 1 контекстна корекція посилює оцінку. Це відповідає логіці методу, оскільки під час розпродажу кожне хибне спрацювання впливає на більшу кількість потенційних покупців. Різниця максимальна виявлена об 11:00: ККЧ = 2.50, ІЕЗ = 0.8768, ІЕЗк = 0.6920 – розрив 0.1848 (рис. 3.23).

Залежність ІЕЗк від ККЧ є монотонною та плавною (рис. 3.23). При ККЧ < 0.5 різниця між ІЕЗ та ІЕЗк мінімальна; при ККЧ = 2.5 ІЕЗк = 0.6304. Відсутність стрибків та розривів підтверджує стабільність формули.

Рисунок 3.24 демонструє значенні показників ефективності роботи систем захисту П₁-П₄. Показники П₂ та П₄ залишаються стабільно високими протягом усієї доби (~1.0), тоді як П₁ коливається в діапазоні 0.77-0.90 через статистичний шум у нічні години при малих обсягах трафіку. Найнижчим є П₃ (0.25–0.32), що відображає посилену політику блокування під час розпродажу та вказує на якість реагування як основне проблемне місце ефективності роботи системи захисту в цей період.

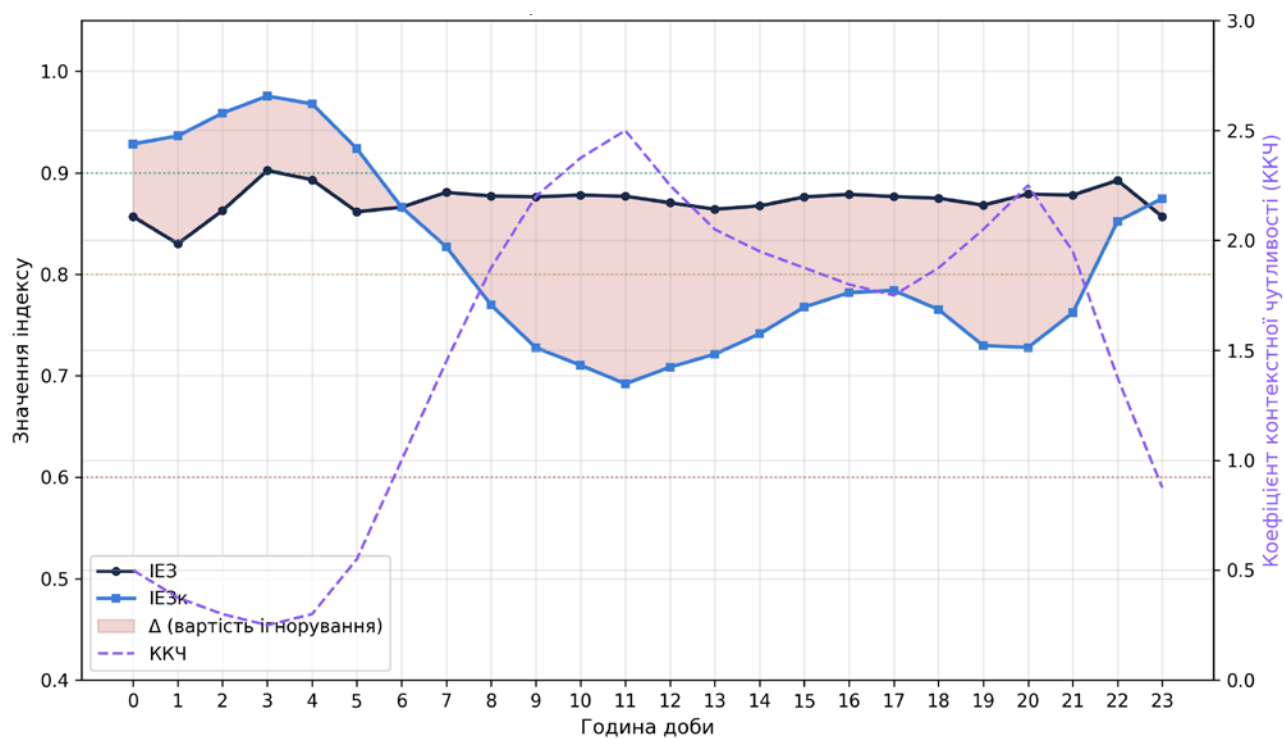


Рис. 3.23. Чорна п'ятниця. ІЕЗ та ІЕЗк протягом доби.

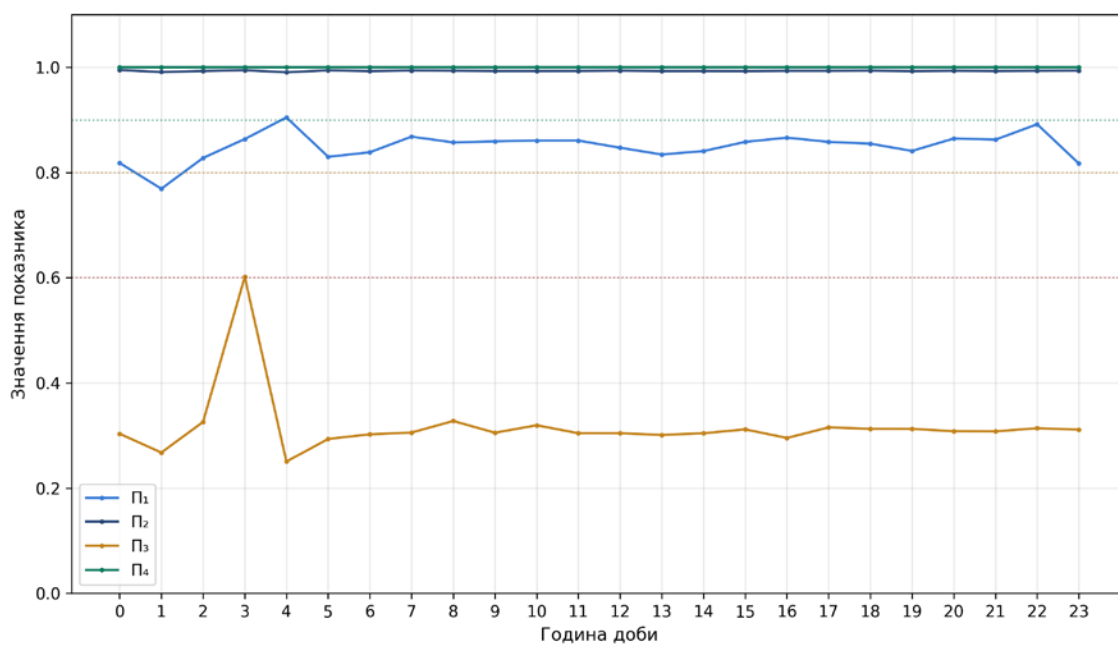


Рис. 3.24. Чорна п'ятниця. Значення показників P_1 - P_4 протягом доби.

На рис. 3.25 представлений розподіл унікальних сесій користувачів в цей період.

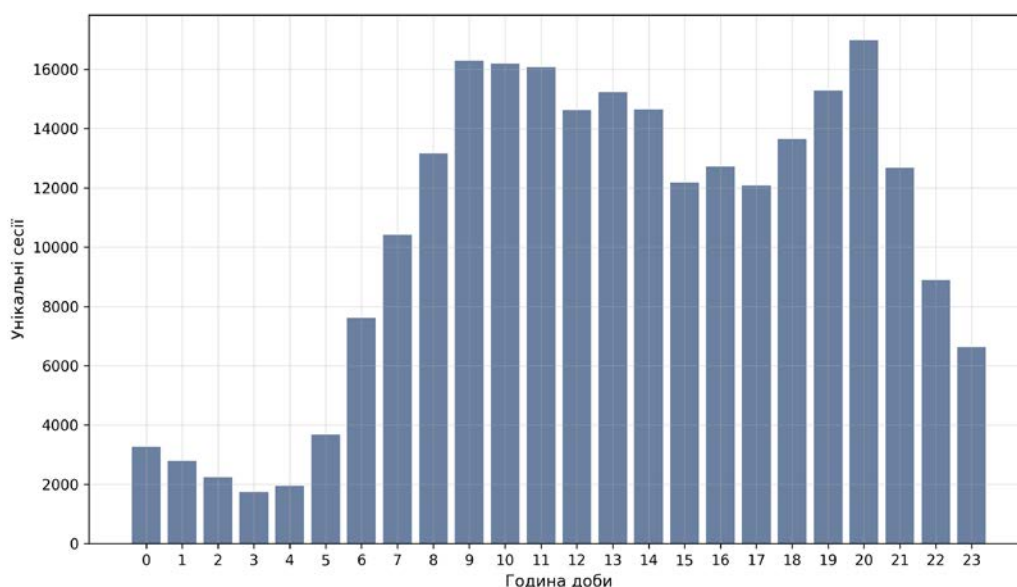


Рис. 3.25. Чорна п'ятниця. Унікальні сесії користувачів.

Рис. 3.26 демонструє як параметри розрахунку ККЧ (ЧФ та БФ) впливають на його значення при високих навантаженнях.

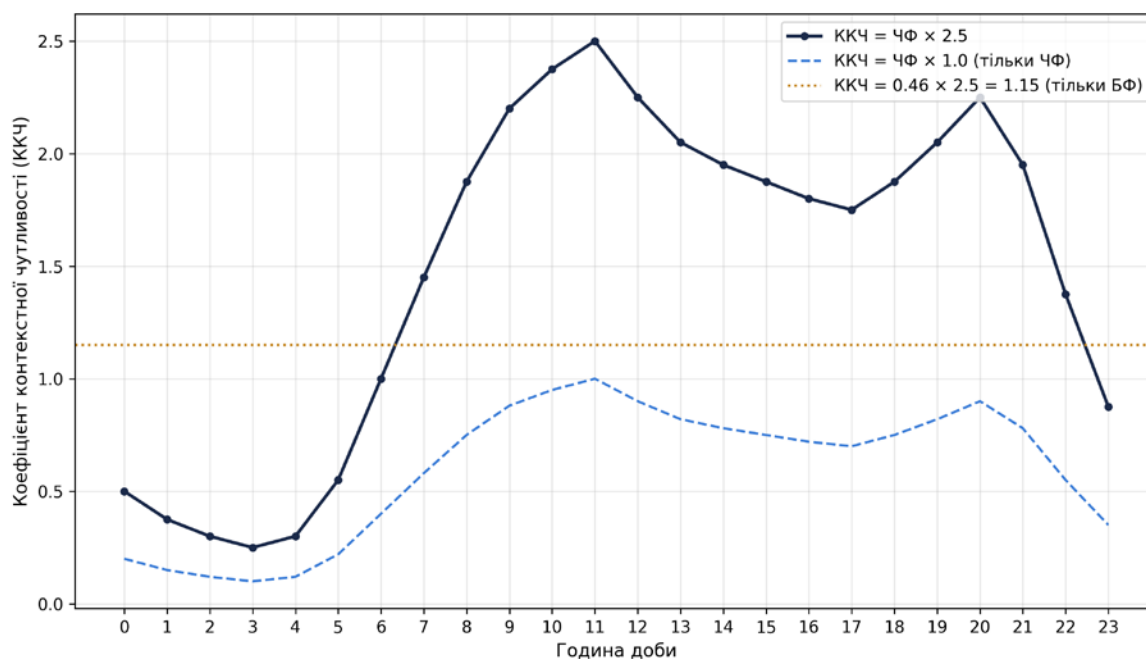


Рис. 3.26. Чорна п'ятниця. Внесок БФ та ЧФ у формування ККЧ

Під час бізнес-подій ($ККЧ > 1$) контекстна корекція посилює оцінку, відображаючи підвищену ціну помилок. Різниця між ІЕЗ та ІЕЗк досягає 0.1848 у пікові години.

Проведемо експеримент 4 "DDoS-атака" (E04), метою якого є підтвердити, що метод не послаблює оцінку при відсутності бізнес-підстави для підвищеного трафіку. Для цього проведемо аналіз 24 погодинних файли сценарію C4 (DDoS-атака 14:00–16:00). При цьому БФ = 1.0, оскільки атака не є запланованою бізнес-подією. Під час атаки базовий трафік зростає у 8 разів. На рис. 3.27 представлено значення ІЕЗ та ІЕЗк під час чорної п'ятниці та DDoS атаки.

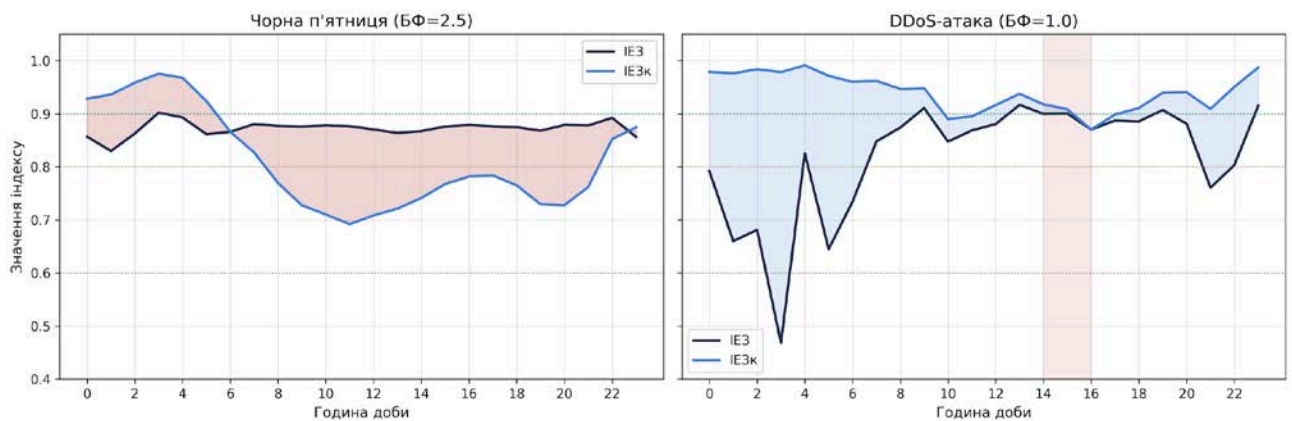


Рис. 3.27. Порівняння: ІЕЗ та ІЕЗк під час чорної п'ятниці та DDoS атаки

Під час DDoS-атаки бізнес-фактор залишається БФ = 1.0. Відповідно $ККЧ = ЧФ * 1.0 = ЧФ$, і середнє значення ККЧ за добу становить 0.46 – таке саме як у звичайний день, оскільки добовий шаблон трафіку не змінюється. При $ККЧ < 1$ формула ІЕЗк послаблює оцінку: $ІЕЗк = 0.9405$, що вище за $ІЕЗ = 0.8194$. Це означає, що технічні проблеми, зафіксовані під час атаки, мають знижений бізнес-вплив у середньому за добу, більшість годин мали низький трафік, і помилки системи захисту торкнулись меншої кількості користувачів.

Порівняння з чорною п'ятницею демонструє принципову різницю: при розпродажі (БФ = 2.5) ІЕЗк нижчий за ІЕЗ ($\Delta = -0.060$), оскільки помилки коштують дорожче, тоді як при DDoS (БФ = 1.0) ІЕЗк вищий за ІЕЗ ($\Delta = +0.121$) – метод не надає DDoS атаці статусу бізнес-критичної події.

Метод розрізняє ситуації за бізнес-контекстом. DDoS-атака (БФ = 1.0) та звичайний день (E02, $\Delta = +0.112$) демонструють порівнянні Δ , тоді як чорна п'ятниця (БФ = 2.5) має відмінне значення.

Проведемо експеримент 5 "Розпродаж, аналіз роботи методу на коротких інтервалах" (E05), метою якого є підтвердити чутливість методу до динаміки на 15-хвилинних інтервалах. Для цього проведемо аналіз 12 файлів, що містять події за 15 хвилин, сценарію С3 (12:00–15:00, розпродаж). При цьому БФ= 2.0, трафік х6 на старті з поступовим зниженням.

У перші 15 хвилин (12:00–12:15) $IE3 = 0.9049$, $IE3_k = 0.8859$. До завершення акції різниця зменшується відповідно до зниження трафіку (рис. 3.28). Середнє $IE3$ за період = 0.8431, $IE3_k = 0.8068$.

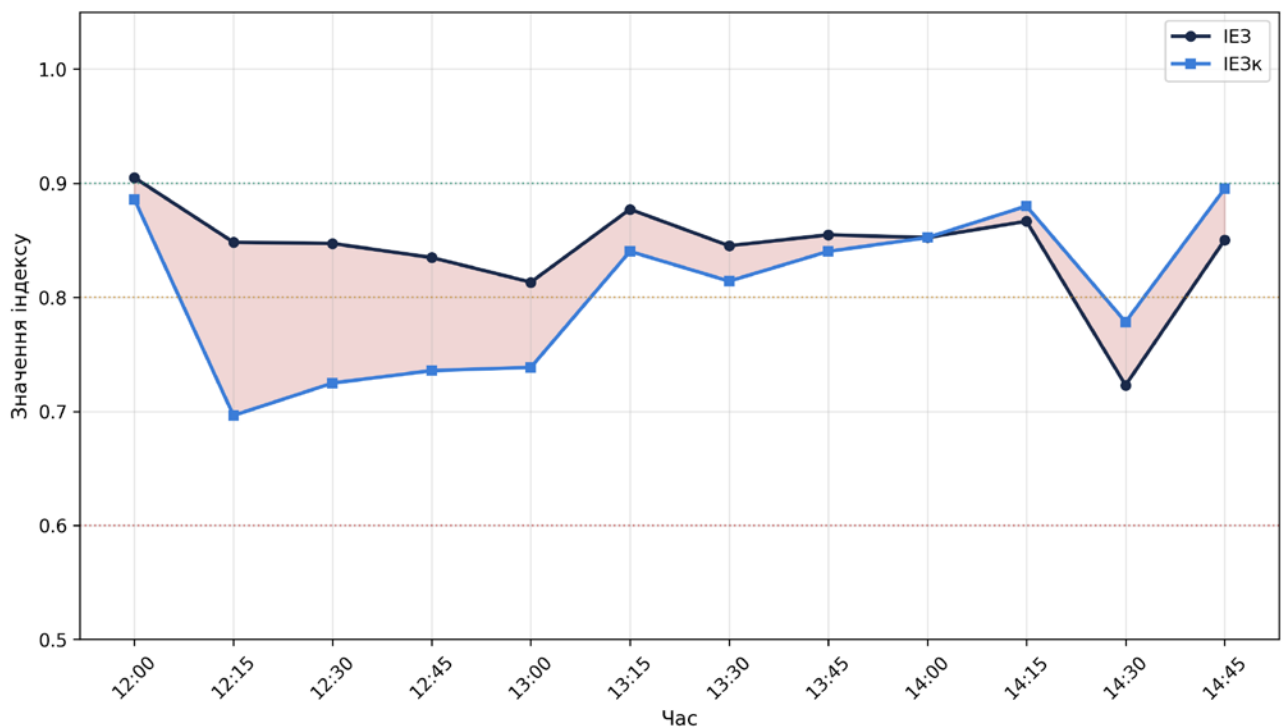


Рис. 3.28. Розпродаж: $IE3$ та $IE3_k$ з аналізом кожні 15 хвилин.

Метод демонструє адекватну чутливість на коротких інтервалах, що дозволяє відслідковувати динаміку перехідних процесів.

