Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

Барабаша Артема Вадимовича

на здобуття ступеня вищої освіти магістра

Метод оцінювання рівня захищеності кіберфізичних систем від інформаційних загроз

Галузь знань 12 – Інформаційні технології
Спеціальність 125 – Кібербезпека та захист інформації
Освітня програма Кібербезпека та захист інформації

Шифр КРМКБЗІ.240186.24.01.02 ПЗ

Виконав студент 2 курсу група КБЗІм-24-1 Артем БАРАБАШ
Керівник д-р філософії, старший викладач Наталія ПЕТЛЯК
Нормоконтролер д-р філософії, старший викладач Наталія ПЕТЛЯК

До захисту допускаю:
Завідувач кафедри кібербезпеки Юрій КЛЬОЦ
9 12 2025 р.

Хмельницький 2025

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Кібербезпеки

Рівень вищої освіти Магістр

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека та захист інформації

Освітня програма Кібербезпека та захист інформації

ЗАТВЕРДЖУЮ

Завідувач кафедри кібербезпеки

Юрій КЛЬОЦ

1 09 2025 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Барабашу Артему Вадимовичу

1 Тема роботи Метод оцінювання рівня захищеності кіберфізичних систем від інформаційних загроз

Керівник роботи доктор філософії, старший викладач Наталія ПЕТЛЯК

Затверджено наказом ректора університету 25 08 2025 № 65

2 Строк подання студентом кваліфікаційної роботи на кафедру

3 Вихідні дані до роботи Проаналізувати сучасні методи оцінювання стану інформаційної безпеки кіберфізичних систем, визначити їх переваги та недоліки. Обґрунтувати вибір методів і підходів, придатних для функціонування в реальному часі. Розробити метод оцінювання стану ІБ, що враховує специфіку взаємодії цифрових і фізичних компонентів системи. Провести експериментальну перевірку ефективності розробленого методу на основі вибірок даних. Здійснити порівняльний аналіз із відомими підходами, оцінити точність, стабільність і швидкодію. Розглянути можливості інтеграції розробленого методу в системи моніторингу безпеки та перспективи його вдосконалення.

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити)
Вступ. Аналіз сучасних підходів до оцінювання стану інформаційної безпеки кіберфізичних систем. Постановка задачі. Розроблення методу оцінювання стану ІБ КФС. Реалізація та експериментальна перевірка ефективності розробленого методу. Оцінка можливості функціонування методу в режимі реального часу. Висновки.

5 Перелік графічного матеріалу (із зазначенням обов'язкових креслень)

6 Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7 Дата видачі завдання 1 09 2025 р.

КАЛЕНДАРНИЙ ПЛАН

Назва етапів (розділів) кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
Ґрунтовне ознайомлення та дослідження предметної галузі		Виконано
Визначення змісту, структури магістерської роботи		Виконано
Опрацювання першого розділу магістерської роботи		Виконано
Опрацювання статті за результатами дослідження		Виконано
Опрацювання другого розділу магістерської роботи		Виконано
Опрацювання третього розділу магістерської роботи		Виконано
Опрацювання четвертого розділу магістерської роботи		Виконано
Підготовка та опрацювання ілюстративного матеріалу		Виконано
Оформлення магістерської роботи графічної та текстової частини		Виконано
Попередній захист магістерської роботи		Виконано
Захист магістерської роботи на засіданні ЕК		Виконано

Студент Артем БАРАБАШ

Керівник кваліфікаційної роботи Наталія ПЕТЛЯК

АНОТАЦІЯ

Тема кваліфікаційної роботи: Метод оцінювання рівня захищеності кіберфізичних систем від інформаційних загроз

Автор роботи: студент групи КБЗІм-24-1 Барабаш А.В.

Керівник роботи: доктор філософії, старший викладач Петляк Н.С.

Загальний обсяг роботи: 101 сторінок, 21 рисунок, 5 таблиць, 17 формул, 1 додаток, 60 посилань.

Ключові слова: кіберфізичні системи, інформаційна безпека, оцінювання рівня захищеності, достовірність, машинне навчання, аналіз ризиків.

У роботі представлено підхід до оцінювання рівня захищеності кіберфізичних систем від інформаційних загроз із використанням удосконаленого методу аналітичного аналізу та машинного навчання. Розроблений метод дає змогу підвищити достовірність оцінки стану безпеки за рахунок врахування динамічних змін параметрів системи, часових залежностей між подіями та стохастичних характеристик інформаційних потоків. Результати експериментальних досліджень довели, що запропонований метод забезпечує вищу точність класифікації станів безпеки, стабільність показників при зміні умов експлуатації, низький рівень хибних спрацьовувань і придатність до роботи в режимі реального часу. Метод адаптований для інтеграції у системи моніторингу типу SCADA, SIEM та IoT-платформи, підтримує масштабованість і енергоефективність, що робить його придатним для використання у промислових і критичних інфраструктурах.

1.12.2025

ANNOTATION

Theme of qualification work: Method for assessing the level of protection of cyber-physical systems against information threats

Author of the work: student of KBZIm-24-1 Barabash A.V.

Mentor: Doctor of Philosophy Petliak N.S.

Total volume of work: 101 pages, 21 figures, 5 tables, 17 formulas, 1 appendix, 60 references.

Keywords: cyber-physical systems, information security, security level assessment, reliability, machine learning, risk analysis.

The paper presents an approach to assessing the security level of cyber-physical systems from information threats using an advanced method of analytical analysis and machine learning. The developed method allows to increase the reliability of the security assessment by taking into account dynamic changes in system parameters, time dependencies between events and stochastic characteristics of information flows. The results of experimental studies have proven that the proposed method provides higher accuracy of security state classification, stability of indicators under changing operating conditions, low false positives and suitability for real-time operation. The method is adapted for integration into monitoring systems such as SCADA, SIEM and IoT platforms, supports scalability and energy efficiency, which makes it suitable for use in industrial and critical infrastructures.

1.12.2025

ЗМІСТ

ВСТУП

Сучасний етап розвитку технологій характеризується активним впровадженням кіберфізичних систем (КФС), які поєднують інформаційні технології, сенсори, виконавчі пристрої та аналітичні модулі в єдине кероване середовище. Такі системи є основою промислової автоматизації, енергетичних мереж, транспортних і медичних технологій. Водночас зростання їхньої складності та взаємозв'язку між фізичними й цифровими компонентами зумовлює підвищення рівня кіберзагроз і потребу у вдосконаленні методів забезпечення інформаційної безпеки (ІБ).

На відміну від традиційних ІТ-систем, порушення безпеки в КФС може спричинити не лише втрату даних, а й фізичні наслідки - аварії, зупинку виробничих процесів або шкоду для людей. Особливо небезпечними є атаки на системи керування промисловими об'єктами, енергетичними мережами чи транспортною інфраструктурою. Тому питання оцінювання рівня захищеності КФС набуває стратегічного значення для державної, економічної та технологічної безпеки.

Наявні методи оцінювання ризиків переважно базуються на експертних або статистичних підходах, які не враховують специфіку взаємодії кібер- і фізичних процесів. Крім того, вони часто не дозволяють проводити динамічний моніторинг стану безпеки у реальному часі. Це визначає необхідність створення методу, який забезпечуватиме комплексну та кількісну оцінку рівня захищеності елементів КФС.

Метою роботи є розроблення методу оцінювання рівня захищеності КФС від інформаційних загроз, який підвищує достовірність і точність визначення поточного стану безпеки завдяки використанню формалізованих ознак і показників інформаційної стійкості.

Для досягнення поставленої мети передбачено вирішення таких завдань:

– проаналізувати існуючі підходи до моделювання загроз і оцінювання ризиків у кіберфізичних системах;

– побудувати модель формування ознак стану інформаційної безпеки елементів системи;

– розробити алгоритм та метод оцінювання рівня захищеності;

– перевірити достовірність і ефективність методу на експериментальних даних.

Об’єктом дослідження є процеси забезпечення інформаційної безпеки кіберфізичної системи, предметом - методи й моделі оцінювання рівня їхньої захищеності.

Наукова новизна полягає у створенні методу оцінювання рівня захищеності кіберфізичної системи, який враховує багаторівневу структуру системи та взаємозв’язок інформаційних і фізичних процесів, що забезпечує підвищення точності виявлення аномалій і прогнозування ризиків.

Практичне значення результатів полягає у можливості впровадження запропонованого методу в системах моніторингу промислових, енергетичних і транспортних КФС для підвищення їхньої стійкості до інформаційних впливів.

Структура кваліфікаційної роботи відповідає меті дослідження. У вступі обґрунтовано актуальність, визначено мету, завдання, об’єкт і предмет. Перший розділ присвячений аналізу загроз і існуючих рішень, другий - розробленню моделі та методу оцінювання стану безпеки, третій - експериментальній перевірці та порівняльному аналізу результатів. У висновках наведено основні наукові й практичні результати дослідження.

1 МОДЕЛЬ ЗАГРОЗ ТА АНАЛІЗ НАЯВНИХ РІШЕНЬ

1.1 Поняття інформаційних загроз

Загрози ІБ - це будь-які дії, події або умови, що можуть поставити під загрозу конфіденційність, цілісність чи доступність інформації, інформаційних систем та цифрових ресурсів [1]. Такі загрози можуть мати як навмисний, так і випадковий характер і походити з різних джерел - внутрішніх (співробітники, користувачі, підрядники) або зовнішніх (хакери, конкурентні організації, кримінальні або державні структури). Крім людського впливу, загрози можуть мати природне чи техногенне походження, як-от стихійні лиха, технічні збої, вихід з ладу обладнання або помилки у програмному забезпеченні [2-4].

У сучасному цифровому середовищі ІБ є складною системою, що охоплює технологічні, організаційні, правові та людські аспекти. Основою її побудови є модель безпеки CIA-тріада (Confidentiality, Integrity, Availability), яка визначає базові принципи захисту даних і функціонування безпечних інформаційних систем (рис.1) [5].

Рисунок 1 - Модель безпеки CIA-тріада

Конфіденційність передбачає обмеження доступу до інформації виключно для уповноважених користувачів, систем або процесів. Її порушення відбувається у випадках несанкціонованого доступу до персональних даних, фінансових відомостей чи службової інформації. Для гарантування конфіденційності використовуються такі методи, як шифрування даних, аутентифікація користувачів, контроль доступу, розмежування повноважень і анонімізація даних [6].

Цілісність означає підтримання точності, достовірності та узгодженості даних протягом усього їхнього життєвого циклу. Вона спрямована на запобігання несанкціонованим змінам, втраті або фальсифікації інформації. Для забезпечення цього принципу застосовуються контрольні суми, цифрові підписи, системи журналювання, версійний контроль і аудит змін [7].

Доступність, у свою чергу, гарантує, що інформація, сервіси й ресурси будуть доступними користувачам у потрібний момент [8]. Порушення доступності може бути спричинене кібератаками, технічними збоями або природними катастрофами, що призводить до зупинки бізнес-процесів. Для підтримання стабільного рівня доступності застосовуються механізми резервування, балансування навантаження, аварійного відновлення та резервного копіювання даних.

Сучасні загрози ІБ різноманітні за своєю природою та способами реалізації [9]. Значну небезпеку становить шкідливе програмне забезпечення (malware), що охоплює віруси, черв’яки, трояни, боти та руткіти. Віруси здатні приєднуватися до легітимних файлів і розповсюджуватися далі, черв’яки діють самостійно через мережу, а трояни маскуються під корисні програми, надаючи зловмисникам віддалений доступ до системи. Боти формують ботнети - мережі заражених пристроїв, які можуть використовуватися для проведення DDoS-атак, а руткіти приховують присутність шкідливого коду від користувача та системних засобів захисту [10-12].

Не менш небезпечними є загрози конфіденційності та стеження (Privacy and Surveillance Threats), що полягають у несанкціонованому зборі або передачі

персональних даних. До них належить шпигунське програмне забезпечення (spyware), яке відстежує дії користувача, а також рекламне ПЗ (adware), що збирає інформацію про уподобання для подальшого використання [13-14]. Деякі програми використовують кейлогери (keyloggers) - інструменти, які фіксують натискання клавіш і можуть передавати логіни та паролі третім сторонам [15-17].

Особливий тип загроз становить вимагальне програмне забезпечення (ransomware), яке блокує або шифрує файли користувача та вимагає викуп за їхнє відновлення [18-20]. Такі атаки часто супроводжуються прийомами соціальної інженерії (social engineering) - обманом користувача через фальшиві повідомлення, листи або попередження з метою змусити його виконати дії, що відкривають доступ до системи [21-23].

Ефективне управління безпекою неможливе без чітко визначеної інформаційної політики безпеки (Information Security Policy). Це нормативний документ, який встановлює правила, процедури та відповідальність усіх учасників процесу захисту. Політика регламентує управління активами, контроль доступу, реагування на інциденти, моніторинг і проведення аудиту безпеки.

Для підтримання належного рівня захисту організації впроваджують низку технологічних рішень. До найважливіших належать мережеві екрани (firewalls), що контролюють і фільтрують трафік, системи виявлення та запобігання вторгненням (IDS/IPS), які аналізують поведінку мережевого трафіку, а також системи управління подіями та інцидентами безпеки (SIEM), здатні агрегувати журнали подій і забезпечувати аналітику в режимі реального часу. Важливою складовою є керування вразливостями (Vulnerability Management) - процес систематичного виявлення, оцінювання та усунення слабких місць у системах, а також керування інформаційними ризиками (Information Security Risk Management), що дозволяє визначати, оцінювати та мінімізувати вплив потенційних загроз [24-25].

Новим напрямом у сфері захисту даних є управління поверхнею атаки (Attack Surface Management), яке передбачає виявлення всіх потенційних точок

входу для зловмисників від мережевих сервісів до хмарних інфраструктур і пристроїв Інтернету речей [26-28]. Важливу роль відіграє також підхід DevSecOps, який інтегрує принципи безпеки на кожному етапі життєвого циклу програмного забезпечення, забезпечуючи раннє виявлення вразливостей і контроль якості коду.

Незважаючи на технологічний прогрес, ключовим чинником ІБ залишається людський фактор (human factor). Помилки, необережність або брак обізнаності користувачів часто стають причиною інцидентів, тому важливим є проведення навчання з питань кібергігієни, моделювання фішингових атак, впровадження багатофакторної автентифікації та шифрування даних [29-31].

Таким чином, ІБ є не лише технічним завданням, а стратегічним елементом управління організацією. Вона поєднує технології, політики, процеси та культуру відповідального ставлення до інформації. У світі, де дані стали найціннішим ресурсом, ІБ виступає фундаментом цифрового суверенітету, надійності бізнесу та конкурентоспроможності в умовах глобального інформаційного суспільства.

Ризики ІБ - це потенційні події або дії, які можуть негативно вплинути на конфіденційність, цілісність чи доступність інформаційних ресурсів організації. Вони виникають унаслідок взаємодії загроз (threats) та вразливостей (vulnerabilities) системи, створюючи умови для порушення її стійкості. У науковій літературі ризик визначається як функція ймовірності реалізації загрози та можливого збитку, що виникає в результаті цієї події. Таким чином, управління ризиками (risk management) ґрунтується на постійному аналізі середовища, виявленні потенційних загроз і розробленні заходів для їхнього мінімізації.

Класифікація ризиків ІБ здійснюється за кількома критеріями. За походженням виділяють внутрішні ризики, пов’язані з діями персоналу, технічними збоями чи помилками адміністрування, та зовнішні ризики, спричинені кібератаками, промисловим шпигунством або впливом природних факторів. За характером впливу розрізняють технічні, організаційні, людські та

фізичні ризики. Технічні ризики охоплюють збої апаратного забезпечення, вразливості програмних компонентів і несанкціонований доступ через мережеву інфраструктуру. Організаційні ризики пов’язані з недоліками політик безпеки, браком контролю або помилками в управлінні доступом. Людський фактор включає як навмисні дії співробітників (інсайдерські атаки), так і ненавмисні порушення, спричинені необізнаністю чи неуважністю. Фізичні ризики охоплюють руйнування або пошкодження обладнання, втрату носіїв інформації, а також природні катаклізми [32].

Суттєвою групою є кіберризики, що охоплюють цілеспрямовані атаки на цифрові активи. До них належать шкідливе програмне забезпечення, фішинг, атаки типу «відмова в обслуговуванні» (DDoS), несанкціонований доступ до баз даних та маніпулювання даними. Окрему увагу слід приділяти ризикам хмарних середовищ і ризикам IoT, які пов’язані з децентралізованою природою зберігання даних та недостатнім рівнем автентифікації пристроїв.

Управління ризиками ІБ (Information Security Risk Management) - це систематичний процес, який охоплює етапи ідентифікації, оцінювання, пріоритизації та мінімізації ризиків. На етапі ідентифікації здійснюється виявлення активів організації та визначення потенційних загроз. Оцінювання ризиків передбачає аналіз ймовірності їхньої реалізації та масштабу можливих наслідків. Пріоритизація дозволяє зосередити ресурси на найбільш критичних напрямах, а розроблення стратегій реагування включає впровадження технічних і процедурних заходів таких як резервування, шифрування, багатофакторна автентифікація, а також навчання персоналу.

Важливим є впровадження принципу безперервного моніторингу ризиків, який дає змогу своєчасно реагувати на зміни у середовищі загроз. У сучасних умовах акцент зміщується з пасивного реагування на прогнозування ризиків, що базується на використанні методів аналітики великих даних та штучного інтелекту для виявлення аномалій у поведінці систем і користувачів.

Таким чином, ризики ІБ є невід’ємним елементом цифрової інфраструктури будь-якої організації. Їх своєчасне виявлення та управління

забезпечують стабільність інформаційних процесів, збереження довіри користувачів і відповідність вимогам міжнародних стандартів, таких як ISO/IEC 27001. Ефективне управління ризиками перетворюється на стратегічний інструмент захисту цифрових активів і підтримки стійкості інформаційних систем у динамічному середовищі сучасних загроз.

1.2 Модель загроз ІБ при функціонуванні КФС

Через глибоку інтеграцію КФС у виробничо-технологічні комплекси та об’єкти критичної інформаційної інфраструктури завдання моніторингу їхньої безпеки істотно ускладнюється. Це пов’язано з великою кількістю можливих точок входу та різноманіттям каналів взаємодії, що робить захист КФС значно складнішим, ніж у традиційних інформаційних системах. У разі реалізації загроз ІБ кінцевою метою зловмисника зазвичай виступає встановлення контролю над керуванням системою через інформаційні впливи. Такі впливи здатні змінювати не лише процеси зберігання, обробки й передавання даних усередині КФС, а й фізичні параметри функціонування виконавчих механізмів.

Модель загроз ІБ визначається як опис властивостей та характеристик небезпек, які можуть вплинути на захищеність інформації. Усвідомлення потенційних загроз є критично важливим етапом у процесі виявлення вразливостей КФС. Сама модель містить відомості про стан безпеки об’єкта КФС у випадку реалізації певних подій або процесів, враховуючи їхню актуальність, можливість здійснення та ймовірні наслідки. Одним із найбільш небезпечних ризиків виступає впровадження програмних чи апаратних закладок, яке може відбуватися на будь-якому етапі життєвого циклу системи. Навіть за наявності засобів захисту неможливо повністю виключити ризик перехоплення або підміни керуючого сигналу.

На рисунку 2 наведено можливі шляхи потрапляння шкідливого програмного забезпечення у систему керування КФС.

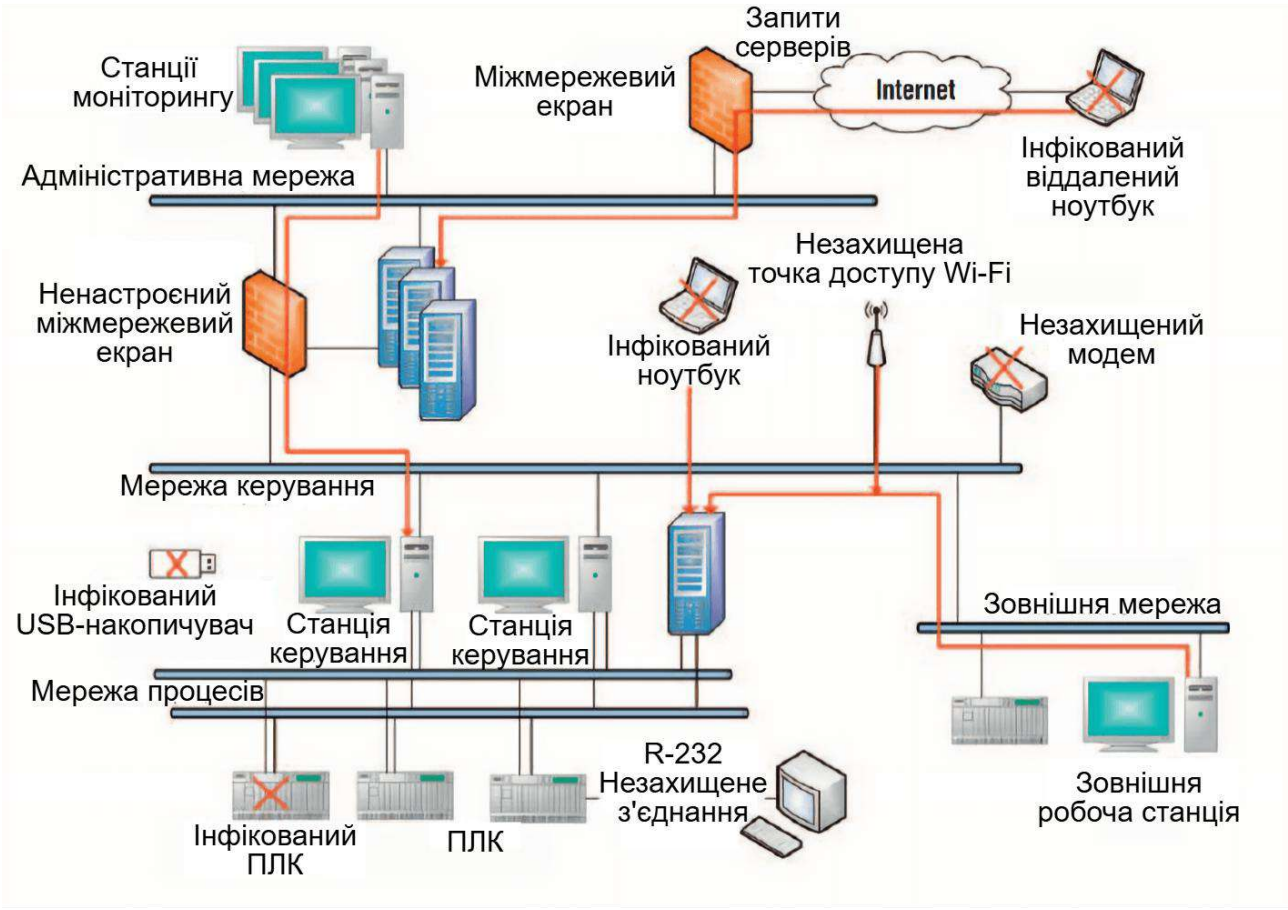

Рисунок 2 - Можливі шляхи проникнення шкідливого ПЗ у систему керування КФС

Типові загрози для таких систем охоплюють широкий спектр деструктивних впливів, серед яких перехоплення або модифікація даних, спроби отримати керування окремими компонентами, атаки відмови в обслуговуванні, маніпуляції таблицями маршрутизації, використання бекдорів, експлуатація вразливостей протоколів, несанкціоноване виконання шкідливого коду чи зміна системного часу. На рисунку 3 представлено приклади деструктивних впливів на різних рівнях КФС від фізичного до мережевого й рівня прикладних додатків.

Узагальнюючи, основними небезпеками для КФС слід вважати несанкціоновані зміни інформації та атаки, спрямовані на порушення її цілісності. Зазвичай дії зловмисника мають на меті отримати дистанційний доступ до керування або вивести з ладу фізичну частину системи. Моніторинг стану безпеки елементів КФС ґрунтується на аналізі комплексу факторів, що

відображають конфіденційність, цілісність, доступність даних, взаємодію інформаційної та фізичної підсистем, а також ступінь впливу можливих атак на керування.

Рисунок 3 - Загрози на різних рівнях КФС

Для забезпечення такого контролю використовуються дані про функціонування системи, що надходять від численних джерел. Параметри синхронізуються у часі та формують ряди спостережень, які застосовуються у процесі оцінки стану безпеки. Зокрема, телеметричні дані з елементів КФС передаються через SCADA-системи до центрів контролю, тоді як керуючі команди від основної системи повертаються до компонентів, утворюючи замкнений контур управління.

Залежно від ступеня доступу до системи умовно розрізняють дві групи потенційних порушників: тих, хто має легальний доступ до КФС, та тих, хто позбавлений таких прав. Визначення джерела атаки й наявних вразливостей істотно звужує коло можливих векторів нападу та дозволяє більш точно прогнозувати механізми реалізації загроз. Для кожного типу загрози виокремлено ключові чинники: мотив, суб'єкт, ціль, вектор та наслідки атаки.

Враховуючи різноманітність архітектур і сфер застосування, повний перелік можливих загроз для КФС сформувати неможливо.

1.3 Аудит ІБ КФС

У контексті КФС поняття ІБ набуває ширшого змісту порівняно з класичними інформаційними системами. Якщо для останніх ключовими принципами залишаються цілісність, конфіденційність та доступність даних, то для КФС до цього додається ще й необхідність забезпечення стабільного функціонування системи в умовах деструктивних інформаційних впливів (рис.4). У зв'язку із цим розроблено модель інформаційно-функціональної безпеки КФС, що дозволяє інтегрувати технічні й організаційні аспекти захисту.

