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 КЛЮЧОВИХ ПОКАЗНИКІВ ЕФЕКТИВНОСТІ ТА РИЗИКІВ (KPI/KRI) ДЛЯ ОЦІНЮВАННЯ РІВНЯ КІБЕРЗАХИЩЕНОСТІ ОБ’ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В ПРОЦЕСІ АУДИТУ ”

на здобуття освітнього ступеня магістра
зі спеціальності 125 Кібербезпека та захист інформації
освітньо-професійної програми Управління інформаційною та кібернетичною безпекою

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

_____ Данило НОВОХАТНІЙ

(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: Здобувач вищої освіти гр. УБДМ-61

Керівник:

д.е.н., професор Світлана ЛЕГОМІНОВА

Рецензент:

д.т.н., професор Галина ГАЙДУР

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут кібербезпеки та захисту інформації

Кафедра Управління кібербезпекою та захистом інформації
Ступінь вищої освіти магістр
Спеціальність 125 Кібербезпека та захист інформації
Освітньо-професійна програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедрою УКБЗІ
_____ Світлана ЛЕГОМІНОВА
"____" _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Студенту Новохатньому Данилу Юрійовичу

Тема кваліфікаційної роботи: "Система ключових показників ефективності та ризиків (KPI/KRI) для оцінювання рівня кіберзахищеності об'єктів критичної інфраструктури в процесі аудиту"

керівник кваліфікаційної роботи Світлана ЛЕГОМІНОВА *доктор економічних наук, професор*

затверджені наказом Державного університету інформаційно-комунікаційних технологій від "30" жовтня 2025 р. № 467.

Строк подання кваліфікаційної роботи "25" грудня 2025 р.

1. Вихідні дані до кваліфікаційної роботи:.
2. Перелік питань, які потрібно розробити:
   1. Дослідити теоретичні основи оцінювання рівня кіберзахищеності об'єктів критичної інфраструктури
   2. Проаналізувати системи ключових показників KPI та KRI
   3. Запропоновути системи ключових показників ефективності та ризиків (KPI/KRI) для оцінювання рівня кіберзахищеності об'єктів критичної інфраструктури в процесі аудиту
3. Перелік ілюстративного матеріалу: *презентація*
4. Дата видачі завдання "02" жовтня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назви етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	10.10.2025	
2.	Збір та аналіз літератури.	23.10.2025	
3.	Дослідження теоретичних основ оцінювання рівня кіберзахищеності об’єктів критичної інфраструктури	27.10.2025	
4.	Аналіз системи ключових показників KPI та KRI	10.11.2025	
5.	Розробка системи ключових показників ефективності та ризиків (KPI/KRI) для оцінювання рівня кіберзахищеності об'єктів критичної інфраструктури в процесі аудиту	15.11.2025	
6.	Формулювання висновків за результатами дослідження.	22.11.2025	
7.	Оформлення роботи.	04.12.2025	
8.	Оформлення презентації.	14.12.2025	
9.	Отримання рецензії на роботу.	18.12.2025	
10.	Захист в ЕК.	__.01.2026	

Здобувач вищої освіти _____ Данило НОВОХАТНІЙ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Світлана ЛЕГОМІНОВА
(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 магістра

Направляється здобувач Новохатній Д.Ю.. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека та захист інформації
(код, найменування спеціальності)
Освітньо-професійної програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: “ Система ключових показників ефективності та ризиків (KPI/KRI) для оцінювання рівня кіберзахищеності об’єктів критичної інфраструктури в процесі аудиту”
Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувач **НОВОХАТНІЙ Данило** у кваліфікаційній роботі дослідив теоретичні основи оцінювання рівня кіберзахищеності об’єктів критичної інфраструктури, проаналізував системи ключових показників KPI та KRI, базуючись на вивченому матеріалі запропонував систему ключових показників ефективності та ризиків (KPI/KRI) для оцінювання рівня кіберзахищеності об'єктів критичної інфраструктури в процесі аудиту. **НОВОХАТНІЙ Данило** показав високу теоретичну і практичну підготовку, володіння науково-дослідницькими методами, вміння самостійно знаходити шляхи вирішення проблеми дослідження. Результати дослідження апробовані на конференції “Стратегії кіберстійкості: управління ризиками та безперервність бізнесу” 28 лютого 2025 року.