Проведемо експеримент 6 "Використання методу аналізу без класифікації безпекових подій" (E06), метою якого є підтвердити, що метод дає корисну діагностику навіть без класифікованих безпекових подій (ТР/ФР/ФН). Для цього здійснюється аналіз 24 погодинних файлів С2 (чорна п'ятниця) без полів ТР/ФР/ФН – тільки кількість сесій (N) та дії систем захисту. Порівняння P_3 та P_4 з аналізом, де були присутні всі дані (E03) (рис. 3.29, рис. 3.30).

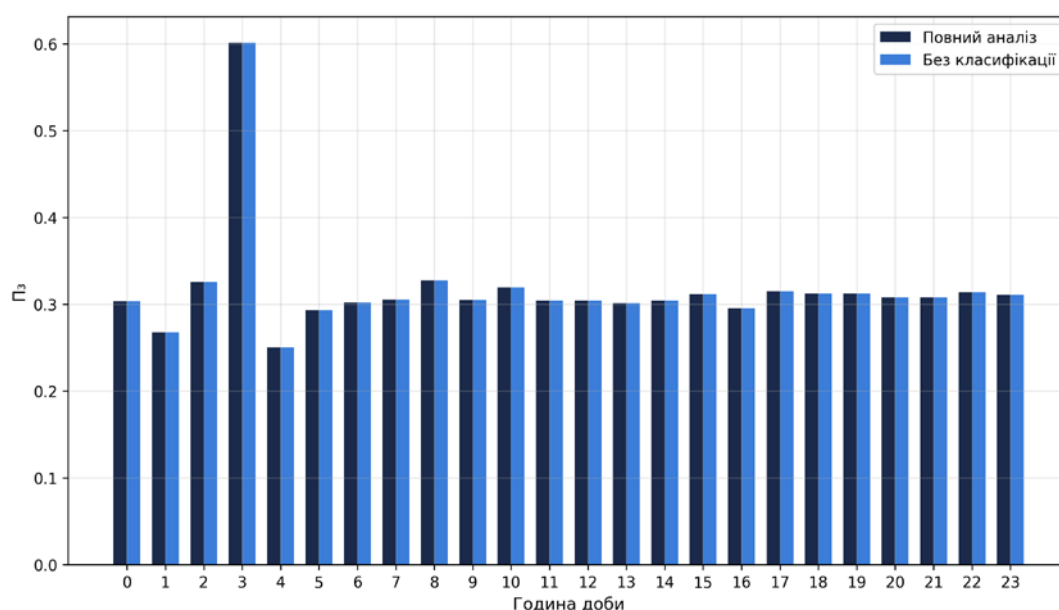


Рис. 3.29. Порівняння значень параметра P_3 з повною та частковою класифікацією подій.

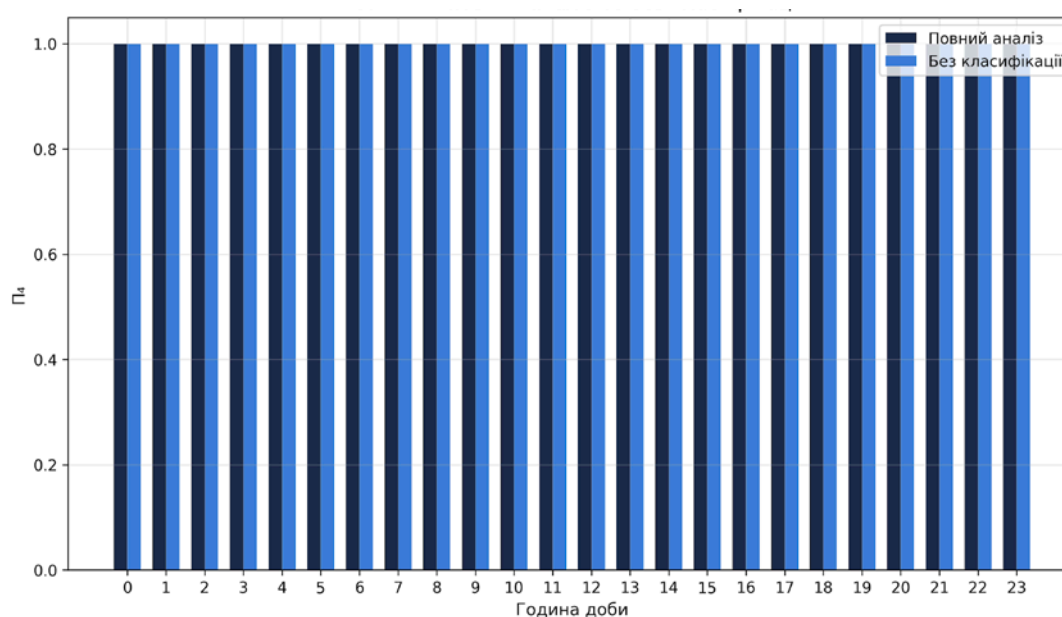


Рис. 3.30. Порівняння значень параметра P_4 з повною та частковою класифікацією подій.

Значення P_3 у повному аналізі та без класифікації ідентичні (0.3034 та 0.3034 для кожної години). Аналогічно P_4 збігається в обох режимах. Показники P_3 (якість реагування) та P_4 (покриття етапів захистом) базуються на розподілі типів дій та наявності спрацювань, а не на класифікації, тому не залежать від наявності класифікованих подій. Метод зберігає діагностичну цінність без

присутньої класифікації безпекових подій, що розширює його застосовність для організацій, які не мають ресурсів для ретроспективного аналізу інцидентів.

Наступний експеримент 7 "Вплив часового масштабу аналізу" (E07), метою якого є показати, що масштаб ретроспективного аналізу впливає на видимість проблем. Для цього дані чорної п'ятниці (E03) об'єднано за різні часові вікна: 1 година, 3 години, 6 годин, 12 годин, 1 день (таблиця 3.10).

Таблиця 3.10

Вплив періоду аналізу на ІЕЗк

Період аналізу	ІЕЗ	ІЕЗк	ККЧ середнє
1 година (11:00)	0.8768	0.6920	2.50
3 години (10:00–12:59)	0.8753	0.7038	2.38
6 годин (08:00–13:59)	0.8738	0.7213	2.21
12 годин (06:00–17:59)	0.8740	0.7577	1.92
1 день (00:00–23:59)	0.8735	0.8117	1.49

При аналізі подій на проміжку в одну годину ІЕЗк = 0.6920 (ККЧ = 2.50). При розширенні до повної доби ІЕЗк зростає до 0.8117 (ККЧ = 1.49), оскільки нічні години з низьким навантаженням згладжують пікову проблему. Різниця між погодинним та подобовим значенням ІЕЗк – 12% (рис. 3.31).

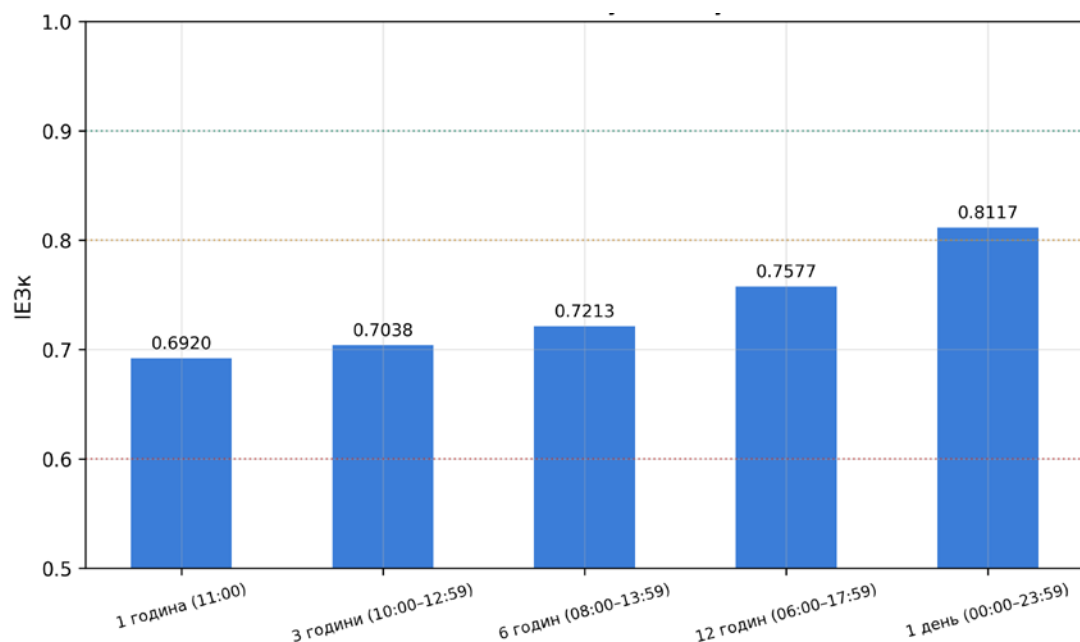


Рис. 3.31. Вплив розміру періоду аналізу на ІЕЗк.

Під час бізнес-подій ретроспективний аналіз слід проводити з погодинним інтервалом для виявлення пікових проблем, що розвиваються на більшому масштабі.

Наступний експеримент 8 "Зведений порівняльний аналіз сценаріїв" (E08), метою якого є підтвердити, що контекстна корекція систематично залежить від ККЧ – при ККЧ > 1 оцінка посилюється, при ККЧ < 1 послаблюється, і ця закономірність виконується для всіх сценаріїв. Для цього результати E02-E05 зібрано в єдину таблицю (таблиця 3.11). Для кожного з сценаріїв обчислено $\Delta = \text{ІЕЗ}_k - \text{ІЕЗ}$, а також обчислено кореляцію між ККЧ та Δ (див. рис. 3.32).

Таблиця 3.11

Зведене порівняння результатів виконання сценаріїв

Сценарій	ІЕЗ середнє	ІЕЗ _к середнє	ККЧ середнє	Δ (ІЕЗ _к – ІЕЗ)
С1 Звичайний день	0.8318	0.9442	0.46	0.1124
С2 Чорна п'ятниця	0.8726	0.8125	1.49	-0.0601
С3 Розпродаж	0.8431	0.8068	1.25	-0.0363
С4 DDoS-атака	0.8194	0.9405	0.46	0.1211

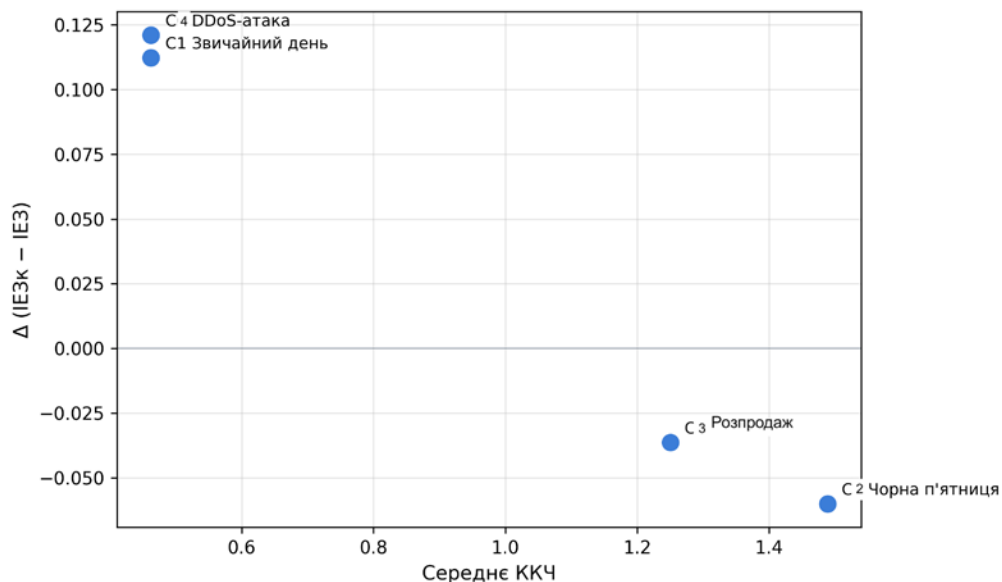


Рис. 3.32. Залежність Δ від ККЧ.

Зведений аналіз чотирьох сценаріїв підтверджує, що контекстна корекція працює передбачувано у всіх випадках (див. рис. 3.33). Коли бізнес-фактор

високий (чорна п'ятниця БФ = 2.5, розпродаж БФ = 2.0), ІЕЗк нижчий за ІЕЗ – метод сигналізує, що помилки системи захисту під час розпродажу коштують бізнесу дорожче. Коли бізнес-фактор дорівнює 1 (звичайний день, DDoS-атака), ІЕЗк вищий за ІЕЗ – метод враховує, що при середньому за добу трафіку нижче пікового вплив помилок на бізнес менший.

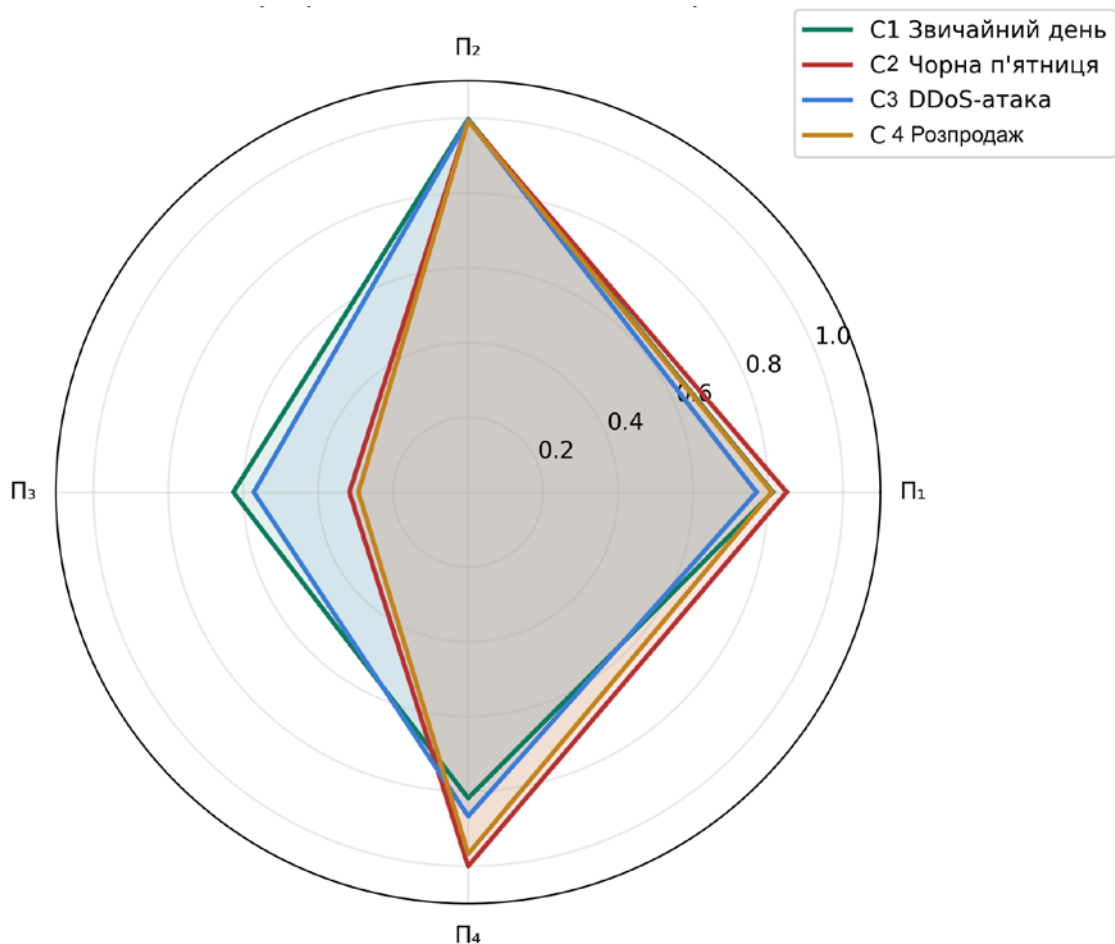


Рис. 3.33. Профілі показників Π_1 - Π_4 за сценаріями

DDoS атака та звичайний день демонструють практично однакову різницю ($\Delta = +0.121$ та $+0.112$ відповідно), хоча під час атаки трафік зростає у 8 разів. Це підтверджує, що контекстна корекція реагує саме на бізнес-фактор, а не на кількість трафіку.

Радарна діаграма профілів показників демонструє, що усі чотири сценарії мають спільне вузьке місце – низький Π_3 (0.25–0.45), що означає надмірну частку жорстких блокувань у всіх режимах роботи. Головна відмінність – по осі Π_1 : під час DDoS атаки виявлення загроз найнижче (~ 0.65), оскільки перевантажена

система пропускає частину атак. В інших сценаріях Π_1 тримається на рівні 0.83–0.87.

Метод дозволяє одночасно оцінити два виміри ефективності – як бізнес-вплив проблем змінюється залежно від контексту (через ІЕЗк), та які саме аспекти захисту потребують покращення (через профіль Π_1 – Π_4).

Наступний експеримент 9 "Оцінка наслідків зміни налаштувань системи захисту" (Е09), метою якого є продемонструвати роботу методу як інструменту оцінки наслідків зміни налаштувань системи захисту. Для цього проведено порівняння двох наборів даних чорної п'ятниці: «до» (С2 оригінальний) та «після» (С2 зі зміненими налаштуваннями: зменшення FP на E_5 – E_7 , менше block на користь challenge/flag).

Після коригування якість реагування Π_3 зросла з 0.3169 до 0.4312 (+36.07%) – система стала менш агресивною. Π_2 незначно зріс (+0.37%) завдяки зниженню хибних спрацювань. Однак виявлення загроз Π_1 знизилось з 0.8497 до 0.8128 (–4.34%) – послаблення правил блокування призвело до пропуску частини загроз (рис. 3.34).