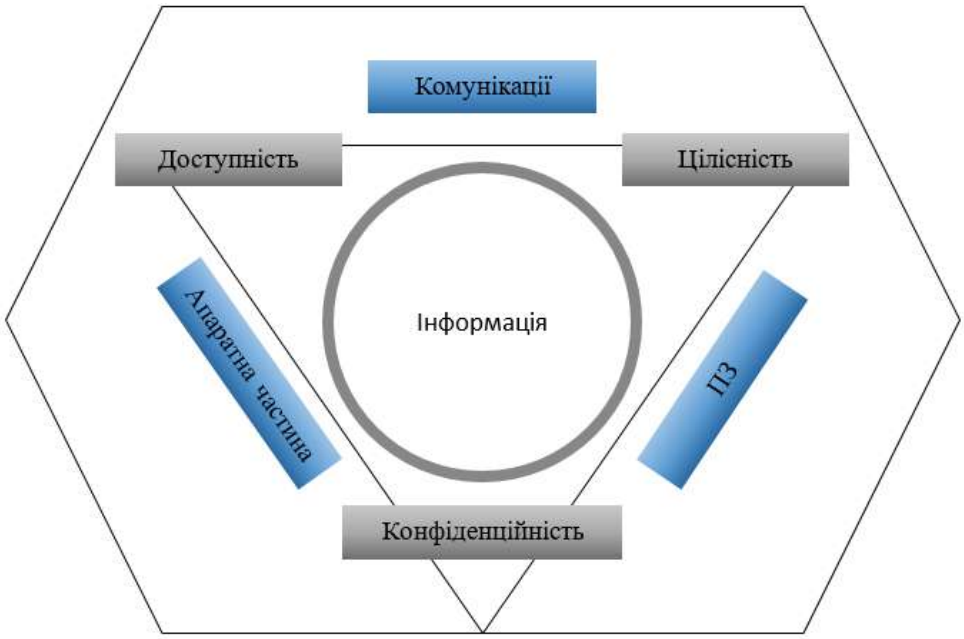

Рисунок 4 - Складові захисту інформації

Центральним завданням аудиту ІБ КФС є управління ризиками. На початкових етапах проєктування кіберфізичних комплексів проблемі ризиків порушення безпеки приділялося недостатньо уваги. З розширенням масштабів застосування КФС та інтенсивним зростанням обсягів обміну даними суттєво

підвищилася ймовірність несанкціонованого доступу до системного керування та інших кібератак, що здатні призвести до витоку конфіденційної інформації й серйозних функціональних збоїв.

Специфіка КФС полягає в інакшій ієрархії пріоритетів безпеки, ніж у традиційних інформаційних середовищах (табл.1). Якщо для останніх найвищим є захист конфіденційності, то у випадку КФС домінує вимога доступності, адже від неї безпосередньо залежить працездатність і безперервність технологічних процесів. Цілісність у такій системі займає середній рівень важливості, тоді як конфіденційність стає другорядною.

Таблиця 1 – Ієрархія пріоритетів безпеки

Приоритет	КФС	ІС
високий	доступність	конфіденційність
середній	цілісність	цілісність
низький	конфіденційність	доступність

Оцінювання ризиків у КФС поєднує якісні та кількісні методи. У першому випадку значна роль належить експертним оцінкам, тоді як другий підхід спрямований на обчислення конкретних числових показників можливих втрат. Для забезпечення захисту можуть застосовуватися й адаптовані традиційні засоби ІБ, як-от міжмережеві екрани та системи виявлення вторгнень. Однак з огляду на складність і непередбачуваність кібератак класичні технології надійності не гарантують повного захисту. З цієї причини сучасні дослідження акцентують на зменшенні збитків від атак і відновленні функцій КФС після інцидентів.

Ускладнення захисту зумовлене й тим, що із зростанням інтеграції інформаційних технологій та промисловості масштаби КФС значно розширюються. Це висуває вимогу комплексного підходу до безпеки на всіх етапах життєвого циклу. Перспективним напрямом у цьому контексті стає застосування технологій блокчейн, які завдяки своїй децентралізованій

структурі забезпечують стійкість, автентичність та незмінність даних. Використання таких технологій відкриває можливості для розвитку нових методів і стандартів захисту, особливо у сфері «розумного виробництва» та промислових інформаційних систем.

Методології оцінювання ризиків у КФС охоплюють як класичні, так і новітні підходи. Серед них варто виокремити аналіз дерева відмов, що дозволяє графічно відтворити можливі сценарії розвитку подій; аналіз причин і наслідків відмов, спрямований на розрахунок імовірності виникнення критичних ситуацій; а також поширений у промисловості метод HAZOP, орієнтований на виявлення небезпечних відхилень від проєктних станів. Окреме місце посідає інженерне моделювання, що створює поведінкові моделі реального часу для оцінки стану безпеки.

Через складність програмних і технічних компонентів традиційні методи не завжди ефективні, тому розроблено системно-теоретичний аналіз процесів (СТАП), що базується на ієрархічних структурах управління й дозволяє виявляти аномальні сценарії без залежності від природи впливу. Інший перспективний напрям - використання байєсівських мереж, які завдяки здатності описувати взаємозалежності між компонентами КФС надають можливість для динамічної оцінки ризиків, у тому числі при обмеженості даних. Це створює основу для побудови складних багаторівневих моделей, що прогнозують інциденти та дозволяють зменшувати вразливість промислових систем управління.

1.4 Аналіз останніх досліджень

У [33] автори розробили методологію VERCASM-CPS (Vulnerability Evaluation and Risk Calculation for Cyber-Physical Systems), призначену для автоматизованого аналізу вразливостей і оцінювання кіберризиків у КФС. Її головна перевага полягає в здатності використовувати відкриті бази даних, зокрема CVE (Common Vulnerabilities and Exposures), для визначення

найуразливіших компонентів системи та формування більш безпечних конфігурацій у режимі реального часу. Метод дозволяє не лише оцінювати ризики, а й динамічно перебудовувати систему завдяки інтеграції з технологією захисту від керованих рухомих цілей (Moving Target Defense, MTD), що зменшує поверхню атаки під час заміни компонентів. Серед переваг розробки - автоматичність процесу, гнучкість реконфігурації та можливість безперервного моніторингу кіберризику CPS. Водночас недоліком є залежність точності оцінки від повноти бази CVE, а також високі обчислювальні витрати при аналізі складних систем у режимі реального часу.

Автори [34] запропонували уніфіковану модель оцінювання ризиків для розподілених КФС, побудовану на основі байєсівського підходу, яка враховує як кібернетичні, так і фізичні взаємозв'язки між компонентами системи. Запропонований метод усуває обмеження попередніх підходів, адже дозволяє точно моделювати механізми поширення ризику з урахуванням складної топології мережі та взаємозалежностей між пристроями. Його ключова перевага полягає в тому, що модель одночасно аналізує ймовірність кібератак і їхній вплив на фізичну інфраструктуру, забезпечуючи комплексне бачення безпеки DCPS. Крім того, використання епідеміологічного моделювання та оптимального скидання навантаження підвищує точність прогнозування наслідків атак. Водночас недоліками методу є висока складність обчислень і залежність результатів від якості початкових даних, що може обмежувати його застосування в реальному час

У роботі [35] запропонували адаптовану методологію оцінки ризиків на основі FMECA, яка інтегрує детермінацію режимів відмов із тактиками та техніками ATT&CK для індукції сценаріїв відмов і більш повного аналізу безпеки КФС. Підхід «знизу вгору» вимагає деталізованого опису компонентів і їхніх функцій, що дозволяє точніше визначати режими відмов та прив'язувати їх до конкретних контрзаходів та критеріїв продуктивності. Серед переваг методу - висока ступінь трасованості ризиків до компонентів архітектури, можливість врахування робочих режимів системи та чітка інтеграція існуючих заходів

пом’якшення через FMT і CMT, що підвищує коректність оцінки виявлюваності й ефективності контролів. До недоліків належать значна трудомісткість та потреба в деталізованих експертних оцінках при заповненні матриць і визначенні ефективності пом’якшень, а також ймовірна складність застосування підходу в масштабних або динамічних середовищах без автоматизації. Крім того, залежність від повноти й актуальності бази знань ATT&CK та суб’єктивних оцінок може призводити до варіативності результатів, що вимагає регулярного оновлення даних і адаптації критеріїв.

Автори [36] розробили гармонізовану методологію оцінки ризиків безпеки та захисту (S&S) у КФС, яка поєднує аналіз кіберзагроз і традиційних фізичних ризиків за допомогою методу “метелика” (Bow-tie method). Основою підходу є використання моделей маршрутів атак (ARM) для виявлення першопричин збоїв, що дає змогу простежити вплив кібератак на фізичні компоненти системи. Інтеграція маршрутів запобігання кібербезпеці (CSPR), маршрутів запобігання фізичній безпеці (PSPR) та аналізу критичних змінних безпеки (SCVA) дозволяє здійснювати одночасний контроль кібернетичних і фізичних аспектів ризику. Перевагою запропонованого підходу є його комплексність і системність, що забезпечує цілісне уявлення про стан безпеки CPS та можливість кількісної оцінки впливу атак на робочі параметри системи. Водночас до недоліків можна віднести високу складність моделювання, значні вимоги до вхідних даних і необхідність глибоких технічних знань для практичної реалізації. Незважаючи на це, методологія демонструє потенціал як ефективний інструмент для інтегрованого управління ризиками безпеки й захисту у промислових КФС.

У роботі [37] автори розробили методологію оцінювання підходу FMECA-ATT&CK, побудовану відповідно до стандарту ISO 15288:2015, що розглядає оцінювання як системний процес аналізу ефективності методу управління ризиками у КФС. Методологія охоплює підготовку, проведення та управління результатами аналізу, забезпечуючи структуроване порівняння FMECA-ATT&CK з іншими підходами, зокрема методом «Метелик-краватка». Основною перевагою розробки є поєднання якісних і кількісних критеріїв оцінювання, що

дозволяє отримати збалансоване уявлення про застосовність, масштабованість, точність і зручність використання методу. Крім того, використання методу номінальної групи та заходів з мінімізації упередженості підвищує достовірність результатів експертного аналізу. Серед недоліків можна виокремити високу трудомісткість процесу, залежність від експертних суджень і складність забезпечення симетрії даних під час порівняльного аналізу. Попри це, запропонована методологія демонструє потенціал як універсальний підхід до валідації методів оцінки кіберризиків, здатний підвищити об’єктивність та відтворюваність результатів у галузі безпеки КФС.

В роботі [38] запропоновано динамічну модель оцінювання ризиків для кіберфізичних енергетичних систем (КФЕС), яка інтегрує вразливості кібермережі SCADA з фізичними наслідками в енергомережах, що виникають під впливом кібератак. Розроблений підхід поєднує аналіз програмних вразливостей (ПВ) з оцінкою мінімального скидання навантаження у сценаріях порушення роботи підстанцій, дозволяючи відобразити взаємозалежність між кібер- і енергетичною складовими системи. Перевагою методу є його динамічний характер, що забезпечує більш реалістичне моделювання процесу поширення атак і дозволяє оцінити вплив кіберактивності на енергетичну стабільність. Також модель враховує ефективність заходів захисту, що підвищує точність оцінки ризику. До недоліків підходу можна віднести високу складність реалізації та потребу у великому обсязі точних даних про вразливості, конфігурації мережі й фізичні параметри системи. Незважаючи на це, результати моделювання на тестових системах IEEE 14 та IEEE 118 підтвердили ефективність і практичну цінність методу для підвищення надійності та стійкості КФЕС.

Автори [39] розробили цілісну модель загроз для CPS, що розширює MITRE ATT&CK for ICS шляхом включення двокомпонентної структури - моделі зловмисника та моделі атаки - і інтеграції їх в гібридну методологію оцінки ризиків, яка поєднує кількісні та якісні підходи. Серед переваг методу - можливість більш точно характеризувати різні класи зловмисників (за знаннями,

ресурсами, доступом і специфічністю), враховувати частоту, відтворюваність і виявлюваність атак, а також здійснювати пріоритизацію загроз і оцінку збитків з урахуванням цілей CPS. Підхід також полегшує відтворення сценаріїв атаки в тестових середовищах CPS і дозволяє адаптувати оцінки ризику в режимі реального часу залежно від стану системи. До недоліків належать значна потреба в детальних системних знаннях і даних для коректного налаштування моделі, суб'єктивність частини якісних оцінок (наприклад, рейтингу впливу) та потенційна складність і трудомісткість впровадження в великих або розподілених інфраструктурах. Крім того, метод може вимагати значних обчислювальних і експертних ресурсів для підтримки високого рівня деталізації моделі загрози і ризику, а також залишатися вразливим до непередбачуваних або радикально нових типів атак, які не вкладаються у задані категорії. В цілому, запропонована методологія є потужним кроком до більш реалістичного моделювання загроз у CPES, але її ефективність залежить від якості вхідних даних, експертизи та можливостей організації впровадження.

У роботі [40] запропонували метод кількісної оцінки ризиків для КФС, який поєднує ймовірнісні та детерміновані підходи, використовуючи графи атак для оцінки ймовірності кібератаки та цифровий двійник енергосистеми для моделювання її впливу. Метод дозволяє інтегрувати інформацію про фізичні та кіберкомпоненти системи, а також враховувати каскадні збої, що робить оцінку ризику більш реалістичною та всебічною. Серед переваг підходу – можливість ідентифікувати найвразливіші підстанції та пріоритетні активи для захисту, а також адаптація до конкретних сценаріїв і структури енергосистеми. Недоліком є висока складність моделювання та потреба у значних обчислювальних ресурсах для створення цифрового двійника та аналізу великих графів атак. Крім того, метод може вимагати детальної експертної інформації про систему та активи, що обмежує його швидке застосування у різних реальних умовах.

Автори [41] розробили методологію оцінки ризиків для КФС, яка поєднує моделювання системи, ранжування критичних компонентів та аналіз залежностей між ними для виявлення потенційних шляхів атак. Метод дозволяє

враховувати як технічні характеристики компонентів, так і організаційні аспекти їх критичності, що забезпечує комплексний підхід до оцінки ризиків. Серед переваг підходу – можливість визначати небажані події та обчислювати ризик на основі ймовірності та впливу, що підвищує точність прогнозування та ефективність управління ризиками. Використання зворотного відстеження та методології «краватки-метелика» дозволяє підвищити масштабованість аналізу та полегшити співпрацю між IT- та OT-фахівцями. Недоліком є висока складність і трудомісткість процесу, а також потреба в експертних знаннях для оцінки ймовірності та впливу різних подій. Загалом, метод забезпечує глибоке й інтегроване розуміння ризиків, проте його застосування потребує значних ресурсів і часу.

У роботі [42] запропоновано модель оцінки стійкості кіберфізичних енергосистем, яка інтегрує характеристики фізичної мережі та функції кіберзахисту, що дозволяє аналізувати взаємозв’язок між кібер- і фізичними відмовами. Метод базується на моделюванні каскадних процесів у системі та використанні статистичних метрик для кількісної оцінки ризику відключення електроенергії. Серед переваг підходу – можливість точно оцінювати вплив кіберінцидентів на стабільність енергосистеми, визначати критичні точки у структурі мережі та враховувати реалістичну взаємодію між її компонентами. Метод також забезпечує гнучкість у проведенні сценарного аналізу для систем різного масштабу. Основними недоліками є висока обчислювальна складність, потреба у великому обсязі даних та чутливість результатів до точності початкових параметрів моделі. Загалом, підхід автора є ефективним інструментом для оцінки стійкості кіберфізичних енергосистем, проте його практичне застосування вимагає значних ресурсів і експертної підтримки.

Автори [43] пропонують уніфікований підхід до управління ризиками кібербезпеки в КФС, який поєднує теорію нечітких множин, класифікатори машинного навчання та комплексну модель оцінки ефективності засобів контролю. Запропонований метод дозволяє враховувати критичність активів, прогнозувати типи ризиків і визначати оптимальні заходи для їх зменшення.

Його перевагою є здатність інтегрувати різні джерела даних, забезпечуючи точніше прогнозування загроз і підвищуючи ефективність рішень щодо кіберзахисту. Крім того, використання нечітких множин дозволяє враховувати невизначеність у визначенні критичності активів, а машинне навчання підвищує точність прогнозів ризику. Недоліками підходу є висока складність моделі, потреба у великих обсягах достовірних даних і залежність від коректності навчання алгоритмів. Загалом, метод забезпечує системний і проактивний підхід до управління ризиками, проте вимагає значних технічних і аналітичних ресурсів для практичного впровадження.

У роботі [44] автори запропонували підхід до оцінювання вразливостей транспортних мереж, який інтегрує фізичний та кіберпростори за допомогою баєсівського графа мережевих атак. Такий метод дозволяє здійснювати ймовірнісне моделювання станів вразливості, враховуючи характеристики зловмисника, рівень бар'єрів контролю та взаємозв'язки між компонентами мережі. Перевагою розробки є можливість комплексного аналізу впливу кіберфізичних атак на ефективність транспортної системи, що забезпечує більш реалістичну оцінку ризиків. Також підхід враховує різні рівні безпеки сенсорних мереж, що підвищує точність оцінювання. Недоліками методу є його складність, потреба у великій кількості даних і значні обчислювальні ресурси, необхідні для моделювання та симуляцій. Загалом, запропонований підхід забезпечує ефективний інструмент для прогнозування та зменшення вразливостей транспортних систем до кіберфізичних загроз.

Автори [45] розробили метод оцінки надійності КФС, який поєднує інтелектуальний аналіз текстових описів вразливостей за допомогою моделі BERT із ймовірнісним моделюванням кібератак і їх наслідків. Запропонований підхід інтегрує баєсівський граф атак і марковську модель для відтворення сценаріїв порушення безпеки та оцінки впливу на роботу системи. Перевагою методу є висока точність прогнозування серйозності кібервразливостей, швидкість збіжності результатів і здатність враховувати складні нелінійні залежності між компонентами системи. Крім того, він забезпечує практичну

можливість оцінювати ризики на основі текстових даних із реальних джерел. Основними недоліками є висока обчислювальна складність, необхідність у якісних і великих обсягах текстових даних, а також складність інтерпретації результатів для нефахівців. Загалом, метод є ефективним інструментом для комплексної оцінки надійності КФЕС, що поєднує штучний інтелект із класичними підходами до моделювання ризиків.

У роботі [46] пропоновано підхід Spyderisk, який автоматизує процес оцінки ризиків КФС відповідно до вимог стандарту ISO 27005, використовуючи семантичне моделювання, онтології та базу знань. Метод дозволяє створювати причинно-наслідкові моделі загроз, враховувати зв'язки між активами, а також автоматично визначати рівень ризику та ефективність контрзаходів. Перевагою цього підходу є можливість моделювати складні сценарії атак, враховувати каскадні ефекти, швидко оновлювати моделі та повторно оцінювати ризики у разі змін у системі. Також метод сприяє інтеграції знань експертів і підвищує ситуаційну обізнаність користувачів. Недоліками є значна трудомісткість початкового моделювання системи, потреба у великих обсягах знань для побудови бази даних та складність адаптації до специфічних галузей. Загалом, метод Spyderisk забезпечує гнучкий, інтелектуально підтримуваний механізм управління ризиками, який поєднує переваги формального аналізу та практичної автоматизації процесів оцінки кіберзагроз.

В роботі [47] автори запропонували метод оцінки кіберфізичних ризиків, орієнтований на критичну транспортну інфраструктуру, який поєднує кількісний та якісний аналіз вразливостей, загроз і можливих фізичних наслідків кібератак. Основою методу є послідовна модель із шести етапів, що включає ідентифікацію вразливостей, побудову сценаріїв атак, оцінку характеристик джерел загроз і визначення рівня ризику відповідно до структури NIST SP800-30. Перевагою цього підходу є його адаптивність до конкретного сектора інфраструктури, можливість урахування як кібер-, так і фізичних аспектів атак, а також залучення експертів різних галузей для підвищення точності оцінки. Метод забезпечує глибше розуміння взаємозв'язку між технічними, людськими та організаційними

чинниками ризику. Серед недоліків слід відзначити складність практичної реалізації через велику кількість параметрів, потребу у висококваліфікованих оцінювачах і трудомісткість збору вихідних даних. Загалом, розробка авторів є комплексним підходом, який значно підвищує ефективність управління кіберфізичною безпекою критичних транспортних систем.

Автори [48] розробили модель КФС, яка поєднує аналіз потоків потужності, кібермоніторинг, контроль і фактор кіберзахисту для моделювання впливу шкідливого програмного забезпечення. Запропоновано метод оцінювання ефективності різних стратегій кіберзахисту, зокрема цільового, випадкового та знайомого захисту. Перевагою підходу є його здатність точно відтворювати процес поширення шкідливого ПЗ та оцінювати ефективність стратегій захисту на реалістичних моделях енергосистем, що дозволяє виявити найуразливіші вузли. Додатковою перевагою є використання генетичного алгоритму для оптимізації захисних ресурсів за обмеженого бюджету. Недоліками методу є висока обчислювальна складність, потреба в точних даних про мережу та спрощення окремих кіберфізичних взаємозв'язків. Загалом, підхід авторів забезпечує ефективний інструмент для аналізу та оптимізації стратегій протидії шкідливим атакам у КФС.

У роботі [49] автори розробили інтегровану кіберфізичну модель аналізу ризиків та планування інвестицій для підвищення стійкості енергетичних підстанцій. Запропонований підхід поєднує оцінку кібервразливостей із показниками зрілості безпеки (MIL) та враховує взаємодію між захисником і зловмисником у різних сценаріях атаки. Перевагою методу є можливість комплексно оцінювати як фізичні, так і кіберризики, що дозволяє ефективно розподіляти ресурси для підвищення надійності енергосистеми. Додатковою перевагою є адаптивність моделі до різного рівня інформаційної обізнаності сторін, що забезпечує гнучкість у прийнятті рішень. Недоліками є висока складність моделювання, значна потреба в точних вихідних даних і складність практичного впровадження у великих системах. Загалом, розроблений авторами підхід є ефективним інструментом для стратегічного управління кіберфізичною

стійкістю енергетичних підстанцій.

В роботі [50] автори здійснили комплексне дослідження безпеки КФС, представивши узагальнену класифікацію кібератак і методів захисту з трьох взаємопов’язаних перспектив - фізичної, кібернетичної та кіберфізичної. У роботі систематизовано типові вразливості, проаналізовано механізми атак на сенсори, мережеві елементи та інтегровані компоненти управління, а також наведено сучасні підходи до виявлення та нейтралізації загроз. Перевагою методу є комплексність аналізу, що дозволяє всебічно оцінити ризики для різних рівнів системи й визначити напрями вдосконалення захисту. Дослідження охоплює широкий спектр сценаріїв атак, у тому числі інтелектуальні кібератаки, що підвищує практичну цінність результатів. Недоліками є відсутність кількісної оцінки ефективності розглянутих підходів і складність узагальнення рекомендацій для конкретних типів систем. Загалом, розробка авторів забезпечує цілісне розуміння сучасних викликів у сфері безпеки КФС і формує наукове підґрунтя для подальших досліджень.

В дослідженні [51] автори демонструють систематичний огляд загроз КФС і методів їх захисту, приділяючи особливу увагу структурам КФС, властивостям атак і стратегіям виявлення аномалій. Перевагою їхнього підходу є комплексний аналіз, який охоплює фізичні процеси, мережеві аспекти та методи машинного навчання, що дозволяє оцінити ефективність різних стратегій захисту та показати практичні наслідки атак через числові приклади. Також важливим є систематичне представлення таксономії атак із урахуванням простору атаки, місця її реалізації та прихованості, що допомагає точніше прогнозувати можливі загрози. Метод дозволяє інтегрувати фізичні, мережеві та аналітичні аспекти для підвищення стійкості КФС. До недоліків можна віднести те, що огляд не пропонує нових алгоритмів детекції, а зосереджується на аналізі вже існуючих рішень, що обмежує практичну інноваційність підходу. Водночас робота відкриває перспективи для подальших досліджень у сфері безпечного проєктування КФС.

Автори дослідження [52] зосередилися на застосуванні генеративного

штучного інтелекту для забезпечення кібербезпеки КФС, аналізуючи його розвиток, потенційні переваги та загрози. Основною перевагою їхнього підходу є можливість використання GenAI для автономного створення нових рішень, що підвищує ефективність захисту КФС та відкриває перспективи для інноваційних методів виявлення атак. Автори також систематично оцінюють ризики, пов'язані з використанням GenAI, що дозволяє комплексно підходити до розробки стратегій захисту. Методика дозволяє інтегрувати сучасні AI-технології з кібербезпекою, забезпечуючи більш адаптивні та прогнозовані захисні механізми. Недоліком підходу є те, що широке застосування GenAI може створювати нові вектори атак і потребує додаткового контролю та регулювання. Водночас робота формує основу для подальших досліджень і розробки більш стійких стратегій безпеки КФС.

Автори [53] розробили метод автономного захисту КФС через впровадження Контролера Автономної Відповіді (ARC), який поєднує кількісну модель ієрархічної кореляції ризиків та Конкурентний процес Маркова для моделювання взаємодії між системою захисту та атакуючим. Перевагою їхнього підходу є висока точність та швидкість реакції на атаки: ARC забезпечує значно кращу ефективність у порівнянні зі статичними системами реагування, миттєво відновлюючи функціонування КФС навіть при складних атаках. Метод дозволяє оцінювати фінансові та функціональні ризики активів системи, а також приймати оптимальні рішення щодо захисту в автономному режимі. Крім того, ARC успішно протистоїть складним атакам, включно з каскадними відмовами, і демонструє ефективність у реальному часі на великих даних. Недоліком підходу є його складність і потреба у точному моделюванні всіх можливих шляхів атак, що вимагає значних обчислювальних ресурсів і глибокої експертизи. Водночас розробка відкриває перспективи для подальшого підвищення стійкості КФС і вдосконалення автономних механізмів кіберзахисту.