Все це дозволяє оцінити кваліфікаційну роботу здобувача **НОВОХАТНЬОГО Данила** на оцінку “відмінно” та присвоїти йому кваліфікацію “Магістр з кібербезпеки та захисту інформації за освітньо-професійною програмою Управління інформаційною та кібернетичною безпекою”.

Керівник кваліфікаційної роботи _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

“____“_____2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Новохатній Д.Ю. 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 магістерську роботу

Здобувач вищої освіти Новохатній Данило Юрійович
на тему " Система ключових показників ефективності та ризиків (KPI/KRI) для оцінювання рівня кіберзахищеності об'єктів критичної інфраструктури в процесі аудиту "

Актуальність. Впровадження системного підходу до визначення рівня кіберзахищеності об'єктів критичної інфраструктури та оптимальної процедури її аудиту завжди буде актуальною проблемою, що обумовлюється динамічними змінами цифрових сфер та виникненням нових загроз, що призводять до матеріальних втрат та порушують загальний безпековий стан. Тому тема є актуальною, має важливе теоретичне та практичне значення.

Позитивні сторони

1. У роботі досліджено систему ключових показників ефективності та ризиків (KPI/KRI), визначено особливості при застосуванні до об'єктів критичної інфраструктури, практична частина містить конкретні заходи та рекомендації щодо побудови системи оцінювання рівня кіберзахищенності об'єктів критичної інфраструктури в процесі аудиту.
2. Кваліфікаційна робота оформлена відповідно до вимог. Виклад матеріалу здійснено відповідно до плану, зроблено логічні висновки. Ключові положення роботи представлено у вигляді рисунків. Автор опрацювала значну джерельну базу: близько 33 публікацій та електронних джерел, в тому числі англомовних.
3. За результатами дослідження запропоновано рекомендації щодо оцінювання рівня кіберзахищеності об'єктів критичної інфраструктури в процесі аудиту.

Недоліки

Доцільно було б детально розкрито економічну ефективність впровадження запропонованої системи ключових показників ефективності та ризиків (KPI/KRI).

Однак, вищезгадане зауваження не впливає на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує позитивної оцінки, а здобувач Новохатній Данило Юрійович заслуговує присвоєння кваліфікації "Магістр з кібербезпеки та захисту інформації за освітньо-професійною програмою Управління інформаційною та кібернетичною безпекою".

Рецензент: завідувач кафедри
Систем та технологій кібербезпеки,

д.т.н, професор _____ *підпис* Галина ГАЙДУР

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 100 сторінок, 13 рисунків, 20 таблиць, 33 використаних джерел.

Мета роботи - розробка системи ключових показників ефективності та ризиків (KPI/KRI) для оцінювання рівня кіберзахищеності об'єктів критичної інфраструктури в процесі аудиту та її практична апробація.

Об'єкт дослідження - забезпечення кіберзахищеності об'єктів критичної інфраструктури.

Предмет дослідження - система ключових показників ефективності та ризиків (KPI/KRI) для оцінювання рівня кіберзахищеності об'єктів критичної інфраструктури в процесі аудиту.

Методи дослідження. Для вирішення поставлених завдань використано методи системного аналізу - для дослідження структури кіберзахисту об'єктів критичної інфраструктури; порівняльного аналізу - для систематизації міжнародних стандартів та нормативних вимог; статистичний метод та метод дерева відмов - для аналізу ризиків; метод експертних оцінок - для визначення ймовірностей та ваг ризиків; нормативний метод - для порівняння фактичних значень показників з еталонними; економіко-математичні методи - для розрахунку показників ефективності інвестицій (ROSI, NPV).