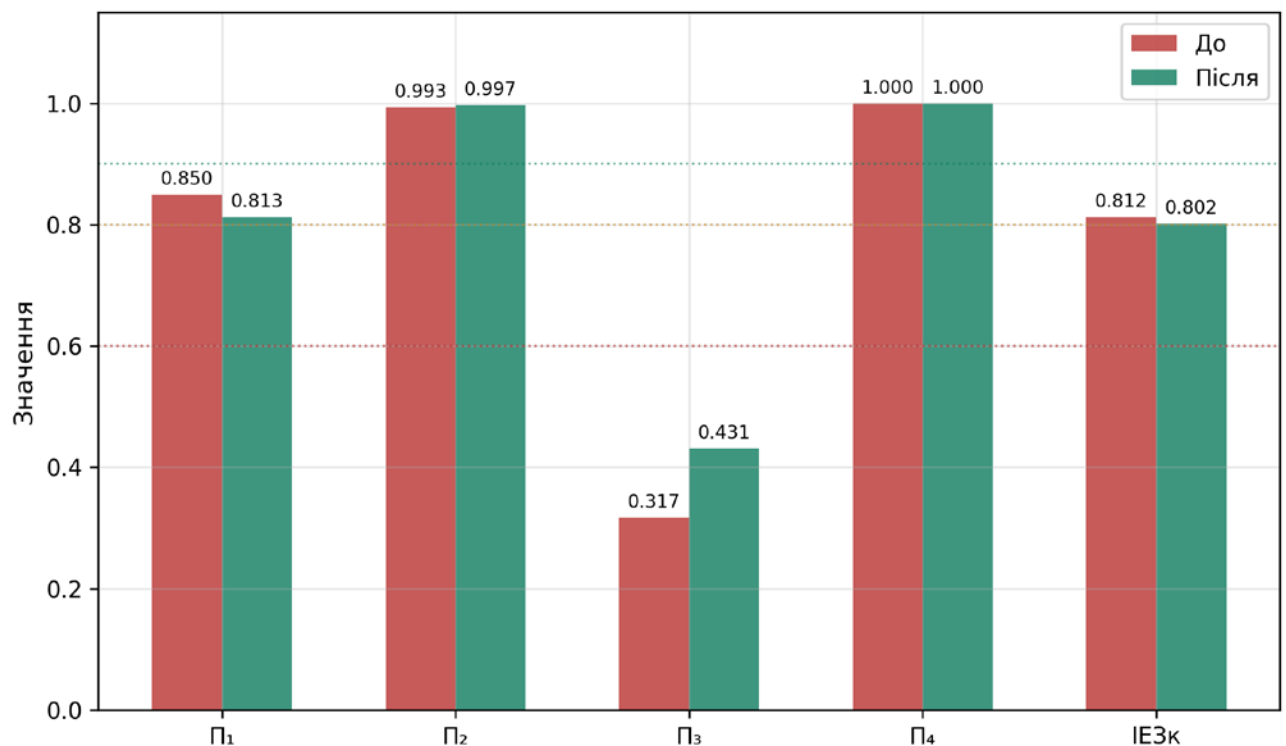


Рис. 3.34. Показники Π_1 – Π_4 та ІЕЗк до та після зміни налаштувань.

Оскільки вага виявлення загроз ($W_1 = 0.476$) у шість разів перевищує вагу якості реагування ($W_3 = 0.080$), ІЕЗк знизився з 0.8125 до 0.8020 (−1.29%) (таблиця 3.12). Рис. 3.35 демонструє ІЕЗк до та після зміни.

Таблиця 3.12

Результати змін налаштувань системи захисту

Показник	До	Після	Δ	$\Delta\%$
Π_1	0.8497	0.8128	−0.0369	−4.34%
Π_2	0.9933	0.9970	+0.0037	+0.37%
Π_3	0.3169	0.4312	+0.1143	+36.07%
Π_4	1.0000	1.0000	0.0000	0.00%
ІЕЗ	0.8726	0.8649	−0.0077	−0.88%
ІЕЗк	0.8125	0.8020	−0.0105	−1.29%

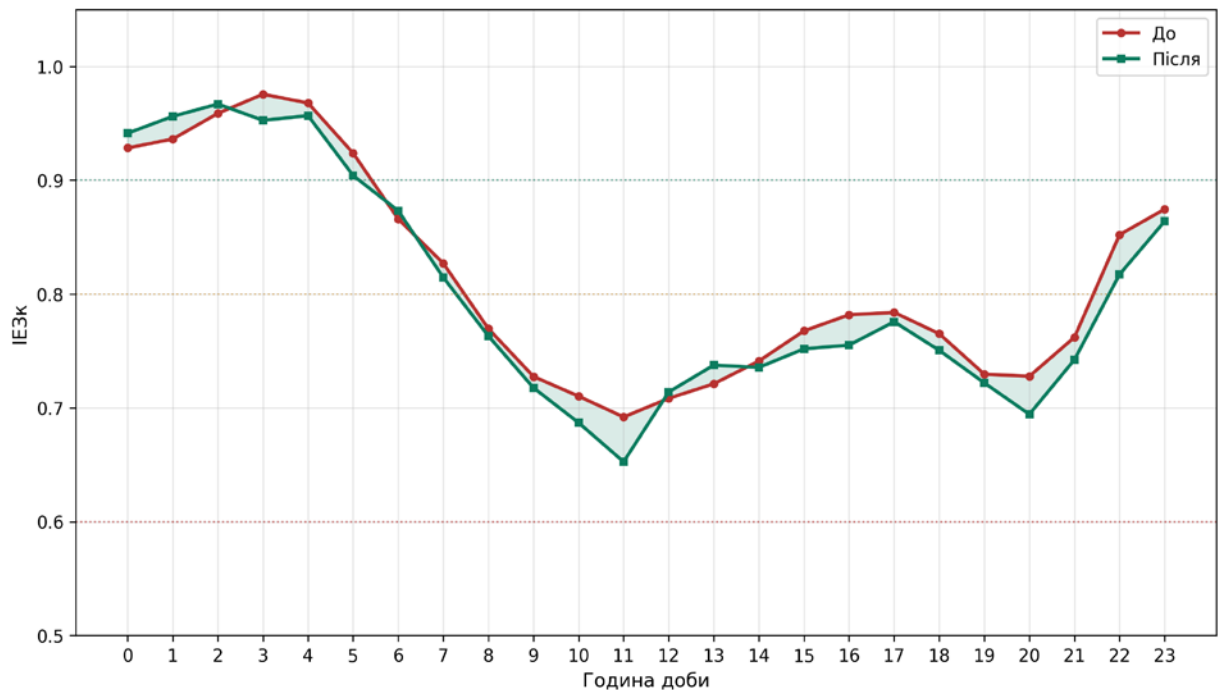


Рис. 3.35. Значення ІЕЗк протягом доби до та після зміни налаштувань.

Отриманий результат демонструє практичну цінність методу, без інтегральної оцінки ІЕЗк користувач бачив би лише покращення Π_3 на 36% і міг вважати зміну налаштувань успішною. Метод сигналізує, що покращення досягнуто ціною зниження виявлення загроз, і загальний стан захисту погіршився, демонструючи побічні ефекти зміни налаштувань, які невидимі при аналізі окремих показників.

Висновки до третього розділу

У третьому розділі "Алгоритми, та програмна реалізація методу аналізу ефективності системи захисту сервісів електронної комерції" представлено алгоритмічне забезпечення методу аналізу ефективності системи захисту сервісів електронної комерції; здійснена програмна реалізація методу аналізу ефективності системи захисту сервісів електронної комерції та системи моделювання; проведені експериментальні дослідження методу аналізу ефективності системи захисту сервісів електронної комерції.

Було розроблено ряд алгоритмів, представлених у вигляді блок-схем, виконано програмну реалізацію аналітичної складової методу аналізу ефективності системи захисту сервісів електронної комерції, реалізовано систему моделювання взаємодії користувачів з сервісом електронної комерції, проведено серію експериментів, що підтверджують коректність та можливість практичного застосування у різних режимах роботи.

Було розроблено специфікацію стандартизованого JSON інтерфейсу, що формалізує комунікацію між зовнішніми джерелами даних (рівень 1-2 методу) та аналітичною складовою (рівень 3-4 методу). Визначено необхідні для роботи аналітичного модуля вхідні дані та параметри, а саме: JSON документ з вхідними агрегованими даними від зовнішньої системи збору та обробки даних; попередньо розраховані параметри методу (K_1 та $W_{П1}$); контекстні параметри ЧФ та БФ. Відмежування аналітичної складової методу та використання для комунікації стандартизованих інтерфейсів дозволяє уникнути залежності від зовнішніх систем, що постачають дані, та розширити можливості інтеграції аналітичної складової методу. Також було розроблено алгоритм отримання та перевірки вхідних даних аналітичної складової методу аналізу системи захисту сервісів електронної комерції.

Для чотирьох показників ефективності систем захисту було розроблено алгоритми розрахунку їх значень. Алгоритм розрахунку показника виявлення загроз (Π_1) реалізує агрегацію значень TP та FN по всіх етапах взаємодії та обчислення частки виявлених загроз. Алгоритм розрахунку показника взаємодії

з користувачами (Π_2) реалізує поетапний розрахунок FPR з урахуванням коефіцієнтів критичності етапів взаємодії E_i . Алгоритм розрахунку показника якості реагування (Π_3) реалізує обчислення середньозваженого коефіцієнта впливу дій для кожного етапу взаємодії E_i . Алгоритм розрахунку показника покриття захистом (Π_4) реалізує визначення наявності активного захисту на кожному етапі взаємодії користувача з сервісом електронної комерції та обчислення зваженої суми з урахуванням критичності етапів взаємодії E_i . Для кожного алгоритму визначено вхідні та вихідні дані, описано послідовність операцій та правила обробки особливих випадків.

Було розроблено алгоритми обчислення інтегрального індексу ефективності захисту (ІЕЗ) та контекстного індексу ефективності захисту (ІЕЗк). Алгоритм розрахунку базового ІЕЗ реалізує обчислення зваженої суми показників $\Pi_1 - \Pi_4$ з використанням значень вагових коефіцієнтів W_{Π_i} . Алгоритм врахування контекстних факторів реалізує перевірку та обчислення контекстного коефіцієнта чутливості на основі часового фактору та бізнес-фактору. Алгоритм розрахунку ІЕЗк реалізує врахування контекстних параметрів впливу на роботу системи захисту.

Розроблено алгоритм системи рекомендацій, що опрацьовує вхідні дані у три послідовні етапи. На першому етапі для кожного показника визначається статус за шкалою інтерпретації з п'яти рівнів – відмінно, добре, задовільно, незадовільно, критично, та обчислюється відхилення від цільового рівня значення показника Π_i . На другому етапі для показників з ненульовим відхиленням розраховується індекс пріоритету рекомендації, що враховує контекстні фактори ЧФ і БФ, та визначається рівень пріоритету за шкалою з чотирьох рівнів – критичний, високий, помірний, низький. На третьому етапі формується структурований звіт рекомендацій, що містить інформацію про показники, статус, базову рекомендацію та рівень пріоритету.

Виконано програмну реалізацію аналітичного модуля мовою програмування Python із застосуванням модульної архітектури. Обґрунтовано

вибір технологій. Програмний модуль складається з чотирьох обчислювальних компонентів для відображення та аналізу отриманих даних.

Розроблено систему моделювання взаємодії користувачів з сервісом електронної комерції. Система моделювання підтримує чотири базові сценарії – штатний режим, чорна п'ятниця, розпродаж, DDoS атака, кожен з яких визначає характерні патерни трафіку, розподіл безпекових подій та контекстні параметри. Система моделювання дозволяє створювати дані із заданою часовою деталізацією, що забезпечує верифікацію методу на різних масштабах аналізу.

Проведено серію з дев'яти експериментів з використанням даних отриманих від системи моделювання взаємодії користувача з сервісом електронної комерції. В ході виконання експериментів було підтверджено незалежність показників $P_1 - P_4$. Отримано підтвердження контекстної кореляції результатів роботи систем захисту, що демонструє зміна значень ІЕЗ та ІЕЗк. Перевірено, що метод методу аналізу ефективності системи захисту сервісів електронної комерції коректно розмежовує вплив на роботу сервісу електронної комерції бізнес-контексту та позаштатних ситуацій. Метод зберігає діагностичну цінність при отриманні часткових даних, а саме тільки показників P_3 та P_4 , розрахунок яких не потребує додаткової інформації ретроспективного аналізу безпекових подій. Було продемонстровано чутливість методу на різних часових масштабах даних, що поступають для аналізу. При великій кількості трафіку різниця між погодинним та добовим значеннями ІЕЗк досягає 12%.

У третьому розділі було розроблено одинадцять алгоритмів, представлених у вигляді блок-схем, виконано програмну реалізацію аналітичної складової методу аналізу ефективності системи захисту сервісів електронної комерції, реалізовано систему моделювання взаємодії користувачів з сервісом електронної комерції, проведено серію експериментів, що підтверджують коректність та можливість практичного застосування у різних режимах роботи.

Результати досліджень представлені в наукових публікаціях здобувача [1].

Висновки

Відповідно до поставленої мети та завдань дослідження з проблеми аналізу ефективності систем захисту сервісів електронної комерції отримано такі основні **результати**: проаналізовано закордонний та вітчизняний досвід з окресленої проблематики; здійснено аналіз наявних методів, засобів та технологій оцінки ефективності роботи систем захисту сервісів електронної комерції та проблеми їх функціонування; обґрунтовано основні показники ефективності систем захисту сервісів електронної комерції в залежності від складності їх структури; розроблено алгоритм та метод аналізу ефективності функціонування систем захисту сервісів електронної комерції; розроблено прототип експериментального програмного забезпечення, що реалізує авторський метод аналізу ефективності систем захисту сервісів електронної комерції та його протестовано.

Результати дослідження дали підстави для таких **висновків**:

1. Проведений комплексний аналіз закордонного та вітчизняного досвіду у галузі розробки та функціонування систем захисту сервісів електронної комерції дозволяє стверджувати, що на сьогоднішній день єдиного, уніфікованого підходу до вирішення питань захисту не існує. Аналіз наукових джерел свідчить про те, що розвиток галузі зосереджено не лише на посиленні захисних механізмів, а й на пошуку підходів до інтеграції нових рішень з уже працюючими інформаційними системами. Якісно новим етапом розвитку є перехід до адаптивних рішень, здатних функціонувати в режимі реального часу, зокрема із застосуванням систем штучного інтелекту.

2. Огляд наявних методів, засобів та технологій оцінки ефективності роботи систем захисту демонструє сталий науковий інтерес до цієї проблематики, проте динамічний розвиток технологій вимагає не лише вдосконалення вже наявних підходів, але й розробки принципово нових інструментів. Визначено, що наявні підходи першочергово фокусуються на оцінці роботи систем захисту за технічними параметрами, залишаючи поза

увагою вплив захисних механізмів на взаємодію користувачів із сервісами електронної комерції та бізнес-показники таких сервісів. Це зумовило необхідність розробки методу, що враховує бізнес-контекст функціонування сервісів електронної комерції.

3. Виокремлено чотири основні показники ефективності систем захисту сервісів електронної комерції: виявлення загроз, взаємодія з користувачами, якість реагування, покриття захистом етапів взаємодії користувачів з сервісом електронної комерції. Для визначення вагових коефіцієнтів показників використано метод аналізу ієрархій. Формалізовано модель взаємодії користувачів з сервісами електронної комерції у вигляді послідовності з семи етапів та визначено коефіцієнти критичності етапів взаємодії користувача з сервісом електронної комерції. Узгодженість отриманих результатів перевірено за допомогою розрахунку індексу узгодженості, що є частиною методу аналізу ієрархій.

4. Розроблено чотирирівневу архітектуру методу аналізу ефективності систем захисту сервісів електронної комерції, що забезпечує повний цикл аналізу від збору метрик до формування інтегрального індексу ефективності захисту. Запропоновано розрахунок контекстного індексу ефективності захисту, що додатково враховує часовий фактор та бізнес-фактор через коефіцієнт контекстної чутливості. Метод забезпечує урахування бізнес-контексту на трьох рівнях: через коефіцієнти критичності етапів взаємодії користувачів з сервісами електронної комерції; через коефіцієнт контекстної чутливості при розрахунку контекстного індексу ефективності захисту; через розрахунок пріоритетів проблемних аспектів при роботі системи рекомендацій. Розроблено ряд алгоритмів, зокрема: алгоритми розрахунку кожного з чотирьох показників ефективності, алгоритми обчислення інтегрального та контекстного індексів ефективності захисту, алгоритм отримання та перевірки вхідних даних аналітичної складової методу, алгоритм системи рекомендацій. Запропоновано систему формування рекомендацій, що дозволяє провести діагностику стану

показників та визначити пріоритети виявлених проблемних аспектів із урахуванням контексту роботи сервісу електронної комерції.

5. Виконано програмну реалізацію прототипу аналітичного модуля мовою програмування Python із застосуванням модульної архітектури. Розроблено специфікацію стандартизованого JSON-інтерфейсу, що формалізує комунікацію між зовнішніми джерелами даних та аналітичною складовою методу. Розроблено систему моделювання взаємодії користувачів з сервісом електронної комерції, що підтримує чотири базові сценарії (штатний режим, чорна п'ятниця, розпродаж, DDoS-атака). Проведено серію з дев'яти експериментів, в ході яких підтверджено незалежність показників ефективності систем захисту, отримано підтвердження контекстної кореляції результатів роботи систем захисту, перевірено, що метод коректно розмежовує вплив бізнес-контексту та позаштатних ситуацій на роботу сервісу електронної комерції. Метод зберігає діагностичну цінність при отриманні часткових даних та демонструє чутливість на різних часових масштабах даних, що підтверджує можливість його практичного застосування у різних режимах роботи.

Виконане дослідження не вичерпує всіх аспектів поставленої проблеми. Продовження наукових досліджень за даною проблематикою доцільно у таких напрямках:

- розширення методу аналізу ефективності систем захисту сервісів електронної комерції шляхом включення фінансової складової, зокрема моделювання економічних втрат від відтоку клієнтів, спричиненого хибними спрацюваннями систем захисту;
- дослідження механізмів інтеграції аналітичної складової методу з реальними сервісами електронної комерції через стандартизовані API існуючих платформ (Shopify, WooCommerce, Magento тощо) та систем захисту (WAF, anti-fraud системи, SIEM), що дозволить забезпечити автоматизований збір даних та перехід від моделювання до аналізу в умовах реального часу;

- адаптація розробленого методу для функціонування в режимі реального часу з інтеграцією у DevSecOps-процеси сервісів електронної комерції, що забезпечить безперервний моніторинг ефективності систем захисту та автоматичне формування рекомендацій у відповідь на зміну бізнес-контексту чи профілю загроз;
- інтеграція сервісів штучного інтелекту в аналітичну складову методу для підвищення точності та адаптивності аналізу ефективності систем захисту, зокрема застосування методів машинного навчання для прогнозування динаміки показників, виявлення прихованих аномалій у поведінкових паттернах користувачів, а також використання великих мовних моделей для автоматичної генерації рекомендацій з урахуванням специфіки конкретного сервісу електронної комерції.