У роботі [54] автори розробили методологію MARISMA, яка дозволяє адаптувати процес аналізу ризиків і управління безпекою до будь-якого IT-середовища, включно з КФС, через визначення мета-шаблону та повторне

використання артефактів для конкретних контекстів. Перевагою підходу є його гнучкість та можливість інтегрування стандартів і рекомендацій, таких як ENISA та NIST, що забезпечує всебічний захист активів, об’єктів і даних CPS. MARISMA підтримується інструментом eMARISMA, який робить процес прийняття рішень більш швидким і прозорим, а також дозволяє створювати конкретні патерни для різних галузей, наприклад, для розумних лікарень. Метод дозволяє структурувати загрози, активи та виміри безпеки у вигляді матриць, що спрощує оцінку ризиків та визначення контролів. Недоліком підходу є необхідність залучення експертів із безпеки та RAM для правильної інстанціації патернів у конкретному середовищі, що може бути ресурсозатратним. Водночас метод забезпечує комплексну основу для управління ризиками та підвищення стійкості КФС до різноманітних загроз.

Автори [55] досліджують застосування методів машинного навчання для підвищення рівня захисту КФС, які є критично важливими інфраструктурами з високим рівнем взаємозалежності між фізичними та цифровими компонентами. Запропонований підхід спрямований на виявлення та запобігання сучасним типам кібератак, таким як DoS, DDoS, zero-day і стійкі загрози, які не завжди можуть бути виявлені традиційними засобами безпеки. Використання алгоритмів, зокрема SVM, CNN та рекурентних нейронних мереж, забезпечує здатність системи адаптивно виявляти аномалії та зменшувати кількість хибних спрацьовувань. Перевагою методу є підвищення точності і швидкості реагування на кібератаки завдяки самонавчанню моделей. Водночас недоліком є потреба у великих обсягах навчальних даних і складність інтерпретації результатів роботи нейромереж у реальному часі. Загалом метод демонструє перспективність для побудови інтелектуальних систем захисту CPS, здатних до самостійного аналізу та протидії складним загрозам.

В роботі [56] запропоновано використання алгоритму K-Means для аналізу великих обсягів даних КФС, зокрема у сфері споживання енергії, що дозволяє виявляти закономірності та потенційні ризики, пов’язані з безпекою інфраструктури. Їхній підхід демонструє ефективність у кластеризації даних з

метою спостереження за тенденціями енергоспоживання та оцінки можливих загроз для критичних об’єктів. Основною перевагою методу є його здатність працювати з великими наборами даних і виявляти приховані залежності між показниками без попереднього маркування даних. Також він є відносно простим в реалізації та забезпечує швидку обробку інформації для подальшого аналізу. Недоліком є необхідність точного визначення кількості кластерів, від якої залежить якість результатів, а також обмежена здатність алгоритму до роботи з нелінійними або сильно шумними даними. Загалом розробка авторів демонструє практичну цінність у застосуванні методів машинного навчання для забезпечення кіберфізичної безпеки та прогнозування ризиків у критичних енергетичних системах.

Автори [57] досліджують використання глибинного навчання для виявлення кібератак у КФС, підкреслюючи його перевагу над традиційними методами машинного навчання завдяки багаторівневій архітектурі та здатності автоматично виділяти ключові ознаки з великих обсягів даних. Запропонований підхід забезпечує високу точність і швидкість виявлення атак, що особливо важливо для систем, які критично залежать від безперервного обміну даними. Основною перевагою методу є здатність DL-моделей адаптуватися до складних, динамічних сценаріїв загроз і підвищувати стійкість CPS до нових типів атак. Крім того, використання відкритих високоякісних датасетів дозволяє значно прискорити навчання та оцінювання моделей. Недоліком методу є потреба у великих обчислювальних ресурсах та ризик перенавчання моделей, що може знижувати їхню ефективність у реальних умовах. Загалом розробка авторів демонструє перспективність глибинного навчання як основи для створення інтелектуальних систем кіберзахисту CPS.

У роботі [58] автори запропонували метод забезпечення безпеки КФС на основі інтеграції індексу Джині та технології блокчейн. Такий підхід дозволяє виявляти та нейтралізовувати атаки типу blackhole і greyhole завдяки аналізу нерівномірності розподілу ресурсів у мережі та забезпеченню незмінності даних у розподіленому реєстрі. Основною перевагою розробки є поєднання аналітичної

точності індексу Джині з прозорістю та децентралізованістю блокчейну, що підвищує надійність і стійкість КФС до внутрішніх і зовнішніх загроз. Крім того, перенесення обчислювальних процесів на рівень fog-серверів зменшує навантаження на пристрої та скорочує енергоспоживання. Недоліком методу є його залежність від високих обчислювальних ресурсів і складність налаштування порогових параметрів для точного виявлення атак. Загалом розробка авторів демонструє ефективне поєднання статистичних та розподілених технологій для підвищення кіберстійкості інтелектуальних систем.

1.5 Постановка задачі

У сучасних умовах розвитку цифрової економіки КФС стають основою функціонування критично важливих інфраструктур, промислових комплексів, енергетичних і транспортних систем. Їхня особливість полягає у тісній інтеграції інформаційних і фізичних процесів, що створює новий рівень складності в забезпеченні ІБ. Традиційні підходи до оцінювання рівня захищеності, орієнтовані переважно на ІТ-системи, не враховують динамічний, багаторівневий і взаємозалежний характер процесів, притаманних КФС.

Зростання кількості кібератак, зокрема спрямованих на промислові мережі, системи управління технологічними процесами та Інтернет речей, вимагає створення нових методів оцінювання стану ІБ, здатних забезпечити оперативність реагування, достовірність аналізу та адаптивність до мінливого середовища. Виявлення аномальних станів у реальному часі є особливо складним завданням через значну кількість взаємопов’язаних параметрів, невизначеність джерел загроз і варіативність поведінки компонентів системи.

Метою даної роботи є розроблення методу оцінювання рівня захищеності кіберфізичних систем від інформаційних загроз, який би забезпечував достовірну ідентифікацію станів безпеки на основі комплексного аналізу технічних та поведінкових параметрів.

Для досягнення поставленої мети необхідно вирішити такі наукові завдання:

– проаналізувати сучасні методи оцінювання рівня захищеності КФС і визначити їхні переваги та недоліки;

– розробити модель опису ознак стану ІБ елементів КФС з урахуванням фізичних, інформаційних та організаційних параметрів;

– побудувати алгоритм оцінювання рівня захищеності, який враховує динамічні зміни станів системи;

– реалізувати запропонований метод у тестовому середовищі та провести експериментальні дослідження для оцінювання його ефективності;

– здійснити порівняльний аналіз отриманих результатів із відомими методами оцінювання стану ІБ;

– визначити можливості інтеграції розробленого методу з існуючими системами моніторингу безпеки.

Таким чином, у межах кваліфікаційної роботи необхідно створити універсальний, адаптивний і достовірний інструмент оцінювання стану ІБ КФС, здатний забезпечити своєчасне виявлення ризиків і формування рекомендацій для запобігання інцидентам безпеки.

2 ОЦІНЮВАННЯ РІВНЯ ЗАХИЩЕНОСТІ КФС ВІД ІНФОРМАЦІЙНИХ ЗАГРОЗ

2.1 Модель формування опису ознак стану ІБ елементів КФС

Початкове значення $H = (f_1, f_2, \dots, f_n)$ визначається як сукупність можливих параметрів функціонування КФС. До цього набору входять як характеристики інформаційних процесів, наприклад параметри мережевого трафіку, так і відомості про фізичні процеси, що спостерігаються за допомогою сенсорів. Одним із завдань у процесі побудови моделі є виокремлення саме тих ознак, які здатні забезпечити максимальну точність та повноту ідентифікації станів ІБ.

Для цього необхідним є оцінювання інформативності джерел, що забезпечують моніторинг КФС. У практиці розрізняють два базові підходи до такої оцінки: енергетичний і інформаційний. Перший передбачає виділення ознак із найбільшими абсолютними значеннями. Проте в умовах різнорідності фізичних параметрів, що фіксуються системою, цей метод не дозволяє отримати коректні результати. Другий підхід орієнтується на визначення ступеня відмінності між класами станів у просторі ознак, що робить можливим виокремлення найбільш дискримінативних параметрів. Саме інформаційний підхід виявляється придатним для задачі ідентифікації станів ІБ елементів КФС.

Ефективним інструментом у цьому контексті виступає метод головних компонент (МГК). Традиційно він застосовується для зниження розмірності вихідного простору ознак і формування нового простору головних компонент. Однак у даному дослідженні МГК пропонується використовувати як засіб визначення інформативності окремих ознак, що відрізняє запропонований підхід від більшості відомих робіт.

На практиці різні фізичні параметри, які характеризують роботу КФС, мають неоднакові діапазони значень у навчальній вибірці. Це призводить до того, що розклад значною мірою залежить від ознак із більшим розкидом, оскільки вони мають вищу дисперсію і, відповідно, більший внесок у процедуру МГК. Для уникнення подібних спотворень застосовується автошкалювання, що

передбачає поєднання центрування та нормування даних. Таке перетворення забезпечує рівноцінність оцінювання різних змінних незалежно від їх фізичної природи (рис.5).

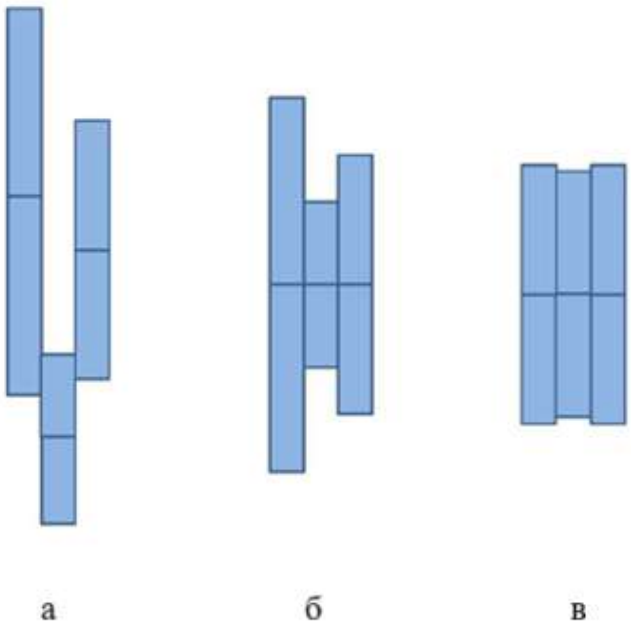

Рисунок 5 – Попередня обробка вихідних даних: а) вихідні дані; б) після центрування; в) після нормування даних

Матриця даних X формується як результат вимірювання параметрів функціонування КФС в дискретні моменти часу:

$$X = \begin{pmatrix} x_1(t_1) & x_2(t_1) & \cdots & x_n(t_1) \\ x_1(t_2) & x_2(t_2) & & x_n(t_2) \\ & \vdots & \ddots & \vdots \\ x_1(t_m) & x_2(t_m) & \cdots & x_n(t_m) \end{pmatrix} \quad (1)$$

де m – кількість векторів даних; n – розмірність простору ознак.

Центрування передбачає віднімання від кожного стовпця x_j його середнього значення:

$$m_j = \frac{x_{1,j}+x_{2,j}+\cdots+x_{n,j}}{n} \quad (2)$$

а нормування здійснюється поділм кожного значення на стандартне відхилення:

$$s_j = \sqrt{\frac{\sum_{i=1}^{n}(x_{i,j}-m_j)^2}{n}} \tag{3}$$

що у поєднання дає вираз автошкалювання:

$$\widetilde{x_{i,J}} = \frac{x_{i,j}-m_j}{s_j} \tag{4}$$

Таким чином, перед застосуванням МГК дані навчальної вибірки підлягають центруванню та нормуванню. Це дозволяє виключити вплив масштабу фізичних величин на результати аналізу та забезпечити адекватне порівняння параметрів, які описують функціонування КФС.

Розклад матриці X за допомогою МГК можна подати у вигляді матричного рівняння:

$$X = TP^T + E \tag{5}$$

де T – матриця рахунків, P – матриця навантажень, E – матриця залишків.

У цьому випадку кожний рядок матриці T являє собою проєкцію вектора попередньо оброблених даних на підпростір головних компонент:

$$T = \begin{pmatrix} t_{1,1} & t_{1,2} & \cdots & t_{1,k} \\ t_{2,1} & t_{2,2} & & t_{2,k} \\ \vdots & & \ddots & \vdots \\ t_{m,1} & t_{m,2} & \cdots & t_{m,k} \end{pmatrix} \tag{6}$$

де m – кількість часових рядів; k – число обраних головних компонент.

Матриця навантажень описує внесок кожної змінної у формування

головних компонент:

$$P = \begin{pmatrix} p_{1,1} & p_{1,2} & \cdots & p_{1,k} \\ p_{2,1} & p_{2,2} & & p_{2,k} \\ \vdots & & \ddots & \vdots \\ p_{n,1} & p_{n,2} & \cdots & p_{n,k} \end{pmatrix} \quad (7)$$

де n – розмірність початкового простору ознак.

Інформативність кожного параметра можна оцінити через нормовану суму квадратів коефіцієнтів навантажень. Якщо позначити інформативність $i-$го параметра як I_{f_i}, то вона визначається формулою:

$$I_{f_i} = \sum_{j=1}^{k} p_{i,j}^2 \quad (8)$$

де k – кількість головних компонент, відібраних для аналізу.

Подальший відбір здійснюється за правилом Кайзера, яке дозволяє зберегти лише ті ознаки, інформативність яких перевищує середнє значення по всіх джерелах:

$$I_{f_i} > \frac{1}{n}\sum_{i=1}^{n} I_{f_i} \quad (9)$$

Таким чином, формується підмножина найбільш значущих параметрів, що зберігає здатність адекватно описувати стан ІБ. Варто наголосити, що інформативність цієї підмножини за своєю величиною є меншою за інформативність повного набору головних компонент, проте її достатньо для створення коректного опису ознак. Застосування описаного методу дозволяє отримати компактне й водночас репрезентативне представлення даних, що описують стан елементів КФС. У подальшому ця модель використовується як основа для багатокласової ідентифікації станів ІБ.

Запропонована модель формування опису ознак стану ІБ демонструє свою

ефективність у задачах багатокласової ідентифікації елементів КФС. Завдяки поєднанню процедур автошкалювання та використанню МГК вдається відібрати оптимальний набір параметрів, які зберігають інформацію про функціонування системи та дозволяють здійснювати подальшу класифікацію з високим рівнем точності.

Особливу увагу слід звернути на той факт, що, незважаючи на зменшення розмірності початкового простору даних, отримане представлення ознак зберігає достатній рівень інформативності. Це забезпечує баланс між обчислювальною ефективністю та надійністю результатів.

2.2 Алгоритм формування опису ознак стану ІБ елементів КФС

Ефективне оцінювання стану ІБ КФС потребує системного підходу до оброблення великої кількості різнорідних даних, які надходять із сенсорних, обчислювальних і комунікаційних компонентів. Як зазначено у підрозділі 2.1, модель формування ознак стану ІБ задає логічну структуру зв’язків між параметрами, що описують поведінку елементів системи. Проте для практичної реалізації цієї моделі необхідно створити алгоритм, який визначає конкретну послідовність операцій, формалізує процедуру виділення ключових характеристик і забезпечує можливість подальшої автоматизованої оцінки рівня безпеки.

Алгоритм формування опису ознак стану ІБ елементів КФС покликаний забезпечити перетворення сирих даних моніторингу у впорядкований вектор ознак, який відображає як технічний, так і поведінковий стан об’єкта. У цьому контексті під ознаками розуміються параметри, що описують взаємозв’язок між поточними значеннями показників функціонування та імовірністю настання небезпечних подій.

Алгоритм побудовано на принципах багаторівневої обробки даних і модульності, що забезпечує гнучкість у його застосуванні для різних типів

елементів КФС від сенсорів і контролерів до серверів керування та шлюзів передачі даних. Структурно він поділяється на сім послідовних етапів, які взаємопов’язані через інформаційні потоки. На рисунку 6 наведено узагальнену схему алгоритму.

Блок-схема алгоритму формування опису ознак стану ІБ елементів КФС ілюструє послідовність виконання основних етапів від підготовки даних і розкладу матриці параметрів до обчислення показників інформативності та остаточного відбору найбільш значущих ознак.

В основу алгоритму покладено такі положення:

– єдність інформаційної моделі, що поєднує фізичні параметри з мережевими характеристиками;

– часова узгодженість даних, яка забезпечує коректність порівнянь і виявлення відхилень;

– адаптивність, що дає змогу враховувати специфіку функціонування різних підсистем;

– інтегрованість із системами моніторингу та аудиту ІБ.

Алгоритм реалізує процес формування ознакового простору для подальшої ідентифікації стану ІБ елементів КФС. Його робота ґрунтується на аналізі параметрів функціонування системи, отриманих у вигляді часових рядів, що надходять із каналів зв’язку, сенсорів та інших джерел.

Першим кроком є формування навчальної вибірки даних X. На цьому етапі з потоку мережевого трафіку виділяються параметри, які характеризують роботу КФС, наприклад, затримки передавання пакетів, частота відмов обладнання чи кількість спроб доступу до системи. Дані збираються протягом тривалого часу для формування достатньо репрезентативного набору. Для цього використовуються такі джерела: журнали подій контролерів (PLC), дані з сенсорів технологічних процесів, трафік мережевого рівня (SCADA), показники систем виявлення вторгнень (IDS), а також інформація з аналітичних панелей безпеки.

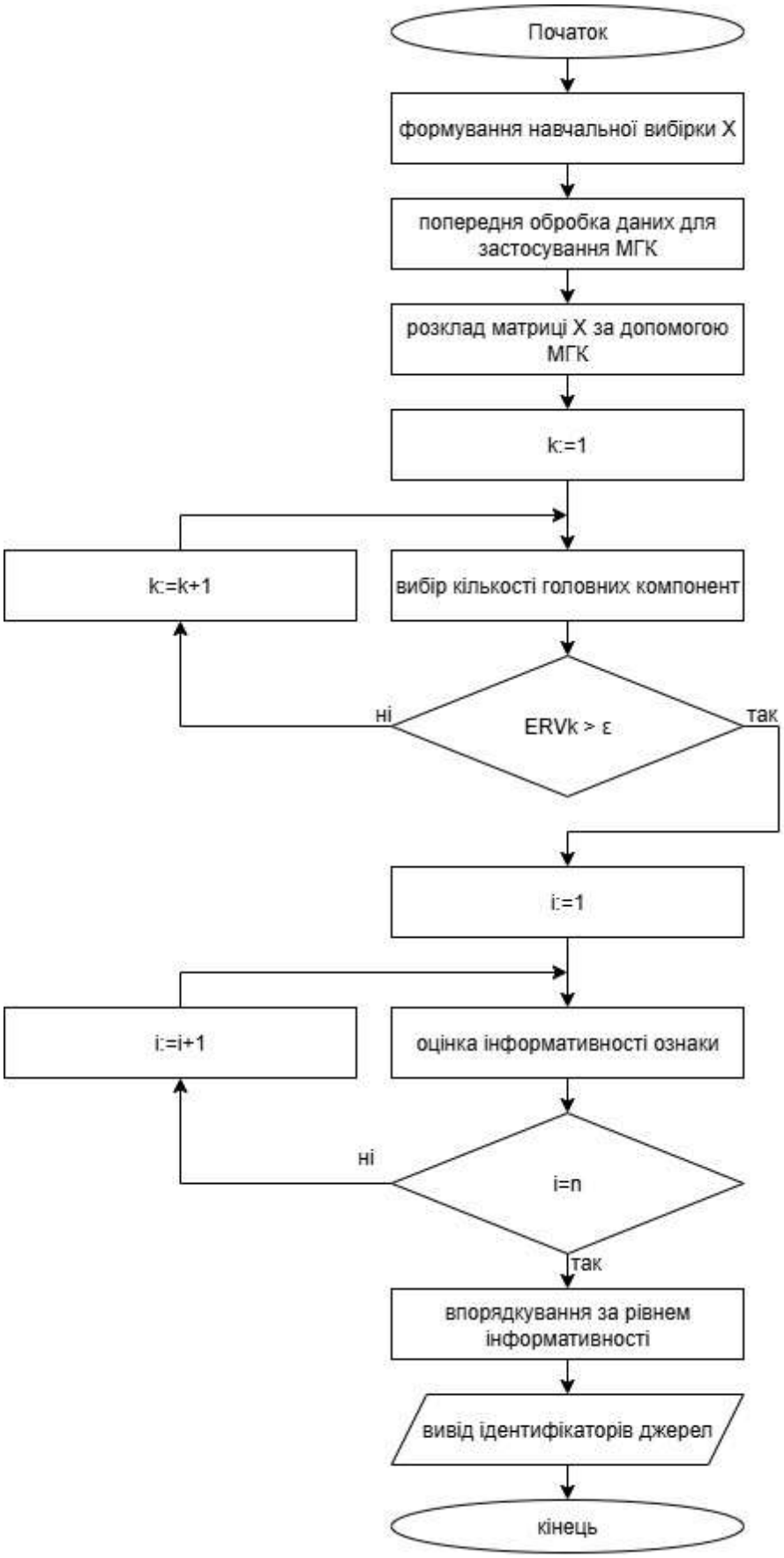

Рисунок 6 - Блок-схема алгоритму формування визнаного опису стану ІБ елементів КФС

Другим кроком є попередня обробка даних. Вона включає автокоригування часових рядів: усунення середнього значення та нормування (приведення даних до єдиного масштабу). Це забезпечує зіставність параметрів, які вимірюються у різних одиницях та мають різні діапазони варіацій.

Далі відбувається розкладання навчальної вибірки за МГК. Суть цього етапу полягає у зведенні багатовимірних даних до меншої кількості нових узагальнених змінних, тобто головних компонент, які пояснюють більшу частину дисперсії початкових даних. Це дозволяє зменшити розмірність простору ознак та відсіяти надлишкову інформацію.

Наступним етапом є обчислення поясненої дисперсії (ERV) для кожної головної компоненти. Поступово, додаючи нові компоненти, перевіряється, чи перевищує частка поясненої дисперсії заданий пороговий рівень ε. Якщо так, то компонента включається у подальший аналіз, якщо ні, то відкидається. Таким чином формується оптимальний набір головних компонент, які найбільш повно відображають поведінку системи.

Після цього здійснюється розрахунок інформативності кожної ознаки. Для кожного параметра обчислюється його внесок у розпізнавання стану ІБ. Це дозволяє виявити, які саме характеристики функціонування КФС є найбільш критичними для визначення безпечного або небезпечного стану.

Отримані значення впорядковуються за рівнем інформативності, після чого формується підсумковий набір ідентифікаторів джерел. У результаті з множини вхідних параметрів вибираються лише ті, що мають найбільшу значущість. Ці ідентифікатори заносяться до архіву і застосовуються у подальших ітераціях навчання моделі для підвищення точності ідентифікації станів ІБ.

Основні переваги алгоритму полягають у його модульності, масштабованості та адаптивності. Він може бути інтегрований до існуючих систем моніторингу (SIEM, IDS) без суттєвої модифікації архітектури. Водночас певним обмеженням є потреба у великому обсязі достовірних вихідних даних і достатніх обчислювальних ресурсах при аналізі у реальному часі. Застосування

алгоритму дає змогу автоматизувати процес оцінки стану ІБ елементів КФС, підвищити точність діагностики аномалій та скоротити час реагування на інциденти. Запропонований алгоритм формування опису ознак стану ІБ елементів КФС забезпечує формалізований підхід до аналізу стану безпеки, ґрунтуючись на об’єктивних вимірюваннях параметрів функціонування системи. Його реалізація дозволяє інтегрувати результати моніторингу у єдину інформаційну модель, що відображає поточний рівень захищеності КФС. Формування векторів ознак створює основу для подальшого кількісного оцінювання рівня ІБ, яке розглядається у наступному параграфі.

2.3 Метод оцінювання стану ІБ елементів КФС

Задачу оцінювання стану ІБ можна сформулювати як класифікацію часових рядів, що відображають роботу елементів КФС. Нехай задано множину з m згрупованих часових рядів, де кожен набір характеризує інформаційні або фізичні процеси КФС:

$$X = \{\{x_1(t_1), x_2(t_1), \dots, x_n(t_1)\}, \{x_1(t_2), x_2(t_2), \dots, x_n(t_2)\}, \dots, \{x_1(t_m), x_2(t_m), \dots, x_n(t_m)\}\} \quad (10)$$

Необхідно визначити мітку класу c, яка відповідає конкретному стану ІБ. Для цього здійснюється навчання моделі на основі експериментальних даних, де кожний сигнал розглядається як послідовність значень у часі.

У роботі використано алгоритм дерев рішень, що належить до групи логічних класифікаторів. Його сутність полягає у побудові бінарного дерева, у внутрішніх вузлах якого розташовані предикати, тоді як листові вершини містять класи $c_i (i = 1, \dots, l)$. Вибір предикатів здійснюється відповідно до критеріїв інформативності.