Короткий зміст роботи. У роботі досліджено теоретичні основи оцінювання кіберзахищеності об'єктів критичної інфраструктури (ОКІ) та проаналізовано міжнародні стандарти (ISO 27001, NIST CSF, IEC 62443) і національне законодавство України у цій сфері. Обґрунтовано методологію формування системи ключових показників ефективності (KPI) та ризиків (KRI), запропоновано класифікацію показників за категоріями: технічні, часові, організаційні, ризикові. Розроблено базовий набір із 20 метрик кібербезпеки, адаптованих до специфіки ОКІ, з визначенням формул розрахунку та цільових значень. Створено інтегральну методику оцінювання на основі комбінованого застосування статистичного методу, методу дерева відмов, експертних оцінок та нормативного аналізу. Проведено практичну апробацію на реальному об'єкті критичної інфраструктури - ТОВ «Трител»

(телекомунікаційна галузь). Виявлено критичні відхилення показників, розраховано інтегральний показник кіберризику, розроблено комплекс рекомендацій з економічним обґрунтуванням ROSI.

Галузь застосування. Розроблена система KPI/KRI може бути впроваджена на об'єктах критичної інфраструктури різних секторів (енергетика, телекомунікації, транспорт, фінанси) для підвищення об'єктивності оцінювання рівня кіберзахищеності. Методика може використовуватися аудиторськими компаніями, внутрішніми службами безпеки та регуляторними органами для проведення комплексних аудитів кібербезпеки.

КЛЮЧОВІ СЛОВА: КРИТИЧНА ІНФРАСТРУКТУРА, КІБЕРБЕЗПЕКА, КЛЮЧОВІ ПОКАЗНИКИ ЕФЕКТИВНОСТІ (KPI), КЛЮЧОВІ ПОКАЗНИКИ РИЗИКІВ (KRI), АУДИТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, ОЦІНЮВАННЯ КІБЕРЗАХИЩЕНОСТІ, УПРАВЛІННЯ КІБЕРРИЗИКАМИ.

ABSTRACT

The text part of the master's qualification work: 100 pages, 13 figures, 20 tables, 33 references.

The purpose of the work is to develop a system of Key Performance Indicators and Key Risk Indicators (KPI/KRI) for assessing the cybersecurity level of critical infrastructure objects during audits and its practical validation.

Object of research - ensuring cybersecurity of critical infrastructure objects.

Subject of research - the system of Key Performance Indicators and Key Risk Indicators (KPI/KRI) for assessing the cybersecurity level of critical infrastructure objects during audits.

Research methods. The following methods were used to solve the research objectives: system analysis - to study the structure of critical infrastructure cybersecurity; comparative analysis - to systematize international standards and regulatory requirements; statistical method and fault tree analysis - for risk assessment; expert evaluation method - to determine probabilities and risk weights; normative method - to compare actual indicator values with reference values; economic and mathematical methods - to calculate investment efficiency indicators (ROSI, NPV).

Brief content of research. The work examines the theoretical foundations of cybersecurity assessment for critical infrastructure objects (CIO) and analyzes international standards (ISO 27001, NIST CSF, IEC 62443) and Ukrainian national legislation in this field. The methodology for forming a system of Key Performance Indicators (KPI) and Key Risk Indicators (KRI) has been substantiated, and a classification of indicators by categories has been proposed: technical, time-based, organizational, and risk-related. A basic set of 20 cybersecurity metrics adapted to CIO specifics has been developed, with calculation formulas and target values defined. An integrated assessment methodology has been created based on the combined application of statistical method, fault tree analysis, expert evaluations, and normative analysis. Practical validation was conducted at a real critical infrastructure

object - LLC "Tritel" (telecommunications sector). Critical deviations in indicators were identified, an integrated cyber risk indicator was calculated, and a set of recommendations with economic justification was developed .

Field of application. The developed KPI/KRI system can be implemented at critical infrastructure objects across various sectors (energy, telecommunications, transport, finance) to improve the objectivity of cybersecurity assessment. The methodology can be used by audit companies, internal security services, and regulatory authorities for conducting comprehensive cybersecurity audits.

KEYWORDS: CRITICAL INFRASTRUCTURE, CYBERSECURITY, KEY PERFORMANCE INDICATORS (KPI), KEY RISK INDICATORS (KRI), INFORMATION SECURITY AUDIT, CYBERSECURITY ASSESSMENT, CYBER RISK MANAGEMENT.