Література

1. Ковалевський В., Вакалюк Т. Використання штучного інтелекту у системах захисту сервісів електронної комерції. *Інформаційні технології та суспільство*, 2025. №3 (18). С. 72-76. DOI: [10.32689/maup.it.2025.3.9](https://doi.org/10.32689/maup.it.2025.3.9)
2. Ковалевський В.В. Безпекові виклики у сфері електронної комерції пов'язані з розвитком технологій штучного інтелекту. *Глобальні виклики та інновації: шляхи розвитку сучасної науки: збірник наукових праць з матеріалами IV Міжнародної наукової конференції, м. Львів, 11 липня, 2025 р.* Львів, 2025. С. 145-148. DOI: [10.62731/mcnd-11.07.2025.005](https://doi.org/10.62731/mcnd-11.07.2025.005)
3. Ковалевський В.В., Вакалюк Т.А. Виклики у сфері захисту сервісів електронної комерції. *Наука, технології, інновації: світові тенденції та регіональний аспект : Матеріали VII Міжнародної науково-практичної конференції (м. Одеса, 27–28 вересня 2024 р.)* / ГО «Інститут інноваційної освіти»; Науково-навчальний центр прикладної інформатики НАН України. Одеса; Запоріжжя : АА Тандем, 2024. С. 62-64. <https://novaosvita.com/wp-content/uploads/2024/10/ScTechInn-Odesa-Sept2024.pdf>
4. Ковалевський В.В., Вакалюк Т.А. Огляд наявних методів оцінки ефективності роботи систем захисту сервісів електронної комерції. *Вісник Херсонського національного технічного університету*, 2023. №3 (86). С. 102-110. DOI: [10.35546/kntu2078-4481.2023.3.13](https://doi.org/10.35546/kntu2078-4481.2023.3.13)
5. Ковалевський В.В., Вакалюк Т.А. Огляд сучасних систем захисту електронних сервісів. *Вісник Хмельницького національного університету. Серія: Технічні науки*, 2024. Том 337, №3(2). С. 176-182. DOI: [10.31891/2307-5732-2024-337-3-26](https://doi.org/10.31891/2307-5732-2024-337-3-26)
6. Ковалевський В.В., Вакалюк Т.А. Стан досліджень у галузі розробки та функціонуванні систем захисту сервісів електронної комерції. *Вчені записки Таврійського національного університету імені В.І. Вернадського. Серія: Технічні науки*, 2022. Том 33 (72), № 6. С. 92-98. DOI: [10.32782/2663-5941/2022.6/16](https://doi.org/10.32782/2663-5941/2022.6/16)

7. Ковалевський В.В., Вакалюк Т.А., Необхідність розробки алгоритмічного та програмного забезпечення аналізу ефективності систем захисту сервісів електронної комерції. *Матеріали V Всеукраїнської науково-практичної інтернет-конференції студентів, аспірантів та молодих вчених за тематикою «Сучасні комп'ютерні системи та мережі в управлінні»:* збірка наукових праць/під редакцією А.А. Григорової. Херсон: Видавництво ФОП Вишемирський В. С., 2022. С. 22-23.
<https://kntu.net.ua/ukr/content/download/99376/566912/file/CICT2022.pdf>
8. Мервінський О. Європейські вимоги щодо захисту персональних даних у сфері електронної комерції. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні.* 2015. Вип. 2 (30). С. 34-40. URL: https://ela.kpi.ua/bitstream/123456789/18033/1/30_p34.pdf (дата звернення: 21.11.2022)
9. Москалик Д.О., Антонюк Д.С., Вакалюк Т.А., Огінський Є.В., Ковалевський В. В. Огляд застосувань теорії графів у розробці та обслуговуванні програмних систем. *Computer Science and Applied Mathematics.* Запоріжжя: Видавничий дім «Гельветика», 2022. № 1. С. 75-82. DOI: [10.26661/2413-6549-2022-1-09](https://doi.org/10.26661/2413-6549-2022-1-09)
- 10.Музиченко Т. О., Скорба О. А., Шевчук А. А. Штучний інтелект як засіб оптимізації бізнес-процесів в електронній комерції. *Академічні візії.* 2023. № 25. URL: <https://academy-vision.org/index.php/av/article/view/696/630>. (дата звернення: 14.02.2023)
- 11.Нісфоян С. С., Сисоліна Н. П., Савеленко Г. В. Розвиток методу аналізу ієрархій як механізму вибору інвестиційного проєкту на підприємстві. *Центральноукраїнський науковий вісник. Економічні науки.* 2020. Вип. 5 (38). С. 228–237. DOI: 10.32515/2663-1636.2020.5(38).228-237.
- 12.Тригубець Б. Технології захисту інформації в електронній комерції. *Матеріали IV Міжнародної студентської науково - технічної конференції.* Тернопіль: Тернопільський національний технічний університет ім. І.Пулую (м. Тернопіль, 28-29 квітня 2021 р.), 2021. С. 11-

12. URL: <https://tntu.edu.ua/storage/pages/00000852/Zbirnyk-studconf2021.pdf> (дата звернення: 21.11.2022)
- 13.149 Black Friday statistics every retailer needs to know in 2026. URL: <https://queue-it.com/blog/black-friday-statistics/> (дата звернення: 21.03.2026)
- 14.2024 Global eCommerce Payments & Fraud Report. URL: <https://www.cybersource.com/content/dam/documents/campaign/fraud-report/global-fraud-report-2024.pdf>. (дата звернення: 25.12.2025)
- 15.2025 Data Breach Investigations Report. URL: <https://www.verizon.com/business/resources/T16f/reports/2025-dbir-data-breach-investigations-report.pdf> (дата звернення: 20.01.2026)
- 16.50 Cart Abandonment Rate Statistics 2026. URL: <https://baymard.com/lists/cart-abandonment-rate> (дата звернення: 21.03.2026)
- 17.A09:2021 – Security Logging and Monitoring Failures. URL: https://owasp.org/Top10/A09_2021-Security_Logging_and_Monitoring_Failures/. (дата звернення: 21.11.2022)
- 18.Abdallah A., Maarof M.A., Zainal A. Fraud detection system: A survey. *Journal of Network and Computer Applications*, 2016. Vol. 68. Pp. 90–113. DOI: 10.1016/j.jnca.2016.04.007
- 19.Agyepong E., Cherdantseva Yu., Reinecke P., Burnap P. A systematic method for measuring the performance of a cyber security operations centre analyst. *Computers & security*. 2023. Vol. 124 (C). Pp. 102959. DOI: [10.1016/j.cose.2022.102959](https://doi.org/10.1016/j.cose.2022.102959).
- 20.Alrumiah S. S., Hadwan M. Implementing Big Data Analytics in E-Commerce: Vendor and Customer View. *IEEE Access*, 2021. Vol. 9. Pp. 37281-37286. DOI: 10.1109/ACCESS.2021.3063615.
- 21.Angermeier D., Wester H., Beilke K., Hansch G., Eichler J. Security risk assessments: modeling and risk level propagation. *ACM Transactions on Cyber-Physical Systems*. 2022. Vol. 7, Iss. 1, Article 8. DOI: [10.1145/3569458](https://doi.org/10.1145/3569458).
- 22.Anro Gracious L. A., Sudha L., Chitra B., Kaur G., Sathya V., Kabitha P., Siva Subramanian R. Advancing E-Commerce Security: Strategic Innovations and

- Future Directions in AI and ML. *Strategic Innovations of AI and ML for E-Commerce Data Security*, 2025. Pp. 79-106. IGI Global Scientific Publishing. DOI: 10.4018/979-8-3693-5718-7.ch004.
23. Antón A.I., Earp J.B. Strategies for Developing Policies and Requirements for Secure and Private Electronic Commerce. *E-Commerce Security and Privacy. Advances in Information Security*, 2001. Vol 2. Springer, Boston, MA. Pp. 67-86. DOI: 10.1007/978-1-4615-1467-1_5
 24. Applebaum S., Gaber T., Ahmed A. Signature-based and machine-learning-based web application firewalls: a short survey. *Procedia Computer Science*. 2021. Vol. 189. P. 359–367. DOI: 10.1016/j.procs.2021.05.105.
 25. Ayan Gain and Mridul Sankar Barik. Attack Graph Based Security Metrics for Dynamic Networks. *Information Systems Security: 19th International Conference, ICISS 2023*, Raipur, India, December 16–20, 2023, Proceedings. Springer-Verlag, Berlin, Heidelberg, 109–128. DOI: 10.1007/978-3-031-49099-6_7
 26. Bansal U., Sikka G., Awasthi L., Bhargava B. Quantitative Evaluation of Extensive Vulnerability Set Using Cost Benefit Analysis. *IEEE Transactions on Dependable and Secure Computing*, 2024. Vol. 21 (1). Pp. 298-308. DOI: 10.1109/TDSC.2023.3253121.
 27. Basalla M., Schneider J., Luksik M., Jaakonmäki R., Vom Brocke J. On Latency of E-Commerce Platforms. *Journal of Organizational Computing and Electronic Commerce*, 2021. Vol. 31 (1). Pp. 1–17. DOI: [10.1080/10919392.2021.1882240](https://doi.org/10.1080/10919392.2021.1882240)
 28. Behbehani D., Komninos N., Al-Begain K., Rajarajan M. Cloud Enterprise Dynamic Risk Assessment (CEDRA): a dynamic risk assessment using dynamic Bayesian networks for cloud environment. *Journal of Cloud Computing*, 2023. Vol. 12, 79. DOI: 10.1186/s13677-023-00454-2
 29. Belton V., Stewart T. J. Multiple Criteria Decision Analysis: An Integrated Approach. Springer New York, 2002. 372 p. DOI: 10.1007/978-1-4615-1495-4.

30. Bennouk K., Ait Aali N., El Bouzekri El Idrissi Y., Sebai B., Faroukhi A. Z., Mahouachi D. A comprehensive review and assessment of cybersecurity vulnerability detection methodologies. *Journal of Cybersecurity and Privacy*, 2024. Vol. 4(4). Pp. 853-908. DOI: 10.3390/jcp4040040
31. Benz M., Chatterjee D. Calculated risk? A cybersecurity evaluation tool for SMEs. *Business Horizons*. 2020. Vol. 63 (4). Pp. 531-540. DOI: 10.1016/j.bushor.2020.03.010.
32. Bernik I, Prislan K. Measuring information security performance with 10 by 10 model for holistic state evaluation. *PLoS ONE*. 2016. Vol. 11, no. 9. DOI: [10.1371/journal.pone.0163050](https://doi.org/10.1371/journal.pone.0163050).
33. Best WAF Solutions in 2024–2025: Real-World Comparison. 2024. URL: <https://www.openappsec.io/post/best-waf-solutions-in-2024-2025-real-world-comparison> (дата звернення: 28.11.2025)
34. Böhme, R. Security Metrics and Security Investment Models. *Advances in Information and Computer Security. IWSEC 2010. Lecture Notes in Computer Science*, 2010. Vol. 6434. Springer, Berlin, Heidelberg. DOI: [10.1007/978-3-642-16825-3_2](https://doi.org/10.1007/978-3-642-16825-3_2)
35. Bold R., Al-Khateeb H., Ersotelos N. Reducing False Negatives in Ransomware Detection: A Critical Evaluation of Machine Learning Algorithms. *Applied Sciences*, 2022. Vol. 12 (24), 12941. DOI: [10.3390/app122412941](https://doi.org/10.3390/app122412941)
36. Bots now dominate e-commerce traffic, warns Radware report. URL: <https://www.intelligentciso.com/2025/04/29/bots-now-dominate-e-commerce-traffic-warns-radware-report/>. (дата звернення: 21.11.2022)
37. Buck C., Olenberger C., Schweizer A., Völter F., Eymann T. Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust. *Computers & Security*. 2021. Vol. 110. P. 102436. DOI: 10.1016/j.cose.2021.102436.
38. Byeong A., Hyung-Tae H. Analysis and extension of ordinal priority approach for multi-attribute group decision-making problems. *Expert Systems with Applications*. 2025. Vol. 297. 128449. DOI: 10.1016/j.eswa.2025.128449.

- 39.Cao Q., Qiao Y., Lyu Z. Machine learning to detect anomalies in web log analysis. *2017 3rd IEEE international conference on computer and communications (ICCC), Chengdu, 13–16 December 2017*. 2017. DOI: 10.1109/compcomm.2017.8322600.
- 40.Cheimonidis P., Rantos K. Dynamic Risk Assessment in Cybersecurity: A Systematic Literature Review. *Future Internet*, 2023. Vol. 15, 324. DOI: 10.3390/fi15100324.
- 41.Chopra I.P., Jebarajakirthy C., Jain T. Maseeh H. I. Electronic shopping cart abandonment: What do we know and where should we be heading?. *Electronic Markets*, 2024.Vol. 34, 25. DOI: [10.1007/s12525-024-00697-0](https://doi.org/10.1007/s12525-024-00697-0)
- 42.Cinelli M., Kadzinski M., Gonzalez M., Slowinski R. How to Support the Application of Multiple Criteria Decision Analysis? Let Us Start with a Comprehensive Taxonomy. *Omega*. 2020. Vol. 96. 102261. DOI: 10.1016/j.omega.2020.102261.
- 43.Cloud WAAP CyberRisk Comparative Validation Report v3.0, 2024 https://secureiqlab.com/wp-content/uploads/2024/05/Cloud-WAAP-v3_0_-_CyberRisk-Comparative-Validation-Report.pdf
- 44.Cloud WAAP CyberRisk Comparative Validation Report v4.0, 2025 https://secureiqlab.com/wp-content/uploads/2025/07/Cloud-WAAP-v4_0_-_CyberRisk-Comparative-Validation-Report.pdf
- 45.Cloud WAAP CyberRisk Validation Report – AWS WAF and Shield, API Gateway, 2025 <https://secureiqlab.com/wp-content/uploads/2025/06/2025-Cloud-WAAP-CyberRisk-Validation-Report-AWS.pdf>
- 46.Conklin L. Threat modeling process. OWASP. URL: https://owasp.org/www-community/Threat_Modeling_Process. (дата звернення: 21.11.2022)
- 47.Cormac Herley. So long, and no thanks for the externalities: the rational rejection of security advice by users. *Proceedings of the 2009 workshop on New security paradigms workshop (NSPW '09)*. Association for Computing Machinery, New York, NY, USA, 2009. Pp. 133–144. DOI: [10.1145/1719030.1719050](https://doi.org/10.1145/1719030.1719050)

- 48.CVSS Common Vulnerability Scoring System version 4.0: Specification Document. URL:: <https://www.first.org/cvss/v4.0/specification-document> (дата звернення: 21.11.2022)
- 49.D’Adamo I., González-Sánchez R., Medina-Salgado M.S., Settembre-Blundo D. E-Commerce Calls for Cyber-Security and Sustainability: How European Citizens Look for a Trusted Online Environment. *Sustainability*. 2021. Vol. 13 (12). 6752. DOI: [10.3390/su13126752](https://doi.org/10.3390/su13126752)
- 50.Dakov S., Malinova A. A survey of e-commerce security threats and solutions. *Proceedings of CBU in Natural Sciences and ICT*, 2021. 2, Pp. 1-9. DOI: 10.12955/pns.v2.135
- 51.Dekou R., Savo S., Kufeld S., Francesca D., Kawase R. Machine Learning Methods for Detecting Fraud in Online Marketplaces. *Proceedings of the CIKM 2021 Workshops co-located with 30th ACM International Conference on Information and Knowledge Management (CIKM 2021)*. URL: <https://ceur-ws.org/Vol-3052/paper15.pdf>. (дата звернення: 21.11.2022)
- 52.Demetrio L., Valenza A., Costa G., Lagorio G. WAF-A-MoLE: Evading Web Application Firewalls through Adversarial Machine Learning. *Proceedings of the 35th Annual ACM Symposium on Applied Computing (SAC '20)*. Association for Computing Machinery, New York, NY, USA, 2020. Pp. 1745–1752. DOI: 10.1145/3341105.3373962.
- 53.Dou Yingtong, Liu Zhiwei, Sun Li, deng Yutong, Peng Hao, Yu Philip. Enhancing Graph Neural Network-based Fraud Detectors against Camouflaged Fraudsters. *Proceedings of the 29th ACM International Conference on Information & Knowledge Management (CIKM '20)*. Association for Computing Machinery, New York, NY, USA, 2020. Pp. 315–324. DOI: 10.1145/3340531.3411903.
- 54.Ecommerce fraud trends and statistics merchants need to know. URL: <https://b2b.mastercard.com/news-and-insights/blog/ecommerce-fraud-trends-and-statistics-merchants-need-to-know-in-2024/>. (дата звернення: 29.12.2025)

- 55.E-commerce Market Data and Ecommerce Benchmarks. URL: <https://www.irpcommerce.com/en/gb/ecommercemarketdata.aspx> (дата звернення: 10.03.2026)
- 56.Ferrag M. A., Ndhlovu M., Tihanyi N., Cordeiro L., Debbah mérrouane, Lestable T., Thandi N. Revolutionizing Cyber Threat Detection with Large Language Models: A privacy-preserving BERT-based Lightweight Model for IoT/IIoT Devices. *IEEE Access*. 2024. DOI. 10.1109/ACCESS.2024.3363469.
- 57.Ghorpode S. The Incident Prioritization Matrix: A Cornerstone of Effective Incident Management. URL: <https://www.itsm-docs.com/blogs/it-operations-playbook/the-incident-prioritization-matrix-a-cornerstone-of-effective-incident-management> (дата звернення: 20.01.2026)
- 58.Global conversion rate of online shoppers worldwide from 4th quarter 2024 to 3rd quarter 2025, by country and region, 2025. URL: <https://www.statista.com/statistics/439576/online-shopper-conversion-rate-worldwide> (дата звернення: 27.01.2026)
- 59.Global cybersecurity outlook 2024. *World Economic Forum*. URL: https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf. (дата звернення: 21.11.2022)
- 60.Goers J., Eckardt M., Blumenthal E., Horton G. CMAA–AHP: combinatorial multicriteria acceptability analysis with the analytic hierarchy process. *Central European Journal of Operations Research*. 2026. Vol. 34. Pp. 21–48. DOI: [10.1007/s10100-024-00936-x](https://doi.org/10.1007/s10100-024-00936-x)
- 61.Goldblum M., Tsipras D., Xie C., Chen X., Schwarzschild A., Song D., Madry A., Li B., Goldstein T. Dataset Security for Machine Learning: Data Poisoning, Backdoor Attacks, and Defenses. *IEEE Transactions on Pattern Analysis and Machine Intelligence*. 2023. Vol. 45, no. 2. Pp. 1563–1580. DOI: 10.1109/TPAMI.2022.3162397.
- 62.González-Granadillo G., González-Zarzosa S., Diaz R. Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. *Sensors*. 2021. Vol. 21, No. 14. 4759. DOI: 10.3390/s21144759.

