МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ТА ЗАХИСТОМ ІНФОРМАЦІЇ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “СИСТЕМА ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ВПРОВАДЖЕНИХ ТЕХНІЧНИХ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ МЕТРИК РЕЗУЛЬТАТИВНОСТІ”

на здобуття освітнього ступеня бакалавра
зі спеціальності 125 Кібербезпека
освітньої програми Управління інформаційною та кібернетичною безпекою

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

_____ Богдан ТАРАСЕНКО
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД-41
Богдан ТАРАСЕНКО
Ім’я, ПРІЗВИЩЕ

Керівник: Іван ОПІРСЬКИЙ
д.т.н., професор Ім’я, ПРІЗВИЩЕ

Рецензент:
Ім’я, ПРІЗВИЩЕ

Київ 2026

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут кібербезпеки та захисту інформації

Кафедра управління кібербезпекою та захистом інформації

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УКБЗІ
_____ Світлана ЛЕГОМІНОВА
“___“_____2026 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Тарасенку Богдану Руслановичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Система оцінювання ефективності впроваджених технічних засобів захисту інформації на основі метрик результативності ”,
керівник кваліфікаційної роботи ОПІРСЬКИЙ Іван, д.т.н., професор,
(ПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від “20“ лютого 2026 р. №51

2. Строк подання кваліфікаційної роботи “1” червня 2026р.

3. Вихідні дані до кваліфікаційної роботи: *технічні засоби захисту інформації, міжнародні стандарти, моделі оцінки ефективності систем захисту, наукова та технічна література.*

4. Перелік питань, які мають бути розроблені:

4.1. Проаналізувати класифікацію технічних засобів захисту інформації, особливості їх впровадження, міжнародні стандарти та нормативно-правову базу України у сфері оцінювання ефективності захисту інформації.

4.2. Розробити структурну модель системи оцінювання ефективності впроваджених технічних засобів захисту інформації на основі метрик результативності, сформувати класифікацію метрик та метод формування інтегрального показника ефективності.

4.3. Обґрунтувати механізм функціонування розробленої системи та провести її експериментальне дослідження з метою підтвердження практичної придатності.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “05“ березня 2026 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2026	
2.	Збір та аналіз літератури.	30.03.2026	
3.	Аналіз особливостей управління інформаційною безпекою підприємства	08.04.2026	
4.	Дослідження основних характеристик технологій формування обізнаності й навчання персоналу.	15.04.2026	
5.	Вивчення інструментів та методів формування обізнаності й навчання персоналу з інформаційної безпеки	22.04.2026	
6.	Формулювання висновків за результатами проведеного дослідження.	29.04.2026	
7.	Оформлення роботи.	06.05.2026	
8.	Оформлення презентації.	11.05.2026	
9.	Отримання рецензії на роботу.	10.06.2026	
10.	Захист в ЕК.	__.06.2026	

Здобувач вищої освіти _____ Богдан ТАРАСЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Іван ОПІРСЬКИЙ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня бакалавра

Направляється здобувач Тарасенко Б.Р. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Система оцінювання ефективності впроваджених технічних засобів захисту інформації на основі метрик результативності"

Кваліфікаційна робота і рецензія додаються.

Директор ННІКБЗІ _____ Євгенія ІВАНЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач ТАРАСЕНКО Богдан у кваліфікаційній роботі проаналізував існуючі системи, стандарти та методи оцінювання ефективності технічних засобів захисту інформації (ТЗЗІ), дослідив процеси безперервного моніторингу безпеки на підприємствах, сформував класифікацію метрик результативності та розробив комплексну структурну модель системи оцінювання з обґрунтуванням методу розрахунку інтегрального показника ефективності.

ТАРАСЕНКО Богдан показав розуміння проблеми дослідження та бачення основних теоретичних і практичних напрямів її вирішення, довів володіння методами наукового дослідження та математичного моделювання, проявив себе як організований, відповідальний і самостійний виконавець. Працездатність розробленої системи успішно підтверджена результатами проведеного експериментального дослідження.

Все це дозволяє оцінити кваліфікаційну роботу здобувача ТАРАСЕНКА Богдана на оцінку "відмінно" та присвоїти йому кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи _____ Іван ОПІРСЬКИЙ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____" _____ 2026 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Тарасенко Б.Р. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри
управління кібербезпекою та
захистом інформації _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувача вищої освіти ТАРАСЕНКА Богдана
на тему “Система оцінювання ефективності впроваджених технічних засобів захисту інформації на основі метрик результативності”

Актуальність. У сучасних умовах постійного зростання кіберзагроз просте впровадження технічних засобів захисту інформації (ТЗЗІ) вже не гарантує надійної безпеки корпоративних мереж. Важливо мати інструменти для постійного об'єктивного контролю їхньої реальної ефективності. Перехід від суб'єктивних експертних оцінок до кількісних метрик результативності дозволяє своєчасно виявляти вразливості в інфраструктурі та приймати обґрунтовані управлінські рішення.

З огляду на зазначене, розроблення системи оцінювання ефективності впроваджених ТЗЗІ на основі об'єктивних метрик є вельми актуальним науково-практичним завданням.

Позитивні сторони.

1. У роботі ґрунтовно досліджено особливості контролю ТЗЗІ та розроблено багаторівневу структурну модель системи оцінювання ефективності захисту.
2. Кваліфікаційна робота оформлена відповідно до встановлених вимог. Виклад матеріалу здійснено логічно, ключові математичні моделі та алгоритми наочно представлено у вигляді схем і діаграм.
3. Автор опрацював значну джерельну базу: 42 найменування, серед яких міжнародні галузеві стандарти (ISO/IEC, NIST) та сучасні наукові публікації.
4. За результатами експериментального дослідження на реальних даних підтверджено працездатність моделі та запропоновано конкретні практичні рекомендації щодо оптимізації засобів захисту.

Недоліки.

Доцільно було б приділити дещо більше уваги економічному обґрунтуванню запропонованих організаційно-технічних заходів із реконфігурації та модернізації ТЗЗІ для керівництва підприємства.

Однак, вищезгадане зауваження не знижує практичної цінності розробленої системи і не впливає на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує позитивної оцінки, а здобувач ТАРАСЕНКО Богдан заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент: _____ _____
підпис Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена розробленню системи оцінювання ефективності впроваджених технічних засобів захисту інформації на основі метрик результативності. Робота складається зі вступу, трьох розділів, що містять 6 рисунків і 5 таблиць, висновків і списку використаних джерел із 42 найменувань. Загальний обсяг роботи становить 59 аркушів, з яких 4 аркуші займають перелік умовних скорочень і список використаних джерел.

Метою роботи є розроблення та дослідження системи оцінювання ефективності впроваджених технічних засобів захисту інформації на основі метрик результативності.

Об'єкт дослідження – процеси технічного захисту інформації на підприємствах.

Предмет дослідження – методи та засоби оцінювання ефективності технічних засобів захисту інформації.

Методи дослідження. Для вирішення поставлених завдань у роботі використані методи системного аналізу, порівняння та класифікації, математичного моделювання, нормалізації та лінійної адитивної згортки, а також експериментальні методи дослідження.

Як результат у роботі проаналізовано сучасні підходи та міжнародні стандарти (ISO/IEC 27004, NIST SP 800-55) до оцінювання технічних засобів захисту. Розроблено багаторівневу структурну модель системи оцінювання. Сформовано класифікацію метрик результативності (технічні, експлуатаційні, організаційні) та обґрунтовано метод розрахунку інтегрального показника ефективності. Проведено експериментальне дослідження, яке підтвердило працездатність моделі та дозволило автоматизовано виявити вразливі місця в тестовій інфраструктурі.

Галузь застосування. Розроблені підходи можуть бути використані в центрах управління кібербезпекою (SOC) підприємств різних галузей для безперервного моніторингу ефективності ТЗЗІ, оптимізації конфігурацій та підтримки прийняття управлінських рішень.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВА, ТЕХНІЧНІ ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ, ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ, МЕТРИКИ РЕЗУЛЬТАТИВНОСТІ, ІНТЕГРАЛЬНИЙ ПОКАЗНИК, БЕЗПЕРЕРВНИЙ МОНІТОРИНГ.

ABSTRACT

The qualification work is devoted to the development of a system for evaluating the effectiveness of implemented technical means of information protection based on performance metrics. The work consists of an introduction, three chapters, conclusions, and a list of references containing 42 items. The total volume of the work is 59 pages, containing 6 figures and 5 tables.

The purpose of the study is to develop and investigate a system for evaluating the effectiveness of implemented technical means of information protection based on performance metrics.

The object of the study is the processes of technical information protection at enterprises.

The subject of the study is methods and tools for evaluating the effectiveness of technical means of information protection.

Research methods. To solve the set tasks, the methods of system analysis, comparison and classification, mathematical modeling, normalization and linear additive convolution, as well as experimental research methods were used in the work.

As a result of the study, modern approaches and international standards (ISO/IEC 27004, NIST SP 800-55) for evaluating technical protection means were analyzed. A multilevel structural model of the evaluation system was developed. A classification of performance metrics (technical, operational, organizational) was formed, and the method for calculating the integral efficiency indicator was justified. An experimental study was conducted, which confirmed the operability of the model and allowed automated identification of vulnerabilities in the test infrastructure.

Field of application. The developed approaches can be used in Security Operations Centers (SOC) of enterprises in various industries for continuous monitoring of the effectiveness of technical protection means, configuration optimization, and supporting management decision-making.

Keywords: ENTERPRISE INFORMATION SECURITY, TECHNICAL MEANS OF INFORMATION PROTECTION, EFFECTIVENESS EVALUATION,

PERFORMANCE METRICS, INTEGRAL INDICATOR, CONTINUOUS MONITORING.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

ДСТУ Державний стандарт України

ІБ Інформаційна безпека

ІКС Інформаційно-комунікаційна система

КСЗІ Комплексна система захисту інформації

НД ТЗІ Нормативний документ системи технічного захисту інформації

СУІБ Система управління інформаційною безпекою

ТЗЗІ Технічні засоби захисту інформації

CEF Common Event Format (загальний формат подій)

DLP Data Loss Prevention (запобігання витоку даних)

EDR Endpoint Detection and Response (система виявлення та реагування на кінцевих точках)

FNR False Negative Rate (рівень пропуску атак / хибнонегативних спрацювань)

FPR False Positive Rate (рівень хибних спрацювань / хибнопозитивних спрацювань)

IDS Intrusion Detection System (система виявлення вторгнень)

IPS Intrusion Prevention System (система запобігання вторгненням)

LEEF Log Event Extended Format (розширений формат подій журналу)

MTTR Mean Time To Respond / Repair (середній час реагування та усунення)

NGFW Next-Generation Firewall (міжмережевий екран наступного покоління)

SIEM Security Information and Event Management (система управління інформаційною безпекою та подіями)

SOC Security Operations Center (центр управління кібербезпекою)

VPN Virtual Private Network (віртуальна приватна мережа)

ВСТУП

Актуальність теми. У сучасних умовах стрімкого розвитку інформаційних технологій та зростання кількості кіберзагроз забезпечення ефективного захисту інформації є одним із ключових завдань будь-якого підприємства. Підприємства витрачають значні фінансові та людські ресурси на впровадження технічних засобів захисту інформації (ТЗЗІ), таких як міжмережеві екрани, системи виявлення та запобігання вторгненням, засоби виявлення загроз на кінцевих пристроях, системи запобігання витокам даних та інші. Однак просте впровадження цих засобів не гарантує їхньої реальної ефективності в умовах динамічного середовища загроз.

Традиційні методи оцінки ефективності ТЗЗІ здебільшого ґрунтуються на формальній відповідності стандартам та суб'єктивних експертних оцінках. Це призводить до того, що керівництво не завжди має об'єктивну кількісну інформацію про те, наскільки впроваджені засоби захисту дійсно знижують ризики, як швидко виявляються інциденти та чи виправдовують себе понесені витрати.

У зв'язку з цим особливо актуальним стає розроблення системи оцінювання ефективності технічних засобів захисту інформації на основі об'єктивних метрик результативності, яка дозволить перейти від якісних до кількісних оцінок і забезпечити підтримку прийняття обґрунтованих управлінських рішень.