ЗМІСТ

ВСТУП

Актуальність теми. Сучасний етап розвитку інформаційного суспільства характеризується стрімким зростанням залежності критичної інфраструктури від інформаційно-комунікаційних технологій. Об'єкти критичної інфраструктури (ОКІ) - підприємства енергетичного, транспортного, телекомунікаційного секторів, фінансові установи - стають дедалі більш вразливими до кібератак, наслідки яких можуть мати катастрофічний характер для національної безпеки та життєдіяльності суспільства.

За даними ДССЗЗІ України, у 2023–2024 роках зафіксовано безпрецедентне зростання кількості кібератак на українську критичну інфраструктуру. Більшість атак мають ознаки цілеспрямованих операцій (APT), що здійснюються державними хакерськими угрупованнями. В умовах гібридної війни забезпечення кіберзахисту ОКІ набуває стратегічного значення.

Чинне законодавство України - Закон «Про критичну інфраструктуру» (2021) та Закон «Про основні засади забезпечення кібербезпеки України» (2017) - встановлює загальні вимоги до захисту ОКІ, однак не містить методик кількісного оцінювання рівня кіберзахищеності. Існуючі підходи до аудиту переважно зосереджені на перевірці відповідності (compliance) та не забезпечують комплексної оцінки реального стану захищеності.

Міжнародні стандарти (ISO 27001, NIST CSF, IEC 62443) пропонують загальні принципи управління безпекою, проте потребують адаптації до специфіки українського регуляторного середовища. Відсутність методології формування вимірюваних показників ускладнює прийняття обґрунтованих рішень щодо інвестицій у кібербезпеку.

Таким чином, актуальність дослідження обумовлена необхідністю розробки системи ключових показників ефективності (KPI) та ризиків (KRI) для оцінювання кіберзахищеності ОКІ, що забезпечить об'єктивність аудиту та обґрунтування економічної доцільності заходів захисту.

Мета і завдання дослідження. Метою роботи є розробка системи ключових показників ефективності та ризиків (KPI/KRI) для оцінювання рівня

кіберзахищеності об'єктів критичної інфраструктури в процесі аудиту та її практична апробація.

Для досягнення поставленої мети необхідно вирішити такі завдання:

- дослідити теоретичні основи оцінювання кіберзахищеності об'єктів критичної інфраструктури та проаналізувати існуючі підходи до аудиту кібербезпеки
- систематизувати міжнародні стандарти та національне законодавство у сфері кібербезпеки критичної інфраструктури
- обґрунтувати методологію формування системи ключових показників ефективності (KPI) та ризиків (KRI) для ОКІ
- розробити базовий набір метрик кібербезпеки, адаптованих до специфіки об'єктів критичної інфраструктури
- розробити інтегральну методику оцінювання стану кіберзахищеності на основі комбінованого застосування кількісних методів аналізу
- провести практичну апробацію розробленої системи KPI/KRI на реальному об'єкті критичної інфраструктури
- обґрунтувати економічну ефективність впровадження рекомендацій з підвищення рівня кіберзахищеності

Об'єкт дослідження - забезпечення кіберзахищеності об'єктів критичної інфраструктури.

Предмет дослідження - система ключових показників ефективності та ризиків (KPI/KRI) для оцінювання рівня кіберзахищеності об'єктів критичної інфраструктури в процесі аудиту.

Методи дослідження. Системний аналіз - для дослідження структури кіберзахисту ОКІ; порівняльний аналіз - для систематизації стандартів; статистичний метод та метод дерева відмов - для аналізу ризиків; метод експертних оцінок - для визначення ймовірностей; нормативний метод - для

порівняння з еталонними значеннями; економіко-математичні методи - для розрахунку ROSI та NPV.

Наукова новизна одержаних результатів полягає:

- удосконалено методологію оцінювання кіберзахищеності ОКІ шляхом інтеграції систем KPI та KRI у єдину комплексну модель, що забезпечує як оцінку результативності заходів захисту, так і прогнозування потенційних загроз;
- дістала подальшого розвитку інтегральна методика оцінювання на основі комбінованого застосування статистичного методу, методу дерева відмов, експертних оцінок та нормативного аналізу;
- вперше запропоновано базовий набір із 20 метрик кібербезпеки, адаптованих до специфіки ОКІ України з урахуванням вимог національного законодавства та міжнародних стандартів.