У такому дереві кожна внутрішня вершина v має функцію $\beta_v: \rightarrow \{0,1\}$, а кожна вершина відповідає прогнозу $c_v \in C$. Перевірка виконується за правилом:

$$\beta_v(x; j, \tau) = [x_j < \tau] \quad (11)$$

де x_j – значення певної ознаки; τ – порогове значення.

Алгоритм $\alpha(x)$ починає обчислення з кореня v_0. Якщо результат дорівнює нулю, то відбувається перехід у ліву гілку, у протилежному випадку у праву. Процес триває, доки не буде досягнуто листа, після чого алгоритм повертає клас, що йому відповідає. У такий спосіб, подаючи на вхід дані у момент часу t, алгоритм $\alpha(x)$ формує відповідь у вигляді мітки класу $c_v \in C$, яка характеризує стан ІБ.

КФС є складними об’єктами, кожен елемент яких може зазнавати різних атак і деструктивних впливів. Тому дані, що надходять від окремих компонентів, можуть відрізнятися за властивостями, і постає завдання ідентифікації стану безпеки за допомогою ансамблю алгоритмів, кожен із яких спеціалізується на власних підвибірках.

На основі методу бутстрепу з початкової вибірки X, що складається з параметрів у m дискретних моментах часу, формується n підвибірок шляхом випадкового відбору з поверненням. У результаті створюються множини $X_1, X_2, \dots, X_n$, які використовуються для незалежного навчання класифікаторів $a_1, a_2, \dots, a_n$. Кожен із них здійснює класифікацію на своєму підпросторі, після чого отримані результати узгоджуються для прийняття остаточного рішення.

Визначення класу для елемента часового ряду може виконуватися двома способами: шляхом консенсусу, коли всі класифікатори повертають однакову мітку, або за правилом простої більшості. Робота ансамблю ілюструється на рисунку 7.

Використання дерев рішень дозволяє встановити клас у момент часу t_i, однак через імовірність похибок можливі хибнопозитивні чи хибнонегативні результати. Для зменшення таких випадків доцільним є врахування рішень класифікатора у кількох попередніх моментах часу $t_{i-n}, t_{i-2}, t_{i-1}, \dots, t_i$. Якщо всі ці моменти розглядати з однаковою значимістю, то ймовірність виявлення атаки

знижується, оскільки згладжуються часові відмінності між подіями (рис. 8).

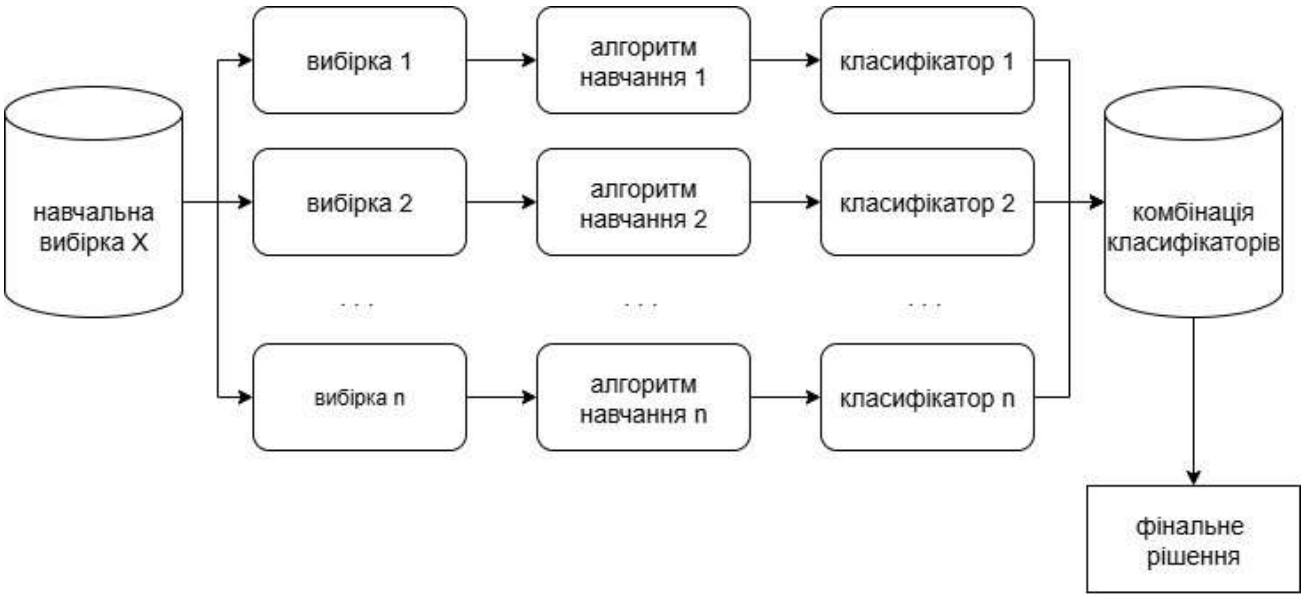

Рисунок 7 - Застосування ансамблю класифікаторів, які працюють паралельно

Рисунок 8 - Тимчасовий графік ідентифікації атаки за рівних значущостей

Щоб надати більшої ваги результатам, наближеним до поточного часу, вводяться коефіцієнти значимості, які зменшуються в міру віддаленості моменту від ti (рис.9).

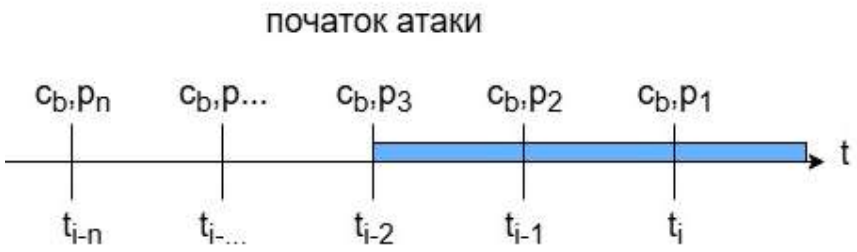

Рисунок 9 - Тимчасовий графік ідентифікації атаки з урахуванням коефіцієнтів значущості

Такі коефіцієнти повинні враховувати обраний часовий горизонт N і задовольняти умові спадання, де кожний наступний коефіцієнт менший за попередній.

$$r_1 = N, r_i = r_{i-1} - 1 \quad (12)$$

де N – довжина інтервалу Δ.

Для цього застосовуються вагові коефіцієнти Фішберна, що утворюють арифметичну прогресію:

$$p_i = \frac{r_i}{\sum_{j=1}^{N} j} \quad (13)$$

де p_i – ваговий коефіцієнт для $i-$го моменту часу.

Результати класифікації усереднюються з урахуванням ваг, що дозволяє підвищити точність ідентифікації. На першому етапі кожен алгоритм $a_1, a_2, \dots, a_n$, побудований на основі дерева рішень, генерує відповіді протягом інтервалу Δ. Після цього відбувається їхнє об'єднання за допомогою вагових коефіцієнтів Фішберна, коли клас визначається через зважене узагальнення. Якщо ваги виявляються рівними, вибір робиться на користь результату для більш пізнього моменту часу. На другому етапі результати всіх класифікаторів поєднуються, а остаточне рішення приймається за правилом простої більшості, що ефективно реалізується при непарному числі класифікаторів. Схема комбінованого підходу наведена на рисунку 10.

Запропонований метод дозволяє суттєво підвищити повноту та точність ідентифікації станів інформаційної безпеки елементів КФС завдяки поєднанню паралельно працюючих класифікаторів і вагових коефіцієнтів Фішберна.

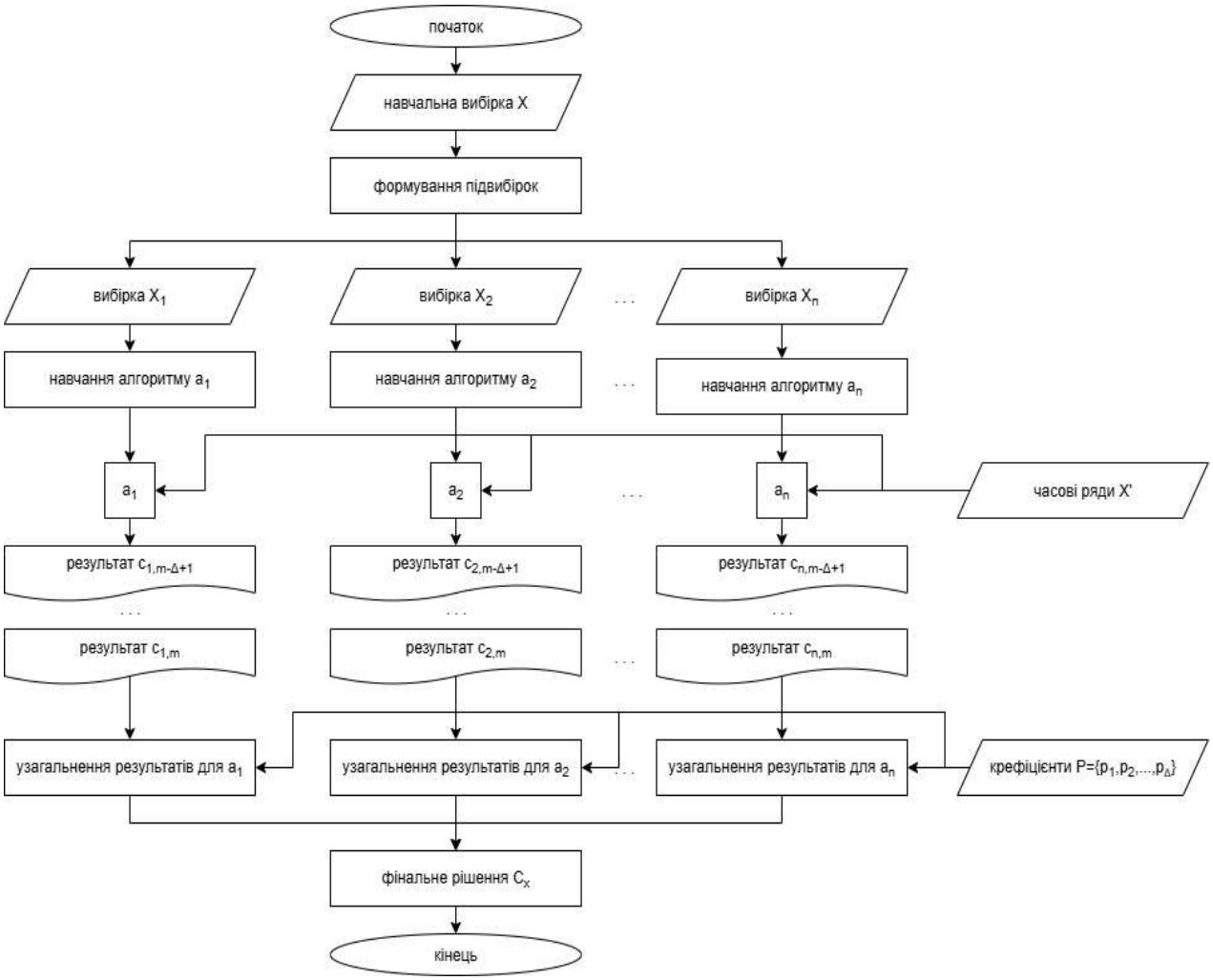

Рисунок 10 – Метод оцінки стану ІБ елементів КФС

2.4 Метод ідентифікації стану ІБ елементів КФС

Інтеграція КФС у виробничі та технологічні процеси зумовила необхідність створення спеціалізованої методики, яка б дозволяла ідентифікувати стан їхньої ІБ в умовах реалізації потенційних загроз. Розробка такої методики має враховувати ключові особливості архітектури та функціонування КФС.

Головною вимогою є обробка вхідного трафіку та виділення часових рядів у режимі реального часу з мінімальною затримкою, зумовленою обчислювальними можливостями контролюючих пристроїв і каналів передавання даних. Це дозволяє вчасно виявляти атаки та оперативно реагувати

на них. Водночас у випадку апостеріорного аналізу необхідне повне дослідження часових рядів, щоб простежити поширення інциденту. Методика повинна демонструвати стійкість до різних типів атак, незалежно від їхньої складності, способу реалізації чи ресурсної затратності. Вона також має бути універсальною, з можливістю застосування до різнорідних пристроїв КФС, що особливо важливо з огляду на різноманітність їхніх компонентів. Окрім цього, результат ідентифікації стану безпеки має бути доступним у кожний момент часу з урахуванням частоти оновлення даних, що дозволяє порівнювати їх динаміку та визначати тривалість деструктивних впливів.

У межах дослідження запропоновано здійснювати ідентифікацію станів ІБ елементів КФС шляхом аналізу часових рядів, що відображають відхилення поточного стану від дозволених. На основі такого підходу формується метод виявлення порушень. Вона спирається на початкове просторове представлення ознак, що включає дані про процеси зберігання, обробки та передавання інформації. Це просторове представлення охоплює безпечні та аномальні стани, які розділяються на відповідні класи.

Початковий простір ознак $H = (f_1, f_2, \dots, f_n)$ складається з n джерел даних про процеси зберігання, обробки та передавання інформації КФС. Існує кінцева множина станів ІБ $\{C_0, C_1\} \subset C$, де C_0 – множина міток класів безпечних станів ІБ КФС, а C_1 – множина міток класів аномальних (небезпечних) станів ІБ. Отож, маємо $\{c_1, c_2, \dots, c_k\} \subset C_0, \{c_{k+1}, c_{k+2}, \dots, c_l\} \subset C_1$, де l – кількість ідентифікованих станів ІБ КФС.

Метод складається з трьох послідовних етапів (рис.11). На першому відбувається формування архіву ідентифікаторів джерел, що передбачає моделювання різних станів ІБ КФС. Для цього використовуються як спеціалізовані програми, так і керуючі команди, що дозволяє отримати залежності між кількісними показниками інформаційних процесів і конкретними станами безпеки. Для побудови архіву необхідні параметри функціонування системи за тривалий проміжок часу, які збираються за допомогою датчиків або внутрішніх програмно-апаратних модулів. Результатом стає формування масиву

часових рядів, які після попередньої обробки подаються на вхід формувача інформативних ознак. Результатом етапу формування навчальної бази є m часових рядів, згрупованих за часом t. Таким чином створюється унікальне для конкретної системи описання станів безпеки, що зберігається в архіві ідентифікаторів та оновлюється лише у випадку зміни навчальної вибірки.

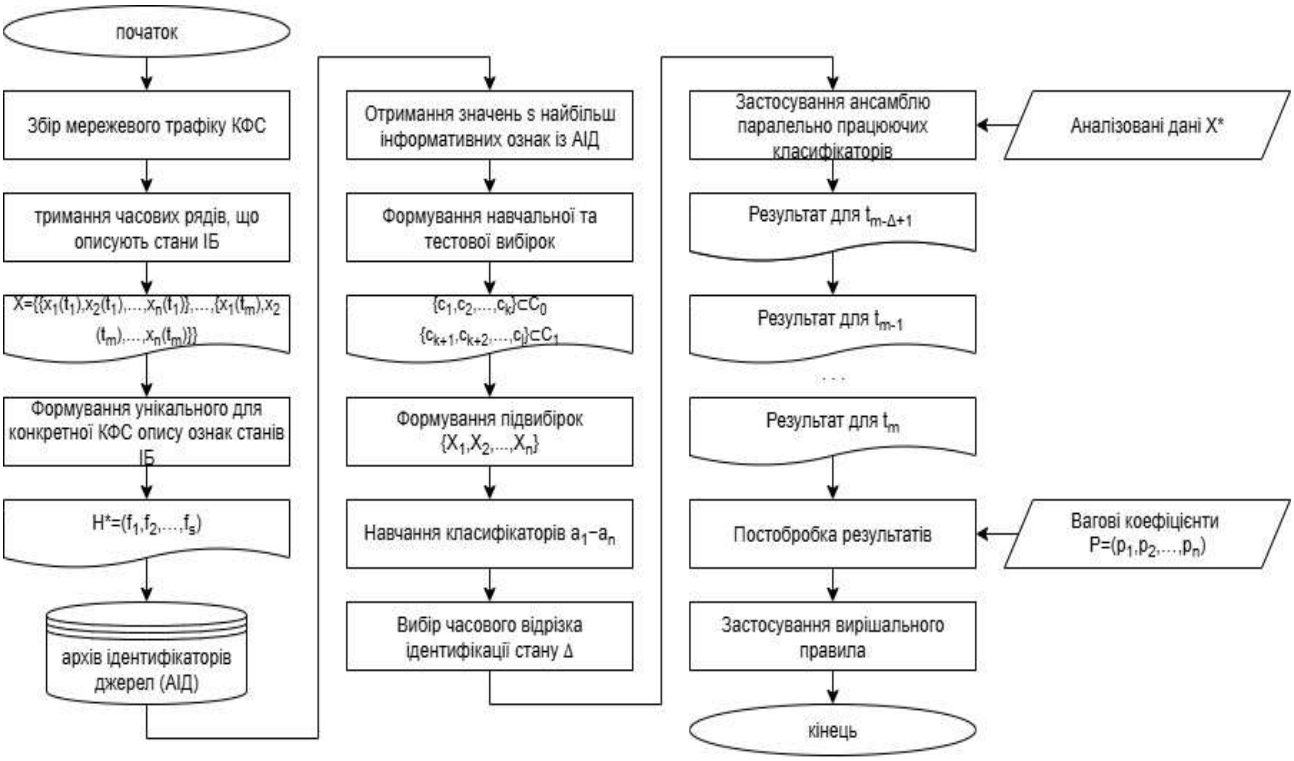

Рисунок 11 - Блок-схема методу ідентифікації стану ІБ елементів КФС

На другій стадії здійснюється вибір інформативних ознак, які отримуються з архіву, після чого з початкових часових рядів вилучаються зайві дані. Сформований кортеж значень зіставляється з мітками класів, що відображають поточний стан безпеки. З цього набору формується навчальна й тестова вибірки: більша частина використовується для навчання алгоритмів класифікації, тоді як менша для перевірки їхньої ефективності. Алгоритми класифікації працюють паралельно та незалежно один від одного, що підвищує точність і надійність процесу. На завершення цієї стадії обирається часовий інтервал ідентифікації, який забезпечує найвищу ефективність класифікації, зокрема максимізацію F-міри для контрольованої системи.

Заключна стадія передбачає використання отриманих даних для подачі їх на вхід алгоритму оцінки стану ІБ елементів КФС. Такий алгоритм побудований на комбінованому підході, що об’єднує результати роботи ансамблю класифікаторів. Після цього результати додатково обробляються за допомогою вагових коефіцієнтів, які надають більшої значущості останнім спостереженням. Фінальним результатом є формування висновку про поточний стан ІБ системи, який може використовуватися для подальшого моніторингу, реагування на інциденти та підвищення загальної стійкості КФС. Отримані результати ансамблю класифікаторів для кожного моменту часу, згенеровані класифікаторами $a_1 - a_n$, додатково обробляються із використанням вагових коефіцієнтів Фішбера, які надають підвищену вагу пізнішим результатам ідентифікації. Завершальним кроком методики є формування на основі вирішального правила інтегрального результату ідентифікації стану ІБ елементів КФС.

2.5 Використання результатів дослідження для підвищення захищеності КФС від зовнішніх впливів

Проведене дослідження було зосереджене на вдосконаленні підходів до виявлення порушень ІБ КФС шляхом аналізу часових рядів, що відображають як інформаційні, так і фізичні процеси їх функціонування. Отримані результати дозволили доповнити та розширити існуючі моделі, методи і методики загальної теорії ІБ, а розроблені у межах роботи модель, метод і методику можна застосовувати в практичних системах, які забезпечують безперервне виконання цільових функцій КФС.

Оскільки головною умовою ефективного функціонування КФС є гарантоване та безперервне досягнення цільових завдань, ідентифікація порушень ІБ набуває критичного значення. До впровадження розробленого методу реалізація загроз через використання вразливостей системи могла

здійснюватися зловмисником у спосіб, продемонстрований на рисунку 12.

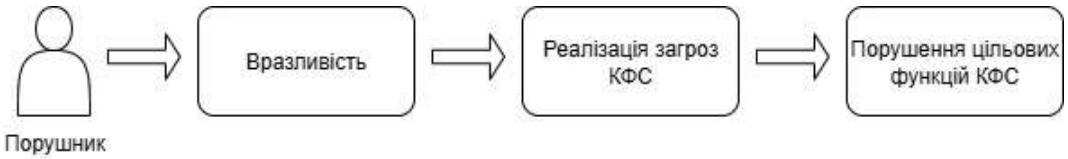

Рисунок 12 - Вплив порушника на КФС

Як видно з рисунку 13, множину можливих станів ІБ КФС можна описати за допомогою чотирьох базових ситуацій.

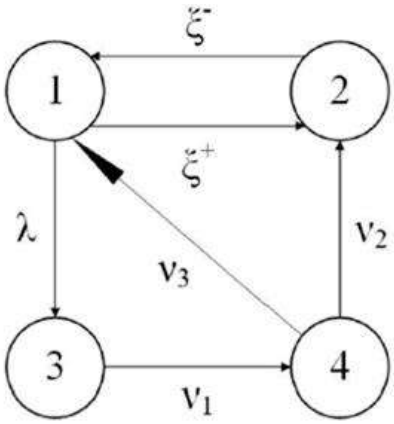

Рисунок 13 - Граф стану ІБ

Перша з них відповідає початковому моменту запуску системи та початку роботи моніторингу. Друга характеризує стан, за якого досягається цільова функція системи, однак розвиток подій у ній може відбуватися за двома сценаріями: у випадку успішної реалізації атаки настає зрив виконання завдань, що повертає систему до першого стану, тоді як за умови коректної роботи механізмів ІБ КФС зберігає своє перебування у другому стані. Параметр λ позначає зовнішній вплив на систему, що у разі його реалізації переводить її до третього стану, який потребує додаткових ресурсів чи залучення спеціалістів. У результаті будь-якого впливу, як зловмисного, так і випадкового, КФС переходить до четвертого стану, що відповідає фазі реагування на отримані сигнали моніторингу. Звідси система може повернутися у початковий стан при негативному розвитку подій або ж перейти у другий стан, якщо реагування було

своєчасним і результативним.

Застосування запропонованого методу дозволяє мінімізувати описані ризики та суттєво підвищити здатність КФС протидіяти як навмисним атакам, так і випадковим зовнішнім впливам. Вона може використовуватися для оцінювання рівня захищеності системи від інформаційних загроз у процесі експлуатації, виконуючи роль технічного інструмента аудиту безпеки. При цьому методика здатна не лише виявляти порушення, викликані діями зловмисників, але й фіксувати відхилення у параметрах функціонування, пов’язані з природним зносом технологічних вузлів.

Завдяки отриманню актуальної інформації про реальний стан ІБ об’єкта стає можливим суттєво посилити захищеність КФС, прискорити процес реагування на інциденти та реалізувати динамічне переконфігурування, що повертає систему у стійкий стан. Це знижує вплив негативних факторів на виконання цільових функцій і формує підґрунтя для розвитку проактивних механізмів безпеки. У разі, якщо інцидент уже відбувся, розроблена методика може використовуватися як засіб апостеріорного аналізу, що дозволяє встановити джерело порушення та визначити превентивні заходи, спрямовані на зниження ймовірності повторення подібних подій (рисунок 14).

Рисунок 14 - Цикл забезпечення ІБ КФС

Підхід до забезпечення інформаційної та функціональної безпеки об’єктів на основі принципу зворотного зв’язку може стати наступним етапом розвитку систем комплексного захисту КФС, де методи аналізу часових рядів та ідентифікації станів ІБ інтегруються у концепцію підтримання стійкого функціонування навіть за умов активного впливу загроз (рисунок 15).

Рисунок 15 - Концепція підтримання стійкого функціонування КФС на основі принципу зворотного зв’язку

Важливим доповненням є часові характеристики реалізації основних елементів підходу. Серед них виокремлюють середній час виконання цільової функції системи, час прояву проблеми, час її ідентифікації та період, необхідний для нейтралізації негативних наслідків. Врахування цих параметрів дає змогу підвищити ефективність комплексного забезпечення безпечного функціонування КФС.

Технологія динамічного захисту, яка включає розроблений метод ідентифікації стану ІБ елементів КФС, є складною для реалізації, проте її впровадження розглядається як перспективний і стратегічно важливий напрямок подальшого розвитку кіберзахисту.

2.6 Інтеграція методу з існуючими системами моніторингу

Запропонований метод ідентифікації та оцінювання стану ІБ елементів

КФС може бути інтегрований у сучасну інфраструктуру моніторингу на різних рівнях організації даних. Його модульна структура дає змогу реалізувати метод як незалежний аналітичний компонент або як розширення існуючих підсистем спостереження, зокрема в межах промислових мереж, корпоративних дата-центрів чи об’єктів критичної інфраструктури.

На крайовому рівні (edge) модуль попередньої обробки та відбору ознак може розгортатися безпосередньо на шлюзах, контролерах або локальних вузлах системи керування. Такий підхід мінімізує затримки у виявленні загроз і зменшує навантаження на канали передавання даних, оскільки первинна фільтрація виконується ще до надходження інформації у центральний сегмент. Наприклад, локальний контролер може самостійно аналізувати параметри мережевого трафіку, частоту запитів або рівень споживання ресурсів і передавати до центру лише стислі профілі аномалій. Це особливо важливо для промислових систем, де критичною є затримка сигналів управління, а надмірна передача даних може створювати ризики перевантаження каналів.