- 63.Higashi S., Kraikritayakul P., Liu Y., Ikeda M., Matsuo K., Barolli L. FSASP: A Fuzzy-Based System for Assessment of Security Posture in 5G/B5G Network Slicing. *Advances on Broad-Band and Wireless Computing, Communication and Applications. BWCCA 2025. Lecture Notes on Data Engineering and Communications Technologies*, 2025. Vol. 278. Springer, Cham. DOI: [10.1007/978-3-032-10347-5_14](https://doi.org/10.1007/978-3-032-10347-5_14)
- 64.Holm H., Ekstedt M. Estimates on the effectiveness of web application firewalls against targeted attacks. *Information Management & Computer Security*, 2013. Vol. 21 No. 4. Pp. 250-265. DOI: 10.1108/IMCS-11-2012-0064
- 65.IDS vs. IPS: Definitions, Comparisons & Why You Need Both. URL: <https://www.okta.com/identity-101/ids-vs-ips/>. (дата звернення: 21.11.2024)
- 66.Introduction to bowtie. How this risk assessment tool works. URL: <https://www.caa.co.uk/safety-initiatives-and-resources/working-with-industry/bowtie/about-bowtie/introduction-to-bowtie/>. (дата звернення: 21.11.2025)
- 67.ISO/IEC 27002:2022. <https://www.iso.org/standard/75652.html> (дата звернення: 10.01.2026)
- 68.Ito M., Iyatomi H. Web application firewall using character-level convolutional neural network. *2018 IEEE 14th international colloquium on signal processing & its applications (CSPA), Batu Feringghi, 9–10 March 2018*. 2018. DOI: 10.1109/cspa.2018.8368694.
- 69.Jakkula A. R. Ensuring Data Privacy and Security in AI-Enabled E-commerce Platforms. *Journal of Artificial Intelligence & Cloud Computing*. 2024. Vol. 3, no. 1. Pp. 1–3. DOI: [10.47363/jaicc/2024\(3\)288](https://doi.org/10.47363/jaicc/2024(3)288).
- 70.Jalalvand F., Chhetri M.B., Nepal S., Paris C. Alert prioritisation in security operations centres: a systematic survey on criteria and methods. *ACM Computing Surveys*, 2024. Vol. 57(2), 42. DOI: 10.1145/3695462.
- 71.Jingyao S., Chandel S., Yunnan Y., Jingji Z., Zhipeng Z. Securing a network: how effective using firewalls and vpns are? *Advances in Information and*

- Communication. FICC 2019. Lecture Notes in Networks and Systems*, 2020. Vol. 70. Springer, Cham. DOI: 10.1007/978-3-030-12385-7_71.
72. Juanli Lan, Lei Hongzhen, Yubo Wang, Ye Liu, Sleiman Kamal, Suliman Mohammed. An empirical investigation of E-loyalty formation for online shopping in China. *Acta psychologica*. 2025. Vol. 258. 105135. DOI: 10.1016/j.actpsy.2025.105135.
73. Kingsley O., Innocent J., Famous C., Yana B., Amadi C., Ibrahim K. Human-Machine Interaction in E-commerce: a Multi-Faceted Examination of CAPTCHA Effect. *2024 Conference of Young Researchers in Electrical and Electronic Engineering*, 2024. Pp. 259-263. DOI: 10.1109/ElCon61730.2024.10468391.
74. Kirvan P. Pen testing guide: Types, steps, methodologies and frameworks. *TechTarget. Search Security*. URL: <https://www.techtarget.com/searchsecurity/tip/Pen-testing-guide-Types-steps-methodologies-and-frameworks>. (дата звернення: 23.12.2025)
75. Kolodiziev O., Mints A., Sidelov P., Pleskun I., Lozynska O. Automatic machine learning algorithms for fraud detection in digital payment systems. *Eastern-European Journal of Enterprise Technologies*. 2020. Vol. 5, no. 9 (107). Pp. 14–26. DOI: [10.15587/1729-4061.2020.212830](https://doi.org/10.15587/1729-4061.2020.212830).
76. Kovalevskyi V. dataset_experiments [Data set]. Zenodo. 2026. DOI: [10.5281/zenodo.20331397](https://doi.org/10.5281/zenodo.20331397)
77. Kukar-Kinney M., Scheinbaum A.C., Orimoloye L.O., Carlson J. R., He H. A model of online shopping cart abandonment: evidence from e-tail clickstream data. *Journal of the Academy of Marketing Science*, 2022. Vol. 50, Pp. 961–980. DOI: 10.1007/s11747-022-00857-8
78. Laybats C., Tredinnick L. Information security. *Business Information Review*. 2016. Vol. 33 (2). Pp. 76-80. DOI: 10.1177/0266382116653061.
79. Lemon K.N., Verhoef P.C. Understanding Customer Experience Throughout the Customer Journey. *Journal of Marketing*, 2016. Vol. 80(6). P. 69-96. DOI: 10.1509/jm.15.0420.

- 80.Liu X., Ahmad S.F., Anser M.K., Ke J., Irshad M., Ul-Haq J., Abbas S. Cyber security threats: A never-ending challenge for e-commerce. *Frontiers in Psychology*, 2022. Vol. 13, 927398. DOI: 10.3389/fpsyg.2022.927398.
- 81.Liu Zhiwei, Dou Yingtong, Yu Philip, deng Yutong, Peng Hao. Alleviating the Inconsistency Problem of Applying Graph Neural Network to Fraud Detection. *Proceedings of the 43rd International ACM SIGIR Conference on Research and Development in Information Retrieval (SIGIR '20)*. Association for Computing Machinery, New York, NY, USA, 2020. Pp. 1569–1572. DOI: 10.1145/3397271.3401253.
- 82.Logging & Monitoring: definitions and best practices. URL: <https://www.vaadata.com/blog/logging-monitoring-definitions-and-best-practices/>. (дата звернення: 21.11.2025)
- 83.Maosa H., Ouazzane K., Ghanem M. C. A Hierarchical Security Event Correlation Model for Real-Time Threat Detection and Response. *Network*. 2024. Vol. 4, No. 1. P. 68-90. DOI: 10.3390/network4010004.
- 84.Marky K., Ragozin K., Chernyshov G., Matviienko A., Schmitz M., Mühlhäuser M., Eghtebas C., Kunze K. “Nah, it’s just annoying!” A Deep Dive into User Perceptions of Two-Factor Authentication. *ACM Trans. Comput.-Hum. Interact.* 2022. Vol. 29, 5, Article 43. DOI: [10.1145/3503514](https://doi.org/10.1145/3503514)
- 85.Marović I., Šopić M., Jurčević M., Radojčić R. Making Informed Choices: AHP and SAW for Optimal Formwork System Selection. *Information*, 2025. Vol. 16 (10), 873. DOI: [10.3390/info16100873](https://doi.org/10.3390/info16100873)
- 86.Matbouli H., Gao Q. An overview on web security threats and impact to e-commerce success. *International Conference on Information Technology and e-Services*, 2012. Pp. 1-6. DOI: 10.1109/ICITeS.2012.6216645.
- 87.Mayer N., Aubert J., Grandry E., Feltus C., Goettelmann E., Wieringa R. An integrated conceptual model for information system security risk management supported by enterprise architecture management. *Software & systems modeling*. 2019. Vol. 18, no. 3. P. 2285–2312. DOI: [10.1007/s10270-018-0661-x](https://doi.org/10.1007/s10270-018-0661-x).

- 88.Milov O., Voitko A., Husarova I., Domaskin O., Ivanchenko Ye., Ivanchenko I., Korol O., Kots H., Opirskyy I., Frazee-Frazenko O. Development of methodology for modeling the interaction of antagonistic agents in cybersecurity systems. *Eastern-European Journal of Enterprise Technologies*. 2019. Vol. 2. Pp. 56-66. DOI: 10.15587/1729-4061.2019.164730.
- 89.Mutemi Abed, Bação Fernando. E-Commerce Fraud Detection Based on Machine Learning Techniques: Systematic Literature Review. *Big Data Mining and Analytics*. 2024. Vol. 7. Pp. 419-444. DOI: 10.26599/BDMA.2023.9020023.
- 90.Naidu N. Logging and monitoring, the essential holistic view of the systems we build!. URL: <https://www.linkedin.com/pulse/logging-monitoring-essential-holistic-view-systems-we-nayan-naidu>. (дата звернення: 26.11.2025)
- 91.Nicholls M. Top 5 penetration testing methodologies. URL: <https://www.redscan.com/news/top-five-penetration-testing-methodologies>. (дата звернення: 21.01.2026)
- 92.Otieno E. A. Data protection and privacy in e-commerce environment. *GSC Advanced Research and Reviews*, 2025. Vol. 22(01). Pp. 238-271. DOI: 10.30574/gscarr.2025.22.1.0024
- 93.OWASP. Explore the world of cyber security. URL: <https://owasp.org/> (дата звернення: 28.11.2025)
- 94.OWASP. WSTG - v4.2. URL: <https://owasp.org/www-project-web-security-testing-guide/v42/> (дата звернення: 21.11.2025)
- 95.Palko D., Babenko T., Bigdan A., Kiktev N., Hutsol T., Kuboń M., Hnatiienko H., Tabor S., Gorbovy O., Borusiewicz A. Cyber security risk modeling in distributed information systems. *Applied sciences*. 2023. Vol. 13, no. 4. P. 2393. DOI: [10.3390/app13042393](https://doi.org/10.3390/app13042393).
- 96.Pendleton M., Garcia-Lebron R., Cho J.-H., Xu S. A Survey on Systems Security Metrics. *ACM Comput. Surv.* 2016. Vol. 49, 4. Article 62 DOI: [10.1145/3005714](https://doi.org/10.1145/3005714)

97. Philippou Eleni, Frey Sylvain, Rashid Awais. Contextualising and aligning security metrics and business objectives: A GQM-based methodology, *Computers & Security*, 2020. Vol. 88, 101634. DOI: [10.1016/j.cose.2019.101634](https://doi.org/10.1016/j.cose.2019.101634).
98. Puccinelli N.M., Goodstein R.C., Grewal D., Price R., Raghubir P., Stewart D. Customer Experience Management in Retailing: Understanding the Buying Process. *Journal of Retailing*, 2009. Vol. 85(1). Pp. 15-30. DOI: 10.1016/j.jretai.2008.11.003
99. Qiu L., Li J. Covering the Monitoring Network: A Unified Framework to Protect E-Commerce Security. *Complexity*. 2017. 6254842. DOI: 10.1155/2017/6254842.
100. Radware. WAF vs. Firewall: Web Application & Network Firewalls. URL: <https://www.radware.com/cyberpedia/application-security/waf-vs-firewall-comparison-and-differences/>. (дата звернення: 21.11.2025)
101. Rajapakse R. N., Zahedi M., Babar M. A., Shen H. Challenges and solutions when adopting DevSecOps: A systematic review. *Information and Software Technology*. 2022. Vol. 141. P. 106700. DOI: 10.1016/j.infsof.2021.106700.
102. Rencelj Ling E., Ekstedt M. A threat modeling language for generating attack graphs of substation automation systems. *International journal of critical infrastructure protection*. 2023. Vol. 41. P. 100601. DOI: [10.1016/j.ijcip.2023.100601](https://doi.org/10.1016/j.ijcip.2023.100601).
103. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture. NIST Special Publication 800-207. 2020. DOI: 10.6028/NIST.SP.800-207.
104. Roy B. Multicriteria Methodology for Decision Aiding. New York : Springer, 1996. 293 p. DOI:10.1007/978-1-4757-2500-1.
105. Ryu D., Lee S., Yang S., Jeong J., Lee Y., Shin D. Enhancing Cybersecurity in Energy IT Infrastructure Through a Layered Defense Approach to Major Malware Threats. *Applied Sciences*, 2024. Vol. 14 (22), 10342. DOI: [10.3390/app142210342](https://doi.org/10.3390/app142210342)

106. Saaty T.L. Decision Making for Leaders: The Analytic Hierarchy Process for Decisions in a Complex World. RWS Publications, Pittsburgh. 2001.
107. Saaty T.L., Vargas L.G. The Seven Pillars of the Analytic Hierarchy Process. *Models, Methods, Concepts & Applications of the Analytic Hierarchy Process. International Series in Operations Research & Management Science*, 2001. Vol. 34. Springer, Boston, MA. DOI: 10.1007/978-1-4615-1665-1_2
108. Saini K. What Is Data Encryption: Algorithms, Methods and Techniques. URL: <https://www.simplilearn.com/data-encryption-methods-article>. (дата звернення: 21.11.2022)
109. Sajeesh S., Singh A., Bhardwaj P. Optimal checkout strategies for online retailers. *Journal of Retailing*, 2022. Vol. 98 (3). Pp. 378-394. DOI: [10.1016/j.jretai.2021.06.001](https://doi.org/10.1016/j.jretai.2021.06.001)
110. Security and Privacy Controls for Information Systems and Organizations. DOI: 10.6028/NIST.SP.800-53r5
111. Sheeraz Muhammad, Paracha Muhammad, Ulhaq Mansoor, Durad Hanif, Mohsin Syed Muhammad, S. Band Shahab, Mosavi Amir. Effective Security Monitoring Using Efficient SIEM Architecture. *Human-centric Computing and Information Sciences*. 2023. Vol. 13. DOI: 10.22967/HCIS.2023.13.023.
112. Sheldon F.T., Abercrombie R. K., Mili A. Evaluating security controls based on key performance indicators and stakeholder mission. *Proceedings of the 4th annual workshop on Cyber security and information intelligence research: developing strategies to meet the cyber security and information intelligence challenges ahead (CSIIRW '08)*. Association for Computing Machinery, New York, NY, USA, 2008. Article 41. DOI: 1413140.1413188
113. Spring J., Hatleback E., Householder A., Manion A., Shick D. Prioritizing vulnerability response: A stakeholder-specific vulnerability categorization (version 1.1). *Workshop on the Economics of Information Security*. 2020. URL: <https://weis2020.econinfosec.org/wp-content/uploads/sites/8/2020/06/weis20-final6.pdf> (дата звернення: 21.11.2022)

114. Stadnik W., Nowak Z. The Impact of Web Pages' Load Time on the Conversion Rate of an E-Commerce Platform. *Information Systems Architecture and Technology: Proceedings of 38th International Conference on Information Systems Architecture and Technology – ISAT 2017. ISAT 2017. Advances in Intelligent Systems and Computing*, 2018. Vol. 655. Springer, Cham. DOI: [10.1007/978-3-319-67220-5_31](https://doi.org/10.1007/978-3-319-67220-5_31)
115. Stallings W. Cryptography and network security: principles and practice. 2020. URL: https://www.uoitc.edu.iq/images/documents/informatics-institute/Competitive_exam/Cryptography_and_Network_Security.pdf (дата звернення: 21.11.2022)
116. Sundar Venkatesh. How does a WAF work? *Indusface*. URL: <https://www.indusface.com/blog/how-web-application-firewall-works/>. (дата звернення: 20.03.2025)
117. Tanenbaum A. S., Wetherall D. J. Computer networks. Pearson Education, Limited, 2010. 960 p.
118. Tavana M., Soltanifar M., Santos-Arteaga F. J. Analytical hierarchy process: revolution and evolution. *Annals of Operations Research*. 2023. Vol. 326. Pp. 879–907. DOI: 10.1007/s10479-021-04432-2.
119. Tax N., Medvet E., Bäck T., Risi S., Looije D. Machine Learning for Fraud Detection in E-Commerce: A Research Agenda. *Deployable Machine Learning for Security Defense. MLHat 2021. Communications in Computer and Information Science*, Vol. 1482. Springer, Cham. Pp. 30-54. DOI: 10.1007/978-3-030-87839-9_2
120. The CORAS Method. URL: <https://coras.sourceforge.net/>. (дата звернення: 20.01.2026)
121. Threat Modeling aExplained: Definition, Benefits, and Best Practices. URL: <https://www.synopsys.com/glossary/what-is-threat-modeling.html>. (дата звернення: 20.01.2026)
122. Tueanrat Y., Papagiannidis S., Alamanos E. A conceptual framework of the antecedents of customer journey satisfaction in omnichannel retailing.

- Journal of Retailing and Consumer Services*, 2021. Vol. 61, 102517. DOI: 10.1016/j.jretconser.2021.102517
123. Vielberth Manfred, Böhm Fabian, Fichtinger Ines, Pernul Günther. Security Operations Center: A Systematic Study and Open Challenges. *IEEE Access*. 2020. Vol. 8. Pp. 227756-227779. DOI: 10.1109/ACCESS.2020.3045514.
 124. Wai E., Lee C.K.M. Depth in Defense: A Multi-layered Approach to Cybersecurity for SCADA Systems in Industry 4.0. *Science and Technology - Recent Updates and Future Prospects*, 2024. Vol. 2. Pp. 124-144. DOI: 10.9734/bpi/strufp/v2
 125. Wen Y., Zhou C., Ma J., Liu K. Research on E-Commerce Security Issues. *Proceedings of the 2008 International Seminar on Business and Information Management - Volume 01 (ISBIM '08)*. IEEE Computer Society, USA, 2008. Pp. 186-189. DOI: 10.1109/ISBIM.2008.168.
 126. What is a next-generation firewall? URL: <https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-next-generation-firewall.html>. (дата звернення: 20.01.2026)
 127. What is a VPN? How vpns work and why you should use one. URL: <https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-vpn>. (дата звернення: 20.01.2026)
 128. What is an intrusion detection system? URL: <https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-detection-system-ids>. (дата звернення: 20.01.2026)
 129. What is next generation firewall (NGFW)? – 2025 Guide. URL: <https://www.sangfor.com/glossary/cybersecurity/what-is-next-generation-firewall-ngfw>. (дата звернення: 20.01.2026)
 130. WSTG – latest. URL: https://owasp.org/www-project-web-security-testing-guide/latest/3-The_OWASP_Testing_Framework/1-Penetration_Testing_Methodologies. (дата звернення: 20.01.2026)

131. Wunder J., Kurtz A., Eichenmüller C., Gassmann F., Benenson Z. Shedding Light on CVSS Scoring Inconsistencies: A User-Centric Study on Evaluating Widespread Security Vulnerabilities. *2024 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2024*. Pp. 1102-1121. DOI: 10.1109/SP54263.2024.00058
132. Yoachimik O., Pacheco J. DDoS threat report for 2023 Q4. URL: <https://blog.cloudflare.com/ddos-threat-report-2023-q4>. (дата звернення: 20.01.2026)
133. Zhang C., Zhang Y., Li F. Feature Extraction of Sequence of Keystrokes in Fixed Text Using the Multivariate Hawkes Process. *Mathematical Problems in Engineering*. 2021. Vol. 2021. 6648726. DOI: [10.1155/2021/6648726](https://doi.org/10.1155/2021/6648726).
134. Zhang Y., Deng X., Wei D., Deng Y. Assessment of E-Commerce security using AHP and evidential reasoning. *Expert Systems with Applications*, 2012. Vol. 39 (3). Pp. 3611–3623. DOI: 10.1016/j.eswa.2011.09.051
135. Zhang Z., Yin H., Rao S.X., Yan X., Wang Z., Liang W., Zhao Y., Shan Y., Zhang R., Lin Y., Jiang J. Identifying E-Commerce Fraud Through User Behavior Data: Observations and Insights. *Data Science and Engineering*, 2025. Vol. 10. Pp. 24–39. DOI: [10.1007/s41019-024-00275-6](https://doi.org/10.1007/s41019-024-00275-6).
136. Zhou B., Sun B., Zang T., Cai Y., Wu J., Luo H.. Security Risk Assessment Approach for Distribution Network Cyber Physical Systems Considering Cyber Attack Vulnerabilities. *Entropy*, 2023. Vol. 25 (1), 47. DOI: [10.3390/e25010047](https://doi.org/10.3390/e25010047)