Практичне значення одержаних результатів. Розроблена система KPI/KRI може бути впроваджена на ОКІ різних секторів для підвищення об'єктивності оцінювання кіберзахищеності. Методика може використовуватися аудиторськими компаніями та регуляторними органами для проведення аудитів. Економічне обґрунтування (ROSI, NPV) забезпечує аргументацію доцільності інвестицій у кібербезпеку.

Галузь застосування. Результати можуть бути застосовані на підприємствах, віднесених до ОКІ; аудиторськими компаніями; органами державної влади у сфері кіберзахисту; у навчальному процесі при підготовці фахівців з кібербезпеки.

Апробація результатів. Основні положення доповідалися на науково-практичному семінарі кафедри управління кібербезпекою та захистом інформації ДУІКТ (2025 р.).

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ОЦІНЮВАННЯ РІВНЯ КІБЕРЗАХИЩЕНОСТІ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

1.1 Об'єкти критичної інфраструктури та їх вразливості для оцінювання рівня кіберзахищеності

Визначення та класифікація об'єктів критичної інфраструктури

Сучасний світ характеризується глибокою залежністю від складних технологічних систем, які забезпечують функціонування базових суспільних процесів. Критична інфраструктура становить фундамент національної безпеки та економічної стабільності будь-якої держави, оскільки її порушення здатне спричинити каскадні наслідки для мільйонів людей. Взаємозалежність різних секторів інфраструктури створює ефект доміно, коли збій в одній системі може призвести до відмови цілого ланцюга пов'язаних сервісів.

Дослідження Національного інституту стандартів і технологій Сполучених Штатів визначає шістнадцять ключових секторів критичної інфраструктури [2]. Серед них особливе місце посідають енергетика як основа функціонування всіх інших секторів, транспортна галузь що забезпечує логістичні зв'язки, системи охорони здоров'я від яких залежить життя громадян, фінансові установи що підтримують економічну діяльність, та телекомунікаційні мережі що є нервовою системою сучасного суспільства. Кожен із цих секторів має власну специфіку кіберзагроз та вимагає адаптованого підходу до захисту.

Європейський Союз у директиві NIS2 розширив визначення критичної інфраструктури, включивши цифрову інфраструктуру, системи водопостачання та поводження з відходами [3]. Таке розширення відображає зростаючу роль цифровізації у повсякденному житті та усвідомлення нових векторів загроз, які раніше не враховувались у регуляторних документах. Директива також вперше включила сектор державного управління як критичну інфраструктуру, визнаючи важливість захисту урядових інформаційних систем.

Українське законодавство, зокрема Закон про критичну інфраструктуру від 2021 року, визначає одинадцять секторів, що потребують особливого захисту [21]. До них належать енергетика, хімічна промисловість, транспорт, інформаційно-комунікаційні технології, електронні комунікації, охорона здоров'я, фінансовий сектор, забезпечення життєдіяльності населення, харчова промисловість, оборонно-промисловий комплекс та космічна галузь. Такий перелік враховує специфіку національної економіки та геополітичне становище країни в умовах збройної агресії.

Класифікація об'єктів критичної інфраструктури може здійснюватися за різними критеріями, що наведено в таблиці 1.1. Така систематизація дозволяє визначити специфічні вимоги до захисту кожної категорії об'єктів та обрати відповідні методи оцінювання кіберзахищеності.