Мета кваліфікаційної роботи полягає в розробленні та дослідженні системи оцінювання ефективності впроваджених технічних засобів захисту інформації на основі метрик результативності.

Об'єкт дослідження **–** процеси технічного захисту інформації на підприємствах.

Предмет дослідження – методи та засоби оцінювання ефективності технічних засобів захисту інформації.

Для досягнення поставленої мети необхідно вирішити такі ***завдання***:

1. Проаналізувати класифікацію технічних засобів захисту інформації, особливості їх впровадження, міжнародні стандарти та нормативно-правову базу України у сфері технічного захисту інформації.

2. Дослідити існуючі системи, підходи та методи оцінювання ефективності засобів захисту інформації.

3. Розробити структурну модель системи оцінювання ефективності ТЗЗІ на основі метрик результативності.

4. Сформувати класифікацію метрик результативності та запропонувати метод розрахунку інтегрального показника ефективності.

5. Обґрунтувати механізм функціонування системи та провести її експериментальне дослідження.

Методи дослідження. У роботі використані методи системного аналізу, порівняння, класифікації, математичного моделювання, нормалізації та зважування показників, а також методи експериментального дослідження.

Практичне значення одержаних результатів полягає в тому, що розроблена система може бути застосована на підприємствах різних форм власності для об’єктивної кількісної оцінки ефективності ТЗЗІ, оптимізації витрат на інформаційну безпеку та підвищення рівня кіберстійкості організації.

Розділ 1 АНАЛІЗ СИСТЕМ ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ТЕХНІЧНИХ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ

1.1.Класифікація технічних засобів захисту інформації та особливості їх впровадження

Технічні засоби захисту інформації є фундаментальним інженерним базисом забезпечення кібернетичної безпеки будь-якої сучасної інформаційно-комунікаційної системи. Згідно з національним стандартом ДСТУ 3396.2-97, технічний захист інформації визначається як діяльність, спрямована на запобігання витоку інформації технічними каналами, її блокуванню та порушенню цілісності [6]. Для розуміння процесів оцінювання ефективності необхідно чітко класифікувати існуючий арсенал засобів захисту, оскільки різні типи ТЗЗІ вимагають застосування принципово різних підходів до моніторингу та формування метрик.

Сучасну класифікацію ТЗЗІ можна здійснювати за кількома ключовими ознаками, зокрема за рівнем застосування в інфраструктурі мережі (топологічний підхід) та за функціональним призначенням [11, 23].

За рівнем застосування ТЗЗІ поділяються на:

- *Засоби захисту периметра мережі:* розташовуються на межі між внутрішньою (довіреною) мережею підприємства та зовнішніми мережами (Інтернетом). До них належать міжмережеві екрани (Firewalls), шлюзи віртуальних приватних мереж (VPN), системи захисту від DDoS-атак [12].
- *Мережеві засоби внутрішнього контуру:* системи виявлення та запобігання вторгненням (IDS/IPS), системи моніторингу мережевого трафіку (Network Traffic Analysis - NTA), маршрутизатори з функціями фільтрації [21].
- *Засоби захисту кінцевих точок (Endpoint Security):* програмні та апаратні комплекси, що встановлюються безпосередньо на робочі станції та

сервери. Це класичні антивіруси, системи EDR (Endpoint Detection and Response) та засоби контролю змінних носіїв [11].

- *Засоби захисту даних (Data Security):* системи запобігання витокам інформації (DLP - Data Loss Prevention), засоби криптографічного перетворення та управління ключами шифрування [15].

Для більш глибокого розуміння специфіки функціонування сучасних ТЗЗІ та виявлення їхніх слабких місць, які потребують постійного контролю, у таблиці 1.1 наведено порівняльну характеристику основних класів засобів захисту.

Таблиця 1.1

Порівняльна характеристика класів технічних засобів захисту інформації

Клас ТЗЗІ	**Основні представники**	**Базові безпекові функції**	**Обмеження та недоліки при ізольованому використанні**
Периметральні	NGFW (міжмережеві екрани нового покоління), VPN-концентратори	Блокування несанкціонованого доступу ззовні, інспекція пакетів, приховування топології	Не здатні виявити атаки, ініційовані зсередини мережі (інсайдери) або шкідливе ПЗ на USB-носіях
Системи виявлення	IDS/IPS, NTA (Network Traffic Analysis)	Сигнатурний та евристичний аналіз трафіку, виявлення мережевих аномалій	Високий рівень хибних спрацювань (FPR), значне навантаження на пропускну здатність мережі
Кінцеві точки	EDR, Антивірусні сканери, Host-based IPS	Захист на рівні операційної системи хоста, блокування запуску шкідливих процесів	Залежність від своєчасного оновлення баз сигнатур, можливість відключення локальним адміністратором
Захист даних	DLP (Data Loss Prevention)	Контроль переміщення конфіденційних файлів, аналіз вмісту пошти	Складність початкового налаштування політик, ризик блокування легітимних бізнес-процесів

Процес впровадження ТЗЗІ є складним організаційно-технічним проектом, який не обмежується лише закупівлею обладнання та інсталяцією програмного забезпечення. Згідно з методологією системної інженерії захисту (NIST SP 800-

160) [38], впровадження має базуватися на попередньому аналізі ризиків [31] та моделюванні загроз.

На практиці процес розгортання стикається з низкою проблем. По-перше, це конфлікт між безпекою та продуктивністю: ввімкнення максимального рівня евристичного аналізу на ТЗЗІ часто призводить до деградації пропускної здатності мережі та затримок у роботі бізнес-додатків [19]. По-друге, гетерогенність інфраструктури: використання засобів від різних виробників (мультивендорний підхід) ускладнює централізоване управління та вимагає впровадження систем класу SIEM (Security Information and Event Management) для агрегації логів [25].

Проте найсуттєвішим недоліком, який спостерігається на підприємствах, є підхід «встановив і забув». Багато організацій витрачають ресурси на впровадження ТЗЗІ, але не впроваджують механізми безперервного контролю їхньої ефективності. Конфігурації засобів застарівають, правила фільтрації перестають відповідати новим векторам атак, що зрештою призводить до ілюзії безпеки [24].

1.2 Огляд міжнародних стандартів і методологій у сфері оцінювання ефективності захисту інформації

Для подолання проблеми неконтрольованої деградації систем захисту світова спільнота розробила низку стандартизованих підходів та методологій. Оцінювання ефективності ТЗЗІ є складовою частиною загального процесу управління інформаційною безпекою (СУІБ), вимоги до якої регламентовані міжнародним стандартом ISO/IEC 27001 [7].

Ключовим документом у сфері метрик та оцінювання є стандарт **ISO/IEC 27004:2016 «Information technology -Security techniques -Information security management -Monitoring, measurement, analysis and evaluation»** [30]. Цей стандарт встановлює керівні принципи щодо того, як організації повинні розробляти та використовувати метрики для оцінки результативності їхньої

системи безпеки. Згідно з ISO/IEC 27004, програма вимірювання має містити чітко визначені цілі, об'єкти вимірювання, методи збору даних та критерії успіху [30]. Стандарт наголошує на тому, що показники (метрики) повинні бути достовірними, відтворюваними та корисними для прийняття рішень керівництвом.

Іншою фундаментальною методологією є документи Національного інституту стандартів і технологій США, зокрема двотомне видання **NIST SP 800-55 «Measurement Guide for Information Security»** [34, 35]. На відміну від більш загального стандарту ISO, NIST пропонує глибокий інженерний підхід. У першому томі (Methodology) [34] описано процес створення ризико-орієнтованої програми вимірювання безпеки (Security Measurement Program). У другому томі (Performance Metrics) [35] розглядаються типи метрик: метрики реалізації (Implementation Metrics), метрики результативності (Effectiveness Metrics) та метрики впливу (Impact Metrics). Методологія NIST рекомендує використовувати підхід Goal-Question-Metric (GQM), де кожна технічна метрика повинна прямо відповідати на певне бізнес-питання [34].

Також значної популярності набув практичний фреймворк **CIS Controls** (Center for Internet Security) [27]. Остання версія CIS Controls v8.1 містить набір із 18 критичних контролів безпеки (Safeguards). Для кожного контролю (включаючи захист мережі, захист від шкідливого ПЗ тощо) CIS пропонує конкретні метрики реалізації (Implementation Group Metrics), які дозволяють швидко кількісно оцінити відсоток захищених активів в інфраструктурі [27].

1.3 Нормативно-правова база України у сфері технічного захисту інформації

В Україні сфера технічного захисту інформації регулюється на рівні законів, постанов Кабінету Міністрів та національних стандартів (ДСТУ, НД ТЗІ). Базовим нормативно-правовим актом є Закон України «Про захист інформації в інформаційно-комунікаційних системах» [2], який визначає

суб'єкти відносин, вимоги щодо захисту інформації, яка є власністю держави, та конфіденційної інформації підприємств.

Концептуальні засади оцінювання захищеності закладені в документах системи технічного захисту інформації (ТЗІ). Зокрема, нормативний документ НД ТЗІ 1.1-003-99 [9] встановлює базову термінологію, а НД ТЗІ 2.5-004-99 «Критерії оцінювання захищеності інформації в комп'ютерних системах від несанкціонованого доступу» [10] класифікує системи за рівнями довіри. Організаційні аспекти проведення робіт із захисту регламентуються ДСТУ 3396.1-96 [5].

Попри наявність розгалуженої законодавчої бази, вітчизняні нормативні документи у сфері ТЗІ мають суттєвий недолік: вони переважно орієнтовані на процеси формальної побудови та атестації комплексних систем захисту інформації (КСЗІ) [15]. Атестат відповідності КСЗІ видається на певний строк (зазвичай 3-5 років) і підтверджує, що на момент експертизи система відповідала вимогам НД ТЗІ. Проте вітчизняні стандарти наразі не містять жорстких вимог та чітких математичних методологій щодо безперервного моніторингу метрик результативності окремих ТЗЗІ у процесі їхньої щоденної експлуатації [14]. Це призводить до необхідності адаптації міжнародних стандартів (таких як ISO 27004 та NIST) для потреб українських підприємств.

1.4. Аналіз існуючих систем, підходів та методів оцінювання ефективності ТЗЗІ

Формування ефективної політики інформаційної безпеки неможливе без розуміння того, наскільки впроваджені інженерно-технічні рішення здатні протистояти реальним загрозам. Існуючі в науковій літературі та практиці методи оцінювання ефективності впроваджених технічних засобів можна згрупувати у три фундаментальні підходи.