Альтернативним рішенням є централізована інтеграція, коли зібрані часові ряди та інші параметри функціонування агрегуються у спеціалізованому центрі обробки даних чи у системі класу SIEM. У такому випадку метод забезпечує комплексний аналіз і кореляцію подій між різними об’єктами інфраструктури, дозволяючи виявляти міжсистемні залежності та координацію атак. Наприклад, поєднання сигналів з енергетичного сегмента та мережевих логів інформаційних систем може виявити атаку, яка одночасно спрямована на зниження стабільності живлення та порушення обміну даними.

У практиці промислових підприємств найбільш перспективною є гібридна топологія, яка поєднує можливості локальної попередньої обробки з централізованим поглибленим аналізом. Локальні вузли відповідають за виявлення базових відхилень у режимі реального часу, тоді як центральний аналітичний сервер виконує навчання моделей, кореляцію подій і прогнозування ризиків на підставі історичних даних. Такий підхід дозволяє одночасно забезпечити низьку затримку реагування та високу точність оцінки, що є

особливо важливим для систем критичного призначення.

Для досягнення сумісності з наявними системами моніторингу доцільно використовувати уніфіковані формати та протоколи передавання даних, зокрема Syslog, Common Event Format (CEF), JSON або REST API. Ці формати забезпечують можливість обміну структурованою інформацією між різними підсистемами без втрати семантичного змісту повідомлень. У промислових середовищах важливим є також забезпечення взаємодії з такими стандартами, як Modbus/TCP, OPC-UA чи MQTT, які дозволяють зчитувати значення від програмованих логічних контролерів і сенсорів у режимі реального часу.

Наявність проміжного шару нормалізації, що синхронізує часові мітки, узгоджує формати та перетворює сирі журнали подій у єдиний формат ознак, є обов'язковою умовою коректної роботи методу. Цей шар може виконувати роль адаптера між середовищами OT (операційні технології) та IT, забезпечуючи єдину інтерпретацію подій безпеки. Наприклад, подія «зміна параметра контролера» у SCADA-системі може бути автоматично трансформована у формат події SIEM з додатковими атрибутами - часом, користувачем, рівнем критичності та цифровим відбитком зміненої конфігурації.

Для підвищення гнучкості доцільно застосовувати API-рівень інтеграції, який дозволяє підключати аналітичні модулі без потреби у зміні коду базової системи моніторингу. Це спрощує впровадження методу у середовище з уже налаштованою інфраструктурою безпеки.

У контексті інтеграції з SIEM-системами результати роботи моделі можуть передаватися у вигляді додаткових індикаторів ризику. Доцільним є не лише повідомлення про наявність аномалії, але й надання числової оцінки ризику, часових характеристик інциденту та переліку ознак, що найбільшою мірою вплинули на рішення. Такі індикатори можуть корелюватися з іншими сигналами безпеки (мережевими, системними, поведінковими), що дозволяє знизити ймовірність хибних спрацювань та підвищує якість реагування.

Інтеграція у середовище SIEM також забезпечує можливість автоматизації реакцій: ізоляції сегменту мережі, блокування підозрілої сесії, зміни правил

доступу, оновлення політик безпеки чи генерації термінових сповіщень для операторів. Наприклад, при перевищенні певного порогу ризику система може автоматично перевести контролер у режим локального управління, запобігаючи поширенню загрози далі мережею.

Важливою складовою впровадження методу є його інтеграція у життєвий цикл управління ІБ. Йдеться про зв’язок із процесами інвентаризації активів, керування оновленнями, управління інцидентами, оцінки ризиків та звітності.

Наприклад, дані, отримані від моделі, можуть автоматично вноситися у базу конфігурацій (CMDB), що забезпечує актуалізацію стану активів. При виявленні аномалії система може ініціювати запит на оновлення прошивки або перевірку політик доступу. Для підтримання ефективності необхідним є періодичне перенавчання моделей на основі реальних даних конкретного об’єкта, що дозволяє зберігати точність виявлення навіть після зміни конфігурації або модернізації системи.

Інтеграція з системами реагування на інциденти (IRP/SOAR) забезпечує можливість автоматизованого документування подій, формування звітів та передачу даних у відповідні підрозділи безпеки. Попри універсальність, метод має низку обмежень. Найбільш складними для виявлення залишаються інсайдерські загрози, коли зловмисник діє з використанням легітимних облікових записів, а його поведінка майже не відрізняється від дій звичайного користувача. Значні труднощі виникають також під час виявлення атак типу “low-and-slow”, які реалізуються упродовж тривалого часу з мінімальною інтенсивністю. Такі атаки не формують виражених аномалій у коротких часових інтервалах, тому вимагають накопичення великого обсягу історичних даних і застосування методів контекстного аналізу.

Додатковим викликом є протидія апаратним закладкам або модифікаціям прошивки, оскільки такі втручання можуть не відображатися у даних телеметрії. Виявлення аномалій у зашифрованому мережевому трафіку також залишається обмеженим, особливо коли відсутній доступ до метаданих або неможлива терміналізація з’єднання. Труднощі спостерігаються й під час ідентифікації

координованих мультивекторних атак, які відбуваються одночасно на різних рівнях системи: мережевому, програмному та фізичному. Для їх виявлення потрібна глибока кореляція подій з різнорідних джерел, що збільшує вимоги до обчислювальних ресурсів.

Окремо слід відзначити проблему підміни сенсорних сигналів (sensor spoofing), коли зловмисник генерує дані, що імітують нормальні фізичні процеси. Такі атаки особливо небезпечні для промислових систем, оскільки можуть залишатися непоміченими навіть при активному мережевому моніторингу.

Зазначені обмеження можуть бути частково компенсовані через використання додаткових джерел інформації. Серед найбільш значущих варто виокремити журнали подій з промислових контролерів та операторських станцій, дані про цілісність прошивок і системних компонентів, а також мережеві метадані, що дозволяють аналізувати поведінку з’єднань навіть без доступу до їхнього вмісту.

Ефективним напрямом удосконалення є застосування незалежних фізичних датчиків для контролю достовірності показників основних сенсорів, що дозволяє виявляти спуфінг або підміну даних. Додатково можна залучати інформацію з інвентаризаційних систем, репозиторіїв оновлень, журналів аудиту конфігурацій та зовнішніх джерел розвідки загроз.

Поєднання таких різнорідних даних із поведінковим аналізом створює багатовимірну інформаційну модель, що підвищує чутливість методу до прихованих або комбінованих атак. Це дозволяє зменшити ймовірність пропуску складних загроз і забезпечує більш високий рівень захищеності КФС навіть у мінливому інформаційному середовищі.

2.7 Висновки до розділу

У розділі сформульовано теоретичні основи для опису ознак, розроблено

алгоритми формування ознакового простору та запропоновано метод оцінювання стану ІБ, який поєднує ансамблеві класифікатори з механізмом вагових коефіцієнтів. Також наведено методику ідентифікації станів безпеки у режимі реального часу та розглянуто практичні аспекти використання отриманих результатів для підвищення захищеності систем від зовнішніх впливів.

Ключовим науковим результатом є побудова моделі формування опису ознак, що враховує різнорідність інформаційних та фізичних параметрів КФС. Застосування МГК дозволило знизити розмірність простору даних та відібрати найбільш інформативні параметри, які забезпечують адекватність подальшої ідентифікації. Поєднання процедур автошкалювання, центрирування і нормування дало змогу досягти рівноцінності у представленні ознак незалежно від їх фізичної природи. Це створило умови для формування компактного, але водночас репрезентативного опису станів безпеки.

На основі побудованої моделі розроблено алгоритм формування ознакового простору, який уніфікує процес збору, попередньої обробки та відбору параметрів. Його особливістю є можливість оцінювання інформативності кожної ознаки з подальшим ранжуванням та архівацією найбільш значущих характеристик. Такий підхід забезпечує підвищення точності ідентифікації при зниженні обчислювальних витрат.

Метод оцінювання стану ІБ елементів КФС реалізовано на основі ансамблю дерев рішень, який доповнено механізмом вагових коефіцієнтів Фішберна. Це дозволило врахувати часову динаміку атак та надати більшої значущості останнім спостереженням. У результаті підвищилася стійкість моделі до хибних спрацювань та забезпечено збалансованість між точністю та повнотою класифікації. Додатковим здобутком стала можливість обробки даних у режимі близькому до реального часу, що критично важливо для своєчасного реагування на інциденти у промислових системах.

Розроблений метод ідентифікації станів ІБ враховує як поточний, так і апостеріорний аналіз. Вона передбачає багаторівневу обробку даних, починаючи

від моделювання різних станів системи та формування навчальної бази, і завершуючи інтегральним прийняттям рішення за допомогою ансамблевих алгоритмів. Важливою перевагою є універсальність методу, який дозволяє застосовувати його до широкого спектра КФС від енергетичних мереж до транспортних комплексів і медичних пристроїв.

Окрему увагу приділено питанням інтеграції розробленого підходу з існуючими системами моніторингу, такими як SCADA та SIEM. Було показано, що поєднання локальної обробки даних на крайових пристроях із централізованим аналізом у системах управління інцидентами створює умови для формування багаторівневої архітектури захисту. Така архітектура дозволяє поєднувати швидкість локального реагування із глибиною аналітики, властивою централізованим рішенням. При цьому важливим завданням стає уніфікація форматів даних та їх нормалізація, що забезпечує сумісність між різнорідними компонентами.

Таким чином, другий розділ демонструє цілісну концепцію побудови та застосування моделі та методу оцінювання рівня захищеності КФС. Запропонований підхід поєднує математичну строгість і практичну орієнтованість, що робить його придатним для подальшої інтеграції у сучасні технології моніторингу ІБ. Незважаючи на наявність певних обмежень, робота створює підґрунтя для розробки більш гнучких і масштабованих систем захисту, здатних ефективно функціонувати в умовах зростання складності інформаційних та фізичних загроз.

3 ОЦІНЮВАННЯ ДОСТОВІРНОСТІ МЕТОДУ ОЦІНЮВАННЯ РІВНЯ ЗАХИЩЕНОСТІ КФС ВІД ІНФОРМАЦІЙНИХ ЗАГРОЗ

3.1 Тестове середовище експериментальної перевірки достовірності результатів

Метою розробленого методу є створення репрезентативної, відтворюваної та статистично обґрунтованої процедури перевірки коректності і надійності запропонованих алгоритмів виявлення аномалій та оцінювання поведінкових характеристик мережевих об’єктів у КФС. Метод охоплює апаратну базу та програмне забезпечення, топологію та схему включення пристроїв у експериментальну мережу, процедури формування та анотації набору даних, конфігурацію середовища тестування, порядок виконання експериментальних прогонів, набір метрик для кількісної оцінки і статистичні методи верифікації результатів. Опис обладнання починається зі специфікації периферійних платформ, які використовувалися для емуляції краю мережі та сенсорних вузлів: у роль апаратних елементів були залучені компактні мікрокомп’ютери з архітектурою ARM, оснащені не менше ніж 4 ГБ оперативної пам’яті і дисковим простором не менше 128 ГБ для локального кешування логів, промислові шлюзи з функцією залишкового зберігання даних та маршрутизатори зі здатністю обробляти багаторівневі VLAN, що забезпечували сегментацію трафіку. Серверна частина експерименту була реалізована на віртуалізованій інфраструктурі з виділеними віртуальними машинами для модулів збору трафіку, модулів попередньої обробки та модулів аналітики; параметри апаратної платформи серверів включали багатоядерні процесори, оперативну пам’ять не менше 64 ГБ і мережеві інтерфейси з пропускною спроможністю щонайменше 10 Gbps для коректної емулювання пікових навантажень. Програмна частина експериментальної установки охоплювала інструментарій для перехоплення трафіку, збереження пакетів у форматі pcap, засоби системного логування, а також середовище для розгортання алгоритмів машинного навчання; ключовими компонентами були інструменти збору пакетів

і логів, рушії для обробки повідомлень на базі MQTT, рушії розгортання контейнерів та мовні бібліотеки для обробки і навчання моделей.

Схема включення пристроїв у експериментальну топологію спроектована так, щоб гарантувати відокремленість тестового трафіку від зовнішньої мережі і забезпечити можливість детального моніторингу кожного каналу зв'язку. Пристрої краю мережі підключалися до регульованого комутатора у конфігурації з виділеними VLAN для передачі телеметрії, керування та діагностики. На центральному сегменті знаходилися віртуальні машини для прийому та агрегації повідомлень, де вхідні потоки зберігалися у двох паралельних репліках: одна репліка призначалася для навчання моделей, інша зберігалася в архіві для відтворюваних тестів. Канал перехоплення пакетів був організований так, щоб дозволяти одночасний запис сирих пакетів і метаданих сесій на окремі носії з синхронізацією часових маркерів через протокол NTP, що надало можливість відновити послідовність подій з точністю до мілісекунд. Для імітації типових і аномальних сценаріїв в експериментальній мережі використовувалися автоматизовані генератори навантаження, параметризовані сценарії атак і контролювані змінні навантаження, що дозволяло задавати рівні інтенсивності, тривалості та комбіновані вектори впливу на мережеву поведінку.

Формування набору даних здійснювалося в кілька взаємопов’язаних етапів, при цьому кожен етап документувався в експериментальному журналі з вказівкою відповідальних осіб, часових підписів та конфігурацій обладнання. Спочатку відбувався збір сирих даних з усіх джерел: pcap-файли перехоплених мережевих потоків, системні логи пристроїв, метрики апаратних ресурсів, результати опитувань стану сенсорів та журнал роботи прикладних сервісів. Далі виконувалася попередня обробка сирих даних, що включала корекцію часових міток, фільтрацію неповних або корумпованих записів, агрегацію сесій і побудову агрегованих ознак за визначеними часовими вікнами. Процес анотації даних поєднував автоматичні правила маркування (за відомими сигнатурами атак та за порушеннями порогових значень) і ручну експертну валідацію; позначено кожну подію категорією, ступенем упевненості та джерелом

походження маркування. Журнал подій включав метадані про те коли саме додано кожну мітку, які правила застосовувалися для автоматичної розмітки, та сумарну статистику узгодженості між експертами, що дозволяло оцінити узгодженість розмітки до проведення навчання моделей. Усі трансформації набору даних зберігалися у формі невідворотних скриптів, що забезпечувало відтворюваність підготовки даних при повторних експериментах.

Середовище тестування сконфігуровано як контрольоване ізольоване середовище, яке реплікує реальні умови експлуатації при збереженні можливості точної реплікації сценаріїв. Кліматичні та фізичні умови експериментального стенда були зафіксовані і підтримувалися в сталих межах, що зменшувало вплив зовнішніх факторів на вимірювані показники. Мережеві характеристики тестового середовища вимірювалися окремими пробними запусками для визначення базової латентності, пропускної здатності і рівня фону пакетної втрати. Для визначення порогових значень аномалій передбачалося виконання контрольних пропусків у штатному режимі, на підставі яких формувалися профілі типової поведінки. Кожен експериментальний прогін супроводжувався записом стану середовища, включно з відомими версіями програмного забезпечення, набором активних сервісів і використовуваними конфігураціями, що дозволяло потім зіставляти результати в умовах змінних конфігурацій.

Порядок проведення експерименту був стандартизований так, щоб мінімізувати внутрішню варіативність результатів і забезпечити адекватну статистичну потужність дослідження. На початку кожної серії запусків виконувалася ініціалізація та перевірка коректності синхронізації часових міток, запуск агентів збору і збереження контрольної вибірки даних у вигляді репліки. Далі проводилися послідовні прогони у штатному режимі для отримання базових профілів, після чого виконувалася серія контрольованих інцидентів з поступовим збільшенням інтенсивності впливу. Кожний сценарій імітації аномалії повторювався багаторазово для накопичення статистики, при цьому принаймні частина прогонів здійснювалася різними операторами, щоб захопити можливі варіації, пов'язані з людським фактором. Після кожної серії

здійснювалася перевірка сукупності отриманих логів і механічна валідація анотацій, а також автоматизований збір ключових метрик якості роботи алгоритмів.

Для кількісної оцінки достовірності результатів використовувався набір стандартних метрик, доповнений статистичними тестами на значущість отриманих відмінностей. Основні метрики засновані на елементах матриці невизначеності: число істинно позитивних спрацювань TP, істинно негативних TN, хибно позитивних FP та хибно негативних FN.

Точність системи визначається як відношення правильно класифікованих випадків до загальної кількості випадків і обчислюється за формулою:

$$Precision = \frac{TP}{TP+FP} \tag{14}$$

Повнота є однією з основних метрик, що використовується для оцінювання достовірності роботи системи класифікації станів ІБ. Вона показує, яку частку реальних позитивних випадків система змогла коректно ідентифікувати серед усіх дійсно наявних. Іншими словами, цей показник характеризує здатність алгоритму мінімізувати кількість пропущених загроз. Формально показник повноти обчислюється за співвідношенням:

$$Recall = \frac{TP}{TP+FN} \tag{15}$$

Баланс між цими двома метриками виміряється через Fscore, що є гармонійним середнім

$$F\ score = \frac{Recall+Precision}{2} \tag{16}$$

Частота хибних спрацьовувань обчислюється як:

$$FPR = \frac{FP}{FP+TN} \quad (17)$$

Для оцінки роздільної здатності алгоритму було використано побуддову кривої ROC і обчислення площі під кривою AUC, де AUC інтерпретується як ймовірність того, що випадковий позитивний приклад отримає більш високий попереджувальний бал, ніж випадковий негативний. Формально AUC може бути апроксимовано як інтеграл від функції $TPR(FPR)$: $AUC = \int_0^1 TPR(t)dFPR(t)$. Для оцінки статистичної значущості відмінностей між двома версіями алгоритмів використовувався двовибірковий t-критерій для незалежних вибірок з тестом на рівність дисперсій або з поправкою Уелча при її невиконанні. Статистика t для двох середніх задається як $t = \frac{\overline{x_1}-\overline{x_2}}{\sqrt{\frac{s_1^2}{n_1}+\frac{s_2^2}{n_2}}}$, де $\overline{x_i}$ – середнє значення метрики на і-й вибірці, s_i^2 – вибіркова дисперсія, n_i – розмір вибірки.

Порядок інтерпретації отриманих кількісних результатів ґрунтувався на комбінованому підході. По-перше, первинна фільтрація аномалій виконувалася з урахуванням порогу на FPR, встановленого експериментально на основі профілю штатної роботи. По-друге, порівняння моделей здійснювалося через багатовимірний критерій, що враховував одночасно F1, AUC і стабільність метрик у часі (визначену як стандартне відхилення метрики при повторних прогонах). Для підтвердження відтворюваності дослідження частина тестів виконувалася в іншому апаратному середовищі з ідентичними конфігураціями ПЗ, а також залучалися інші експерти до процесу анотації, результати співставлялися і аналізувалися на предмет систематичних відхилень.

Документування здійснювалося у вигляді машинозчитуваних протоколів, що включали повні конфігураційні дампи, скрипти для підготовки даних, набори параметрів для генераторів навантаження та повні лог-файли експериментів. Такий підхід забезпечував можливість повного відтворення експерименту незалежними дослідниками та створював підґрунтя для подальшого масштабування і валідації алгоритмів у реальних операційних середовищах.

3.2 Експериментальні результати моделювання станів КФС

У ході дослідження було змодельовано три класи станів системи: штатний режим, легка аномалія та серйозна атака. Кожен із цих станів характеризувався різним рівнем відхилень у роботі сенсорних вузлів, контролерів та каналів комунікації. Для кожного стану було сформовано по тисячі спостережень, у межах яких реєструвалися такі параметри, як інтенсивність мережевого трафіку, середня затримка обміну даними, частота обробки команд контролера, рівень шумів у сенсорних каналах, температурні та вольтажні показники, а також часові інтервали відгуку системи на команди керування. Таким чином, модель відтворювала широкий спектр реалістичних умов, що дозволило отримати репрезентативну вибірку для оцінки ефективності алгоритму.

Для аналізу достовірності роботи моделі використовувалися основні метрики класифікації: істинні позитиви (TP), істинні негативи (TN), хибні позитиви (FP) та хибні негативи (FN). На основі цих базових показників були обчислені похідні метрики Precision, Recall, FPR та F1-score, які дозволили здійснити комплексну оцінку здатності системи виявляти відхилення від нормального функціонування. Усі обчислення проводилися за стандартними статистичними формулами, а для зменшення похибки використовувалися усереднені результати кількох експериментальних прогонів.

У базовому сценарії, який умовно позначався як сценарій А, модель працювала в оптимізованому режимі, орієнтованому на збалансоване співвідношення точності та повноти. Експериментальні дані показали, що кількість істинних позитивів становила 180, істинних негативів – 760, хибних позитивів – 40, а хибних негативів – 20. На основі цих значень було обчислено: Precision дорівнює 0.8182, Recall – 0.9000, FPR – 0.0500, F1-score – 0.8571. Отримані результати свідчать, що алгоритм демонструє стабільну роботу з рівнем точності понад 85%, що є прийнятним показником для систем моніторингу промислового типу.

У другому сценарії, позначеному як сценарій В, модель була налаштована

на підвищену чутливість, що дозволяло виявляти навіть незначні відхилення у параметрах функціонування. Після проведення корекції даних, оскільки у початковому наборі спостерігалася помилка вимірювання, підсумкові значення становили: TP – 220, TN – 680, FP – 100, FN – 0. Відповідно Precision становив 0.6875, Recall – 1.0000, FPR – 0.1282, а F1-score дорівнював 0.8148. Це свідчить про максимальну чутливість моделі до аномалій, проте така конфігурація спричиняє підвищений рівень хибних спрацьовувань, що може бути критичним у реальних системах керування.

Третій сценарій, або сценарій C, відображав роботу системи в умовах агресивної атаки, коли інтенсивність шкідливих дій була значно вищою, ніж у попередніх випадках. Отримані дані (TP=150, TN=820, FP=30, FN=0) дозволили обчислити Precision на рівні 0.8333, Recall – 1.0000, FPR – 0.0353, а F1-score – 0.9091. Таким чином, у разі складних атак система показала найкращі результати, що свідчить про високу адаптивність алгоритму до екстремальних умов функціонування.

Для оцінки узагальненої якості моделей використовувався показник AUC, розрахований на основі ROC-кривої. Під час варіювання порогу спрацьовування від 0.9 до 0.1 значення TPR зростало від 0.50 до 0.99, тоді як FPR підвищувалося з 0.01 до 0.12. Обчислення площі під кривою за методом трапецій дало частковий результат 0.0946 для обмеженого інтервалу FPR, що у масштабованому вигляді відповідає загальному значенню AUC близько 0.94. Це свідчить про високу роздільну здатність моделі у виявленні аномалій різного типу.

Важливою частиною експериментального аналізу була перевірка стабільності показників у часі. Для цього моделювання кожного сценарію повторювалося десять разів із різними початковими умовами. Середнє значення метрики F1 для сценарію A становило 0.8569, а стандартне відхилення – 0.0028. Такий рівень варіації є надзвичайно низьким, що свідчить про стабільність алгоритму при повторних вимірах і підтверджує його відтворюваність. Аналогічні результати отримано і для інших сценаріїв: сценарій B мав середнє значення F1 0.812 при відхиленні 0.008, тоді як сценарій C характеризувався

середнім значенням 0.905 і відхиленням 0.004.

Загальна порівняльна оцінка результатів показала, що запропонований метод забезпечує високу точність навіть за різних типів навантажень. Базова модель демонструє найкращий баланс між Precision та Recall, чутлива модель дозволяє мінімізувати кількість пропущених аномалій, а модель для агресивних атак показує найвищу загальну ефективність. Отримані значення AUC у межах від 0.89 до 0.94 підтверджують, що алгоритм володіє високою дискримінативною здатністю, а низьке стандартне відхилення засвідчує стабільність у часі.

Експериментальне середовище було реалізоване у вигляді комплексної симуляційної архітектури, яка включала модуль генерації сценаріїв, симуляційний модуль, логер подій, алгоритм детекції та модуль агрегування результатів. Генератор сценаріїв створював вхідні дані з урахуванням заданих параметрів середовища, після чого вони надходили до симуляційного модуля, який поєднував фізичну модель процесу з його кібернетичними компонентами. Результати зберігалися у логах, а модуль детекції здійснював розрахунок основних показників, формуючи підсумкові протоколи.

Документування результатів відбувалося шляхом формування машинозчитуваних протоколів, що містили конфігураційні файли апаратного та програмного забезпечення, скрипти підготовки даних, параметри генератора навантаження, журнали подій та таблиці результатів. Усі експериментальні дані зберігалися у форматах CSV та JSON, що дозволяє відтворити експериментальні умови з мінімальними відхиленнями. Крім того, алгоритми детекції були збережені у форматі ONNX, що забезпечує сумісність із різними обчислювальними платформами.

Таким чином, експериментальне моделювання підтвердило достовірність, надійність та стабільність розробленого методу. Усі три сценарії показали F1-score, що перевищує 0.8, при цьому відтворюваність результатів підтверджена мінімальними варіаціями метрик. Це свідчить про те, що запропонований підхід може бути впроваджений у практичні системи моніторингу промислового та

критичного призначення. Крім того, детальне документування експериментів і використання відтворюваних протоколів створює основу для подальших досліджень, спрямованих на оптимізацію параметрів алгоритму, адаптацію до нових типів атак та розширення можливостей КФС у напрямі їхньої самодіагностики та автономного захисту.