Додатки

Додаток А

Лістинги програмного коду

main.py

```
import json
import os
from datetime import datetime

from modules.validation import validate_input
from modules.indicators import calculate_all, calculate_per_stage
from modules.index import calculate_all_indexes
from modules.recommendations import determine_status, prioritize,
generate_report

def load_thresholds(path="config/thresholds.json"):
    with open(path, encoding="utf-8") as f:
        return json.load(f)

def save_result(result, output_dir="data/output",
history_dir="data/history", tag=None):
    os.makedirs(output_dir, exist_ok=True)
    os.makedirs(history_dir, exist_ok=True)

    output_path = os.path.join(output_dir, "result.json")
    with open(output_path, "w", encoding="utf-8") as f:
        json.dump(result, f, indent=4, ensure_ascii=False)

    if tag:
        history_path = os.path.join(history_dir,
f"result_{tag}.json")
    else:
        ts = datetime.now().strftime("%Y-%m-%d_%H-%M-%S")
        history_path = os.path.join(history_dir,
f"result_{ts}.json")
    with open(history_path, "w", encoding="utf-8") as f:
        json.dump(result, f, indent=4, ensure_ascii=False)

    return output_path, history_path

def run_analysis(input_path="data/input/test_normal.json",
config_path="config/settings.json"):

    if not os.path.exists(input_path):
```

```

        print(f"No input data found: {input_path}")
        return None
    if not os.path.exists(config_path):
        print(f"No config found: {config_path}")
        return None

    validated = validate_input(input_path, config_path)
    if validated["warnings"]:
        print("Warnings:")
        for w in validated["warnings"]:
            print(f"    - {w}")

    stages = validated["stages"]
    cfg = validated["config"]
    unique_sessions = validated["unique_sessions"]
    print(f"Unique sessions: {unique_sessions}")

    indicators = calculate_all(stages, cfg["K"],
cfg["action_weights"])
    per_stage = calculate_per_stage(stages, cfg["K"],
cfg["action_weights"])
    print(f"Indicators:
P1={indicators['P1']},
P2={indicators['P2']},
P3={indicators['P3']},
P4={indicators['P4']}")

    indexes = calculate_all_indexes(indicators, cfg["W"],
cfg["context"]["f_T"], cfg["context"]["f_B"])
    print(f"iez={indexes['iez']},
(ksc={indexes['kcs']})")

    thresholds = load_thresholds()
    status_results = determine_status(indicators, thresholds)
    priority_list = prioritize(status_results,
cfg["context"]["f_T"], cfg["context"]["f_B"], thresholds)
    report = generate_report(status_results, priority_list,
indexes, validated["period"], cfg["context"])

    print(f"\nRecommendations:
{report['summary']['total_recommendations']}")
    for rec in report["recommendations"]:
        print(f"
[{rec['priority_label']}]
{rec['indicator_name']}: {rec['value']} ({rec['status']}")

    result = {
        "period": validated["period"],
        "unique_sessions": unique_sessions,
        "indicators": indicators,
        "per_stage": per_stage,
        "indexes": indexes,

```

```

        "recommendations": report,
        "analyzed_at": datetime.now().strftime("%Y-%m-%dT%H:%M:%SZ"),
    }

```

```

    tag = os.path.splitext(os.path.basename(input_path))[0]
    output_path, history_path = save_result(result, tag=tag)
    print(f"\nResults saved to: {output_path}")
    print(f"History saved to: {history_path}")

    return result

```

```

def run_all_inputs(input_dir="data/input",
config_path="config/settings.json"):
    import glob
    files = sorted(glob.glob(os.path.join(input_dir, "*.json")))
    if not files:
        print(f"No input files found in {input_dir}")
        return []

    results = []
    for f in files:
        print(f"\n{'=' * 60}")
        print(f"  Analyzing: {os.path.basename(f)}")
        print(f"{'=' * 60}")

        with open(f, encoding="utf-8") as fh:
            input_data = json.load(fh)
            ctx = input_data.get("metadata", {}).get("context")

        if ctx:
            with open(config_path, encoding="utf-8") as cfh:
                cfg = json.load(cfh)
                cfg["context"] = ctx
            with open(config_path, "w", encoding="utf-8") as cfh:
                json.dump(cfg, cfh, indent=4, ensure_ascii=False)

        r = run_analysis(f, config_path)
        if r:
            results.append(r)

    print(f"\n{'=' * 60}")
    print(f"  Analyzed {len(results)} files")
    print(f"{'=' * 60}")
    return results

if __name__ == "__main__":
    import sys

```

```
if len(sys.argv) > 1:
    result = run_analysis(sys.argv[1])
else:
    run_all_inputs()

print("\nStarting web interface...")
from web.app import app
app.run(debug=True, port=5000)
```

validation.py

```

import json
import os

stage_keys = ["e1_landing", "e2_catalog", "e3_search", "e4_product",
              "e5_cart", "e6_checkout", "e7_payment"]
action_keys = ["block", "challenge", "flag", "allow"]

def validate_input(input_path, config_path):
    warnings = []

    if not os.path.exists(input_path):
        raise ValueError(f"File not found: {input_path}")
    with open(input_path) as f:
        data = json.load(f)

    if "period" not in data or "stages" not in data:
        raise ValueError("Input must have 'period' and 'stages'")

    if "start" not in data["period"] or "end" not in data["period"]:
        raise ValueError("'period' must have 'start' and 'end'")

    stages = {}
    for key in stage_keys:
        if key not in data["stages"]:
            raise ValueError(f"Missing stage: {key}")

        s = data["stages"][key]

        for field in ("N", "TP", "FP", "FN"):
            if not isinstance(s.get(field), int) or s[field] < 0:
                raise ValueError(f"{key}: '{field}' must be a non-
negative integer")

        if "actions" not in s:
            raise ValueError(f"{key}: missing 'actions'")
        for action in action_keys:
            if not isinstance(s["actions"].get(action), int) or
s["actions"][action] < 0:
                raise ValueError(f"{key}: action '{action}' must be
a non-negative integer")

        if s["TP"] + s["FP"] + s["FN"] > s["N"]:
            raise ValueError(f"{key}: TP + FP + FN exceeds N")

        tn = s["N"] - s["TP"] - s["FP"] - s["FN"]
        if tn < 0:
            warnings.append(f"{key}: TN was negative, set to 0")
            tn = 0

```

```

        stages[key] = {"N": s["N"], "TP": s["TP"], "FP": s["FP"],
"FN": s["FN"], "TN": tn, "actions": dict(s["actions"])}

    if not os.path.exists(config_path):
        raise ValueError(f"Config not found: {config_path}")
    with open(config_path) as f:
        cfg = json.load(f)

    K = cfg["stage_weights"]["K"]
    W = cfg["indicator_weights"]["W"]

    if len(K) != 7 or abs(sum(K) - 1.0) > 0.01:
        raise ValueError("K must have 7 values summing to 1.0")
    if len(W) != 4 or abs(sum(W) - 1.0) > 0.01:
        raise ValueError("W must have 4 values summing to 1.0")

    f_T = cfg["context"]["f_T"]
    f_B = cfg["context"]["f_B"]
    context_label = cfg["context"]["context_label"]

    if f_T < 0 or f_T > 1.0:
        warnings.append(f"f_T={f_T} out of range [0, 1.0]")
        f_T = max(0, min(1.0, f_T))
    if f_B < 0:
        warnings.append(f"f_B={f_B} negative, setting to 0")
        f_B = 0

    unique_sessions = stages["e1_landing"]["N"]

    return {
        "period": data["period"],
        "stages": stages,
        "unique_sessions": unique_sessions,
        "config": {
            "K": K,
            "W": W,
            "action_weights": cfg["action_weights"],
            "context": {"f_T": f_T, "f_B": f_B, "context_label":
context_label}
        },
        "warnings": warnings
    }

```

Indicators.py

```
stage_keys = ["e1_landing", "e2_catalog", "e3_search", "e4_product",
              "e5_cart", "e6_checkout", "e7_payment"]
```

```
def calculate_p1(stages):
    tp_total = 0
    fn_total = 0
    for key in stage_keys:
        tp_total += stages[key]["TP"]
        fn_total += stages[key]["FN"]

    if tp_total + fn_total == 0:
        return 1.0
    return tp_total / (tp_total + fn_total)
```

```
def calculate_p2(stages, K):
    p2 = 0.0
    for j, key in enumerate(stage_keys):
        fp = stages[key]["FP"]
        tn = stages[key]["TN"]
        if fp + tn == 0:
            fpr = 0.0
        else:
            fpr = fp / (fp + tn)
        p2 += K[j] * (1 - fpr)
    return p2
```

```
def calculate_p3(stages, K, action_weights):
    p3 = 0.0
    w_min = 1 # allow
    w_max = 4 # block
    for j, key in enumerate(stage_keys):
        actions = stages[key]["actions"]
        n_block = actions["block"]
        n_challenge = actions["challenge"]
        n_flag = actions["flag"]
        n_allow = actions["allow"]
        n_total = n_block + n_challenge + n_flag + n_allow

        if n_total == 0:
            m = 1.0
        else:
            w_avg = (action_weights["block"] * n_block +
                    action_weights["challenge"] * n_challenge +
                    action_weights["flag"] * n_flag +
                    action_weights["allow"] * n_allow) / n_total
            m = 1 - (w_avg - w_min) / (w_max - w_min)

        p3 += K[j] * m
```

```

return p3

def calculate_p4(stages, K):
    p4 = 0.0
    for j, key in enumerate(stage_keys):
        actions = stages[key]["actions"]
        n_total = actions["block"] + actions["challenge"] +
actions["flag"] + actions["allow"]
        g = 1 if n_total > 0 else 0
        p4 += K[j] * g
    return p4

def calculate_per_stage(stages, K, action_weights):
    w_min = 1
    w_max = 4
    per_stage = {}

    for j, key in enumerate(stage_keys):
        s = stages[key]
        fp = s["FP"]
        tn = s["TN"]
        fpr = fp / (fp + tn) if (fp + tn) > 0 else 0.0
        p2_val = round(K[j]*(1 - fpr), 4)

        actions = s["actions"]
        n_total = actions["block"] + actions["challenge"] +
actions["flag"] + actions["allow"]
        if n_total == 0:
            p3_val = 1.0
        else:
            w_avg = (action_weights["block"] * actions["block"] +
action_weights["challenge"] *
actions["challenge"] +
action_weights["flag"] * actions["flag"] +
action_weights["allow"] * actions["allow"]) /
n_total
            p3_val = round(K[j]*(1 - (w_avg - w_min) / (w_max -
w_min)), 4)

        p4_val = 1 if n_total > 0 else 0
        per_stage[key] = {
            "K": K[j],
            "P2": p2_val,
            "P3": p3_val,
            "P4": p4_val,
        }

    return per_stage

def calculate_all(stages, K, action_weights):

```

```
return {  
    "P1": round(calculate_p1(stages), 4),  
    "P2": round(calculate_p2(stages, K), 4),  
    "P3": round(calculate_p3(stages, K, action_weights), 4),  
    "P4": round(calculate_p4(stages, K), 4),  
}
```

index.py

```

def calculate_iez(indicators, W):
    keys = ["P1", "P2", "P3", "P4"]
    iez = 0.0
    for i, key in enumerate(keys):
        iez += W[i] * indicators[key]
    return round(iez, 4)

def calculate_kcs (f_T, f_B):
    return round(f_T * f_B, 4)

def calculate_iez_k(iez, kcs):
    delta = 1 - iez
    iez_k = max(0, 1 - kcs * delta)
    return round(iez_k, 4)

def calculate_all_indexes(indicators, W, f_T, f_B):
    iez = calculate_iez(indicators, W)
    kcs = calculate_kcs(f_T, f_B)
    iez_k = calculate_iez_k(iez, cm)
    return {
        "iez": iez,
        "kcs ": kcs,
        "iez_k": iez_k,
        "f_T": f_T,
        "f_B": f_B,
    }

```

app.py

```

import json
import os
from flask import Flask, render_template, request
import plotly
import plotly.graph_objects as go

app = Flask(__name__)

data_output = os.path.join(os.path.dirname(os.path.dirname(__file__)), "data", "output")
data_history = os.path.join(os.path.dirname(os.path.dirname(__file__)), "data", "history")

colors = {
    "primary": "#1B2A4A",
    "secondary": "#2D4A7A",
    "accent": "#3B7DD8",
    "success": "#0D7C5F",
    "warning": "#C4841D",
    "danger": "#B83230",
    "muted": "#6B7B8D",
    "light": "#E8ECF1",
    "bg": "#F4F6F9",
}

chart_layout = dict(
    template="plotly_white",
    font=dict(family="Inter, -apple-system, sans-serif", size=13,
color=colors["primary"]),
    paper_bgcolor="rgba(0,0,0,0)",
    plot_bgcolor="rgba(0,0,0,0)",
    margin=dict(t=60, b=50, l=60, r=30),
    title_font=dict(size=16, color=colors["primary"]),
    legend=dict(orientation="h", yanchor="bottom", y=1.02,
xanchor="right", x=1),
)

def load_latest_result():
    path = os.path.join(data_output, "result.json")
    if not os.path.exists(path):
        return None
    with open(path, encoding="utf-8") as f:
        return json.load(f)

def load_history():
    if not os.path.exists(data_history):
        return []
    files = sorted(

```

```

        [f for f in os.listdir(data_history) if
f.endswith(".json")],
        reverse=True,
    )
    results = []
    for fname in files:
        path = os.path.join(data_history, fname)
        with open(path, encoding="utf-8") as f:
            data = json.load(f)
            data["_filename"] = fname
            results.append(data)
    return results

def color_for_value(value):
    if value >= 0.80:
        return colors["success"]
    elif value >= 0.60:
        return colors["warning"]
    return colors["danger"]

def make_plotly_div(fig):
    return plotly.offline.plot(fig, output_type="div",
include_plotlyjs=False)

def scalar_value(value, index=None):
    if isinstance(value, list):
        if len(value) == 0:
            return 0.0
        if index is not None and len(value) == len(stage_keys):
            return float(value[index])
        return float(value[0])
    return float(value)

@app.route("/")
def dashboard():
    records = load_history()
    if not records:
        return render_template("dashboard.html", result=None)

    idx = request.args.get("index", 0, type=int)
    idx = max(0, min(idx, len(records) - 1))
    result = records[idx]

    return render_template(
        "dashboard.html",
        result=result,
        color_for_value=color_for_value,
        current_index=idx,
        total=len(records),
    )

```

```

stage_labels = {
    "e1_landing": "Стартова сторінка (E1)",
    "e2_catalog": "Перегляж каталогу (E2)",
    "e3_search": "Пошук (E3)",
    "e4_product": "Перегляд товару (E4)",
    "e5_cart": "Додавання в кошик (E5)",
    "e6_checkout": "Оформлення замовлення (E6)",
    "e7_payment": "Оплата замовлення (E7)",
}
stage_keys = list(stage_labels.keys())

@app.route("/details")
def details():
    records = load_history()
    if not records:
        return render_template("details.html", result=None,
charts={})

    idx = request.args.get("index", 0, type=int)
    idx = max(0, min(idx, len(records) - 1))
    result = records[idx]

    ind = result["indicators"]
    per_stage = result.get("per_stage", {})

for j, key in enumerate(stage_keys):
    if key in per_stage:
        per_stage[key]["K"] = scalar_value(per_stage[key].get("K"), j)
        per_stage[key]["P2"] = scalar_value(per_stage[key].get("P2"), j)
        per_stage[key]["P3"] = scalar_value(per_stage[key].get("P3"), j)
        per_stage[key]["P4"] = scalar_value(per_stage[key].get("P4"), j)

charts = {}

    keys = ["P1", "P2", "P3", "P4"]
    names = ["П1 Виявлення", "П2 Взаємодія", "П3 Реагування", "П4
Покриття"]
    values = [ind[k] for k in keys]
    bar_colors = [colors["accent"], colors["secondary"],
colors["warning"], colors["success"]]

    fig = go.Figure()
    fig.add_trace(go.Bar(
        x=names, y=values, marker_color=bar_colors,
        text=[f"{v:.4f}" for v in values], textposition="none",
        width=0.3,
        marker_line=dict(width=0),
    ))
    for level, color in [
        (0.90, colors["success"]),
        (0.80, colors["warning"]),
        (0.70, "#D4652A"),

```

```

        (0.60, colors["danger"]),
    ]:
        fig.add_hline(y=level, line_dash="dot", line_color=color,
line_width=1.5)
        annotations = []
        for i, (name, val) in enumerate(zip(names, values)):
            annotations.append(dict(
                x=name, y=-0.18, xref="x", yref="paper",
                text=f"<b>{val:.4f}</b>",
                showarrow=False,
                font=dict(size=14, color=color_for_value(val)),
            ))
        fig.update_layout(
            **chart_layout,
            title="Показники ефективності П1-П4",
            yaxis_range=[0, 1.15],
            height=480,
            yaxis=dict(gridcolor=colors["light"], gridwidth=1,
title="Значення"),
            xaxis=dict(title=""),
            bargap=0.3,
            showlegend=False,
            annotations=annotations,
        )
        fig.update_layout(margin=dict(b=100))
        charts["indicators"] = make_plotly_div(fig)

if per_stage:
    stage_names = [stage_labels[k] for k in stage_keys]
    p2_vals = [per_stage[k]["P2"] for k in stage_keys]
    p3_vals = [per_stage[k]["P3"] for k in stage_keys]
    p4_vals = [per_stage[k]["P4"] for k in stage_keys]
    k_vals = [per_stage[k]["K"] for k in stage_keys]

    fig2 = go.Figure()
    fig2.add_trace(go.Bar(
        name="П2 (взаємодія)", x=stage_names, y=p2_vals,
        marker_color=colors["secondary"], width=0.22,
    ))
    fig2.add_trace(go.Bar(
        name="П3 (якість дій)", x=stage_names, y=p3_vals,
        marker_color=colors["warning"], width=0.22,
    ))
    fig2.add_trace(go.Bar(
        name="П4 (покриття)", x=stage_names, y=p4_vals,
        marker_color=colors["success"], width=0.22,
    ))
    fig2.add_trace(go.Scatter(
        name="Значення К", x=stage_names, y=k_vals,
        mode="lines+markers", yaxis="y2",
        line=dict(color=colors["danger"], width=2, dash="dot"),
        marker=dict(size=8),
    ))

```

```

    ))
    layout2 = dict(chart_layout)
    layout2["legend"] = dict(orientation="h", yanchor="bottom",
y=1.02, xanchor="center", x=0.5)
    fig2.update_layout(
        **layout2,
        title=" ",
        barmode="group",
        height=480,
        yaxis=dict(title="Значення показника", range=[0, 1.15],
                    gridcolor=colors["light"], gridwidth=1),
        yaxis2=dict(title="Bara          К", overlaying="y",
side="right",
                    range=[0, 0.5], showgrid=False),
        xaxis=dict(title=""),
    )
    charts["per_stage"] = make_plotly_div(fig2)

    return render_template(
        "details.html",
        result=result,
        charts=charts,
        per_stage=per_stage,
        stage_labels=stage_labels,
        stage_keys=stage_keys,
        color_for_value=color_for_value,
        current_index=idx,
        total=len(records),
    )

@app.route("/history")
def history():
    records = load_history()
    chart_div = ""

    if len(records) >= 2:
        ordered = list(reversed(records))
        dates = [r.get("period", {}).get("start",
r.get("analyzed_at", r["_filename"]))[:10] for r in ordered]

        fig = go.Figure()
        line_styles = [
            ("iez", "ІЕЗ", colors["primary"], "solid", 3),
            ("P1", "П1 Виявлення", colors["accent"], "dash", 2),
            ("P2", "П2 Взаємодія", colors["secondary"], "dash", 2),
            ("P3", "П3 Реагування", colors["warning"], "dash", 2),
            ("P4", "П4 Покриття", colors["success"], "dash", 2),
        ]
        for key, name, color, dash, width in line_styles:
            if key == "iez":
                vals = [r["indexes"]["iez"] for r in ordered]
            else:

```

```

        vals = [r["indicators"][key] for r in ordered]
    fig.add_trace(go.Scatter(
        x=dates, y=vals, mode="lines+markers", name=name,
        line=dict(color=color, dash=dash, width=width),
        marker=dict(size=7),
    ))

    fig.add_hline(y=0.90, line_dash="dot",
line_color=colors["muted"], line_width=1,
        annotation_text="Цільове значення (0.90)",
        annotation_font_size=10,
annotation_font_color=colors["muted"])
    fig.update_layout(**chart_layout, title="Динаміка
показників ефективності",
        yaxis_range=[0, 1.15], height=420,
        yaxis=dict(gridcolor=colors["light"],
gridwidth=1),
        xaxis=dict(gridcolor=colors["light"],
gridwidth=1))
    chart_div = make_plotly_div(fig)

    return render_template("history.html", records=records,
chart_div=chart_div)