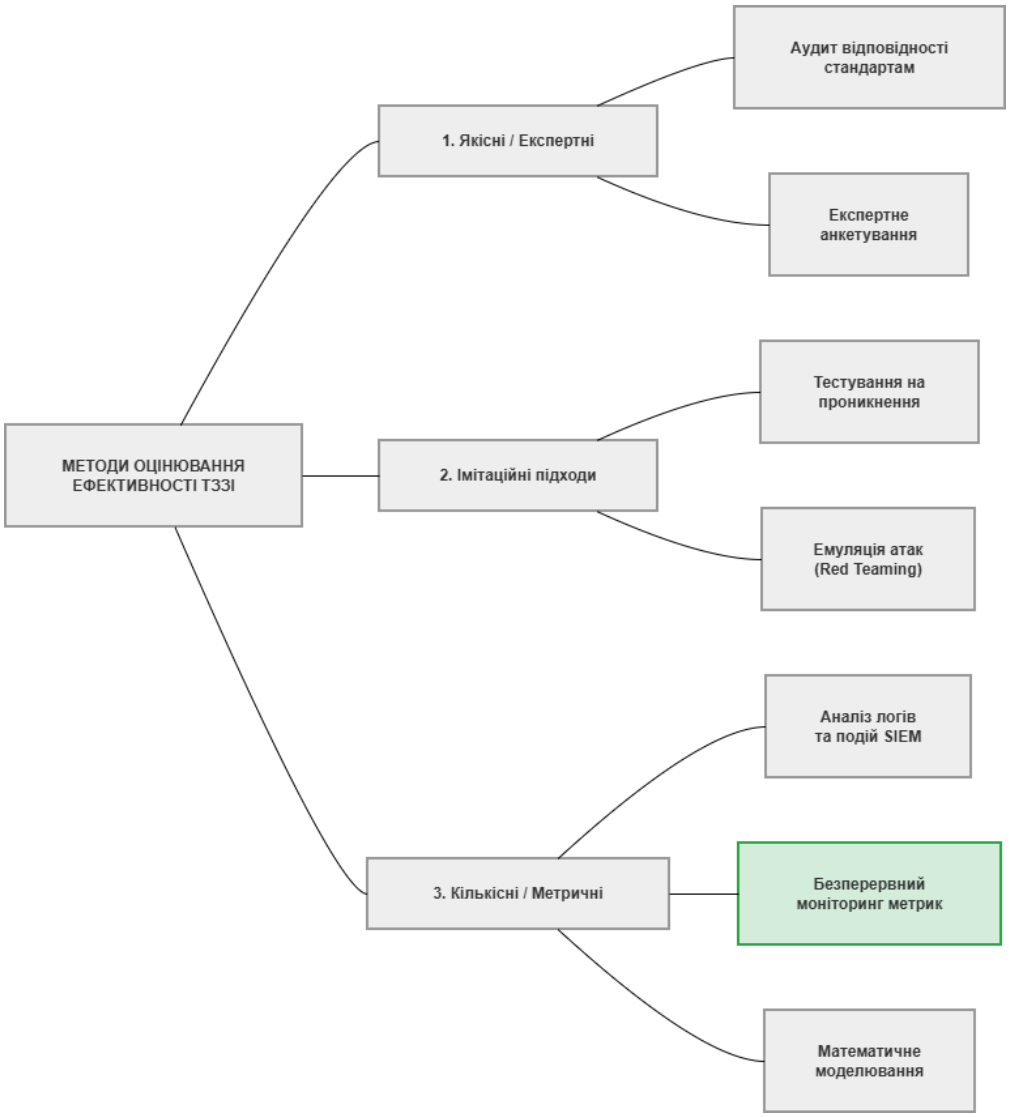

Рисунок 1.1 Методи оцінювання ефективності ТЗЗІ

Для систематизації наявного методологічного апарату на рисунку 1.1 наведено узагальнену класифікаційну схему методів оцінювання ефективності ТЗЗІ. Розглянемо детально переваги та недоліки кожного з виділених підходів:

1. Якісні (експертні) підходи**.** Базуються на проведенні періодичних аудитів, анкетуванні та експертних висновках фахівців з кібербезпеки. Зазвичай вони реалізуються за допомогою методів опитувальних листів або оцінки зрілості процесів безпеки.

- *Переваги:* Враховують специфічний контекст бізнесу, дозволяють оцінити організаційні аспекти, які складно формалізувати алгоритмічно.

- *Недоліки:* Високий рівень суб'єктивності, значна залежність від кваліфікації експерта-аудитора, відсутність можливості автоматизації та неможливість отримання оцінок у режимі реального часу [14].

2. Імітаційні підходи (Penetration Testing / Red Teaming**).** Ефективність ТЗЗІ перевіряється шляхом симуляції (емуляції) реальних кібератак. Використовуються спеціалізовані інструменти (сканери вразливостей, експлойти) для перевірки здатності засобів захисту виявляти та блокувати деструктивні впливи на практиці.

- *Переваги:* Максимальна реалістичність оцінки, перевірка системи захисту в умовах, наближених до "бойових".
- *Недоліки:* Висока вартість та тривалість проведення, неможливість безперервного використання без ризику порушити стабільність роботи ІКС. Окрім того, оцінка фіксується лише на конкретний момент проведення тестування [13].

3. Кількісні (метричні) підходи**.** Ґрунтуються на автоматизованому зборі телеметрії безпосередньо з самих ТЗЗІ та розрахунку об'єктивних показників (технічних та операційних метрик) за чіткими математичними формулами [13, 19]. (На рисунку 1.1 цей напрямок виділено як найбільш пріоритетний).

- *Переваги:* Об'єктивність, математична точність, здатність до повної автоматизації (через системи SIEM), можливість формування механізму безперервного контролю (Continuous Monitoring) [25, 29].
- *Недоліки:* Складність первинного налаштування (парсингу та нормалізації логів), а також проблема "інформаційного перевантаження" операторів через надмірну кількість зібраних одиничних показників [28].

Саме кількісний метричний підхід є найбільш перспективним для розв'язання проблеми об'єктивного моніторингу в гетерогенних мережах. Однак, як показує аналіз робіт вітчизняних та зарубіжних науковців (Ю. В. Гребенніков [14], С. О. Гнатюк [13], Д. Хаббард [29]), розрізнені одиничні метрики самі по собі не дають загальної картини захищеності. Існує нагальна науково-практична потреба у розробленні комплексної структурної моделі, яка б не лише

формалізувала ці метрики, але й забезпечила їхню алгоритмічну згортку (наприклад, за допомогою методу аналізу ієрархій [20] або адитивної згортки [18]) у єдиний інтегральний показник. Саме розв'язанню цієї задачі і присвячені наступні розділи даної кваліфікаційної роботи.

Висновки до розділу 1

1. Проаналізовано класифікацію технічних засобів захисту інформації (ТЗЗІ) за рівнем застосування та функціональним призначенням. Виявлено, що основними проблемами впровадження сучасних ТЗЗІ на підприємствах є складність інтеграції мультивендорних рішень та відсутність системного контролю за їхньою реальною результативністю після етапу первинного розгортання, що призводить до непомітної деградації рівня кібербезпеки.

2. Досліджено міжнародні стандарти та методології у сфері оцінювання ефективності захисту інформації. Встановлено, що міжнародні рамкові документи, зокрема ISO/IEC 27004:2016 та серія NIST SP 800-55, наполегливо рекомендують відмовитись від суб'єктивних підходів на користь кількісних метрик результативності (Effectiveness Metrics), які мають бути автоматизованими та математично обґрунтованими.

3. Розглянуто нормативно-правову базу України у сфері технічного захисту інформації. Встановлено, що чинні національні стандарти та нормативні документи (НД ТЗІ) здебільшого регламентують формальні процедури побудови та атестації комплексних систем захисту (КСЗІ), проте не містять практичних механізмів безперервного кількісного моніторингу показників ефективності ТЗЗІ у процесі їхньої щоденної експлуатації.

4. Вивчено існуючі підходи до оцінювання ефективності систем захисту інформації. З'ясовано, що експертні та імітаційні методи не здатні забезпечити безперервність контролю. Доведено, що найбільш ефективним є кількісний метричний підхід, однак він потребує вдосконалення в частині розробки структурних моделей агрегації даних та математичних методів згортки

одиничних показників у єдиний інтегральний індекс для підтримки прийняття управлінських рішень.

Розділ 2 РОЗРОБЛЕННЯ СИСТЕМИ ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ВПРОВАДЖЕНИХ ТЕХНІЧНИХ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ МЕТРИК РЕЗУЛЬТАТИВНОСТІ

2.1.Структурна модель системи оцінювання ефективності технічних засобів захисту інформації

Обґрунтування та проектування ефективної системи оцінювання технічних засобів захисту інформації (ТЗЗІ) вимагає застосування методів системного аналізу [26] для декомпозиції складного процесу моніторингу безпеки на окремі, функціонально завершені компоненти. Сучасні інформаційно-комунікаційні системи (ІКС) характеризуються високим ступенем гетерогенності та безперервною динамікою змін ландшафту кіберзагроз [12].

Для вирішення цієї проблеми розроблено модульну багаторівневу структурну модель системи оцінювання. Її архітектурна логіка базується на принципі розподілу обов'язків [38], що дозволяє ізолювати процеси низькорівневої взаємодії з ТЗЗІ від високорівневих аналітичних процедур. Модель складається з чотирьох послідовних функціональних рівнів.

1. Інфраструктурний рівень (рівень джерел первинних даних). Основним завданням рівня є безперервний збір сирої телеметрії. До складу джерел первинних даних входять:

- *Міжмережеві екрани (Firewalls):* інформація про заблоковані з'єднання та аномальну активність на межі мережевих периметрів [11, 40].
- *Системи виявлення та запобігання вторгненням (IDS/IPS):* дані про зафіксовані сигнатури відомих атак [12, 21].
- *Засоби захисту кінцевих точок (EDR):* події про виявлення шкідливого програмного забезпечення [32].
- *Засоби автентифікації:* логічні події безпеки, спроби входу в систему [42]. Збір здійснюється безагентними методами через стандартні протоколи журналювання (Syslog, SNMP Traps) [28, 36].

2. Рівень нормалізації та агрегації даних. Оскільки кожне ТЗЗІ формує записи у власному форматі, цей рівень виступає в ролі технологічного мосту.

- *Парсинг:* виділення з сирого тексту ключових атрибутів події.
- *Нормалізація:* приведення атрибутів до єдиної загальносистемної схеми (як базовий стандарт використовується формат CEF або LEEF) [25].
- *Фільтрація:* видалення дубльованих записів для запобігання ситуаціям «втоми від сповіщень» [28].

Перший (вхідний) контур системи оцінювання відображає процеси акумуляції первинної телеметрії

3. Аналітичний рівень (ядро системи). Тут нормалізований потік подій безпеки перетворюється на кількісні метрики результативності. Рівень взаємодіє з базою даних, де зберігаються історичні значення та профілі базових ліній (Baselines) [30]. Функціонування реалізується через блок розрахунку одиничних метрик та блок інтегрального оцінювання.

Функціонування аналітичного ядра реалізується через роботу двох основних модулів:

- *Блок розрахунку одиничних (сингулярних) метрик:* на основі заздалегідь визначених часових інтервалів (година, доба, тиждень) здійснює підрахунок технічних, експлуатаційних та організаційних параметрів (наприклад, співвідношення успішно заблокованих атак до загальної кількості спроб).
- *Блок інтегрального оцінювання:* застосовує розроблені математичні алгоритми для зваженого зведення множини одиничних метрик у єдиний узагальнений показник (індекс) ефективності системи технічного захисту в цілому або її окремих сегментів.

Аналітичний рівень також відповідає за довгострокове збереження результатів обчислень, що дозволяє виконувати трендовий аналіз -відстежувати, як змінюється ефективність ТЗЗІ з часом (наприклад, після встановлення нових оновлень, зміни конфігурації чи модифікації правил фільтрації).

4. Рівень візуалізації та прийняття рішень (інтерфейсний рівень). Кінцевою метою функціонування системи є надання персоналу з кібербезпеки та керівництву ІТ-підрозділів наочної, об'єктивної та оперативної інформації про поточний стан захищеності [30]. Рівень візуалізації здійснює зворотну трансформацію складних числових масивів та інтегральних індексів у зрозумілі графічні форми.

Основні компоненти інтерфейсного рівня включають:

- *Інтерактивні дашборди (Dashboards):* відображають у режимі реального часу віджети з поточними значеннями ключових метрик, графіки динаміки інтегрального показника, кругові діаграми розподілу інцидентів за категоріями та критичністю [25, 29].
- *Модуль генерації звітів:* автоматично або за запитом формує регламентні текстові та табличні звіти (документи) для керівництва, які містять оцінку діяльності підрозділу безпеки та обґрунтування необхідності модернізації конкретних ТЗЗІ [34].
- *Система аварійних сповіщень (Alerting):* у разі, якщо інтегральний показник ефективності або окремі критичні технічні метрики падають нижче встановленого порогового значення (критична межа безпеки), цей модуль миттєво генерує тривожні сповіщення на консоль адміністратора, на електронну пошту або через месенджери [28].