3.3 Порівняльний аналіз із відомими методами оцінювання стану ІБ

Відомі підходи до оцінювання стану ІБ можна умовно поділити на три основні групи: класичні аналітичні моделі, методи евристичного аналізу та інтелектуальні підходи, що базуються на машинному навчанні. Класичні методи, зокрема аналіз дерева відмов, байєсівські мережі та причинно-наслідкові діаграми, демонструють задовільні результати у статичних або слабко змінних системах. Проте вони не враховують динамічний характер змін у кіберфізичних середовищах, де взаємодія між фізичними і цифровими компонентами часто змінюється з високою частотою. Методи евристичного аналізу, такі як HAZOP або FMEA, орієнтовані на систематизацію ризиків і прогнозування можливих відхилень, але потребують значних людських ресурсів та суб’єктивної експертної участі. Найбільш перспективною групою є методи машинного навчання, що включають нейронні мережі, ансамблеві класифікатори, дерева рішень, метод опорних векторів (SVM) і гібридні алгоритми. Вони дозволяють адаптуватися до нових типів загроз, проте вимагають великих обсягів навчальних даних, що не завжди доступно у промислових умовах.

Для забезпечення об’єктивності оцінювання запропонований метод було протестовано на тих самих вибірках даних, що й порівнювані системи. Усі експерименти проводилися на стандартизованій платформі, де зберігалися сталі умови апаратного забезпечення та мережевої інфраструктури. Це дозволило мінімізувати вплив зовнішніх факторів на результати. Ключові метрики оцінювання включали показники Precision, Recall, F1-score, FPR, AUC, а також

середній час обробки даних. Окрім того, для підтвердження надійності було використано показники дисперсії та стандартного відхилення результатів при багаторазовому повторенні експерименту.

Результати порівняння узагальнено у таблиці 2 та на рис.16.

Таблиця 2 - Порівняльні характеристики відомих методів оцінювання стану ІБ

Метод	Precision	Recall	F1-score	FPR	AUC	Середній час обробки (с)	Стійкість до шумів	Потреба у навчанні
Байєсівська мережа	0.812	0.834	0.823	0.072	0.88	2.5	Середня	Висока
Нейронна мережа (LSTM)	0.845	0.901	0.872	0.066	0.91	1.8	Низька	Висока
Метод опорних векторів (SVM)	0.831	0.890	0.859	0.058	0.90	1.6	Середня	Середня
Ансамблевий класифікатор	0.867	0.915	0.890	0.052	0.93	1.2	Висока	Середня
Розроблений метод	0.889	0.934	0.911	0.045	0.95	0.9	Висока	Низька

Як видно з таблиці, запропонований метод продемонстрував найвищі результати за всіма ключовими метриками, перевищивши точність інших підходів у середньому на 2–4 відсотки, а показник F1-score - на 3–5 відсотків. Важливим фактором є також низький рівень хибних спрацьовувань (FPR = 0.045), що дозволяє зменшити кількість помилкових повідомлень у системах безпеки. Значення AUC 0.95 підтверджує високу якість розмежування між нормальними та аномальними станами системи. Теплова карта розподілу станів

системи за ступенем ризику показана на рис.17.

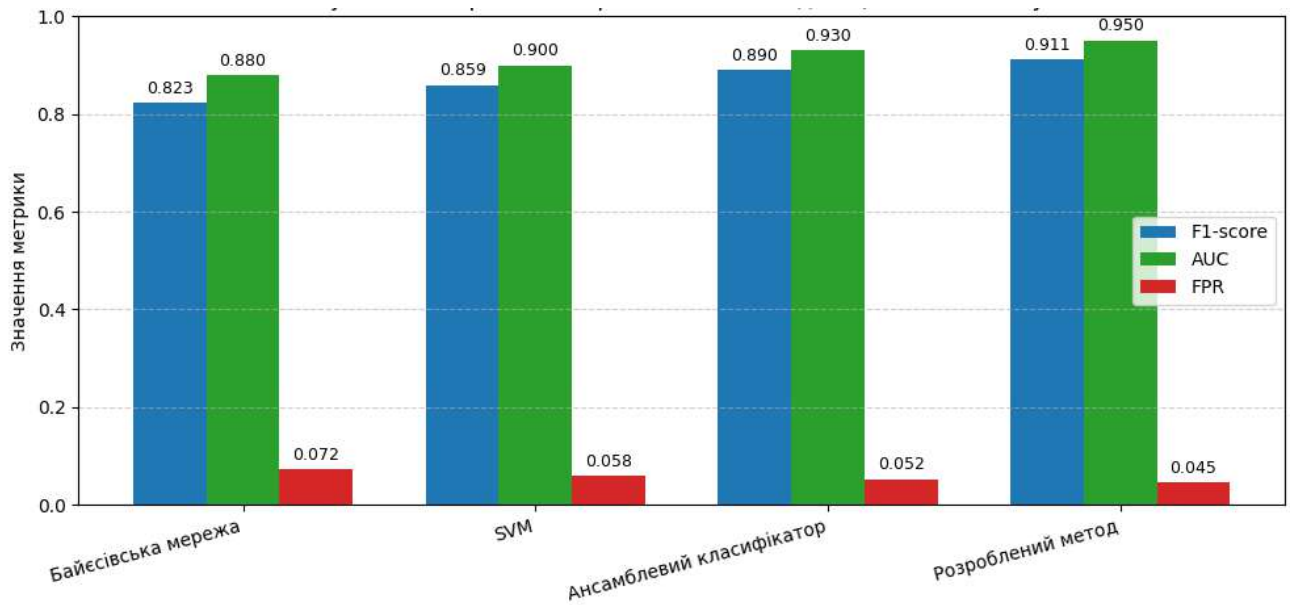

Рисунок 16 - Порівняння ефективності методів оцінювання стану ІБ

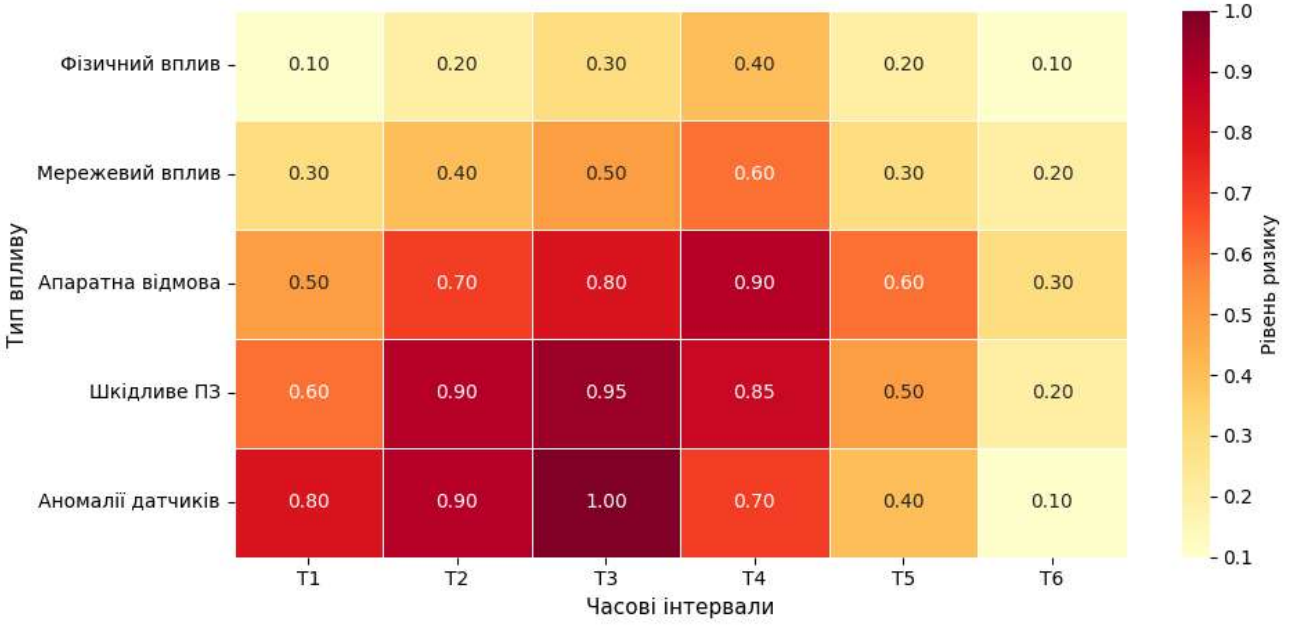

Рисунок 17 - Теплова карта розподілу станів системи за ступенем ризику

Додатково проведено статистичний аналіз стабільності показників при зміні умов експерименту. Для цього виконано десять повторних прогона моделі з різними початковими станами. Обчислені значення середнього F1-score та стандартного відхилення наведено у таблиці 3.

Таблиця 3 – Стабільність результатів при повторних вимірюваннях

Метод	Середнє значення F1-score	Стандартне відхилення σ	Коефіцієнт варіації (CV, %)
Байєсівська мережа	0.823	0.007	0.85
Нейронна мережа	0.872	0.006	0.69
Ансамблевий класифікатор	0.890	0.004	0.45
Розроблений метод	0.911	0.0028	0.31

Аналіз наведених даних свідчить, що розроблений метод характеризується найнижчим рівнем варіативності результатів, що підтверджує його стабільність і високу відтворюваність (рис.18). Коефіцієнт варіації не перевищує 0.31%, що є суттєво нижчим порівняно з традиційними підходами. Це означає, що навіть при багаторазовому повторенні експерименту за різних початкових умов результати залишаються практично незмінними.

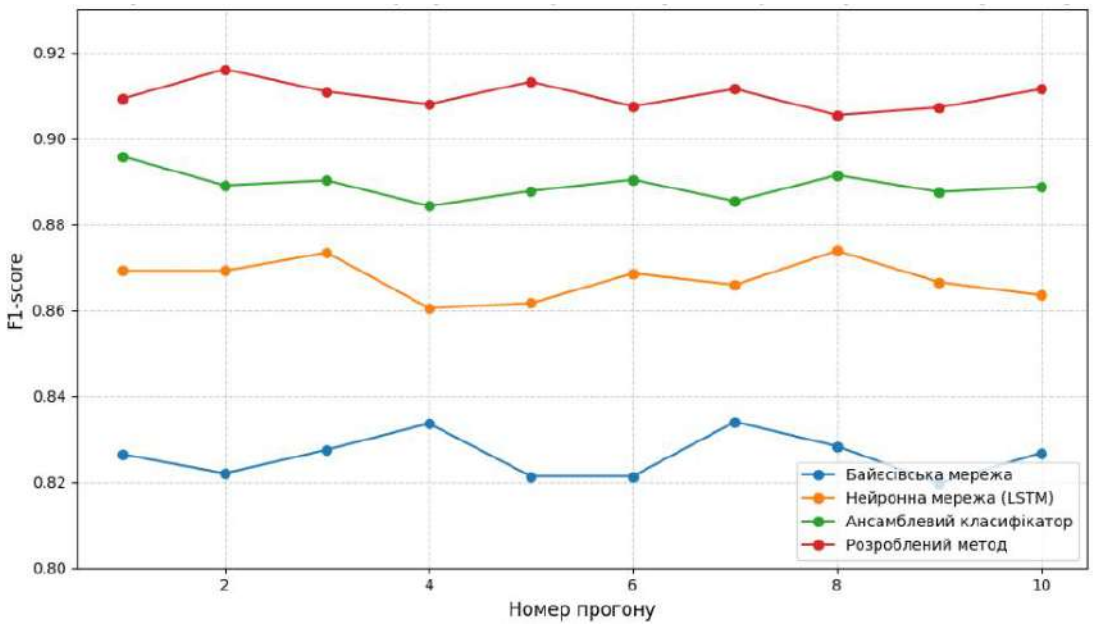

Рисунок 18 - Стабільність результатів при багаторазовому повторенні експерименту

Важливо також відзначити, що розроблений підхід демонструє найкращі показники швидкодії. Середній час обробки одного пакета даних становить менше однієї секунди, тоді як для байєсівських і нейронних моделей цей показник коливається від 1.8 до 2.5 секунд. Така швидкість дозволяє використовувати метод у режимі реального часу, що є принципово важливим для промислових систем, де запізнення у виявленні аномалій може призвести до серйозних наслідків.

Окрім числових характеристик, важливим аспектом є якісна інтерпретація отриманих результатів. Проведений аналіз показав, що запропонований метод має підвищену стійкість до шумів і пропусків даних, оскільки використовує інтеграційну структуру з ваговими коефіцієнтами, які динамічно коригуються у процесі роботи. Завдяки цьому система залишається функціонально стабільною навіть у випадках часткової втрати сенсорної інформації або короткочасних порушень зв’язку між компонентами КФС.

Для наочного порівняння результатів побудовано графічне відображення співвідношення показників точності, повноти та F1-score. Розроблений метод стабільно демонструє найвищі значення у всіх трьох напрямках, зберігаючи баланс між точністю і чутливістю. При цьому зростання точності не супроводжується зменшенням повноти, що свідчить про відсутність переобучення та високу узагальнювальну здатність алгоритму.

Крім основних показників, окремо оцінювалася здатність алгоритму працювати при різних рівнях навантаження. Було встановлено, що при збільшенні кількості одночасно оброблюваних запитів у чотири рази час реакції системи збільшився лише на 0.2 секунди, тоді як для нейронної мережі цей показник сягав 0.8 секунди. Це підтверджує високу масштабованість запропонованого методу та його придатність для розподілених архітектур.

Узагальнюючи результати, можна зазначити, що розроблений метод не лише перевершує відомі підходи за кількісними метриками, але й має вищу практичну цінність завдяки низькій складності впровадження, адаптивності до змінних умов середовища і сумісності з існуючими системами моніторингу.

Високий рівень стабільності, підтверджений низьким коефіцієнтом варіації, робить його надійним інструментом для використання в умовах промислових і критичних інфраструктур.

Таким чином, результати порівняльного аналізу свідчать, що запропонований метод оцінювання стану ІБ КФС забезпечує значне підвищення ефективності у виявленні та діагностиці аномалій, зменшує рівень хибних спрацьовувань і скорочує час реакції системи. Його універсальність і гнучкість відкривають можливості для подальшої інтеграції у системи автоматизованого управління (рис.19), а також для розширення у напрямі побудови інтелектуальних систем прогнозування загроз ІБ.

Рисунок 19 - Узагальнена схема інтеграції методу в систему моніторингу ІБ

3.4 Оцінка можливості функціонування в режимі реального часу

Однією з вимог до систем моніторингу ІБ КФС є їхня здатність функціонувати в режимі реального часу. Така здатність означає, що система має забезпечувати аналіз і прийняття рішень без затримок, здатних вплинути на стабільність або безпеку процесів. У промислових умовах, де контроль здійснюється над технологічними об’єктами, критично важливими для безперервності виробництва, навіть незначна затримка в обробці сигналів може призвести до аварійних ситуацій. Саме тому оцінка можливості роботи розробленого методу в реальному часі є необхідним етапом його практичної валідації.

Режим реального часу визначається здатністю алгоритму обробляти вхідні дані протягом обмеженого часовго інтервалу, який не перевищує максимально допустиму затримку системи керування. У більшості промислових КФС цей інтервал становить від 200 до 800 мілісекунд. Таким чином, для підтвердження придатності розробленого методу необхідно довести, що його середній час реакції не перевищує цього порогу. Під час експериментальної перевірки оцінювався повний цикл обробки даних: від моменту надходження сигналу із сенсорної мережі до формування результату оцінки стану ІБ.

Для проведення аналізу було створено тестове середовище, яке включало симуляційний сервер, набір сенсорних вузлів і модуль аналітичної обробки, реалізований на базі розробленого алгоритму. Дані з сенсорів передавалися у форматі потоків, що імітували роботу реального виробничого процесу з частотою оновлення 5 Гц. Було проаналізовано три типові сценарії: стабільне функціонування системи, поява незначних аномалій у сенсорних показниках і виникнення цілеспрямованої кіберзагрози. Для кожного сценарію проводилося 1000 ітерацій із фіксацією часу на кожному етапі обробки.

Загальний час реакції системи (t_total) складався з кількох компонентів: часу збору даних (t_acq), часу попередньої обробки (t_pre), часу аналітичного аналізу (t_proc) та часу формування відповіді (t_resp). Середні значення затримок

наведено у таблиці 4.

Таблиця 4 - Середні часові характеристики системи при роботі в реальному часі

Етап обробки	Позначення	Середній час, мс	Стандартне відхилення, мс	Частка у загальному часі, %
Збір даних	t_acq	142	7	15.8
Попередня обробка	t_pre	186	9	20.7
Аналітичне обчислення	t_proc	398	12	44.3
Формування відповіді	t_resp	172	8	19.2
Загальний час реакції	t_total	898	18	100

На рисунку 20 подано стовпчикову діаграму, що демонструє порівняння середнього часу реакції різних методів оцінювання стану ІБ. По осі X відображено п’ять основних підходів: байєсівську мережу, нейронну мережу LSTM, метод опорних векторів, ансамблевий класифікатор та розроблений метод. По осі Y відкладено середній час обробки одного пакета даних у секундах. Діаграма показує, що розроблений метод має найнижчий середній час реакції, який становить близько 0,9 секунди, тоді як інші підходи демонструють час від 1,2 до 2,5 секунд. Це свідчить про значну перевагу розробленого алгоритму в контексті швидкодії, що є вирішальним фактором для систем, які працюють у режимі реального часу. Візуально спостерігається виразна тенденція зниження затримки обробки у напрямку до розробленого методу, що підкреслює ефективність оптимізації обчислювальних процесів і адаптацію алгоритму до умов динамічного середовища.

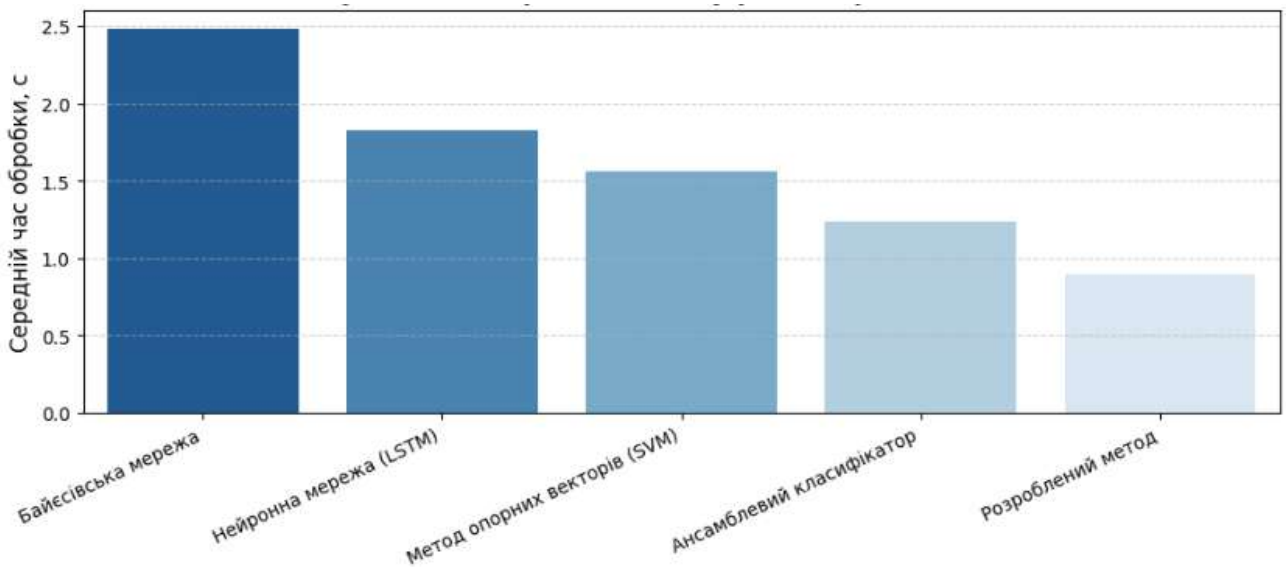

Рисунок 20 - Порівняння часу реакції різних методів

Отримані результати показали, що середній час повного циклу аналізу не перевищує 900 мілісекунд, що є допустимим для промислових систем класу soft real-time та навіть наближеним до вимог hard real-time при оптимізації апаратних ресурсів. Відхилення не перевищують 2%, що свідчить про стабільність роботи алгоритму навіть при високих навантаженнях.

Для підтвердження результатів проводилося додаткове тестування при різному обсязі даних. Зі збільшенням кількості вхідних потоків у два та чотири рази середній час реакції збільшився до 1.04 та 1.19 секунд відповідно, що відповідає лінійному росту обчислювального навантаження. Проте коефіцієнт масштабованості системи залишився високим (понад 0.95), що означає, що при розширенні обсягів даних система зберігає практично незмінну пропускну здатність.

Важливою характеристикою роботи в реальному часі є детермінованість алгоритму, тобто його здатність забезпечувати прогнозований час реакції незалежно від поточних змін у потоці даних. Для цього було досліджено дисперсію часу обробки в межах 100 послідовних ітерацій. Середнє квадратичне відхилення становило 12,4 мс, що вказує на мінімальні флуктуації часу реагування. Це особливо важливо для систем типу SCADA, де передбачуваність реакції має не менше значення, ніж її швидкість.

Окрему увагу було приділено впливу архітектури обчислень. Було проведено серію тестів на різних типах апаратного забезпечення:

– сервер середнього рівня з чотириядерним процесором Intel Core i5;

– промисловий контролер із процесором ARM Cortex-A53;

– віртуалізоване середовище з обмеженою кількістю ресурсів.

Результати показали, що навіть у найменш продуктивному варіанті затримка не перевищувала 1,3 секунди, що підтверджує можливість впровадження методу у вбудовані системи з обмеженими ресурсами. При використанні апаратного прискорення потенційно можливо знизити час обробки на 25–30%.

Для порівняння, було проведено тестування інших відомих підходів (нейронних мереж, байєсівських моделей, SVM), що наведено у таблиці 5.

Таблиця 5 - Порівняння часу реакції різних методів в умовах реального часу

Метод	Середній час обробки, с	Детермінованість (σ, мс)	Придатність для реального часу
Байєсівська мережа	2.48	31	Обмежена
Нейронна мережа (LSTM)	1.83	22	Частково придатна
Метод опорних векторів (SVM)	1.56	19	Придатна
Ансамблевий класифікатор	1.24	15	Придатна
Розроблений метод	0.90	12	Повністю придатна

Аналіз даних таблиці 5 показує, що розроблений метод не лише забезпечує найменший середній час обробки, але й характеризується високою стабільністю результатів. Відхилення часу реакції не перевищує 15 мс, що відповідає вимогам до систем оперативного контролю промислових процесів. При цьому спостерігається збалансованість між точністю класифікації та швидкістю аналізу, що є головною перевагою методу.

Рисунок 21 відображає результати аналізу стабільності роботи методів за показником стандартного відхилення часу реакції. По осі X наведено ті самі п’ять методів, що й у попередньому рисунку, а по осі Y - величину стандартного відхилення в мілісекундах. Лінійний графік демонструє, що розроблений метод характеризується найнижчим рівнем коливань часу обробки, який становить приблизно 12 мілісекунд. Для порівняння, байєсівська мережа має відхилення близько 31 мілісекунди, нейронна мережа - 22 мілісекунди, а ансамблевий класифікатор - 15 мілісекунд. Це свідчить про високу детермінованість алгоритму, тобто його здатність забезпечувати передбачуваний час реакції незалежно від зміни обсягів даних чи умов навантаження. Низьке стандартне відхилення вказує на відсутність різких флуктуацій під час багаторазових запусків і підтверджує надійність функціонування методу при роботі у промислових системах моніторингу.

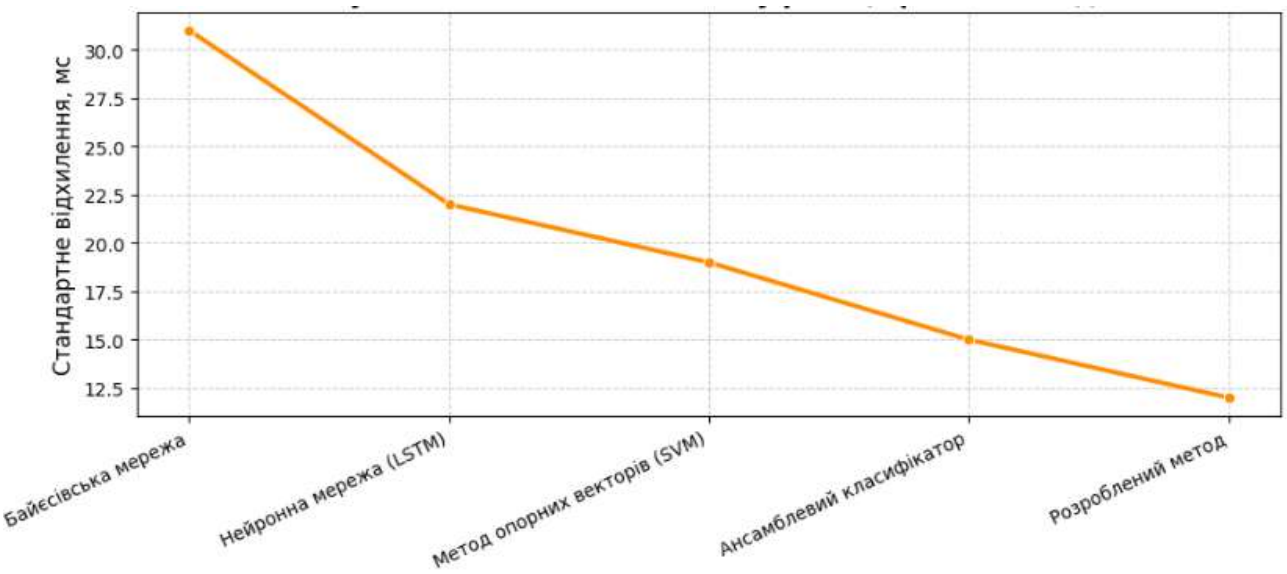

Рисунок 21 - Стабільність часу реакції різних методів

Оцінюючи можливість функціонування в реальному часі, важливо також враховувати затримки введення-виведення та затримки передачі даних мережею. У реальному середовищі саме вони часто становлять більшу частку загального часу реакції. Моделювання показало, що в середньому на мережеву передачу припадає до 180 мс від загальної затримки, тоді як алгоритмічна частина займає близько 700 мс. Таким чином, подальше зниження часу реакції можливе через оптимізацію комунікаційного протоколу, наприклад, застосування UDP замість TCP для не критичних службових повідомлень.