```

settings.json

```

{
  "stage_weights": {
    "K": [
      0.055,
      0.05,
      0.057,
      0.069,
      0.115,
      0.257,
      0.397
    ],
    "labels": [
      "e1_landing",
      "e2_catalog",
      "e3_search",
      "e4_product",
      "e5_cart",
      "e6_checkout",
      "e7_payment"
    ]
  },
  "indicator_weights": {
    "W": [
      0.476,
      0.176,
      0.08,
      0.268
    ],
    "labels": [
      "P1_detection",
      "P2_interaction",
      "P3_response",
      "P4_coverage"
    ]
  },
  "action_weights": {
    "block": 4,
    "challenge": 3,
    "flag": 2,
    "allow": 1
  },
  "context": {
    "f_T": 0.6,
    "f_B": 1.0,
    "context_label": "Недостатний захист"
  }
}

```

thresholds.json

```
{
  "status_thresholds": {
    "excellent": 0.90,
    "good": 0.80,
    "satisfactory": 0.70,
    "unsatisfactory": 0.60
  },
  "target_value": 0.90,
  "priority_thresholds": {
    "critical": 0.30,
    "high": 0.20,
    "moderate": 0.10
  },
  "status_labels": {
    "excellent": "Відмінно",
    "good": "Добре",
    "satisfactory": "Задовільно",
    "unsatisfactory": "Незадовільно",
    "critical": "Критично"
  },
  "priority_labels": {
    "P1": "Критичний",
    "P2": "Високий",
    "P3": "Помірний",
    "P4": "Низький"
  }
}
```

attack.json

```

{
  "period": {
    "start": "2024-11-15T00:00:00Z",
    "end": "2024-11-15T23:59:59Z"
  },
  "stages": {
    "e1_landing": {
      "N": 53201,
      "TP": 3156,
      "FP": 3391,
      "FN": 1051,
      "actions": {
        "block": 3598,
        "challenge": 1440,
        "flag": 853,
        "allow": 656
      }
    },
    "e2_catalog": {
      "N": 41058,
      "TP": 1544,
      "FP": 3583,
      "FN": 575,
      "actions": {
        "block": 2821,
        "challenge": 1129,
        "flag": 664,
        "allow": 513
      }
    },
    "e3_search": {
      "N": 36406,
      "TP": 1755,
      "FP": 2820,
      "FN": 383,
      "actions": {
        "block": 2514,
        "challenge": 1006,
        "flag": 594,
        "allow": 461
      }
    },
    "e4_product": {
      "N": 27161,
      "TP": 873,
      "FP": 1851,
      "FN": 561,
      "actions": {
        "block": 1496,
        "challenge": 597,

```

```

        "flag": 355,
        "allow": 276
    }
},
    "e5_cart": {
        "N": 13783,
        "TP": 802,
        "FP": 1234,
        "FN": 333,
        "actions": {
            "block": 1118,
            "challenge": 446,
            "flag": 265,
            "allow": 207
        }
    },
    "e6_checkout": {
        "N": 8325,
        "TP": 291,
        "FP": 551,
        "FN": 150,
        "actions": {
            "block": 465,
            "challenge": 186,
            "flag": 108,
            "allow": 83
        }
    },
    "e7_payment": {
        "N": 5451,
        "TP": 301,
        "FP": 374,
        "FN": 93,
        "actions": {
            "block": 372,
            "challenge": 148,
            "flag": 88,
            "allow": 67
        }
    }
},
}

```

black_friday.json

```

{
  "period": {
    "start": "2024-11-30T00:00:00Z",
    "end": "2024-11-30T23:59:59Z"
  },
  "stages": {
    "e1_landing": {
      "N": 187161,
      "TP": 2380,
      "FP": 43710,
      "FN": 5301,
      "actions": {
        "block": 33186,
        "challenge": 5992,
        "flag": 4608,
        "allow": 2304
      }
    },
    "e2_catalog": {
      "N": 178848,
      "TP": 2163,
      "FP": 44896,
      "FN": 7365,
      "actions": {
        "block": 33881,
        "challenge": 6115,
        "flag": 4706,
        "allow": 2357
      }
    },
    "e3_search": {
      "N": 152477,
      "TP": 2651,
      "FP": 32099,
      "FN": 3463,
      "actions": {
        "block": 25022,
        "challenge": 4515,
        "flag": 3473,
        "allow": 1740
      }
    },
    "e4_product": {
      "N": 108545,
      "TP": 1425,
      "FP": 28367,
      "FN": 4159,
      "actions": {
        "block": 21451,
        "challenge": 3871,

```

```

        "flag": 2980,
        "allow": 1490
    }
},
    "e5_cart": {
        "N": 54960,
        "TP": 717,
        "FP": 14096,
        "FN": 1103,
        "actions": {
            "block": 10666,
            "challenge": 1925,
            "flag": 1482,
            "allow": 740
        }
    },
    "e6_checkout": {
        "N": 31136,
        "TP": 0,
        "FP": 0,
        "FN": 263,
        "actions": {
            "block": 0,
            "challenge": 0,
            "flag": 0,
            "allow": 0
        }
    },
    "e7_payment": {
        "N": 20853,
        "TP": 0,
        "FP": 0,
        "FN": 197,
        "actions": {
            "block": 0,
            "challenge": 0,
            "flag": 0,
            "allow": 0
        }
    }
}
}
}

```

result.json

```

{
  "period": {
    "start": "2025-10-06T00:00:00Z",
    "end": "2025-10-06T23:59:59Z"
  },
  "unique_sessions": 47608,
  "indicators": {
    "P1": 0.2277,
    "P2": 0.9911,
    "P3": 0.9002,
    "P4": 0.231
  },
  "per_stage": {
    "e1_landing": {
      "K": 0.055,
      "P2": 0.962,
      "P3": 0.5671,
      "P4": 1
    },
    "e2_catalog": {
      "K": 0.05,
      "P2": 0.9644,
      "P3": 0.5684,
      "P4": 1
    },
    "e3_search": {
      "K": 0.057,
      "P2": 0.9619,
      "P3": 0.5667,
      "P4": 1
    },
    "e4_product": {
      "K": 0.069,
      "P2": 0.9584,
      "P3": 0.5692,
      "P4": 1
    },
    "e5_cart": {
      "K": 0.115,
      "P2": 1.0,
      "P3": 1.0,
      "P4": 0
    },
    "e6_checkout": {
      "K": 0.257,
      "P2": 1.0,
      "P3": 1.0,
      "P4": 0
    },
    "e7_payment": {

```

```

        "K": 0.397,
        "P2": 1.0,
        "P3": 1.0,
        "P4": 0
    }
},
"indexes": {
    "iez": 0.4167,
    "kcs": 0.6,
    "iez_k": 0.65,
    "f_T": 0.6,
    "f_B": 1.0
},
"recommendations": {
    "period": {
        "start": "2025-10-06T00:00:00Z",
        "end": "2025-10-06T23:59:59Z"
    },
    "context_label": "Недостатній захист",
    "f_T": 0.6,
    "f_B": 1.0,
    "iez": 0.4167,
    "iez_k": 0.65,
    "recommendations": [
        {
            "indicator": "P1",
            "indicator_name": "Виявлення загроз",
            "value": 0.2277,
            "status": "Критично",
            "recommendation": "Термінова перевірка та втручання
у процесі реагування",
            "IPR": 0.4034,
            "priority": "P1",
            "priority_label": "Критичний"
        },
        {
            "indicator": "P4",
            "indicator_name": "Покриття захистом",
            "value": 0.231,
            "status": "Критично",
            "recommendation": "Термінова перевірка та втручання
у процесі реагування",
            "IPR": 0.4014,
            "priority": "P1",
            "priority_label": "Критичний"
        }
    ]
},
"summary": {
    "total_recommendations": 2,
    "P1_count": 2,
    "P2_count": 0,
    "P3_count": 0,
    "P4_count": 0,

```

```
        "indicators_ok": 2
    },
    "analyzed_at": "2025-05-25T02:51:29Z"
}
```

generate.py

```

import copy
import json
import os
import random
import shutil
import sys
from datetime import datetime, timedelta

BASE = os.path.join(os.path.dirname(__file__), "data",
                    "experiments")

def ensure_dir(path):
    os.makedirs(path, exist_ok=True)

def save_json(path, data):
    with open(path, "w", encoding="utf-8") as f:
        json.dump(data, f, indent=2, ensure_ascii=False)

def copy_files(src_dir, dst_dir):
    ensure_dir(dst_dir)
    for fname in sorted(os.listdir(src_dir)):
        if fname.endswith(".json"):
            shutil.copy2(os.path.join(src_dir, fname),
                        os.path.join(dst_dir, fname))

def generate_hourly_set(scenario, date_str, output_dir,
                        seed_prefix):
    random.seed(f"{seed_prefix}_{date_str}")
    ensure_dir(output_dir)

    start = datetime.strptime(date_str, "%Y-%m-%d")
    results = []

    for hour in range(24):
        period_start = start + timedelta(hours=hour)
        period_end = period_start + timedelta(minutes=59,
                                                seconds=59)

        data = generate_file(scenario, period_start, period_end)
        errors = validate_invariants(data)
        if errors:
            for e in errors:
                print(f"WARNING: {e}")

        fname = _filename_for_period(period_start, 60)
        save_json(os.path.join(output_dir, fname), data)

```

```

        results.append(data)

    return results

def low_detection():
    sc = copy.deepcopy(scenario_c1)
    sc["name"] = "low_detection"
    sc["security_profile"]["TP_pct"] = {
        "e1": 0.0005, "e2": 0.0004, "e3": 0.0003, "e4": 0.0004,
        "e5": 0.0005, "e6": 0.0008, "e7": 0.0010,
    }
    sc["security_profile"]["FN_pct"] = {
        "e1": 0.0015, "e2": 0.0010, "e3": 0.0010, "e4": 0.0015,
        "e5": 0.0015, "e6": 0.0020, "e7": 0.0020,
    }
    return sc

def high_fpr():
    sc = copy.deepcopy(scenario_c1)
    sc["name"] = "high_fpr"
    sc["security_profile"]["FP_pct"] = {
        "e1": 0.0072, "e2": 0.0056, "e3": 0.0056, "e4": 0.0056,
        "e5": 0.0080, "e6": 0.0104, "e7": 0.0128,
    }
    return sc

def aggressive():
    sc = copy.deepcopy(scenario_c1)
    sc["name"] = "aggressive"
    sc["security_profile"]["action_distribution"] = {
        "e1": {"block": 80, "challenge": 10, "flag": 7, "allow": 3},
        "e2": {"block": 80, "challenge": 10, "flag": 7, "allow": 3},
        "e3": {"block": 80, "challenge": 10, "flag": 7, "allow": 3},
        "e4": {"block": 85, "challenge": 8, "flag": 5, "allow": 2},
        "e5": {"block": 85, "challenge": 8, "flag": 5, "allow": 2},
        "e6": {"block": 90, "challenge": 5, "flag": 3, "allow": 2},
        "e7": {"block": 90, "challenge": 5, "flag": 3, "allow": 2},
    }
    return sc

def no_coverage():
    sc = copy.deepcopy(scenario_c1)
    sc["name"] = "no_coverage"
    sc["security_profile"]["TP_pct"]["e6"] = 0.0
    sc["security_profile"]["TP_pct"]["e7"] = 0.0
    sc["security_profile"]["FP_pct"]["e6"] = 0.0
    sc["security_profile"]["FP_pct"]["e7"] = 0.0
    sc["security_profile"]["FN_pct"]["e6"] = 0.0020
    sc["security_profile"]["FN_pct"]["e7"] = 0.0030

```

```

return sc

scenario_c3_improved = copy.deepcopy(scenario_c3)
scenario_c3_improved["name"] = "c3_black_friday_improved"
scenario_c3_improved["security_profile"] = {
    "TP_pct": {
        "e1": 0.0029, "e2": 0.0024, "e3": 0.0021, "e4": 0.0023,
        "e5": 0.0038, "e6": 0.0052, "e7": 0.0065,
    },
    "FP_pct": {
        "e1": 0.0030, "e2": 0.0025, "e3": 0.0022, "e4": 0.0022,
        "e5": 0.0025, "e6": 0.0030, "e7": 0.0035,
    },
    "FN_pct": {
        "e1": 0.0006, "e2": 0.0005, "e3": 0.0005, "e4": 0.0006,
        "e5": 0.0007, "e6": 0.0009, "e7": 0.0012,
    },
    "action_distribution": {
15},      "e1": {"block": 18, "challenge": 32, "flag": 35, "allow":
15},      "e2": {"block": 18, "challenge": 32, "flag": 35, "allow":
15},      "e3": {"block": 18, "challenge": 32, "flag": 35, "allow":
15},      "e4": {"block": 20, "challenge": 35, "flag": 30, "allow":
15},      "e5": {"block": 22, "challenge": 35, "flag": 30, "allow":
13},      "e6": {"block": 25, "challenge": 35, "flag": 28, "allow":
12},      "e7": {"block": 30, "challenge": 35, "flag": 25, "allow":
10},    },
}

def gen_e01():
    exp_dir = os.path.join(BASE, "E01_indicator_verification")
    input_dir = os.path.join(exp_dir, "input")
    ensure_dir(input_dir)
    ensure_dir(os.path.join(exp_dir, "output"))
    ensure_dir(os.path.join(exp_dir, "charts"))

    date_str = scenario_c1["date"]
    start = datetime.strptime(date_str, "%Y-%m-%d")
    end = start + timedelta(hours=23, minutes=59, seconds=59)

    random.seed("E01_baseline")
    data = generate_file(scenario_c1, start, end)
    save_json(os.path.join(input_dir, "baseline_normal.json"),
data)

```

```

profiles = [
    ("low_detection", low_detection()),
    ("high_fpr", high_fpr()),
    ("aggressive", aggressive()),
    ("no_coverage", no_coverage()),
]
for name, scenario in profiles:
    random.seed(f"E01_{name}")
    data = generate_file(scenario, start, end)
    save_json(os.path.join(input_dir, f"{name}.json"), data)

    save_json(os.path.join(exp_dir, "config.json"),
generate_config_no_context())
    print(f" Done: {len(os.listdir(input_dir))} files")
def gen_e02():
    exp_dir = os.path.join(BASE, "E02_baseline_daily")
    input_dir = os.path.join(exp_dir, "input")
    ensure_dir(os.path.join(exp_dir, "output"))
    ensure_dir(os.path.join(exp_dir, "charts"))

    generate_hourly_set(scenario_c1, scenario_c1["date"],
input_dir, "E02_C1")

    save_json(os.path.join(exp_dir, "config_no_context.json"),
generate_config_no_context())
    save_json(os.path.join(exp_dir, "config_with_context.json"),
generate_config_with_context(1.0, "normal"))
    print(f" Done: {len(os.listdir(input_dir))} files")

def gen_e02_1():
    exp_dir = os.path.join(BASE, "E02_1_isolated_time_factor")
    input_dir = os.path.join(exp_dir, "input")
    ensure_dir(input_dir)
    ensure_dir(os.path.join(exp_dir, "output"))
    ensure_dir(os.path.join(exp_dir, "charts"))

    date_str = scenario_c1["date"]
    start = datetime.strptime(f"{date_str} 16:00", "%Y-%m-%d %H:%M")
    end = start + timedelta(minutes=59, seconds=59)
    random.seed("E04_base")
    base_data = generate_file(scenario_c1, start, end)

    variants = [
        ("same_events_night.json", 0.05),
        ("same_events_morning.json", 0.42),
        ("same_events_peak.json", 1.00),
    ]
    for fname, f_T in variants:
        data = copy.deepcopy(base_data)

```

```

        data["metadata"]["f_T"] = f_T
        save_json(os.path.join(input_dir, fname), data)

    save_json(os.path.join(exp_dir, "config.json"),
              generate_config_with_context(1.0, "normal"))
    print(f"   Done: 3 files")

def gen_e03():
    exp_dir = os.path.join(BASE, "E03_black_friday")
    dir_with = os.path.join(exp_dir, "input",
"with_classification")
    dir_without = os.path.join(exp_dir, "input",
"without_classification")
    ensure_dir(dir_with)
    ensure_dir(dir_without)
    ensure_dir(os.path.join(exp_dir, "output"))
    ensure_dir(os.path.join(exp_dir, "charts"))

    files = generate_hourly_set(scenario_c3, scenario_c3["date"],
dir_with, "E03_C3")

    for fname in sorted(os.listdir(dir_with)):
        if not fname.endswith(".json"):
            continue
        with open(os.path.join(dir_with, fname), encoding="utf-8")
as f:
            data = json.load(f)
            stripped = remove_classification(data)
            save_json(os.path.join(dir_without, fname), stripped)

    save_json(os.path.join(exp_dir, "config_no_context.json"),
generate_config_no_context())
    save_json(os.path.join(exp_dir, "config_with_context.json"),
              generate_config_with_context(2.5, "sale"))
    print(f"   Done: {len(files)} + {len(files)} files")

def gen_e04():
    exp_dir = os.path.join(BASE, "E04_ddos")
    input_dir = os.path.join(exp_dir, "input")
    ensure_dir(os.path.join(exp_dir, "output"))
    ensure_dir(os.path.join(exp_dir, "charts"))

    generate_hourly_set(scenario_c6, scenario_c6["date"],
input_dir, "E04_C6")

    save_json(os.path.join(exp_dir, "config_no_context.json"),
generate_config_no_context())
    save_json(os.path.join(exp_dir, "config_with_context.json"),
              generate_config_with_context(1.0, "normal"))
    print(f"   Done: {len(os.listdir(input_dir))} files")

```

```

def gen_e05():
    exp_dir = os.path.join(BASE, "E05_flash_sale")
    input_dir = os.path.join(exp_dir, "input")
    ensure_dir(input_dir)
    ensure_dir(os.path.join(exp_dir, "output"))
    ensure_dir(os.path.join(exp_dir, "charts"))

    date_str = scenario_c5["date"]
    random.seed(f"E05_C5_{date_str}")
    start = datetime.strptime(f"{date_str} 12:00", "%Y-%m-%d %H:%M")

    for i in range(12):
        period_start = start + timedelta(minutes=i * 15)
        period_end = period_start + timedelta(minutes=14,
seconds=59)
        data = generate_file(scenario_c5, period_start, period_end)
        fname = _filename_for_period(period_start, 15)
        save_json(os.path.join(input_dir, fname), data)

        save_json(os.path.join(exp_dir, "config_no_context.json"),
generate_config_no_context())
        save_json(os.path.join(exp_dir, "config_with_context.json"),
generate_config_with_context(2.0, "sale"))
        print(f" Done: {len(os.listdir(input_dir))} files")

def gen_e06():
    exp_dir = os.path.join(BASE, "E06_no_classification")
    input_dir = os.path.join(exp_dir, "input")
    ensure_dir(os.path.join(exp_dir, "output"))
    ensure_dir(os.path.join(exp_dir, "charts"))

    src = os.path.join(BASE, "E03_black_friday", "input",
"without_classification")
    copy_files(src, input_dir)

    save_json(os.path.join(exp_dir, "config.json"),
generate_config_with_context(2.5, "sale"))
    print(f" Done: {len(os.listdir(input_dir))} files copied")

def gen_e07():
    exp_dir = os.path.join(BASE, "E07_time_scale")
    input_dir = os.path.join(exp_dir, "input")
    ensure_dir(os.path.join(exp_dir, "output"))
    ensure_dir(os.path.join(exp_dir, "charts"))

    src = os.path.join(BASE, "E03_black_friday", "input",
"with_classification")
    copy_files(src, input_dir)

    save_json(os.path.join(exp_dir, "config.json"),
generate_config_with_context(2.5, "sale"))