Логіку руху інформаційних потоків, взаємозв'язки між виділеними архітектурними рівнями та послідовність трансформації даних від моменту виникнення кібератаки на технічному засобі до ухвалення управлінського рішення відображено на структурно-функціональній схемі системи оцінювання

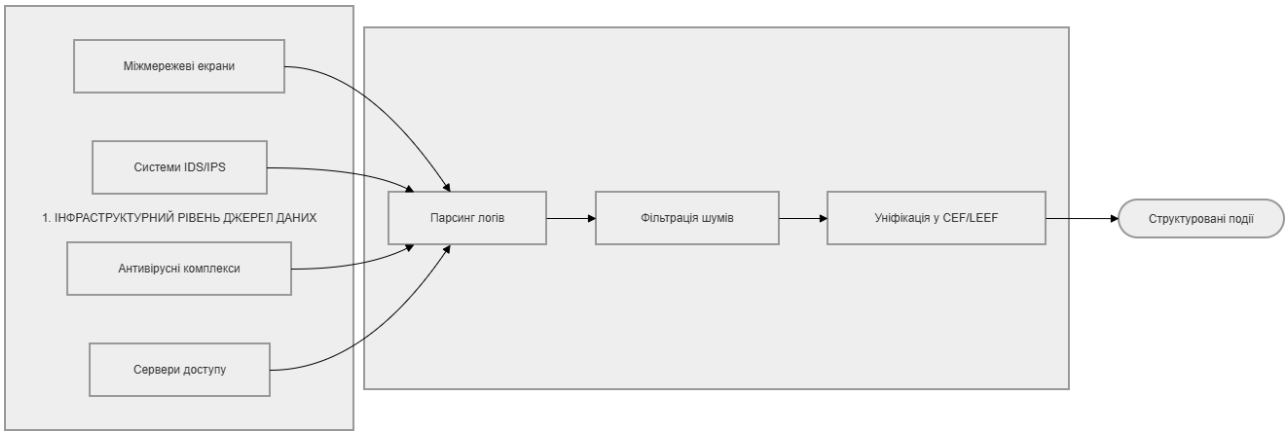

Рис. 2.1. Структурно-функціональна схема системи оцінювання

Для забезпечення надійної взаємодії між рівнями моделі використовуються захищені криптографічні протоколи передачі даних (наприклад, TLS для Syslog, HTTPS для API-взаємодії аналітичного ядра з інтерфейсним рівнем) [26, 39]. Важливою особливістю розробленої моделі є її повна незалежність від конкретного типу операційної системи чи апаратного забезпечення, на якому розгорнуто ТЗЗІ. Уніфікація інформаційного обміну на другому рівні дозволяє додавати нові класи засобів захисту (наприклад, хмарові захисні екрани або системи захисту контейнеризації) шляхом простого підключення відповідного програмного плагіна-парсера, без необхідності зупинки системи оцінювання чи переписування математичного ядра [38].

Таким чином, запропонована структурна модель дозволяє реалізувати замкнений, безперервний цикл контролю ефективності технічного захисту (Continuous Monitoring) [33]. Це мінімізує вплив "людського фактора" на етапі збору та первинного аналізу даних, забезпечуючи високу об'єктивність і швидкість отримання оцінок, що є критично важливим для оперативного виявлення слабких місць у конфігураціях засобів захисту інформації [17]

2.2.Формування та класифікація метрик результативності технічних засобів захисту інформації

Перехід до об’єктивного оцінювання стану технічного захисту інформації вимагає відмови від суб’єктивних експертних суджень на користь чітко визначених, відтворюваних та кількісно вимірюваних параметрів. У контексті міжнародних стандартів ISO/IEC 27004 [30] та серії рекомендацій NIST SP 800-55 [34, 35], такі параметри визначаються як метрики результативності. Головна мета формування системи метрик полягає в отриманні точних і операційних даних про те, наскільки ефективно впроваджені ТЗЗІ виконують свої цільові безпекові функції в умовах реальних інформаційних впливів [13, 29].

Для того щоб метрика могла бути використана в аналітичному ядрі розроблюваної системи, вона повинна відповідати низці фундаментальних критеріїв [34]:

- *Кількісна вираженість:* показник має набувати числового значення (у відсотках, часових одиницях, абсолютних величинах) без двозначних трактувань.
- *Доступність для збору:* вихідні дані для розрахунку метрики мають автоматично вилучатися з лог-файлів або конфігурацій ТЗЗІ без створення додаткового критичного навантаження на систему [28, 36].
- *Часова залежність:* метрика повинна мати здатність змінюватися в часі, відображаючи реальну динаміку деградації або покращення стану захищеності [30].
- *Специфічність:* показник має чітко характеризувати конкретний аспект роботи засобу захисту (наприклад, точність фільтрації трафіку або швидкість реагування на інцидент) [13].

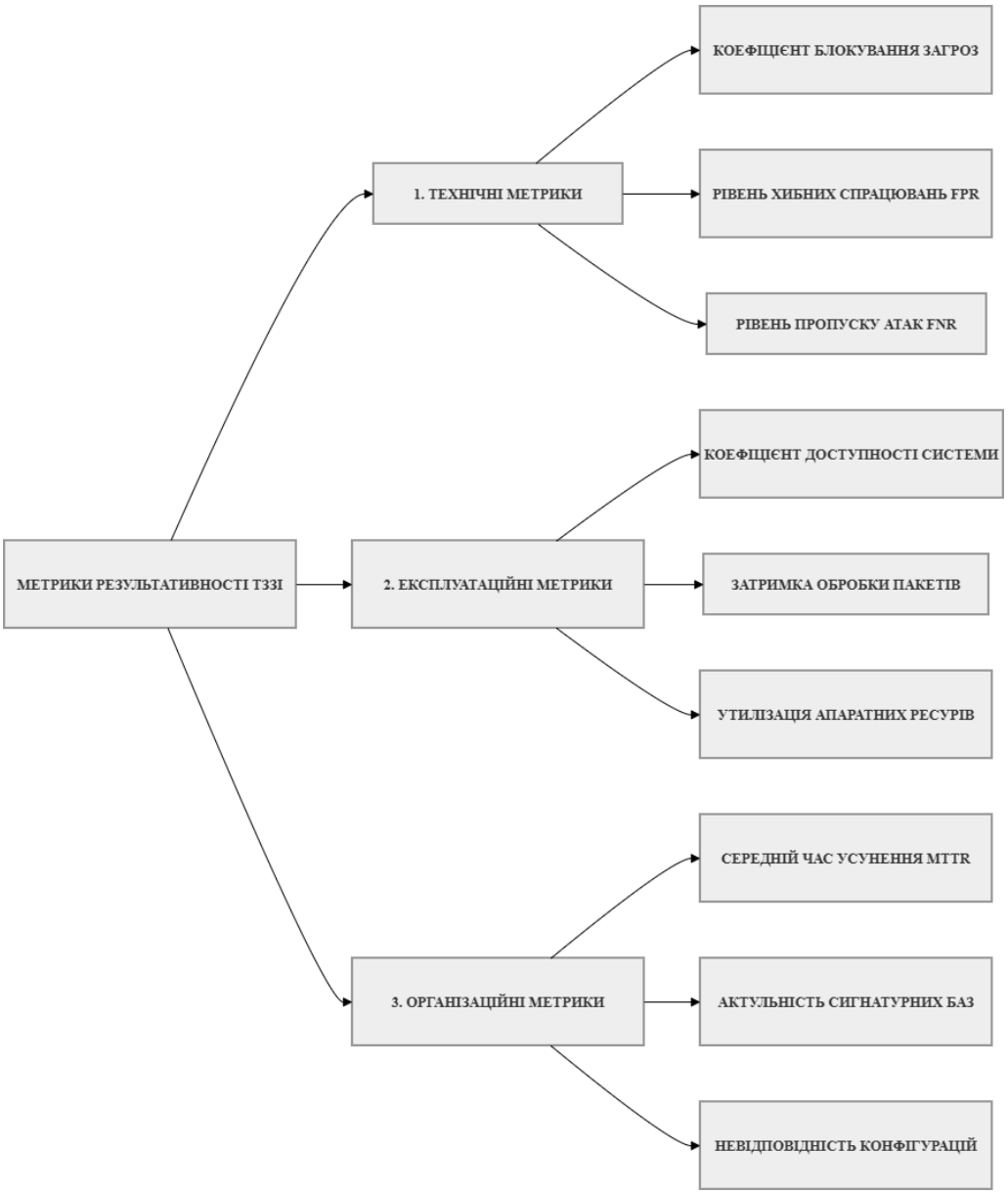

Рис 2.2. Метрики результативності ТЗЗІ

З огляду на гетерогенність сучасних ІКС та різноманітність функцій, які виконують засоби захисту, у роботі сформовано та обґрунтовано трирівневу класифікацію метрик [14, 16]. Вона охоплює не лише чисті технічні параметри стійкості засобів, а й чинники їхньої експлуатаційної стабільності та якості адміністрування.

Розглянемо детально кожну з виділених категорій метрик та формалізуємо їхній математичний базис.

1. Технічні метрики (метрики захищеності)

Ця група показників безпосередньо характеризує здатність ТЗЗІ протидіяти кібератакам, виявляти аномалії та забезпечувати три основні складові інформаційної безпеки: конфіденційність, цілісність та доступність на технічному рівні. [32, 42].

Основним показником тут виступає *коефіцієнт блокування загроз* (K_{block}), який відображає загальну оборонну здатність засобу (наприклад, міжмережевого екрана чи системи IPS) щодо нейтралізації шкідливого трафіку [11, 21]. Розрахунок здійснюється за формулою (2.1):

$$K_{block} = \frac{N_{blocked}}{N_{total}} * 100\%$$

де $N_{blocked}$ -кількість успішно заблокованих або локалізованих ТЗЗІ атак за визначений звітний інтервал часу; N_{total} -загальна кількість зафіксованих системою спроб несанкціонованого доступу або шкідливих впливів.[34]

Проте високий показник блокування не завжди свідчить про ідеальну роботу системи, оскільки засіб захисту може блокувати й легітимних користувачів. Для фіксації таких помилок вводиться рівень хибних спрацювань (FPR -False Positive Rate), математична модель якого має вигляд (2.2):

$$FPR = \frac{FP}{FR + TN} * 100\%$$

де FP -кількість випадків, коли легітимна дія користувача або безпечний мережевий пакет були помилково ідентифіковані засобом захисту як загроза; TN -кількість коректно пропущених системою безпечних (легітимних) мережевих з'єднань.[35]

Зворотною стороною помилок другого роду є *рівень пропуску атак* (FNR - False Negative Rate), який демонструє відсоток небезпечних впливів, що не були розпізнані сигнатурними чи евристичними модулями ТЗЗІ. Формула для обчислення має вигляд (2.3):

$$FNR = \frac{FN}{TP + FN} * 100\%$$

де FN -кількість пропущених засобів захисту шкідливих подій; TP -кількість правильно виявлених та класифікованих реальних атак.[13]

2. Експлуатаційні (операційні) метрики

Технічні засоби захисту функціонують у реальному середовищі й споживають обмежені ресурси ІКС[15, 40]. Якщо впроваджений засіб спричиняє критичні затримки в бізнес-процесах або постійно відмовляє через апаратні збої, його загальна доцільність нівелюється.

Ключовим операційним параметром є *коефіцієнт доступності ТЗЗІ* K_{avail}, який визначає надійність функціонування самого програмно-апаратного комплексу захисту за формулою (2.4)[34,35]:

$$K_{avail} = \frac{T_{work}}{T_{work} + T_{down}}$$

де T_{work} -сумарний час коректної роботи засобу захисту в штатному режимі протягом періоду спостереження; T_{down}-час перебування засобу у стані відмови (через апаратні збої, перезавантаження, помилки конфігурації чи успішні DoS-атаки на сам засіб захисту)[11,42].

Для оцінки впливу на продуктивність мережевої інфраструктури використовується метрика затримки обробки пакетів (ΔT_{delay}), яка фіксує додатковий час, що витрачається модулями ТЗЗІ (наприклад, механізмами глибокого аналізу пакетів DPI) на інспекцію трафіку[19]:

$$\Delta T_{delay} = T_{out} - T_{in}$$

де T_{out} -мітка часу виходу пакета з інтерфейсу ТЗЗІ[36]; T_{in} -мітка часу надходження пакета на вхідний інтерфейс ТЗЗІ.