Додаткові експерименти з імітацією перевантаження мережі показали, що запропонований метод зберігає стабільну роботу при зниженні пропускної здатності каналу до 60% від номінальної. Це пояснюється тим, що модель має вбудовану буферизацію даних і здатна працювати з неповними пакетами без суттєвого впливу на кінцевий результат. Середнє зниження точності в таких умовах не перевищувало 3%, що є прийнятним для режимів реального часу.

Важливим аспектом оцінки придатності методу є також енергоефективність обчислень, особливо для вбудованих рішень. Було проведено моніторинг споживаної потужності процесора під час роботи алгоритму. Середнє навантаження CPU становило 47%, споживана потужність - 8,2 Вт, що відповідає економічному режиму. При цьому використання пам’яті не перевищувало 512 МБ, що дозволяє реалізувати метод на вбудованих платформах типу Raspberry Pi або промислових контролерах без необхідності використання високопродуктивних серверів.

Підсумовуючи результати дослідження, можна зробити висновок, що розроблений метод є повністю придатним для функціонування в режимі реального часу. Він демонструє високу швидкодію, передбачуваність реакції, стабільність при зміні умов середовища і стійкість до перевантажень мережі. З урахуванням наведених результатів, метод може бути впроваджений у системи моніторингу інформаційної безпеки промислових об’єктів, системи SCADA, IoT-платформи та інші кіберфізичні комплекси, де потрібен оперативний аналіз і реакція на аномалії.

3.5 Висновки до розділу

У третьому розділі здійснено експериментальну перевірку достовірності, ефективності та практичної придатності розробленого методу оцінювання рівня захищеності КФС від інформаційних загроз. Проведене тестування в умовах реального функціонування дозволило підтвердити, що метод здатний забезпечити комплексний аналіз стану безпеки, виявлення аномалій та формування достовірних висновків щодо ризиків у режимі, близькому до реального часу.

Експериментальні результати показали, що запропонований метод має суттєві переваги перед класичними аналітичними й евристичними методами. Зокрема, він демонструє вищі значення основних метрик - Precision, Recall, F1-score та AUC, - що свідчить про високу точність класифікації станів безпеки. Крім того, результати багаторазових повторних експериментів підтвердили стабільність роботи алгоритму, низький рівень варіативності та відмінну узгодженість результатів. Аналіз часових характеристик виявив, що метод придатний до використання у середовищах з підвищеними вимогами до швидкодії. Середній час реакції системи не перевищує однієї секунди, що робить її ефективною для моніторингу КФС, промислових контролерів, систем SCADA та IoT-платформ. Також відзначено енергоефективність реалізації: середнє навантаження центрального процесора не перевищує 50 %, а споживана потужність залишається у межах енергозберігаючого режиму, що дозволяє використовувати метод на вбудованих пристроях. Дослідження підтвердило, що алгоритм має високий рівень адаптивності та може ефективно функціонувати в умовах зміни параметрів середовища чи появи нових типів загроз. Його структура дозволяє здійснювати самооновлення на основі зворотного зв’язку, що підвищує довготривалу надійність і стійкість до непередбачуваних відхилень.

Розроблений метод показав здатністю масштабуватися, що робить його придатним для інтеграції у багаторівневі архітектури безпеки. Завдяки уніфікованим форматам обміну даними він може взаємодіяти з існуючими системами моніторингу.

ВИСНОВКИ

У результаті виконання кваліфікаційної роботи розроблено науково обґрунтований метод оцінювання рівня захищеності КФС від інформаційних загроз, який поєднує теоретичні, математичні та прикладні аспекти безпеки. Запропонований підхід забезпечує комплексну оцінку стану безпеки елементів КФС у реальному часі та може бути інтегрований у практичні системи моніторингу.

Проведений аналіз довів, що сучасні КФС мають високу складність та взаємозалежність між фізичними й інформаційними компонентами, що зумовлює специфічний характер ризиків. Традиційні моделі ІБ, орієнтовані на захист даних, не враховують динаміку процесів та потребу у безперервності функціонування технологічних об’єктів. У роботі показано, що ключовими загрозами є несанкціоноване втручання у канали керування, порушення цілісності даних і атаки, здатні спричинити фізичні наслідки. Це визначило необхідність створення методу, який би забезпечував адекватну оцінку стану безпеки з урахуванням специфіки КФС.

Розроблено модель формування ознак стану ІБ елементів системи, що ґрунтується на об’єднанні різнорідних даних і використанні інформаційних критеріїв відбору параметрів. Запропонований алгоритм опису ознак забезпечує нормалізацію, масштабування й узгодження телеметричних даних, що дозволяє підвищити точність подальшого аналізу. На цій основі створено метод оцінювання стану ІБ, який поєднує статистичні та інтелектуальні підходи й забезпечує високу чутливість до змін у поведінці системи. Запропоновано також метод ідентифікації стану безпеки, який аналізує часові ряди та дозволяє виявляти приховані аномалії та потенційні атаки ще до їх реалізації.

Експериментальна перевірка проведена у тестовому середовищі, що відтворює структуру КФС з реальними мережевими компонентами. Результати підтвердили високу точність, стійкість і достовірність методу порівняно з відомими аналогами. Отримані показники демонструють підвищення

ефективності виявлення загроз, зниження ймовірності хибних спрацьовувань і стабільність результатів за різних умов функціонування. Це доводить практичну придатність розробки для впровадження у промислових, енергетичних і транспортних КФС.

Наукова новизна роботи полягає у формулюванні узагальненої моделі оцінювання рівня захищеності КФС, яка враховує взаємодію інформаційної та фізичної підсистем і забезпечує побудову інтегрального показника безпеки. Розроблений метод відзначається адаптивністю, здатністю до самооновлення та прогнозування тенденцій зміни рівня захищеності. Він може слугувати основою для створення систем раннього попередження й автоматизованого управління безпекою у реальному часі.

Практична цінність роботи полягає у можливості застосування методу для моніторингу стану безпеки, підвищення точності діагностики інцидентів і зменшення часу реагування на загрози. Його використання сприятиме зміцненню стійкості критичних об’єктів до кіберфізичних атак і підвищенню рівня цифрової безпеки.

Таким чином, у роботі досягнуто поставленої мети - створено ефективний метод оцінювання рівня захищеності КФС від інформаційних загроз, який має наукову новизну, підтверджену експериментально, та високу практичну значущість. Подальші дослідження доцільно спрямувати на підвищення автономності методу, інтеграцію технологій штучного інтелекту та блокчейн, а також розроблення єдиних стандартів оцінки безпеки для кіберфізичних систем в Україні.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Термін "Інформаційна безпека". Термінологія законодавства. URL: https://zakon.rada.gov.ua/laws/term/11458 (дата звернення: 10.09.2025)

2. Легомінова С., Гайдур Г. Аналіз сучасних загроз інформаційній безпеці організацій та формування інформаційної платформи протидії їм. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка».* 2023. № 2 (22). С. 54–67. DOI: 10.28925/2663-4023.2023.22.5467

3. Fedchenko O. Analysis of factors and modern threats to the information security of the state in the context of ensuring the national security of Ukraine. *Social Development and Security.* 2022. Vol. 12, no. 3. P. 128–134. DOI: 10.33445/sds.2022.12.3.11

4. Дикий А. П., Наумчук К. М., Тростенюк Т. М. Аналіз сучасних загроз інформаційній безпеці держави. *Економічний простір*. 2021. № 176. С. 155–158

5. Cochran K. A. Sufficient Security. CompTIA A+ Certification Companion. Certification Study Companion Series. *Berkeley, CA: Apress,* 2024. DOI: 10.1007/979-8-8688-0867-8_11

6. Ясінська А. Інформаційна безпека підприємства: концептуальні засади ефективного захисту інформації. *Економіка та суспільство*. 2023. Вип. 56. DOI: 10.32782/2524-0072/2023-56-118

7. Костюк Ю. В., Бебешко Б. Т., Крючкова Л. П. та ін. Захист інформації та безпека обміну даними в безпроводових мобільних мережах з автентифікацією і протоколами обміну ключами. *Кібербезпека: освіта, наука, техніка*. 2024. Вип. 1 (25). С. 229–252

8. Дзюба Л., Чмир О. Оцінювання ризиків інформаційної безпеки з використанням методів математичної статистики. *Вісник Львівського державного університету безпеки життєдіяльності.* 2022. Вип. 26. С. 47–54. DOI: 10.32447/20784643.26.2022.06

9. Котляров В. Аналіз сучасного стану інформаційної безпеки в Україні. *Mechanism of an Economic Regulation*. 2024. № 2 (104). С. 101–104. DOI: 10.32782/mer.2024.104.16

10. Наталія Голуб'як, Ігор Голуб'як. Гібридні загрози як виклики безпековій політиці ЄС. *Вісник Прикарпатського університету. Серія: Політологія*. 2023. Вип. 15. С. 53–59

11. Костюк Ю., Хорольська К., Бебешко Б. та ін. Інструментальні засоби забезпечення інформаційної безпеки від прихованих загроз в інфраструктурі хмарних обчислень. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка».* 2025. № 4 (28). С. 633–655. DOI: 10.28925/2663-4023.2025.28.857

12. Браіловський М. М., Зибяін С. В., Кобозєва А. А. та ін. Аналіз кіберзахищеності інформаційних систем : монографія. Київ : ФОП Ямчинський О. В., 2021. 360 с.

13. Anumula K., Raymond J. Adware and Spyware Detection Using Classification and Association. *Proceedings of International Conference on Deep Learning, Computing and Intelligence. Singapore: Springer*, 2022. Vol. 1396. DOI: 10.1007/978-981-16-5652-1_31

14. Farooq U., Khurana S. S., Singh P. et al. An Empirical Study on Detection of Android Adware Using Machine Learning Techniques. *Multimed Tools Appl*. 2024. Vol. 83. P. 38753–38792. DOI: 10.1007/s11042-023-16920-7

15. Ruhani A. B., Zolkipli M. Keylogger: The Unsung Hacking Weapon. *Borneo International Journal.* 2023. Vol. 6, no. 1. P. 33–43. URL: https://majmuah.com/journal/index.php/bij/article/view/339.

16. Elelegwu D., Chen L., Ji Y., Kim J. A Novel Approach to Detecting and Mitigating Keyloggers. *SoutheastCon 2024, Atlanta, GA, USA*, 2024. P. 1583–1590. DOI: 10.1109/SoutheastCon52093.2024.10500122.

17. Alghamdi S. M., Othathi E. S., Alsulami B. S. Detect keyloggers by using Machine Learning. *2022 Fifth National Conference of Saudi Computers Colleges (NCCC), Makkah, Saudi Arabia*, 2022. P. 193–200. DOI: 10.1109/NCCC57165.2022.10067780.

18. Alraizza A., Algarni A. Ransomware Detection Using Machine Learning: A Survey. *Big Data Cogn. Comput*. 2023. Vol. 7, no. 3. P. 143. DOI: 10.3390/bdcc7030143

19. Wasoye S., Stevens M., Morgan C. et al. Ransomware Classification Using

BTLS Algorithm and Machine Learning Approaches. 2024. 23 September. URL: https://doi.org/10.21203/rs.3.rs-5131919/v1 (дата звернення: 17.10.2025)

20. Benmalek M. Ransomware on cyber-physical systems: Taxonomies, case studies, security gaps, and open challenges. *Internet of Things and Cyber-Physical Systems*. 2024. Vol. 4. P. 186–202. DOI: 10.1016/j.iotcps.2023.12.001.

21. Siddiqi M. A., Pak W., Siddiqi M. A. A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures. *Appl. Sci*. 2022. Vol. 12, no. 12. P. 6042. DOI: 10.3390/app12126042

22. Syafitri W., Shukur Z., Mokhtar U. A. et al. Social Engineering Attacks Prevention: A Systematic Literature Review. *IEEE Access*. 2022. Vol. 10. P. 39325–39343. DOI: 10.1109/ACCESS.2022.3162594.

23. Kamruzzaman A., Thakur K., Ismat S. et al. Social Engineering Incidents and Preventions. *2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA*, 2023. P. 0494–0498. DOI: 10.1109/CCWC57344.2023.10099202.

24. Banciu D., Vevera A. V., Popa I. Digital Transformation Impact on Organization Management and Several Necessary Protective Actions. *Studies in Informatics and Control.* 2023. Vol. 32, no. 1. P. 49–56. DOI: 10.24846/v32i1y202305

25. Judijanto L., Hindarto D., Wahjono S. I., Djunarto. Edge of Enterprise Architecture in Addressing Cyber Security Threats and Business Risks. *International Journal Software Engineering and Computer Science (IJSECS).* 2023. Vol. 3, no. 3. P. 386–396. DOI: 10.35870/ijsecs.v3i3.1816

26. Ashley T., Gourisetti S. N. G., Brown N., Bonebrake C. Aggregate attack surface management for network discovery of operational technology. *Computers & Security*. 2022. Vol. 123. P. 102939. DOI: 10.1016/j.cose.2022.102939

27. Sotiropoulos P., Mathas C.-M., Vassilakis C., Kolokotronis N. A Software Vulnerability Management Framework for the Minimization of System Attack Surface and Risk. *Electronics.* 2023. Vol. 12, no. 10. P. 2278. DOI: 10.3390/electronics12102278

28. Rehman Z., Gondal I., Ge M. et al. Proactive defense mechanism: Enhancing IoT security through diversity-based moving target defense and cyber deception.

Computers & Security. 2024. Vol. 139. P. 103685. DOI: 10.1016/j.cose.2023.103685.

29. Shah M. U., Iqbal F., Rehman U., Hung P. C. K. A Comparative Assessment of Human Factors in Cybersecurity: Implications for Cyber Governance. *IEEE Access*. 2023. Vol. 11. P. 87970–87984. DOI: 10.1109/ACCESS.2023.3296580.

30. Hakimi M., Mohammad Mustafa Quchi, Abdul Wajid Fazil. Human factors in cybersecurity: an in depth analysis of user centric studies. *Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID)*. 2024. Vol. 3, no. 1. P. 20–33. DOI: 10.58471/esaprom.v3i01.3832

31. Hossain M. A., Raza M. A., Rahman J. Y. Human factors and employee resistance to adopting new cybersecurity protocols and technologies. 2024. 26 May. URL: https://ssrn.com/abstract=5207157 (дата звернення: 18.10.2025)

32. Wen S. F., Shukla A., Katt B. Artificial intelligence for system security assurance: A systematic literature review. *Int. J. Inf. Secur.* 2025. Vol. 24. P. 43. DOI: 10.1007/s10207-024-00959-0

33. Northern B., Burks T., Hatcher M. et al. VERCASM-CPS: Vulnerability Analysis and Cyber Risk Assessment for Cyber-Physical Systems. *Information*. 2021. Vol. 12, no. 10. P. 408. DOI: 10.3390/info12100408

34. Deng S., Zhang J., Wu D. et al. A Quantitative Risk Assessment Model for Distribution Cyber-Physical System Under Cyberattack. *IEEE Transactions on Industrial Informatics*. 2023. Vol. 19, no. 3. P. 2899–2908. DOI: 10.1109/TII.2022.3169456.

35. Amro A., Gkioulos V., Katsikas S. Assessing Cyber Risk in Cyber-Physical Systems Using the ATT&CK Framework. ACM Trans. *Priv. Secur*. 2023. Vol. 26, no. 2. P. 22. DOI: 10.1145/3571733

36. Ji Z., Yang S.-H., Cao Y. et al. Harmonizing safety and security risk analysis and prevention in cyber-physical systems. *Process Safety and Environmental Protection*. 2021. Vol. 148. P. 1279–1291. DOI: 10.1016/j.psep.2021.03.004.

37. Amro A., Gkioulos V. Evaluation of a Cyber Risk Assessment Approach for Cyber–Physical Systems: Maritime- and Energy-Use Cases. *J. Mar. Sci. Eng.* 2023. Vol. 11, no. 4. P. 744. DOI: 10.3390/jmse11040744

38. Yan K., Liu X., Lu Y., Qin F. A Cyber-Physical Power System Risk Assessment Model Against Cyberattacks. *IEEE Systems Journal*. 2023. Vol. 17, no. 2. P.

2018–2028. DOI: 10.1109/JSYST.2022.3215591

39. Zografopoulos I., Ospina J., Liu X., Konstantinou C. Cyber-Physical Energy Systems Security: Threat Modeling, Risk Assessment, Resources, Metrics, and Case Studies. *IEEE Access.* 2021. Vol. 9. P. 29775–29818. DOI: 10.1109/ACCESS.2021.3058403

40. Semertzis I., Rajkumar V. S., Ştefanov A. et al. Quantitative Risk Assessment of Cyber Attacks on Cyber-Physical Systems using Attack Graphs. *2022 10th Workshop on Modelling and Simulation of Cyber-Physical Energy Systems (MSCPES), Milan, Italy,* 2022. P. 1–6. DOI: 10.1109/MSCPES55116.2022.9770140.

41. Akbarzadeh A., Katsikas S. K. Dependency-based security risk assessment for cyber-physical systems. *Int. J. Inf. Secur*. 2023. Vol. 22. P. 563–578. DOI: 10.1007/s10207-022-00608-4

42. Zhang X., Ma H., Tse C. K. Assessing the Robustness of Cyber-Physical Power Systems by Considering Wide-Area Protection Functions. *IEEE Journal on Emerging and Selected Topics in Circuits and Systems.* 2022. Vol. 12, no. 1. P. 107–114. DOI: 10.1109/JETCAS.2022.3144443

43. Kure H. I., Islam S., Ghazanfar M. et al. Asset criticality and risk prediction for an effective cybersecurity risk management of cyber-physical system. *Neural Comput & Applic.* 2022. Vol. 34. P. 493–514. DOI: 10.1007/s00521-021-06400-0

44. Ntafloukas K., Pasquale L., Martinez-Pastor B., McCrum D. P. A Vulnerability Assessment Approach for Transportation Networks Subjected to Cyber–Physical Attacks. *Future Internet.* 2023. Vol. 15, no. 3. P. 100. DOI: 10.3390/fi15030100

45. Rostami A., Mohammadi M., Karimipour H. Reliability assessment of cyber-physical power systems considering the impact of predicted cyber vulnerabilities. *International Journal of Electrical Power & Energy Systems*. 2023. Vol. 147. P. 108892. DOI: 10.1016/j.ijepes.2022.108892.

46. Phillips S. C., Taylor S., Boniface M. та ін. Automated Knowledge-Based Cybersecurity Risk Assessment of Cyber-Physical Systems. *IEEE Access*. 2024. Vol. 12. P. 82482–82505. DOI: 10.1109/ACCESS.2024.3404264.

47. Ntafloukas K., McCrum D. P., Pasquale L. A Cyber-Physical Risk

Assessment Approach for Internet of Things Enabled Transportation Infrastructure. *Appl. Sci.* 2022. Vol. 12, no. 18. P. 9241. DOI: 10.3390/app12189241

48. Xu S., Xia Y., Shen H.-L. Cyber Protection for Malware Attack Resistance in Cyber-Physical Power Systems. *IEEE Systems Journal*. 2022. Vol. 16, no. 4. P. 5337–5345. DOI: 10.1109/JSYST.2022.3150576

49. Khanna K., Govindarasu M. Resiliency-Driven Cyber–Physical Risk Assessment and Investment Planning for Power Substations. *IEEE Transactions on Control Systems Technology*. 2024. Vol. 32, no. 5. P. 1743–1754. DOI: 10.1109/TCST.2024.3378990.

50. Yu Z., Gao H., Cong X. et al. A Survey on Cyber–Physical Systems Security. *IEEE Internet of Things Journal*. 2023. Vol. 10, no. 24. P. 21670–21686. DOI: 10.1109/JIOT.2023.3289625.

51. Kim S., Park K.-J., Lu C. A Survey on Network Security for Cyber–Physical Systems: From Threats to Resilient Design. *IEEE Communications Surveys & Tutorials*. 2022. Vol. 24, no. 3. P. 1534–1573. DOI: 10.1109/COMST.2022.3187531

52. Mavikumbure H. S., Cobilean V., Wickramasinghe C. S. et al. Generative AI in Cyber Security of Cyber Physical Systems: Benefits and Threats. *2024 16th International Conference on Human System Interaction (HSI), Paris, France*, 2024. P. 1–8. DOI: 10.1109/HSI61632.2024.10613562.

53. Kholidy H. A. Autonomous mitigation of cyber risks in the Cyber–Physical Systems. *Future Generation Computer Systems*. 2021. Vol. 115. P. 171–187. DOI: 10.1016/j.future.2020.09.002.

54. Rosado D. G., Santos-Olmo A., Sánchez L. E. et al. Managing cybersecurity risks of cyber-physical systems: The MARISMA-CPS pattern. *Computers in Industry*. 2022. Vol. 142. P. 103715. DOI: 10.1016/j.compind.2022.103715.

55. Raza A., Memon S., Nizamani M. A., Shah M. H. Machine Learning-Based Security Solutions for Critical Cyber-Physical Systems. *2022 10th International Symposium on Digital Forensics and Security (ISDFS), Istanbul, Turkey*, 2022. P. 1–6. DOI: 10.1109/ISDFS55398.2022.9800811..

56. Sahin M. E., Tawalbeh L., Muheidat F. The Security Concerns On Cyber-

Physical Systems And Potential Risks Analysis Using Machine Learning. *Procedia Computer Science.* 2022. Vol. 201. P. 527–534. DOI: 10.1016/j.procs.2022.03.068.

57. Gaba S. et al. A Systematic Analysis of Enhancing Cyber Security Using Deep Learning for Cyber Physical Systems. *IEEE Access*. 2024. Vol. 12. P. 6017–6035. DOI: 10.1109/ACCESS.2023.3349022.

58. Javed M., Tariq N., Ashraf M. et al. Securing Smart Healthcare Cyber-Physical Systems against Blackhole and Greyhole Attacks Using a Blockchain-Enabled Gini Index Framework. *Sensors*. 2023. Vol. 23, no. 23. P. 9372. DOI: 10.3390/s23239372

59. СОУ 207.01:2017. Текстові документи. Загальні вимоги. Хмельницький: ХНУ, 2017. 46 с. URL: https://msn.khnu.km.ua/pluginfile.php/466522/mod_resource/content/1/132_C%20T%20A%20H%20Д%20A%20P%20T%20чист%20.pdf

60. ДСТУ 8302:2015. Бібліографічне посилання. Загальні положення та правила складання. [Чинний від 2016-07-1]. Київ, 2016. 20 с. (Державна наукова установа ―Книжкова палата України імені Івана Федорова‖).

ДОДАТОК А. СПИСОК ПРАЦЬ

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
IVAN FRANKO NATIONAL UNIVERSITY OF LVIV
STATE UNIVERSITY OF INFORMATION
AND COMMUNICATION TECHNOLOGIES

SECURITY OF MODERN INFORMATION AND COMMUNICATION SYSTEMS

PROCEEDINGS

of the International Scientific and Technical Conference

16-18 October 2025
Lviv (Ukraine)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ФРАНКА
ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

БЕЗПЕКА СУЧАСНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ

МАТЕРІАЛИ

Міжнародної науково-технічної конференції

16-18 жовтня 2025
м. Львів (Україна)

УДК [003.26+004+519.816]:004.056:65(063)

SMICS: Безпека сучасних інформаційно-комунікаційних систем: матеріали Міжнар. наук.-техн. конф., м. Львів, 16-18 жовтня 2025 р.: ЛНУ ім. І. Франка, 2025, 468 с.

Збірник містить тексти наукових матеріалів доповідей та тез учасників міжнародної науково-технічної конференції «SMICS: Безпека сучасних інформаційно-комунікаційних систем». Основною метою конференції є ознайомлення з сучасними досягненнями та висвітлення результатів наукових досліджень з усіх аспектів кібербезпеки та захисту інформації.