```

```

print(f"   Done: {len(os.listdir(input_dir))} files copied")

def gen_e08():
    exp_dir = os.path.join(BASE, "E08_comparision")
    ensure_dir(os.path.join(exp_dir, "output"))
    ensure_dir(os.path.join(exp_dir, "charts"))
    print("   Done: directories created")

def gen_e09():
    exp_dir = os.path.join(BASE, "E09_configuration_change")
    before_dir = os.path.join(exp_dir, "input", "before")
    after_dir = os.path.join(exp_dir, "input", "after")
    ensure_dir(os.path.join(exp_dir, "output"))
    ensure_dir(os.path.join(exp_dir, "charts"))

    src      = os.path.join(BASE,      "E03_black_friday",      "input",
"with_classification")
    copy_files(src, before_dir)

    generate_hourly_set(scenario_c3_improved,  scenario_c3["date"],
after_dir, "E09_C3_improved")

    save_json(os.path.join(exp_dir, "config.json"),
              generate_config_with_context(2.5, "sale"))
    print(f"       Done:  {len(os.listdir(before_dir))} before  +
{len(os.listdir(after_dir))} after")

def main():
    print("=" * 60)
    print("Generating experiment data")
    print("=" * 60)

    gen_e01()
    gen_e02()
    gen_e02_1()
    gen_e03()
    gen_e04()
    gen_e05()
    gen_e06()
    gen_e07()
    gen_e08()
    gen_e09()

    print("\n" + "=" * 60)
    print(" Complete!")
    print("=" * 60)

if __name__ == "__main__":
    main()

```

Список публікацій здобувача за темою дисертації

Ковалевського В'ячеслава Валерійовича

«Алгоритмічне та програмне забезпечення аналізу ефективності систем захисту
сервісів електронної комерції»

121 Інженерія програмного забезпечення

Публікації в наукових фахових виданнях України

1. Москалик Д.О., Антонюк Д.С., Вакалюк Т.А., Огінський Є.В., Ковалевський В. В. Огляд застосувань теорії графів у розробці та обслуговуванні програмних систем. *Computer Science and Applied Mathematics*. Запоріжжя: Видавничий дім «Гельветика», 2022. № 1. С. 75-82. DOI: [10.26661/2413-6549-2022-1-09](https://doi.org/10.26661/2413-6549-2022-1-09)
2. Ковалевський В.В., Вакалюк Т.А. Стан досліджень у галузі розробки та функціонуванні систем захисту сервісів електронної комерції. *Вчені записки Таврійського національного університету імені В.І. Вернадського. Серія: Технічні науки*, 2022. Том 33 (72), № 6. С. 92-98. DOI: [10.32782/2663-5941/2022.6/16](https://doi.org/10.32782/2663-5941/2022.6/16)
3. Ковалевський В.В., Вакалюк Т.А. Огляд наявних методів оцінки ефективності роботи систем захисту сервісів електронної комерції. *Вісник Херсонського національного технічного університету*, 2023. №3 (86). С. 102-110. DOI: [10.35546/kntu2078-4481.2023.3.13](https://doi.org/10.35546/kntu2078-4481.2023.3.13)
4. Ковалевський В.В., Вакалюк Т.А. Огляд сучасних систем захисту електронних сервісів. *Вісник Хмельницького національного університету. Серія: Технічні науки*, 2024. Том 337, №3(2). С. 176-182. DOI: [10.31891/2307-5732-2024-337-3-26](https://doi.org/10.31891/2307-5732-2024-337-3-26)
5. Ковалевський В., Вакалюк Т. Використання штучного інтелекту у системах захисту сервісів електронної комерції. *Інформаційні технології та суспільство*, 2025. №3 (18). С. 72-76. DOI: [10.32689/maup.it.2025.3.9](https://doi.org/10.32689/maup.it.2025.3.9)

Наукові праці, що засвідчують апробацію матеріалів дисертації

6. Ковалевський В.В., Вакалюк Т.А. Виклики у сфері захисту сервісів електронної комерції. *Наука, технології, інновації: світові тенденції та регіональний аспект : Матеріали VII Міжнародної науково-практичної конференції (м. Одеса, 27–28 вересня 2024 р.)* / ГО «Інститут інноваційної освіти»; Науково-навчальний центр прикладної інформатики НАН України. Одеса; Запоріжжя : АА Тандем, 2024. С. 62-64. <https://novaosvita.com/wp-content/uploads/2024/10/ScTechInn-Odesa-Sept2024.pdf>
7. Ковалевський В.В., Вакалюк Т.А., Необхідність розробки алгоритмічного та програмного забезпечення аналізу ефективності систем захисту сервісів електронної комерції. *Матеріали V Всеукраїнської науково-практичної інтернет-конференції студентів, аспірантів та молодих вчених за тематикою «Сучасні комп'ютерні системи та мережі в управлінні»: збірка наукових праць /під редакцією А.А. Григорової.* Херсон: Видавництво ФОП Вишемирський В. С., 2022. С. 22-23. <https://kntu.net.ua/ukr/content/download/99376/566912/file/CICT2022.pdf>
8. Ковалевський В.В. Безпекові виклики у сфері електронної комерції пов'язані з розвитком технологій штучного інтелекту. *Глобальні виклики та інновації: шляхи розвитку сучасної науки: збірник наукових праць з матеріалами IV Міжнародної наукової конференції, м. Львів, 11 липня, 2025 р.* Львів, 2025. С. 145-148. DOI: [10.62731/mcnd-11.07.2025.005](https://doi.org/10.62731/mcnd-11.07.2025.005)

Відомості про апробацію результатів дисертації

Ковалевського В'ячеслава Валерійовича

"Алгоритмічне та програмне забезпечення аналізу ефективності систем захисту
сервісів електронної комерції"

121 Інженерія програмного забезпечення

Масові науково-практичні заходи міжнародного рівня:

1. VII Міжнародна науково-практична конференція "Наука, технології, інновації: світові тенденції та регіональний аспект" (Україна, м. Одеса, 27–28 вересня 2024 р.). Форма участі – публікація матеріалів на тему *"Виклики у сфері захисту сервісів електронної комерції"*.
2. IV Міжнародна наукова конференція "Глобальні виклики та інновації: шляхи розвитку сучасної науки" (Україна, м. Львів, 11 липня, 2025 р.) Форма участі – публікація матеріалів на тему *"Безпекові виклики у сфері електронної комерції пов'язані з розвитком технологій штучного інтелекту"*.

Масові науково-практичні заходи всеукраїнського рівня:

1. V Всеукраїнська науково-практична інтернет-конференція студентів, аспірантів та молодих вчених "Сучасні комп'ютерні системи та мережі в управлінні". Форма участі – публікація матеріалів на тему *"Необхідність розробки алгоритмічного та програмного забезпечення аналізу ефективності систем захисту сервісів електронної комерції"*.

Масові науково-практичні заходи регіонального рівня:

1. Засідання міжкафедрального науково-методологічного семінару для молодих учених Державного університету "Житомирська політехніка" (Україна, м. Житомир, Державний університет "Житомирська політехніка", 21 січня 2026 р.). Форма участі – виступ з презентацією за результатами дисертаційного дослідження на тему: *"Алгоритмічне та програмне забезпечення аналізу ефективності систем захисту сервісів електронної комерції"*.

Довідки про впровадження результатів дисертації

Ковалевського В'ячеслава Валерійовича

«Алгоритмічне та програмне забезпечення аналізу ефективності систем захисту
сервісів електронної комерції»

121 Інженерія програмного забезпечення

(СКАНОВАНІ КОПІЇ)

ДОВІДКА

про впровадження результатів наукового дослідження
на тему «Алгоритмічне та програмне забезпечення аналізу ефективності
систем захисту сервісів електронної комерції»

КОВАЛЕВСЬКОГО В'ячеслава Валерійовича

на здобуття наукового ступеня доктора філософії
за спеціальністю 121 Інженерія програмного забезпечення
у галузі знань 12 Інформаційні технології

Дана довідка підтверджує, що науково-теоретичні та практичні результати дисертаційного дослідження КОВАЛЕВСЬКОГО В'ячеслава Валерійовича на тему «Алгоритмічне та програмне забезпечення аналізу ефективності систем захисту сервісів електронної комерції» проходили апробацію в роботі підприємства ТОВ «САНА КОМЕРС УКРАЇНА» у вигляді експериментального тестування розробленого методу аналізу ефективності систем захисту сервісів електронної комерції та програмного забезпечення, що реалізує його роботу. Тестування проводилось з використанням робочих даних підприємства отриманих з систем, що обслуговують реальних користувачів. Застосування методу для аналізу зібраних даних підтвердило його працездатність та потенціал використання для покращення показників функціонування інформаційних систем підприємства. Апробація методу, як частини робочих процесів підприємства, отримала позитивні відгуки та зацікавленість у подальшому використанні.

Важливість отриманих результатів дисертаційного дослідження КОВАЛЕВСЬКОГО В.В. визначається потребою своєчасного виявлення проблемних аспектів функціонування систем захисту, що мають безпосередній вплив на бізнес-показники підприємства. Тому запропоновані здобувачем моделі, методи, алгоритми та технології є актуальними, своєчасними та мають практичну цінність.

Директор
ТОВ «САНА КОМЕРС УКРАЇНА»


АНТОНЮК Д.С.




VISEVEN EUROPE LLC
 Tax Number: 38428784
 Peremohy St.99, Zhytomyr 10003, Ukraine
 +380 412 425 904
 finance@viseven.com

25-Є/26

ДОВІДКА

про впровадження результатів наукового дослідження

на тему «Алгоритмічне та програмне забезпечення аналізу ефективності систем захисту сервісів електронної комерції»

КОВАЛЕВСЬКОГО В'ячеслава Валерійовича

на здобуття наукового ступеня доктора філософії

за спеціальністю 121 Інженерія програмного забезпечення

у галузі знань 12 Інформаційні технології

Дана довідка підтверджує, що результати дисертаційного дослідження КОВАЛЕВСЬКОГО В'ячеслава Валерійовича на тему «Алгоритмічне та програмне забезпечення аналізу ефективності систем захисту сервісів електронної комерції» проходили апробацію в діяльності ТОВ «Візеვენ Європа».

В рамках апробації на підприємстві було проведено експериментальне тестування розробленого методу аналізу ефективності систем захисту сервісів електронної комерції та програмного забезпечення, що забезпечує його практичну реалізацію. Тестування здійснювалося з використанням фактичних даних підприємства, отриманих із робочих інформаційних систем.

За результатами проведеної апробації встановлено, що запропонований метод і програмне забезпечення є працездатними та придатними до практичного застосування. Використання розробленого підходу для аналізу зібраних даних підтвердило можливість його застосування для виявлення факторів функціонування систем захисту, що впливають на роботу інформаційних систем підприємства та пов'язані з ними бізнес-показники.

Практичне значення отриманих результатів дисертаційного дослідження КОВАЛЕВСЬКОГО В.В. обумовлене актуальними потребами з виявлення чинників впливу на сервіси електронної комерції систем захисту, що викликані взаємодією з системами захисту. Розроблені здобувачем моделі, методи, алгоритми та технології мають прикладне значення, відповідають сучасним потребам і становлять інтерес для подальшого практичного використання.

Заступник директора з операційної діяльності
 ТОВ «Візеვენ Європа»



Василенко В'ячеслав

Звіт подібності дисертації**Ковалевського В'ячеслава Валерійовича****«Алгоритмічне та програмне забезпечення аналізу ефективності систем захисту
сервісів електронної комерції»**

Метадані

ДОКУМЕНТ

Заголовок: kovalevskyi_phd_paper7
Автор: Вячеслав Ковалевський
Науковий керівник / Експерт: Zhytomyr Polytechnic
ІД документу: 333547164

ОРГАНІЗАЦІЯ

Назва організації: State University "Zhytomyr Polytechnic"
підрозділ: State University "Zhytomyr Polytechnic"

ЗВІТ

Дата звіту: 4/7/2026
Дата редагування: 4/7/2026

Обсяг знайдених подібностей

Коефіцієнт подібності визначає, який відсоток тексту по відношенню до загального обсягу тексту було знайдено в різних джерелах. Зверніть увагу, що високі значення коефіцієнта не автоматично означають плагіат. Звіт має аналізувати компетентна / уповноважена особа.



25
Довжина фрази для коефіцієнта подібності 2



37077
Кількість слів

273303
Кількість символів

Тривога

У цьому розділі ви знайдете інформацію щодо текстових спотворень. Ці спотворення в тексті можуть говорити про МОЖЛИВІ маніпуляції в тексті. Спотворення в тексті можуть мати навмисний характер, але частіше характер технічних помилок при конвертації документа та його збереженні, тому ми рекомендуємо вам підходити до аналізу цього модуля відповідально. У разі виникнення запитань, просимо звертатися до нашої служби підтримки.

Заміна букв	ß	147
Інтервали	A→	0
Мікропробіли	␣	27
Білі знаки	␣	1
Парафрази (SmartMarks)	↔	212

Джерела

Нижче наведений список джерел. В цьому списку є джерела із різних баз даних. Копію тексту означає в якому джерелі він був знайдений. Ці джерела і значення Коефіцієнту Подібності не відображають прямого плагіату. Необхідно відкрити кожне джерело і проаналізувати зміст і правильність оформлення джерела.

10 найдовших фразКопію тексту

#	НАЗВА ТА АДРЕСА ДЖЕРЕЛА URL (НАЗВА БАЗИ)	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
1	https://dspace.bdpv.org.ua/server/api/core/bitstreams/26b856ec-d9e3-4baa-b41a-ea053a6561d0/content	216 (0.58 %)

2	https://tech.vemadskyjournals.in.ua/journals/2022/6_2022/16.pdf	147 (0.40 %)
3	https://cyberleninka.ru/article/n/oglyad-nayavniy-metodiv-otsinki-efektivnosti-roboti-sistem-zahistu-servisiv-elektronnoyi-komertsiji	133 (0.36 %)
4	https://cyberleninka.ru/article/n/oglyad-nayavniy-metodiv-otsinki-efektivnosti-roboti-sistem-zahistu-servisiv-elektronnoyi-komertsiji	107 (0.29 %)
5	https://tech.vemadskyjournals.in.ua/journals/2022/6_2022/16.pdf	97 (0.26 %)
6	https://cyberleninka.ru/article/n/oglyad-nayavniy-metodiv-otsinki-efektivnosti-roboti-sistem-zahistu-servisiv-elektronnoyi-komertsiji	80 (0.22 %)
7	https://cyberleninka.ru/article/n/oglyad-nayavniy-metodiv-otsinki-efektivnosti-roboti-sistem-zahistu-servisiv-elektronnoyi-komertsiji	77 (0.21 %)
8	https://cyberleninka.ru/article/n/oglyad-nayavniy-metodiv-otsinki-efektivnosti-roboti-sistem-zahistu-servisiv-elektronnoyi-komertsiji	76 (0.20 %)
9	https://cyberleninka.ru/article/n/oglyad-nayavniy-metodiv-otsinki-efektivnosti-roboti-sistem-zahistu-servisiv-elektronnoyi-komertsiji	74 (0.20 %)
10	https://tech.vemadskyjournals.in.ua/journals/2022/6_2022/16.pdf	72 (0.19 %)
Програма обміну базами даних (0.00 %)		
#	ЗАГОЛОВОК	КІЛЬКІСТЬ ІДЕНТИФІКАЦІЙНИХ СЛІВ (ФРАГМЕНТІВ)
Інтернет (10.33 %)		
#	ДЖЕРЕЛО URL	КІЛЬКІСТЬ ІДЕНТИФІКАЦІЙНИХ СЛІВ (ФРАГМЕНТІВ)
1	https://tech.vemadskyjournals.in.ua/journals/2022/6_2022/16.pdf	1471 (50) (3.97 %)
2	https://cyberleninka.ru/article/n/oglyad-nayavniy-metodiv-otsinki-efektivnosti-roboti-sistem-zahistu-servisiv-elektronnoyi-komertsiji	1356 (50) (3.66 %)
3	https://dspace.bdpu.org.ua/server/api/core/bitstreams/26b856ec-d9e3-4baa-b41a-ea053a6561d0/content	401 (9) (1.08 %)
4	http://lib.iitta.gov.ua/715709/1/dis_15.pdf	148 (10) (0.40 %)
5	http://perpustakaan.poltekkes-malang.ac.id/assets/file/kti/1602450014/LAMPIRAN.pdf	110 (14) (0.30 %)
6	http://economics.kntu.kr.ua/pdf/5(38)/26.pdf	66 (1) (0.18 %)
7	https://repository.unika.ac.id/21406/9/13.40.0070%20ANTHONY%20SEBASTIAN%20-LAMPIRAN.pdf	54 (7) (0.15 %)
8	https://support.minitab.com/en-us/minitab/help-and-how-to/statistical-modeling/doe/supporting-topics/taguchi-designs/catalogue-of-taguchi-designs/	49 (7) (0.13 %)
9	https://www.emecpumps.com/en/chemical-compatibility/	39 (5) (0.11 %)
10	http://www.guitaretab.com/o/offspring/23755.html	32 (5) (0.09 %)
11	https://chmnu.edu.ua/wp-content/uploads/2020/10/Vipusk-12.pdf	24 (2) (0.06 %)
12	https://americaspq.com/article/download/2721	19 (1) (0.05 %)
13	https://lib.iitta.gov.ua/id/eprint/710849/1/aref_Antoniuk_Printed.pdf	18 (2) (0.05 %)

14	https://cyberleninka.ru/article/n/kompleksnaya-otsenka-usloviy-truda-rabotayuschih-v-tsekhah-spetsialnogo-litya	11 (2) (0.03 %)
15	https://www.irejournals.com/formatedpaper/1702746.pdf	10 (1) (0.03 %)
16	https://reposit.nuop.edu.ua/bitstream/PolNTU/20034/1/Основи_проектування_захисних_споруд_цивільного_захисту_Навчальний_посібник.pdf	10 (1) (0.03 %)
17	https://openarchive.nure.ua/bitstreams/f762e53e-4889-4d21-b4fc-54fd69f5ef34/download	7 (1) (0.02 %)
18	http://er.nau.edu.ua/bitstream/NAU/17400/2/avt_%D0%93%D0%A3%D0%9C%D0%86%D0%9D%D0%A1%D0%AC%D0%9A%D0%98%D0%99.pdf	5 (1) (0.01 %)

Список прийнятих фрагментів

#	ЗМІСТ	КІЛЬКІСТЬ ОДНАКОВИХ СЛІВ (ФРАГМЕНТІВ)
	https://tech.vernadskyjournals.in.ua/journals/20... 	1471 (3.97%)
	https://cyberleninka.ru/article/n/oglyad-nayavni... 	1356 (3.66%)
	https://dspace.bdpu.org.ua/server/api/core/bitst... 	401 (1.08%)