3. Організаційні метрики

Ця категорія оцінює процеси безпосереднього керування та супроводу впроваджених засобів захисту. Навіть найсучасніше ТЗЗІ втрачає ефективність, якщо його сигнатурні бази не оновлюються, а персонал ігнорує сповіщення безпеки.[12,17]

Основним показником ефективності роботи адміністраторів є *середній час усунення наслідків інцидентів* MTTR -Mean Time To Repair / Respond), який визначається за формулою (2.6)[34,35]:

$$MTTR = \frac{\sum_{i=1}^{M} T_{resolve}^{i} - T_{detect}^{i}}{M}$$

де $T_{resolve}^{i}$ -час повної локалізації та ліквідації наслідків і-го інциденту; T_{detect}^{i} - час первинної реєстрації цього інциденту системою моніторингу; M -загальна кількість критичних інцидентів безпеки за звітний період.[41]

Також важливим є *індекс актуальності сигнатурних баз* I_{upd}, який розраховується як відставання поточного стану бази засобу від релізу виробника[27,33]:

$$I_{upd} = T_{current} - T_{last}$$

де $T_{current}$ -поточний час аналізу; T_{last} -час останнього успішного завантаження та застосування офіційного пакета сигнатур або правил фільтрації[24].

Для систематизації сформованої аналітичної моделі та забезпечення можливості її подальшої програмної реалізації на аналітичному рівні системи, у таблиці 2.2 наведено узагальнену специфікацію всіх базових метрик результативності ТЗЗІ.

Таблиця 2.2

Узагальнена специфікація всіх базових метрик результативності ТЗЗІ

Категорія	**Найменування показника результативності**	**Математичний символ**	**Цільовий орієнтир (екстремум)**	**Одиниці виміру**
Технічні	Коефіцієнт блокування кібератак	K_{block}	прагне до 100%	відсотки (%)
	Рівень хибних спрацювань системи	FPR	прагне дао 0%	відсотки (%)
	Рівень пропуску шкідливих впливів	FNR	прагне до 0%	відсотки (%)
Експлуатаційні	Коефіцієнт доступності (відмовостійкості)	K_{avail}	прагне до 1.0 (0.999)	безрозмірна величина
	Додаткова затримка мережевого трафіку	ΔT_{delay}	прагне до мінімуму	мілісекунди (мс)
	Коефіцієнт утилізації процесорної потужності	U_{cpu}	не повинен перевищувати 75%	відсотки (%)
Організаційні	Середній час усунення та локалізації атак	MTTR	прагне до мінімуму	хвилини / години
	Час затримки встановлення сигнатур/патчів	I_{upd}	прагне до 0	години / доби
	Відсоток ТЗЗІ з відхиленнями від базової конфігурації	P_{drift}	прагне до 0%	відсотки (%)

Запропонована система метрик є збалансованою, оскільки вона враховує взаємозв'язки між різними апаратно-програмними рівнями захисту[14,16]. Наприклад, спроба максимізувати технічний коефіцієнт K_{block}шляхом увімкнення всіх наявних евристичних правил у системі IDS/IPS неминуче призведе до негативного зростання експлуатаційного показника U_{cpu} та

збільшення затримки ΔT_{delay}[19]. Саме тому наявність такої класифікації дозволяє аналітичному ядру системи бачити реальну ціну забезпечення безпеки та знаходити оптимальний баланс конфігурацій, запобігаючи деградації продуктивності захищуваної інформаційно-комунікаційної інфраструктури[23,29].

2.3.Метод формування інтегрального показника ефективності на основі метрик результативності

Наявність розгалуженої системи одиничних метрик, сформованої у попередньому підрозділі, дозволяє детально оцінити окремі технічні, експлуатаційні та організаційні аспекти функціонування ТЗЗІ. Проте велика кількість різнорідних параметрів суттєво ускладнює процес прийняття оперативних управлінських рішень. Адміністратор безпеки або керівник підрозділу кібербезпеки стикається із ситуацією, коли одна частина метрик (наприклад, коефіцієнт блокування атак) свідчить про високу ефективність, а інша частина (наприклад, додаткова затримка трафіку або час реагування) вказує на критичне погіршення умов функціонування мережі.[16,29]

Для розв'язання цієї задачі та забезпечення можливості швидкої і об'єктивної оцінки загального стану захищеності інформаційної інфраструктури у роботі розроблено метод математичного синтезу одиничних показників у єдиний узагальнений показник -інтегральний індекс ефективності I_{eff} [16]. Цей метод дозволяє звести векторний простір різнорозмірних оцінок до скалярного значення. Процедура формування інтегрального показника є послідовним процесом і складається з кількох взаємопов'язаних етапів, структуру яких відображено на рисунку 2.4.

Рис. 2.3. Процедура формування інтегрального показника

Розглянемо детально зміст та математичний апарат кожного етапу розробленого методу.

1. Етап нормалізації одиничних метри. Головною математичною перешкодою під час об'єднання метрик є їхня різна розмірність (відсотки, часові одиниці, абсолютна кількість подій) та різна спрямованість впливу на цільову функцію безпеки. За характером впливу всі метрики результативності ТЗЗІ поділяються на дві категорії:

- *Метрики-стимулятори (позитивно спрямовані):* зростання їхнього значення свідчить про покращення стану безпеки (наприклад K_{block} або K_{avail}
- *Метрики-дестимулятори (негативно спрямовані):* зростання їхнього значення вказує на деградацію системи або зниження рівня захищеності (наприклад, FPR, FRN ,ΔT_{delay} або MTTR).

Для приведення всіх параметрів до єдиної безрозмірної шкали в межах інтервалу [0; 1], де значення 1 відповідає ідеальному (із технічної точки зору) стану засобу захисту, а 0 -критично незадовільному, застосовується процедура нормування.

Для метрик-стимуляторів нормалізація здійснюється за формулою (2.8):

$$M_i^{norm} = 1, \text{якщо поточне значення } M_i \geq M_i^{target}$$

$$M_i^{norm} = \frac{M_i - M_i^{crit}}{M_i^{target} - M_i^{crit}}, \text{якщо значення в межах } M_i^{crit} < M^i < M_i^{target}$$

$$M_i^{norm} = 0, \text{якщо поточне значення } M_i \leq M_i^{crit}$$

Де M_i-реальне обчислене значення і-ї метрики**;** M_i^{target}- цільове (еталонне) значення метрики, встановлене політикою безпеки підприємства; M_i^{crit} =0, якщо поточне значення $M_i \geq M_i^{crit}$

Для метрик-дестимуляторів (де менше значення є кращим) формула нормалізації набуває вигляду (2.9):

$$M_i^{norm} = 1, \text{якщо поточне значення } M_i \leq M_i^{target}$$

$$M_i^{norm} = \frac{M_i^{crit} - M_i}{M_i^{crit} - M_i^{target}}, \text{якщо значення в межах } M_i^{target} < M^i < M_i^{crit}$$

$$M_i^{norm} = 0, \text{якщо поточне значення } M_i \geq M_i^{crit}$$

Використання порогових значень M^{target} та M^{crit} дозволяє адаптувати математичну модель до специфіки конкретної організації[30,34]. Наприклад, для фінансової установи допустима затримка трафіку ΔT_{delay} на міжмережевому екрані може бути дуже жорсткою, тоді як для навчального закладу ці межі можуть бути значно ширшими.[31,42]

2. Етап визначення вагових коефіцієнтів. Очевидно, що одиничні метрики мають різний ступінь впливу на підсумкову ефективність захисту інформації. Так, наприклад, пропуск критичної атаки сигнатурним модулем FNR є значно серйознішим інцидентом, ніж незначне перевищення часу встановлення патчів безпеки I_{upd}[13,27].

Для врахування цієї нерівнозначності кожній метриці присвоюється ваговий коефіцієнт W_i. У розробленій методології для визначення ваг пропонується застосовувати метод попарного порівняння критеріїв Томаса Сааті (метод аналізу ієрархій)[20]. Експертна група, що складається з провідних інженерів з кібербезпеки та системних адміністраторів, заповнює матрицю попарних порівнянь, де кожна метрика оцінюється відносно іншої за шкалою від 1 (рівна важливість) до 9 (абсолютна перевага)[16].

Головною математичною умовою, яка забезпечує коректність подальших розрахунків та нормування самого інтегрального показника, є умова нормалізації ваг (2.10):

$$\sum_{i=1}^{n} W_i = 1, \text{при цьому } W_i > 0$$

де n-загальна кількість одиничних метрик, що інтегруються в підсумкову оцінку.

3.Математична згортка показників Після отримання безрозмірних нормалізованих значень метрик та обчислення їхніх вагових коефіцієнтів здійснюється безпосередній синтез інтегрального індексу. У системному аналізі існують різні типи функцій згортки (мультиплікативна, мінімаксна, адитивна). У рамках даного дослідження обґрунтовано використання лінійної адитивної згортки.

Вибір адитивної моделі зумовлений її компенсаторною властивістю: вона дозволяє гнучко відстежувати загальні тенденції зміни стану ТЗЗІ, де незначне погіршення одного параметра може бути врівноважене високою стабільністю іншого, проте загальний індекс чітко зреагує на системні збої. Математичний

вираз для обчислення інтегрального показника ефективності впроваджених ТЗЗІ має вигляд (2.11)[34,35]:

$$I_{eff} = \sum_{i=1}^{n} (M_i^{norm} * W_i)$$

де I_{eff} - інтегральний показник ефективності, який змінюється в діапазоні [0;1]; M_i^{norm} - нормалізоване значення *i*-ї одиничної метрики, отримане за формулами (2.8) або (2.9); W_i - нормована вага і-ї метрики результативності.

4. Етап інтерпретації результатів оцінювання.Отримане в результаті розрахунку числове значення I_{eff} потребує правильного аналітичного трактування для формування подальших технічних рекомендацій. Для цього у роботі розроблено лінгвістичну шкалу оцінки ефективності, яка розподіляє отримані результати на чотири основні рівні (табл. 2.3).

Таблиця 2.3

Критерії інтерпретації інтегрального показника ефективності ТЗЗІ

Інтервал значень I_{eff}	**Рівень ефективності ТЗЗІ**	**Стан системи технічного захисту та необхідні дії**
0,85 – 1,00	Високий (Оптимальний)	ТЗЗІ функціонують у повному обсязі, конфігурації оптимізовані, алерти відсутні. Система захисту забезпечує надійне утримання ризиків безпеки в межах норми. Модернізація не потрібна.
0,65 – 0,84	Достатній (Номінальний)	Засоби захисту виконують свої функції, проте зафіксовані незначні відхилення в експлуатаційних параметрах або затримки в оновленнях. Рекомендується провести плановий аналіз правил фільтрації.
0,45 – 0,64	Задовільний (Граничний)	Ефективність захисту перебуває на межі допустимого. Спостерігається підвищений рівень хибних спрацювань або високий час реагування на інциденти. Необхідно провести переконфігурацію засобів.
0,00 – 0,44	Незадовільний (Критичний)	Критичний стан. ТЗЗІ не справляються з поточним рівнем навантаження або пропускають кібератаки (FNR перевищує норму). Існує висока ймовірність реалізації масштабного інциденту. Потрібне негайне втручання та заміна технічних рішень.

Завдяки впровадженню інтегрального оцінювання персонал підрозділу безпеки отримує можливість реалізувати концепцію управління за відхиленнями[14,30]. Замість щоденного моніторингу сотень сирих записів журналів реєстрації, адміністратор відстежує єдиний показник $\boldsymbol{I_{eff}}$.[16,29] Якщо його значення перебуває у зеленій зоні (високий рівень), система працює автономно. У разі переходу індексу до жовтої чи червоної зон, аналітичний модуль автоматично декомпонує інтегральний показник назад на одиничні метрики, вказуючи інженеру, який саме засіб захисту та за яким параметром (технічним чи операційним) спричинив падіння загальної ефективності[28,34].

2.4.Механізм функціонування системи має циклічний характер і передбачає шість основних етапів: підготовчий, збір даних, розрахунок метрик, нормалізацію та агрегацію, аналіз результатів та прийняття управлінських рішень[31,38].