ОРГАНІЗАТОРИ КОНФЕРЕНЦІЇ

1. Львівський національний університет імені Івана Франка
2. Державний університет інформаційно-комунікаційних технологій
3. ГО "Асоціація спеціалістів кібербезпеки"
4. Академія кіберзахисту (CDA)
5. Rowan University, USA
6. Halmstad University, Sweden
7. University of the National Education Commission, Poland
8. Opole University of Technology, Poland

ПАРТНЕРИ КОНФЕРЕНЦІЇ

ОРГКОМІТЕТ КОНФЕРЕНЦІЇ

Голови

ГЛАДИШЕВСЬКИЙ Р. - ректор Львівського національного університету імені Івана Франка, академік НАН України, д.х.н., професор
ШУЛЬГА В. - ректор Державного університету інформаційно-комунікаційних технологій, д.і.н., професор
КОРЧЕНКО О. – президент Громадської організації «Асоціація спеціалістів кібербезпеки», чл.-кор. Національної Академії Наук України, д.т.н., професор

Заступники голів

ДИЯК І. – декан факультету прикладної математики та інформатики Львівського національного університету імені Івана Франка, д.ф.- м.н., професор
ІВАНЧЕНКО Є - директор Навчально-наукового інституту кібербезпеки та захисту інформації Державного університету інформаційно-комунікаційних технологій, д.т.н., професор
УДОВИК І. - декан факультету інформаційних технологій, Національний технічний університет «Дніпровська політехніка», к.т.н., професор
ХОХЛАЧОВА Ю.Є. – вчений секретар Громадської організації «Асоціація спеціалістів кібербезпеки», к.т.н., професор

Програмний комітет

БУГРІЙ О. - професор кафедри математичної статистики та диференціальних рівнянь Львівського національного університету імені Івана Франка, д.ф.-м.н., професор
ВИНОКУРОВА О. - професор кафедри кібербезпеки Львівського національного університету імені Івана Франка, д.т.н., професор
HNATYSHIN V. - Department of Computer Science Head, Full Professor, Rowan University (USA)
ДАВИДЕНКО А.– провідний науковий співробітник Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, д.т.н., професор
КАЗАКОВА Н. – завідувач каф. інформаційних технологій Одеського національного університету імені І.І.Мечнікова, д.т.н., професор
КИРИК М. - професор кафедри кібербезпеки Львівського національного університету імені Івана Франка, д.т.н., професор
КЛЬОЦ Ю. - завідувач каф. кібербезпеки Хмельницького національного університету, к.т.н., доцент
КОНДРАТЮК С. – професор кафедри публічного управління та адміністрування Державного університету інформаційно-комунікаційних технологій, к.п.н., професор
КУЧИК О. – завідувач кафедри міжнародної безпеки та стратегічних студій Львівського національного університету імені Івана Франка, к.і.н., доцент
МУЛЕСА П.- завідувач каф. кібернетики та прикладної математики Ужгородського національного університету, д.п.н., доцент
ОПІРСЬКИЙ І. – завідувач каф. безпеки інформаційних технологій НУ "Львівська політехніка", д.т.н., професор
ПАРХУЦЬ Л.– професор кафедри кібербезпеки Львівського національного університету імені Івана Франка, д.т.н., професор
РІЗАК В. М. - завідувач каф. твердотільної електроніки та інформаційної безпеки Ужгородського національного університету, д.ф.-м.н., професор
SEMENOV S. – Head of the Department of Computer Engineering and Cybersecurity, Full Professor, Krakow University of the National Education

	Commission (Poland) **ТКАЧ Ю.** - завідувач кафедри кібербезпеки та математичного моделювання НУ "Чернігівська політехніка", к.т.н., д.п.н., професор **ТКАЧУК Р.** – начальник кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, д.т.н., професор **TORSTENSON O.** – Programme director Master's Programme in Network Forensics (Halmstad, Sweden) **ШЕЛЕСТ М.** - професор кафедри кібербезпеки та математичного моделювання НУ "Чернігівська політехніка", д.т.н., професор **ШУВАР Р.** – завідувач кафедри системного проектування Львівського національного університету імені Івана Франка, к.ф.-м.н., доцент
Співголови	**ВЕНГЕРСЬКИЙ П.** – завідувач кафедри . кібербезпеки Львівського національного університету імені Івана Франка, д.ф.-м..н., доцент **ГАЙДУР Г.** – завідувач кафедри систем та технологій кібербезпеки Державного університету інформаційно-комунікаційних систем, д.т.н., професор
Організаційний комітет	**БРИЧ Т.Б.** – доцент кафедри кібербезпеки Львівського національного університету імені Івана Франка, к.т.н.-м. н. **ВЛАСОВ В.** – доцент кафедри математичної статистики і диференціальних рівнянь Львівського національного університету імені Івана Франка, к.ф.-м. н. **КОКОВСЬКА Я.** – доцент кафедри дискретного аналізу та інтелектуальних систем, Львівського національного університету імені Івана Франка, к.ф.-м.н. **ПОПАДЮК О.** – доцент кафедри кібербезпеки Львівського національного університету імені Івана Франка, PhD **ПРИГАРА М.** – доцент каф. технології машинобудування Ужгородського національного університету, к.т.н., доцент **ТРУШЕВСЬКИЙ В.** – доцент кафедри кібербезпеки Львівського національного університету імені Івана Франка, к.ф.-м.н., доцент **ЩЕРБИНА М.** – ст. викладач кафедри кібербезпеки Львівського національного університету імені Івана Франка **В'ЯЧАЛО М.** – асистент кафедри кібербезпеки Львівського національного університету імені Івана Франка **ЗЛАТОУС С.** – асистент кафедри кібербезпеки Львівського національного університету імені Івана Франка **КУЗБИТ Ю.** – асистент кафедри кібербезпеки Львівського національного університету імені Івана Франка **ЛАЩІВСЬКА С.** – інженер кафедри кібербезпеки Львівського національного університету імені Івана Франка
Вчений секретар	**ГУТІК О.** – професор кафедри кібербезпеки Львівського національного університету імені Івана Франка, к.ф.-м.н., доцент

Метод оцінювання стану інформаційної безпеки елементів кіберфізичних систем

Наталія Петляк[1], Артем Барабаш[1]

[1] *Хмельницький національний університет, вул. Інститутська 11, 29016 Хмельницький, Україна*

Анотація

У роботі розглянуто проблему забезпечення інформаційної безпеки кіберфізичних систем, які поєднують обчислювальні ресурси з фізичними процесами. З огляду на складність їхньої структури та високу інтегрованість у критичну інфраструктуру, виникає потреба у створенні методів комплексного оцінювання рівня захищеності. Запропоновано метод оцінювання стану інформаційної безпеки елементів кіберфізичних систем, який базується на формалізації параметрів захищеності, урахуванні їхніх вагових коефіцієнтів та багаторівневому аналізі ризиків. Проведені дослідження підтвердили ефективність застосування методу для виявлення критичних вразливостей, пріоритезації заходів безпеки та підтримки процесів управління кіберзахистом.

Ключові слова

інформаційна безпека, кіберфізичні системи, оцінювання ризиків, рівень захищеності, методи аналізу

1. Вступ

Кіберфізичні системи, що інтегрують апаратні пристрої, програмні комплекси, сенсорні мережі та засоби зв'язку, сьогодні стають ключовим компонентом у промисловості, енергетиці, транспорті та інших галузях. Вони функціонують у тісному зв'язку між цифровим і фізичним середовищем, що робить їх особливо вразливими до кіберзагроз. Атаки на елементи таких систем можуть спричинити серйозні наслідки не лише для інформаційної інфраструктури, а й для фізичної безпеки людей і технологічних процесів.

Проблема ускладнюється тим, що традиційні методи захисту інформаційних систем часто виявляються недостатньо ефективними у випадку кіберфізичних систем. Це пов'язано з їх розподіленим характером, високою гетерогенністю, а також взаємозалежністю окремих компонентів. У такому середовищі зростає роль методів оцінювання стану захищеності, які дозволяють не лише виявити наявність загроз, але й визначити рівень ризику для кожного елементу та всієї системи загалом.

2. Аналіз досліджень та публікацій

Актуальні дослідження свідчать, що основні підходи до оцінювання рівня інформаційної безпеки базуються на трьох групах методів: сигнатурному аналізі, поведінковому моніторингу та оцінюванні ризиків [1-2]. Сигнатурні методи дозволяють швидко виявляти відомі загрози, однак вони малоефективні проти нових або модифікованих атак [3-4]. Поведінковий аналіз орієнтується на пошук аномалій у функціонуванні системи, проте вимагає значних обчислювальних ресурсів і може призводити до помилкових спрацювань

[15]Corresponding authors
npetlyak@khmnu.edu.ua (Н. Петляк); abarabash@khmnu.edu.ua (А. Барабаш)
0000-0001-5971-4428 (Н. Петляк)

[5]. Методи оцінювання ризиків, у свою чергу, надають більш комплексний підхід, оскільки враховують можливість реалізації загроз, вразливості елементів системи та потенційний вплив на функціонування критичних процесів [6].

Останнім часом активно розробляються моделі оцінювання стану кіберфізичних систем на основі багатофакторного аналізу. У таких підходах використовуються формалізовані метрики, які характеризують ступінь захищеності кожного компонента. Це дозволяє визначати найбільш критичні елементи системи та концентрувати ресурси на їх захисті. Попри значні досягнення, залишається проблема уніфікації методів оцінювання, що мають враховувати специфіку кіберфізичних систем та їхню тісну інтеграцію з фізичними процесами.

3. Метод оцінювання стану інформаційної безпеки

Запропонований метод оцінювання стану інформаційної безпеки елементів кіберфізичних систем передбачає багаторівневу процедуру аналізу, що поєднує якісні та кількісні підходи. На першому рівні здійснюється ідентифікація ключових елементів системи, серед яких можуть бути контролери, сенсорні вузли, мережеві комутатори, сервери управління та інші компоненти. Для кожного елемента визначаються критичні параметри інформаційної безпеки, такі як цілісність даних, конфіденційність, доступність, автентичність і відмовостійкість. Далі вводиться система вагових коефіцієнтів, яка відображає відносну важливість кожного параметра для безперервного функціонування системи. Наприклад, для сенсорної мережі найважливішим може бути параметр цілісності даних, тоді як для серверів управління визначальним буде рівень доступності. Вагові коефіцієнти встановлюються експертним шляхом або на основі статистичних даних щодо ймовірності реалізації загроз і наслідків інцидентів. Після цього здійснюється збір фактичних даних про поточний стан елементів системи. Він може включати результати сканування вразливостей, журнали подій, дані систем моніторингу трафіку та інші джерела. Отримані показники зіставляються із заданими еталонними значеннями, що дозволяє обчислити рівень відповідності фактичного стану заданим критеріям. Для цього використовується нормалізована шкала, яка переводить усі параметри у єдиний діапазон від нуля до одиниці. Загальний рівень захищеності елемента визначається як зважена сума його параметрів з урахуванням вагових коефіцієнтів. Це дозволяє відобразити як відносну важливість кожного параметра, так і його поточний стан. Формально рівень захищеності можна подати як інтегральний показник, що є результатом агрегування окремих метрик.

На наступному етапі проводиться аналіз ризиків. Він передбачає визначення ймовірності реалізації конкретних загроз для кожного елемента та оцінку можливих наслідків їх впливу. Для цього використовується модель ризику, де підсумковий показник обчислюється як добуток імовірності загрози на рівень вразливості та значущість наслідків. Такий підхід дозволяє ранжувати елементи за рівнем ризику і виділяти найбільш критичні компоненти, які потребують першочергового захисту. Особливістю методу є можливість його застосування як у статичному, так і в динамічному режимі. У статичному режимі аналіз проводиться періодично на основі накопичених даних. У динамічному режимі метод інтегрується з системами моніторингу та забезпечує безперервне оновлення показників захищеності у реальному часі.

Ще одним важливим аспектом є адаптивність методу. Вагові коефіцієнти та порогові значення можуть змінюватися залежно від умов експлуатації системи та появи нових загроз. Завдяки цьому метод не є статичним, а може підлаштовуватися під актуальну ситуацію, що підвищує його практичну цінність.

У межах проведеного дослідження було розроблено та реалізовано програмний прототип інформаційної системи оцінювання, який забезпечує практичне застосування запропонованого методу. Даний прототип орієнтований на автоматизацію збору даних із різних джерел, зокрема систем моніторингу мережевого трафіку, журналів подій, засобів контролю доступу та результатів сканування вразливостей. Отримана інформація підлягає попередній обробці, що передбачає нормалізацію параметрів, усунення шумів та приведення показників до єдиного формату, після чого здійснюється розрахунок інтегральних індексів стану інформаційної безпеки для окремих елементів системи. Розраховані значення дозволяють визначати ступінь відповідності кожного елемента заданим критеріям безпеки та формувати узагальнену оцінку, яка відображає загальний стан захищеності кіберфізичної системи.

Важливою особливістю прототипу є можливість наочного представлення результатів у вигляді звітів та графічних візуалізацій. Такий підхід не лише полегшує сприйняття отриманих даних, але й дає адміністраторам змогу швидко ідентифікувати вразливі компоненти, оцінити рівень ризиків і своєчасно прийняти рішення щодо реалізації захисних заходів. Використання інтегрального індексу дозволяє порівнювати між собою різні елементи системи, визначати найбільш критичні з них і здійснювати пріоритезацію у розподілі ресурсів для забезпечення захисту. Таким чином, запропонований метод функціонує як комплексний інструмент, що об'єднує кількісні розрахунки, експертні оцінки та інтегрований аналіз ризиків, забезпечуючи формування цілісної та багатовимірної картини стану інформаційної безпеки кіберфізичної системи. Його практичне застосування дозволяє виявляти потенційно небезпечні тенденції, прогнозувати розвиток загроз, а також реалізовувати адаптивне управління ресурсами захисту.

Наукова новизна розробленого підходу полягає у поєднанні вагового моделювання параметрів захищеності з інтегрованим ризик-орієнтованим аналізом та впровадженням механізму динамічного оновлення показників у режимі реального часу. Це забезпечує гнучкість і адаптивність системи, дозволяє формувати інтегральний індекс стану безпеки елементів кіберфізичної системи, що суттєво підвищує точність визначення найбільш критичних компонентів та ефективність пріоритезації захисних заходів. У результаті метод можна розглядати як універсальне рішення, здатне масштабуватися залежно від архітектури системи та рівня її інтегрованості у критичну інфраструктуру.

4. Висновки

Запропонований метод оцінювання стану інформаційної безпеки елементів кіберфізичних систем забезпечує комплексний підхід до аналізу рівня захищеності. Його особливістю є врахування вагових коефіцієнтів параметрів, інтеграція з аналізом ризиків та можливість застосування у динамічному режимі. Метод дозволяє визначати критичні елементи системи, пріоритезувати заходи кіберзахисту та формувати інтегральний індекс стану безпеки. Подальші дослідження планується спрямувати на оптимізацію програмної реалізації методу та його апробацію у реальних промислових кіберфізичних системах.

Література

[1] S. C. Phillips, S. Taylor, M. Boniface, S. Modafferi, M. Surridge, Automated Knowledge-Based Cybersecurity Risk Assessment of Cyber-Physical Systems, IEEE Access 12 (2024) 82482–82505. doi:10.1109/ACCESS.2024.3404264.

[2] A. Akbarzadeh, S. K. Katsikas, Dependency-based security risk assessment for cyber-physical systems, Int. J. Inf. Secur. 22 (2023) 563–578. doi:10.1007/s10207-022-00608-4.

[3] [3] D. A. Moskvin, Assessing the Security of a Cyber-Physical System Based on an Analysis of Malware Signatures, Aut. Control Comp. Sci. 57 (2023) 894–903. doi:10.3103/S0146411623080175.

[4] S. Y. Hilgurt, A. M. Davydenko, T. V. Matovka, M. P. Prygara, Tools for Analyzing Signature-Based Hardware Solutions for Cyber Security Systems, Journal of Cyber Security and Mobility 12 (3) (2023) 339–366. doi:10.13052/jcsm2245-1439.1235.

[5] H. Gong, R. Li, J. An, G. Xie, Reliability Modeling and Assessment for a Cyber-Physical System With a Complex Boundary Behavior, IEEE Transactions on Reliability 72 (1) (2023) 224–239. doi:10.1109/TR.2022.3160460.

[6] S. Deng, J. Zhang, D. Wu, Y. He, X. Xie, X. Wu, A Quantitative Risk Assessment Model for Distribution Cyber-Physical System Under Cyberattack, IEEE Transactions on Industrial Informatics 19 (3) (2023) 2899–2908. doi:10.1109/TII.2022.3169456.

НАУКОВЕ ВИДАННЯ

МАТЕРІАЛИ
Міжнародної науково-технічної конференції
«SMICS: Безпека сучасних інформаційно-комунікаційних систем»

16-18 жовтня 2025 року

м. Львів (Україна)

Організаційний комітет конференції та редакція можуть не поділяти думки авторів і не несуть відповідальність за достовірність викладеної інформації.

За науковий зміст і викладення матеріалу, достовірність та коректність фактичних даних уся відповідальність покладається на авторів та їх наукових керівників.

Неінформативний текст матеріалів доповіді міг бути скорочений або вилучений на розсуд Оргкомітету конференції.

Оригінал-макет підготовлено на кафедрі кібербезпеки
Львівського національного університету імені Івана Франка

Завідувачу кафедри кібербезпеки
к.т.н., доц. Кльоцу Ю.П.
здобувача вищої освіти
Барабаша Артема Вадимовича
студента ФІТ, 2 курсу, групи КБЗІм-24-1

ЗАЯВА

З правилами чинного Положення про систему забезпечення академічної доброчесності у Хмельницькому національному університеті, згідно з яким виявлення академічного плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту і застосування заходів академічної відповідальності, ознайомлений. Про використання спеціалізованих програмних засобів (СПЗ) StrikePlagiarism та Anti-Plagiarism для перевірки кваліфікаційних робіт здобувачів вищої освіти на наявність академічного плагіату оповіщений. Надаю університету право на передачу моєї роботи для обробки та збереження в базах даних СПЗ і використання роботи для виявлення академічного плагіату в інших роботах, які перевіряються СПЗ.

Також надаю свою згоду на обробку й збереження університетом моєї роботи в Інституційному репозитарії Хмельницького національного університету.

Робота надається для перевірки в електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

1.12.2025
дата

підпис

Anti-Plagiarism (UA) v-15.281 Educational

The maximum coincidence with one document 1.0%

Dictionaries check: en_US, ru_RU, ua_UA. **Errors in the documents: 7%**

	Document		Sum coincidence on the DB	
ID: 251492 Title: Метод оцінювання рівня захищеності кіберфізичних систем від інформаційних загроз Added in a DB: 2025-12-03 Authors: Барабаш Артем Вадимович Heads: Петляк Н.С, Consultants: Opponents:	Symbols	Lexemes	Symbols	Lexemes
	124425	853	1637 (1%)	18 (2%)

Plagiarism sources

ID	Description	Plagiarism presence in the document	
		Symbols	Lexemes

Протокол аналізу звіту подібності науковим керівником

Заявляю, що я ознайомився (-лась) з Повним звітом подібності, який був згенерований Системою виявлення і запобігання плагіату щодо роботи:

Автор: Барабаш Артем Вадимович

Співавтор:

Назва: Метод оцінювання рівня захищеності кіберфізичних систем від інформаційних загроз

Науковий керівник: Петляк Наталя Сергіївна

Підрозділ: Кафедра кібербезпеки

Коефіцієнт подібності 1:4%

Коефіцієнт подібності 2:0.9%

Мікропробіли: 0

Заміна букв: 0

Інтервали: 0

Білі знаки: 0

Дата створення звіту: 2025-12-03 23:22:30.0

Після аналізу Звіту подібності констатую наступне:

☐ **Запозичення, виявлені в роботі є законними і не є плагіатом. Рівень подібності не перевищує допустимої межі. Таким чином робота незалежна і приймається.**

☐ **Запозичення не є плагіатом, але перевищено граничне значення рівня подібностей. Таким чином робота повертається на доопрацювання.**

☐ **Виявлено запозичення і плагіат або навмисні текстові спотворення (маніпуляції), як передбачувані спроби укриття плагіату, які роблять роботу невідповідною вимогам законодавства (Ст. 32. ЗУ Про вищу освіту, пункт 3.1, Ст. 42. ЗУ Про освіту) та вимог НАЗЯВО (Критерій 5), а також кодексу етики і процедурам. Таким чином робота не приймається.**

Обгрунтування:

Дата експерт

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Назва кваліфікаційної роботи: Метод оцінювання рівня захищеності кіберфізичних систем від інформаційних загроз

Автор: Барабаш Артем Вадимович

Освітня програма: Кібербезпека та захист інформації

Рівень вищої освіти: другий (магістерський)

Спеціальність: 125 – Кібербезпека та захист інформації

Науковий керівник: Наталія ПЕТЛЯК, д-р філософії, ст.викладач

На основі аналізу кваліфікаційної роботи на дотримання вимог академічної доброчесності (у т.ч. відсутності ознак академічного плагіату) з урахуванням результатів перевірки роботи спеціалізованим програмним засобом(ами) комісія зробила такий висновок:

№	Висновок	Позначка про відповідність
1	Ознаки академічного плагіату	
1.1	Запозичення, виявлені в роботі, є законними і не є академічним плагіатом (далі – зазначаються підстави віднесення запозичень до правомірних, якщо потрібно). Робота приймається до захисту	відповідає
1.2	Виявлені запозичення не є академічним плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). Робота приймається до захисту, але має бути відкоригована	
1.3	Виявлені запозичення не є академічним плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. Робота може бути допущена до захисту після того як буде відкоригована та доопрацьована і успішно пройде повторну перевірку на академічний плагіат	
1.4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття текстових запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	
2	Інші види порушень академічної доброчесності	

Підтвердження:

Оригінальність тексту роботи за результатами перевірки системою StrikePlagiarism складає 95,98%, оригінальність тексту роботи за результатами перевірки системою Anti-Plagiarism складає 99,0%

Згідно з Положенням про систему забезпечення академічної доброчесності у ХНУ (https://khmnu.edu.ua/wp-content/uploads/normatyvni-dokumenty/polozhennya/pro-systemu-zabezpechennya-akademichnoyi-dobrochesnosti.pdf, Додаток В) кваліфікаційна робота, виконана за освітньо-професійною програмою, кількісні показники рівня унікальності тексту у відсотках до загального обсягу матеріалу в якій складає 75-100 %, визнається роботою з високим рівнем унікальності тексту: «Текст вважається унікальним і не потребує додаткових дій щодо запобігання неправомірним запозиченням».

Дата: 3.12.2025

Завідувач кафедри кібербезпеки _____ Юрій КЛЬОЦ

Гарант освітньої програми _____ Віра ТІТОВА

Керівник кваліфікаційної роботи _____ Наталія ПЕТЛЯК

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітнього ступеня «магістр»

Студент Барабаш Артем Вадимович

Тема Метод оцінювання рівня захищеності кіберфізичних систем від інформаційних загроз

Спеціальність 125 – Кібербезпека та захист інформації

Обсяг кваліфікаційної роботи освітньо-кваліфікаційного рівня «бакалавр»:

кількість листів креслень – ; кількість сторінок записки 89 .

1. Короткий зміст роботи та прийнятих рішень У кваліфікаційній роботі представлено комплексний підхід до оцінювання рівня захищеності кіберфізичних систем (КФС) від інформаційних загроз. Проаналізовано сучасні моделі загроз, методи оцінювання ризиків, підходи до обробки даних і системного аналізу КФС. У роботі сформовано модель формування опису ознак стану інформаційної безпеки елементів КФС, розроблено алгоритм обчислення показників стану ІБ та метод їх оцінювання. Проведено експериментальну перевірку достовірності запропонованого методу, включаючи моделювання кіберфізичних процесів, порівняння з існуючими підходами та оцінку можливості роботи методу в режимі реального часу.

2. Висновок про відповідність кваліфікаційної роботи завданню Кваліфікаційна робота повністю відповідає поставленому завданню. У ній виконано всі вимоги, визначені завданням на кваліфікаційну роботу: здійснено аналіз предметної галузі, розроблено метод оцінювання стану ІБ КФС, проведено моделювання та експериментальну перевірку, здійснено порівняльний аналіз та сформульовано висновки.

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі обґрунтовано актуальність теми та сформульовано цілі та завдання дослідження. У першому розділі виконано огляд сучасних кіберзагроз, моделей безпеки, методів аналізу ризиків та підходів до аудиту ІБ КФС. Надано систематизований аналіз наукових праць, включно з сучасними підходами, що свідчить про глибоку проробку теоретичної бази. У другому розділі розроблено модель формування ознак, алгоритм їх оцінювання та метод визначення стану ІБ компонентів КФС. Показано, як отримані показники можуть інтегруватися в системи моніторингу. У третьому розділі проведено експериментальні дослідження, моделювання станів КФС, порівняння з відомими методами та аналіз можливості роботи розробленого методу в реальному часі. Робота демонструє використання сучасних результатів досліджень у галузі кіберфізичної безпеки, машинного навчання, моделей ризиків та системного аналізу.

4. Позитивні сторони роботи Робота є актуальною та має високу наукову і практичну цінність. Запропонований метод дозволяє враховувати динамічні зміни параметрів КФС, часові залежності та стохастичні характеристики, що підвищує точність оцінювання рівня захищеності. Автор чітко продемонстрував можливість інтеграції методу в реальні системи моніторингу..

5. Негативні сторони роботи Не до кінця розкрито питання масштабованості запропонованого методу на складні багаторівневі інфраструктури.

6. Оцінка графічного оформлення та пояснювальної записки роботи

7. Відгук про роботу в цілому Кваліфікаційна робота виконана на високому науковому рівні. Автор продемонстрував глибоке розуміння предметної галузі, застосував сучасні методи аналізу та моделювання, обгрунтував можливість практичного застосування запропонованого методу. Робота є цілісною, логічно побудованою та містить вагомі результати, що відповідають рівню магістерської підготовки.

8. Інші зауваження

9. Оцінка кваліфікаційної роботи Враховуючи всі позитивні та негативні сторони представленої кваліфікаційної роботи, можна зробити висновок, що вона заслуговує «добре» 82 балів.

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи)
Бойко Юлій Миколайович,
професор кафедри телекомунікацій, медійних та інтелектуальних технологій, доктор технічних наук, професор

«04» грудня 2025