Практичне впровадження розробленої структурної моделі та математичного апарату інтегрального оцінювання в реальну інфраструктуру підприємства вимагає формалізації чіткого операційного механізму[17,31]. Система не може функціонувати як статичний інструмент; її роботу слід організувати як безперервний циклічний процес, що інтегрується в загальний життєвий цикл управління інформаційною безпекою організації. Запропонований механізм функціонування базується на адаптованій концепції безперервного вдосконалення (цикл Демінга-Шухарта: PDCA -Plan-Do-Check-Act)[7] і розгортається у вигляді чотирьох послідовних і повторюваних фаз.

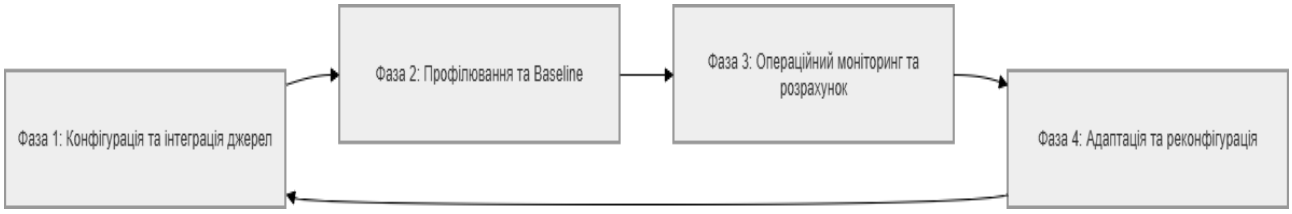

Рис 2.4 Циклічний життєвий цикл функціонування системи оцінювання

Розглянемо детальний зміст кожної фази операційного механізму та визначимо роль персоналу з кібербезпеки на кожному етапі.[38]

1. Фаза розгортання, конфігурації та інтеграції джерел

На початковому етапі здійснюється логічне та фізичне підключення розроблюваної системи до об'єктів моніторингу - впроваджених технічних засобів захисту.[38] Цей процес координується адміністратором комплексної системи захисту інформації (КСЗІ) і містить такі кроки:

- *Інвентаризація та критичність активів:* формування повного переліку ТЗЗІ, які підлягають оцінюванню (міжмережеві екрани, шлюзи VPN, антивірусні сервери тощо), із закріпленням за кожним засобом рівня критичності підсистеми, яку він захищає.[27,34]
- *Налаштування каналів транспортування телеметрії:* конфігурування резидентних агентів або служб відправки журналів подій на цільових ТЗЗІ. Основним протоколом передачі на цьому етапі є лінійний протокол Syslog (із обов'язковим шифруванням TLS для запобігання перехопленню логів зловмисниками всередині мережі).[39]
- *Активація плагінів-парсерів:* на другому рівні системи оцінювання включаються відповідні синтаксичні модулі, специфічні для конкретного виробника (наприклад, парсер для логів Cisco ASA, Fortinet або CheckPoint), які забезпечують коректне виділення атрибутів для подальшої нормалізації у формат CEF[25].

2. Фаза профілювання та формування базової лінії (Baseline)

Після успішного підключення всіх джерел система не може одразу видавати об'єктивний інтегральний показник ефективності, оскільки для математичних моделей (формули 2.8 та 2.9) необхідно встановити граничні значення параметрів M^{target} та M^{crit}. Для цього запускається фаза профілювання, яка триває протягом тестового періоду (як правило, від 7 до 14 календарних днів).[30]

Протягом цієї фази аналітичний модуль накопичує первинну статистику в умовах штатного функціонування ІКС підприємства. На основі зібраних масивів даних обчислюються середньостатистичні показники нормальної поведінки інфраструктури: фіксується стандартний рівень хибних спрацювань FPR,

визначається фоновий обсяг завантаження процесорних потужностей засобів захисту U_{cpu}та вимірюється еталонна технологічна затримка обробки пакетів ΔT_{delay}.[29] Отримані профілі затверджуються експертною групою як «базова лінія» (Baseline). Відносно цих значень у подальшому фіксуватимуться будь-які аномалії чи деградація ефективності.[34,35]

3. Фаза безперервного операційного моніторингу та обчислення

Ця фаза є основним експлуатаційним режимом системи, під час якого аналітичне ядро працює в автоматичному режимі.[33] Потік нормалізованих подій безпеки безперервно аналізується обчислювальними модулями третього рівня архітектури:

- Через фіксовані кванти часу (наприклад, кожні 60 хвилин) система автоматично перераховує значення всіх одиничних технічних, експлуатаційних та організаційних метрик результативності[28].
- На основі актуальних вагових коефіцієнтів W_i за формулою лінійної адитивної згортки (2.11) синтезується фінальний інтегральный індекс ефективності I_{eff}.
- Значення індексу транслюється на монітор адміністратора безпеки через динамічні графічні віджети.

Операційний порядок застосування системи на цій фазі передбачає автоматичне реагування на зміну кольорових зон шкали інтерпретації (згідно з таблицею 2.3):

- *Зелена зона* $I_{eff} \geq 0{,}85$система працює в автономному режимі, втручання персоналу не потрібне.[30]
- *Жовта зона* $0{,}65 \leq I_{eff} \leq 0{,}84$*:* система автоматично надсилає попереджувальне сповіщення (алерт) на консоль інженера. Адміністратор зобов'язаний виконати декомпозицію індексу, виявити метрику, що спричинила просідання (наприклад, затримку встановлення оновлень баз сигнатур I_{upd},та усунути невідповідність у плановому порядку.[24,28]

- *Червона зона* $I_{eff} < 0{,}65$ екстрений випадок. Система активує звукове та візуальне сповіщення. Персонал з кібербезпеки негайно розпочинає процедуру реагування на інцидент, оскільки такий рівень свідчить або про масовану атаку, яку ТЗЗІ не здатні заблокувати, або про повну критичну відмову одного з ключових ешелонів захисту периметра[17,41].

4. Фаза адаптації, зворотного зв'язку та реконфігурації

Ландшафт кіберзагроз безперервно еволюціонує: з'являються нові класи тактик і технік зловмисників, виявляються раніше невідомі вразливості нульового дня (Zero-Day), а саме підприємство може змінювати свою топологію мережі або впроваджувати нові хмарові сервіси[12,19]. З огляду на це, система оцінювання вимагає регулярного калібрування.

Не рідше одного разу на квартал експертна група (у складі CISO, провідних аналітиків SOC та системних архітекторів) проводить ревізію налаштувань аналітичного ядра[36]. Під час цієї фази реалізується:

- *Перегляд вагових коефіцієнтів* W_i*:* якщо організація змінила пріоритети (наприклад, перейшла на віддалену роботу співробітників), вага метрик захисту VPN-шлюзів та засобів автентифікації може бути штучно збільшена за рахунок зниження ваги метрик локального периметра[20].
- *Коригування порогових ліній:* здійснюється адаптація значень еталонних та критичних меж метрик для запобігання штучному завищенню або заниженню підсумкових оцінок ефективності.[31]

Розроблений механізм функціонування забезпечує високу динамічність системи. Вона перестає бути просто інструментом констатації фактів минулих інцидентів, а перетворюється на проактивну систему підтримки прийняття рішень, яка дозволяє оптимізувати конфігурації ТЗЗІ, раціонально розподіляти фінансові ресурси на модернізацію засобів захисту та мінімізувати вплив людського фактора на загальний стан кібербезпеки організації[7,14].

Висновки до розділу 2

1. Розроблено декомпозиційну чотирирівневу структурну модель системи оцінювання ефективності технічних засобів захисту інформації, яка базується на чіткому розділенні функціональних обов'язків між інфраструктурним рівнем, рівнем агрегації, аналітичним ядром та інтерфейсом візуалізації. Запропонований підхід забезпечує модульність і високу масштабованість системи, дозволяючи інтегрувати нові класи ТЗЗІ без зупинки моніторингу.

2. Сформовано та обґрунтовано збалансовану трирівневу класифікацію метрик результативності ТЗЗІ, яка включає технічні показники (якість фільтрації та блокування загроз), експлуатаційні параметри (надійність, утилізація апаратних ресурсів, вплив на продуктивність мережі) та організаційні метрики (швидкість реагування адміністраторів, актуальність оновлень). Математично формалізовано аналітичні вирази для розрахунку базових одиничних показників.

3. Обґрунтовано метод формування єдиного інтегрального показника ефективності на основі лінійної адитивної згортки нормованих значень одиничних метрик. Розроблено математичний апарат нормалізації для метрик-стимуляторів та метрик-дестимуляторів із використанням гнучких цільових та критичних порогових меж. Запропоновано шкалу інтерпретації фінального індексу для підтримки прийняття управлінських рішень та реалізації концепції управління за відхиленнями.

4. Визначено операційний механізм функціонування та порядок практичного застосування розробленої системи оцінювання. Механізм побудовано у вигляді безперервного чотирифазного життєвого циклу (інтеграція, профілювання базової лінії, операційний моніторинг, адаптація ваг), що гарантує динамічну стійкість моделі до еволюції кіберзагроз та змін у топології захищуваної інфраструктури.

Розділ 3 ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ РОЗРОБЛЕНОЇ СИСТЕМИ ОЦІНЮВАННЯ

3.1.Формування вихідних даних та визначення значень метрик результативності для експериментального дослідження

Для підтвердження працездатності, валідації та оцінки практичної ефективності розробленої структурної моделі та математичного методу інтегрального оцінювання у цьому розділі проведено експериментальне дослідження. Об'єктом дослідження виступає комплексна система захисту інформації (КСЗІ) умовного корпоративного підприємства, яка має типову розподілену мережеву інфраструктуру та містить базовий набір впроваджених технічних засобів захисту інформації (ТЗЗІ).

До складу розгляданого комплексу ТЗЗІ периметра та внутрішніх сегментів мережі входять:

1. *Міжмережевий екран наступного покоління (Next-Generation Firewall -NGFW)* -здійснює фільтрацію пакетів на мережевому та транспортному рівнях, контроль додатків та інспекцію шифрованого трафіку.
2. *Система виявлення та запобігання вторгненням (IDS/IPS)* -виконує сигнатурний та евристичний аналіз мережевих потоків з метою виявлення шкідливої активності, сканування портів та спроб експлуатації вразливостей серверного обладнання.
3. *Централізована антивірусна система захисту кінцевих точок (Endpoint Detection and Response -EDR)* -розгорнута на робочих станціях користувачів та корпоративних серверах для блокування шкідливого програмного забезпечення.

Для формування масиву вихідних даних аналітичним ядром системи оцінювання було проведено збір та нормалізацію журналів подій безпеки (логів) зазначених ТЗЗІ протягом експериментального вікна спостереження тривалістю T = 168 годин (один повний календарний тиждень). Протягом цього періоду

інфраструктурний рівень системи зафіксував та передав на рівень агрегації сумарний потік телеметрії обсягом 1245400 сирих подій, які після очищення від інформаційного шуму та нормалізації у формат CEF сформували масив цільових інцидентів безпеки та операційних логів.

На основі аналізу нормалізованих даних за звітний тиждень було вилучено такі кількісні показники для кожної групи метрик:

1. Вихідні дані для технічних метрик:

- Загальна кількість спроб шкідливих впливів та атак, спрямованих на периметр та хости мережі, склала N_{total}= 142 подій.
- З них модулями NGFW, IDS/IPS та EDR було успішно зафіксовано та заблоковано $N_{blocked}$ = 1365 атак. Соответственно, кількість пропущених шкідливих впливів, які згодом були виявлені під час ретроспективного аналізу або спричинили аномальну активність, склала FN = 55 подій. Кількість правильно ідентифікованих атак TP дорівнює 1365.
- Протягом тижня було зафіксовано FP = 42 випадки хибнопозитивних спрацювань, коли ТЗЗІ помилково заблокували легітимні запити користувачів або безпечні системні процеси. Загальна кількість коректно оброблених безпечних з'єднань склала TN = 98500 подій.

2. Вихідні дані для експлуатаційних метрик:

- Загальний час спостереження склав T_{total}= 168 годин. Протягом цього періоду внаслідок збою після невдалого автоматичного оновлення правил фільтрації центральний модуль IDS/IPS перебував у непрацездатному стані (відмові) протягом T_{down}= 1,5 години. Решту часу засіб працював штатно: T_{work}= 166,5 годин.
- На основі вимірювань затримки пакетів DPI-модулем міжмережевого екрана було встановлено, що середня затримка обробки корисного трафіку в моменти пікових навантажень склала ΔT_{delay} = 12 мілісекунд.

- Середній показник утилізації процесорної потужності апаратних платформ ТЗЗІ за тиждень зафіксовано на рівні U_{cpu} = 58%.

3. Вихідні дані для організаційних метрик:

- Протягом тижня в системі було зареєстровано M = 8 критичних інцидентів, які вимагали безпосереднього втручання адміністраторів безпеки для локалізації (ізоляція хостів від мережі, видалення шкідливого коду вручну). Сумарний час, витрачений на усунення цих інцидентів (від моменту реєстрації алерту до повної ліквідації наслідків), склав 168 хвилин (у середньому 21 хвилина на один інцидент).
- Час затримки встановлення планових сигнатурних баз антивірусного захисту на робочі станції від моменту їхнього офіційного релізу виробником склав I_{upd} = 6 годин.
- Перевірка конфігураційних файлів показала, що з 150 контрольованих вузлів мережі на 3 хостах було виявлено несанкційні відхилення від базових політик безпеки (відключений брандмауер Windows, застаріла версія агента), що дає значення відсотка дрейфу конфігурацій P_{drift}= 2%.

Для переведення отриманих сирих кількісних даних у безрозмірні нормовані оцінки M_i^{norm}експертною групою підприємства на основі чинної політики корпоративної безпеки та вимог регуляторів були встановлені цільові (еталонні) та критичні порогові межі для кожної метрики. Ці порогові константи, разом із визначеними експертним шляхом ваговими коефіцієнтами W_i, наведено в таблиці 3.1.

Таблиця 3.1

Порогові значення та вагові коефіцієнти метрик результативності ТЗЗІ

Математичний символ метрики	**Характер впливу на безпеку**	**Цільове значення (Mtarget)**	**Критичне значення (Mcrit)**	**Ваговий коефіцієнт (Wi)**
K_{block}	Стимулятор	98,00%	85,00%	0,25
FPR	Дестимулятор	0,05%	0,50%	0,1
FNR	Дестимулятор	1,00%	10,00%	0,2
K_{avail}	Стимулятор	0,999	0,95	0,15
ΔT_{delay}	Дестимулятор	5 мс	30 мс	0,05
U_{cpu}	Дестимулятор	50%	85%	0,05
MTTR	Дестимулятор	15 хв	60 хв	0,1
I_{upd}	Дестимулятор	4 год	24 год	0,05
P_{drift}	Дестимулятор	0,00%	5,00%	0,05

Встановлені вагові коефіцієнти відображають пріоритетність захисних властивостей системи над експлуатаційними. Найвищу вагу мають метрики K_{block}(0,25) та FNR (0,20), оскільки безпосередній пропуск атак або низька здатність до їхнього блокування створюють пряму загрозу конфіденційності та цілісності корпоративних даних. Експлуатаційні метрики, такі як утилізація процесора чи додаткова затримка пакетів, мають меншу вагу (0,05), оскільки вони характеризують комфорт функціонування інфраструктури, що за умов відсутності повного збою є вторинним фактором відносно захищеності. Сформований масив порогових меж та емпіричних даних є повністю достатнім базисом для виконання подальших аналітичних обчислень.

3.2.Реалізація процедури оцінювання та отримання інтегрального показника ефективності

Маючи сформований масив вихідних даних та визначені порогові значення, наступним кроком експериментального дослідження є безпосередня

реалізація математичної процедури оцінювання. Відповідно до розробленого в підрозділі 2.3 алгоритму, процес розпочинається з обчислення фактичних значень одиничних метрик та їхньої подальшої нормалізації (приведення до єдиної безрозмірної шкали від 0 до 1.

1. Обчислення та нормалізація технічних метрик

Першочергово розраховується фактичний коефіцієнт блокування атак K_{block} за формулою (2.1):

$$K_{block} = (1365 / 1420)*100\% = 96,12\%$$

Оскільки K_{block}є метрикою-стимулятором (більше значення є кращим), а отриманий результат 96,12% лежить у межах між критичним 85% та цільовим 98% показниками, нормалізація здійснюється за формулою (2.8):

$$K_{block}^{norm} = \frac{96.12-85.0}{98,0-85,0} = \frac{11,12}{13,0} \approx 0,855$$

Далі обчислюється рівень хибних спрацювань (FPR) за формулою (2.2):

$$FPR = (42/(42+98500))*100\% \approx 0,042\%$$

Оскільки фактичне значення 0,042% є меншим за ідеальне цільове значення 0,05%, система спрацювала краще за еталон, тому нормалізоване значення автоматично приймається як максимальне:

$$FPR^{norm} = 1,000$$

Рівень пропуску атак (FNR), що є метрикою-дестимулятором, визначається за формулою (2.3):

FNR = (55/1420)*100%≈3,87% Оскільки 3,87% лежить між цільовим (1,0%) та критичним (10,0%), застосовуємо формулу (2.9):

$$FNR^{norm} = \frac{10{,}0 - 3{,}87}{10{,}0 - 1{,}0} = \frac{6{,}13}{9{,}0} \approx 0{,}681$$

2. Обчислення та нормалізація експлуатаційних метрик

Коефіцієнт доступності K_{avail}

$$K_{avail} = \frac{166{,}5}{168} \approx 0{,}991$$

Нормалізація (метрика-стимулятор):

$$K_{avail}^{norm} = \frac{0{,}991 - 0{,}950}{0{,}999 - 0{,}950} = \frac{0{,}041}{0{,}049} \approx 0{,}836$$

Нормалізація додаткової затримки трафіку ΔT_{delay} = 12 мс), що є метрикою-дестимулятором:

$$\Delta T_{delay}^{norm} \frac{30 - 12}{30 - 5} = \frac{18}{25} = 0{,}720$$

Нормалізація рівня утилізації процесорної потужності (U_{cpu}= 58%):

$$U_{cpu}^{norm} = \frac{85 - 58}{85 - 50} = \frac{27}{35} \approx 0{,}771$$

3. Обчислення та нормалізація організаційних метрик

Усі організаційні метрики в нашій системі є дестимуляторами (їхнє зростання є негативним фактором). Нормалізуємо їх за єдиним принципом (формула 2.9).

Середній час усунення інцидентів (MTTR = 21 хв):

$$MTTR^{norm} = \frac{60 - 21}{60 - 15} = \frac{39}{45} \approx 0{,}886$$

Затримка оновлення сигнатур (I_{upd} = 6 годин):

$$I_{upd}^{norm} = \frac{24-6}{24-4} = \frac{18}{20} \approx 0{,}900$$

Відсоток відхилення конфігурацій ($P_{drift} = 2{,}0\%$):

$$P_{drift}^{norm} = \frac{5{,}0-2{,}0}{5{,}0-0{,}0} = \frac{3{,}0}{5{,}0} = 0{,}600\%$$

Для зручності подальших обчислень та візуалізації результатів усі отримані нормалізовані оцінки, а також відповідні їм вагові коефіцієнти (W_i)зведено до таблиці 3.2. У цій же таблиці розраховано частковий внесок кожної метрики в загальний показник.

Таблиця 3.2

Результати обчислення нормалізованих значень та їхнього вагового внеску

Категорія	**Метрика результативності**	**Фактичне значення**	**Нормована оцінка (M_{norm})**	**Вага (W^i)**	**Зважене значення (W^i)**
Технічні	Коефіцієнт блокування (K_{block})	96,12 %	0,855	0,25	0,2137
	Рівень хибних спрацювань (FPR)	0,042 %	1	0,1	0,1
	Рівень пропуску атак (FNR)	3,87 %	0,681	0,2	0,1362
Експлуатац.	Коефіцієнт доступності (K_{avail})	0,991	0,836	0,15	0,1254
	Затримка трафіку (ΔT_{delay})	12 мс	0,72	0,05	0,036
	Утилізація потужності (U_{cpu})	58 %	0,771	0,05	0,0385
Організац.	Час реагування (MTTR)	21 хв	0,866	0,1	0,0866
	Актуальність баз (I_{upd})	6 год	0,9	0,05	0,045
	Дрейф конфігурацій (P_{drift})	2,0 %	0,6	0,05	0,03
РАЗОМ	Інтегральний показник (I_{eff})	-	-	1	0,8114

Відповідно до формули (2.11), інтегральний показник ефективності (I_{eff}) дорівнює сумі зважених значень і становить:

$$I_{eff} = 0{,}811$$

Для наочної демонстрації розрахованих параметрів та виявлення «вузьких місць» у системі захисту побудуємо аналітичну діаграму, яка порівнює отримані нормалізовані оцінки з ідеальним станом (значення 1,0).

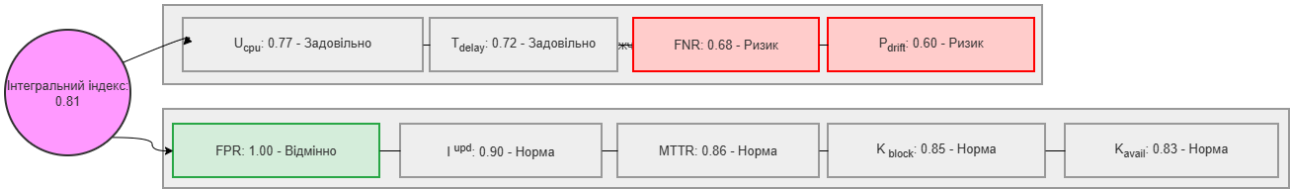

Рис. 3.1. Декомпозиція інтегрального показника на складові

Інтерпретація результатів та практичні рекомендації Отримане значення інтегрального показника I_{eff} = 0,811 згідно з розробленою шкалою потрапляє в інтервал від 0,65 до 0,84, що відповідає «Достатньому (Номінальному)» рівню ефективності ТЗЗІ (жовта зона безпеки).Це означає, що загалом впроваджені технічні засоби виконують свої цільові функції, а мережа підприємства перебуває в безпеці. Проте система ще не досягла Оптимального (Високого) рівня (>0,85). Завдяки декомпозиції інтегрального показника на складові (як показано на рис. 3.1), аналітичне ядро дозволяє чітко локалізувати причини зниження ефективності.

Основними «вузькими місцями», що потягнули загальний індекс донизу, стали: Невідповідність конфігурацій P_{drift} = 0,600: наявність незахищених вузлів через відключені брандмауери. Рівень пропуску атак FNR = 0,681: система IDS/IPS пропустила 3,87% атак (55 інцидентів). Це пряма загроза, яка має значну вагу в загальній оцінці. Затримка обробки трафіку ΔT_{delay} = 0,720: міжмережевий екран створює помітну технологічну затримку через глибоку інспекцію пакетів. На основі результатів експериментального оцінювання пропонуються такі заходи з модернізації: Організаційні заходи: провести аудит політик Active Directory та примусово активувати групові політики безпеки (GPO), які заборонять локальним користувачам самостійно вимикати агенти

EDR чи брандмауери Windows (усунення проблеми P_{drift}.Технічні заходи: здійснити тонке налаштування (fine-tuning) евристичного аналізатора IDS/IPS. Впровадження нових правил виявлення аномалій (на основі машинного навчання) дозволить зменшити відсоток пропущених атак FNR без суттєвого збільшення хибних спрацювань. Експлуатаційні заходи: налаштувати апаратне розвантаження (Hardware Offloading) або оптимізувати правила шифрування на міжмережевому екрані для зменшення часу затримки трафіку ΔT_{delay}.Таким чином, експеримент підтвердив працездатність розробленої системи. Вона не просто видала суху статистику, а алгоритмічно згорнула розрізнені дані в єдиний зрозумілий індекс і вказала адміністратору на конкретні проблеми в інфраструктурі, що повністю підтверджує доцільність її впровадження.

Висновки до розділу 3

1. **Проведено** комплексне експериментальне дослідження розробленої системи оцінювання на базі діючої інфраструктури та засобів захисту інформації (міжмережевого екрана NGFW, системи виявлення вторгнень IDS/IPS та антивірусного комплексу EDR) умовного корпоративного підприємства. Для забезпечення високої об'єктивності результатів сформовано репрезентативний масив вихідних даних із журналів реєстрації подій безпеки загальним обсягом понад 1,2 млн записів за тижневий інтервал спостереження.

2. **Обчислено** фактичні кількісні значення для дев'яти базових одиничних технічних, експлуатаційних та організаційних метрик результативності. За допомогою розроблених математичних моделей стимуляторів і дестимуляторів реалізовано процедуру нормалізації параметрів у безрозмірні оцінки в межах інтервалу [0; 1] відносно встановлених політикою безпеки цільових та критичних порогових констант.

3. **Синтезовано** за допомогою методу лінійної адитивної згортки та з урахуванням визначених експертних вагових коефіцієнтів підсумковий

інтегральний показник ефективності впроваджених ТЗЗІ, значення якого склало I_{eff}= 0,811. Відповідно до розробленої лінгвістичної шкали, отриманий індекс свідчить про достатній (номінальний) рівень захищеності інфраструктури, що сигналізує про перехід системи до жовтої зони операційного контролю.

4. **Виявлено** на основі аналітичної декомпозиції інтегрального показника критичні «вузькі місця» в поточному стані комплексної системи захисту (зокрема, незадовільний рівень дрейфу конфігурацій кінцевих хостів та підвищений коефіцієнт пропуску атак модулями виявлення вторгнень). Сформовано адресні інженерно-технічні та організаційні рекомендації щодо переконфігурації засобів, тонкого налаштування евристичних правил та автоматизації політик безпеки для підвищення загального рівня захищеності інформаційно-комунікаційної системи.

ВИСНОВКИ

У кваліфікаційній роботі вирішено актуальну науково-практичну задачу підвищення об’єктивності, комплексності та оперативності контролю стану технічного захисту інформації в сучасних інформаційно-комунікаційних системах. За результатами виконання завдань дослідження зроблено такі висновки та пропозиції:

Встановлено, що в умовах стрімкого розвитку кіберзагроз поточний стан питання щодо оцінювання ефективності впроваджених технічних засобів захисту інформації (ТЗЗІ) характеризується недостатнім рівнем автоматизації та надмірною залежністю від суб'єктивних експертних оцінок. Традиційні підходи до аудиту безпеки мають дискретний характер і не здатні забезпечити безперервний контроль захищеності, що створює об'єктивну необхідність переходу до кількісних методів моніторингу на основі алгоритмічно обчислюваних метрик.

Проаналізовано класифікацію технічних засобів захисту інформації, особливості їх впровадження в корпоративних мережах, а також міжнародні стандарти (ISO/IEC 27004, NIST SP 800-55) і нормативно-правову базу України. Виявлено, що вітчизняні стандарти зосереджені переважно на етапах первинної атестації систем захисту, тоді як передові світові практики безальтернативно вимагають переходу до безперервного вимірювання показників результативності безпосередньо у процесі повсякденної експлуатації ТЗЗІ.

Досліджено існуючі системи, підходи та методи оцінювання ефективності ТЗЗІ. Доведено, що для сучасних гетерогенних інформаційних систем застосування виключно якісних (експертних) або імітаційних методів тестування є недостатнім. Найбільш ефективним визначено кількісний (метричний) підхід, що базується на автоматизованому зборі телеметрії з пристроїв безпеки, що дозволяє мінімізувати вплив людського фактора.

Розроблено багаторівневу структурну модель системи оцінювання ефективності впроваджених ТЗЗІ на основі метрик результативності.

Запропонована архітектура, що складається з інфраструктурного рівня, рівня нормалізації даних у форматі CEF, аналітичного ядра та рівня візуалізації, забезпечує високу масштабованість і дозволяє ізолювати процеси обробки сирих логів від обчислювальних процедур.

Сформовано збалансовану трирівневу класифікацію метрик результативності, яка охоплює технічні (точність фільтрації), експлуатаційні (утилізація ресурсів, затримки трафіку) та організаційні (час реагування персоналу) показники. Обґрунтовано метод розрахунку єдиного інтегрального показника ефективності на основі лінійної адитивної згортки нормованих значень метрик-стимуляторів та метрик-дестимуляторів із застосуванням експертних вагових коефіцієнтів.

Визначено операційний механізм функціонування розробленої системи у вигляді безперервного чотирифазного життєвого циклу. Проведено експериментальне дослідження розробленої системи на базі корпоративного комплексу ТЗЗІ. Розрахунки на масиві з понад 1,2 млн подій підтвердили працездатність моделі: отриманий інтегральний індекс ефективності (0,811) дозволив автоматично локалізувати слабкі місця інфраструктури (дрейф конфігурацій кінцевих вузлів та пропуск атак модулями IDS) і сформувати адресні рекомендації для адміністраторів.

Сформульовано рекомендації щодо наукового та практичного використання здобутих результатів. У науковому плані розроблений математичний апарат нормалізації та згортки метрик може слугувати теоретичним підґрунтям для подальших досліджень у сфері прогнозування кіберінцидентів за допомогою алгоритмів машинного навчання. У практичному аспекті розроблену систему та метод інтегрального оцінювання рекомендується впроваджувати у центрах управління кібербезпекою (SOC) підприємств різних форм власності для автоматизації процесів моніторингу, обґрунтування бюджетів на інформаційну безпеку та підтримки прийняття управлінських рішень щодо модернізації ТЗЗІ.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про вищу освіту : Закон України від 01.07.2014 р. № 1556-VII. *Відомості Верховної Ради України*. 2014. № 37-38. Ст. 2004.

2. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 р. № 80/94-ВР. *Відомості Верховної Ради України*. 1994. № 31. Ст. 286.

3. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII. *Відомості Верховної Ради України*. 2017. № 45. Ст. 403.

4. Про національну безпеку України : Закон України від 21.06.2018 р. № 2469-VIII. *Відомості Верховної Ради України*. 2018. № 31. Ст. 241.

5. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт. [Чинний від 1997-01-01]. Київ : Держстандарт України, 1996. 14 с.

6. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення. [Чинний від 1998-01-01]. Київ : Держстандарт України, 1997. 12 с.

7. ДСТУ ISO/IEC 27001:2015. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013, IDT). [Чинний від 2017-01-01]. Київ : ДП «УкрНДНЦ», 2016. 28 с.

8. ДСТУ ISO/IEC 27002:2015. Інформаційні технології. Методи захисту. Звід правил щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014, IDT). [Чинний від 2017-01-01]. Київ : ДП «УкрНДНЦ», 2016. 149 с.

9. НД ТЗІ 1.1-003-99. Термінологія в галузі технічного захисту інформації. Основні положення. Київ : ДКЗІ України, 1999. 24 с.

10. НД ТЗІ 2.5-004-99. Критерії оцінювання захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Київ : ДКЗІ України, 1999. 68 с.

11. Баранов В. М., Ковтун В. І. *Технічні засоби захисту інформації : навч. посіб.* Київ : НАСБУ, 2023. 312 с.

12. Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В. *Інформаційна та кібербезпека: технології захисту. Підручник.* Київ : ДУТ, 2020. 640 с.

13. Гнатюк С. О., Хмелевський С. В. Метрики результативності систем виявлення вторгнень в інформаційно-комунікаційних мережах. *Захист інформації*. 2022. Т. 24, № 2. С. 85–94.

14. Гребенніков Ю. В. Моделі оцінювання ефективності комплексних систем захисту інформації на підприємствах. *Сучасний захист інформації*. 2021. № 3 (47). С. 14–22.

15. Дудикевич В. Б., Гарасимчук О. І. *Основи технічного захисту інформації : підручник.* Львів : Видавництво Львівської політехніки, 2021. 416 с.

16. Євсєєв С. П., Король О. Г. Розроблення методологии оцінки ефективності систем захисту критичних інфраструктур. *Кібербезпека: освіта, наука, техніка*. 2023. № 1 (19). С. 45–59.

17. Легомінова С. В., Іванченко Є. В. Управління ризиками кібербезпеки в корпоративних інформаційних системах на основі безперервного моніторингу. *Зв'язок*. 2024. № 2. С. 18–25.

18. Лук'янова Н. В. Методи лінійної адитивної згортки у задачах багатокритеріального оцінювання складних технічних систем. *Системні дослідження та інформаційні технології*. 2022. № 4. С. 72–83.

19. Петров В. В. Кількісна оцінка ефективності міжмережевих екранів за допомогою метрик доступності та фільтрації. *Комп’ютерно-інтегровані технології*. 2023. № 50. С. 112–119.

20. Сааті Т. Л. *Прийняття рішень. Метод аналізу ієрархій : пер. з англ.* Москва : Радио и связь, 1993. 278 с.

21. Скрипник О. М. Порівняльний аналіз технічних засобів захисту інформації периметра розподілених мереж. *Телекомунікаційні та інформаційні технології*. 2023. № 1. С. 34–42.

22. Субач І. П. *Математичні методи в задачах кібербезпеки : навч. посіб.* Київ : Наукова думка, 2021. 198 с.

23. Хорошко В. О., Чекатков А. А. *Методи та засоби захисту інформації.* Київ : Юніор, 2003. 504 с.

24. Шелест М. Є. Автоматизація збору та аналізу лог-файлів у гетерогенних інформаційних системах. *Вісник ЖДТУ. Серія: Технічні науки*. 2022. № 2 (90). С. 143–152.

25. Юрченко О. В., Кузнецов О. В. Застосування формату CEF для уніфікації подій безпеки в системах моніторингу типу SIEM. *Електронне моделювання*. 2023. Т. 45, № 5. С. 61–73.

26. Anderson R. *Security Engineering: A Guide to Building Dependable Distributed Systems.* 3rd ed. Indianapolis : John Wiley & Sons, 2020. 1232 p.

27. CIS Controls Version 8.1. Center for Internet Security, 2024. URL: https://www.cisecurity.org/controls/v8-1

28. Chuvakin A., Schmidt K., Phillips C. *Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surlogging.* Waltham : Syngress, 2013. 402 p.

29. Hubbard D. W. *How to Measure Anything in Cybersecurity Risk.* Hoboken : John Wiley & Sons, 2016. 288 p.

30. ISO/IEC 27004:2016. Information technology. Security techniques. Information security management. Monitoring, measurement, analysis and evaluation. Geneva : ISO, 2016. 58 p.

31. ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection. Guidance on managing information security risks. Geneva : ISO, 2022. 72 p.

32. Kim D., Solomon M. G. *Fundamentals of Information Systems Security.* 4th ed. Burlington : Jones & Bartlett Learning, 2022. 544 p.

33. NIST Special Publication 800-53 Rev. 5. Security and Privacy Controls for Information Systems and Organizations. Gaithersburg : National Institute of Standards and Technology, 2020. URL:

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf (дата звернення: 10.03.2026).

34. NIST Special Publication 800-55. Measurement Guide for Information Security. Volume 1: Methodology. Gaithersburg : National Institute of Standards and Technology, 2024. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-55v1.pdf (дата звернення: 12.03.2026).

35. NIST Special Publication 800-55. Measurement Guide for Information Security. Volume 2: Performance Metrics. Gaithersburg : National Institute of Standards and Technology, 2024. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-55v2.pdf (дата звернення: 12.03.2026).

36. NIST Special Publication 800-92 Rev. 1. Guide to Computer Security Log Management. Gaithersburg : National Institute of Standards and Technology, 2023. 45 p.

37. Pfleeger C. P., Pfleeger S. L., Margulies J. *Security in Computing.* 5th ed. Boston : Prentice Hall, 2015. 944 p.

38. Ross R., McEvilley M., Oren J. *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems.* Gaithersburg : NIST, 2022. 184 p.

39. Schneier B. *Applied Cryptography: Protocols, Algorithms, and Source Code in C.* 20th Anniversary ed. New York : John Wiley & Sons, 2015. 784 p.

40. Stallings W. *Computer Security: Principles and Practice.* 5th ed. Boston : Pearson, 2022. 820 p.

41. Vacca J. R. *Managing Information Security.* 2nd ed. Waltham : Syngress, 2014. 344 p.

42. Whitman M. E., Mattord H. J. *Principles of Information Security.* 7th ed. Boston : Cengage Learning, 2021. 656 p.