Таблиця 1.1

Класифікація об'єктів критичної інфраструктури

Критерій	Типи об'єктів	Приклади	Особливості захисту
За галузевою належністю	Енергетичні системи	Електростанції, підстанції, нафтопроводи	Пріоритет доступності, ізоляція SCADA
	Транспортна інфраструктура	Аеропорти, залізниці, порти	Резервування, захист АСУ ТП
	Телекомунікації	Дата-центри, базові станції	DDoS-захист, шифрування
За ступенем цифровізації	Повністю автоматизовані	SCADA, ICS, роботизовані лінії	Сегментація IT/OT, моніторинг
	Частково автоматизовані	Гібридні системи управління	Контроль людського фактору
За критичністю	Національного значення	АЕС, магістральні мережі	Державний контроль, SL4
	Регіонального значення	Обласні енергосистеми	Регуляторний нагляд, SL3

Технологічну основу сучасних об'єктів критичної інфраструктури складають кілька ключових компонентів. Системи диспетчерського контролю та збору даних, відомі як SCADA (Supervisory Control and Data Acquisition), забезпечують централізований моніторинг та управління розподіленими процесами. Розподілені системи управління DCS (Distributed Control System)

використовуються для автоматизації виробничих процесів на великих промислових об'єктах. Програмовані логічні контролери PLC (Programmable Logic Controller) виконують функції локального управління окремими технологічними операціями. Промисловий Інтернет речей IIoT (Industrial Internet of Things) забезпечує підключення датчиків, виконавчих механізмів та інших пристроїв до єдиної мережі для збору та аналізу даних у реальному часі.

Інтеграція цих компонентів створює складне середовище, де кіберфізичні системи тісно переплітаються з операційними технологіями. Така конвергенція IT та OT, з одного боку, підвищує ефективність виробничих процесів та дозволяє впроваджувати предиктивне обслуговування обладнання, а з іншого - суттєво розширює поверхню потенційних атак та створює нові вектори загроз, які раніше не існували в ізольованих промислових системах.

Математично поверхню атаки можна виразити через добуток кількості підключених компонентів, середньої кількості вразливостей на кожен компонент та рівня взаємопов'язаності системи:

$$AS = N \times V \times C \tag{1.1}$$

де AS позначає поверхню атаки (Attack Surface), N - кількість підключених компонентів системи, V - середню кількість вразливостей на один компонент, C - коефіцієнт взаємопов'язаності системи в діапазоні від одного до десяти. Ця залежність демонструє, що навіть незначне збільшення кількості підключених пристроїв може експоненційно збільшувати загальний ризик компрометації системи, особливо за умови недостатньої сегментації мережі та відсутності належного контролю міжсистемних з'єднань.

Таксономія вразливостей об'єктів критичної інфраструктури

Вразливість у контексті кібербезпеки визначається як слабке місце в системі безпеки, що може бути експлуатоване зловмисником для порушення конфіденційності, цілісності або доступності інформаційних ресурсів [6]. На відміну від загрози, яка є потенційною можливістю негативного впливу,

вразливість є конкретним недоліком у конфігурації, архітектурі або процесах, який може бути використаний для реалізації загрози.

Вразливості об'єктів критичної інфраструктури можна систематизувати за трьома основними категоріями: технічні, організаційні та пов'язані з людським фактором. Кожна категорія має власну специфіку та потребує відповідних методів виявлення та усунення.

Технічні вразливості охоплюють широкий спектр недоліків у програмному забезпеченні, апаратному забезпеченні та мережевій інфраструктурі. Мережеві вразливості включають відсутність належної сегментації між корпоративною та промисловою мережами, використання застарілих протоколів без шифрування таких як Telnet, FTP або Modbus, недостатній захист периметру та відсутність систем виявлення вторгнень. Програмні вразливості проявляються у наявності критичних недоліків з показником CVSS понад сім балів, відсутності своєчасних оновлень безпеки, використанні застарілих версій операційних систем та прикладного програмного забезпечення. Апаратні вразливості включають фізично незахищені контролери з доступними інтерфейсами налагодження, наявність прихованих точок доступу від виробників обладнання, використання обладнання з закінченим терміном підтримки виробника.

Організаційні вразливості пов'язані з недоліками в управлінні та процесах забезпечення безпеки. До них належать відсутність або застарілість політик інформаційної безпеки, неефективне управління процесами виявлення та усунення вразливостей, недостатній моніторинг мережевої активності та відсутність системи раннього попередження, нечіткий розподіл відповідальності за кібербезпеку між підрозділами, відсутність планів реагування на інциденти або їх невідповідність сучасним загрозам, недостатнє фінансування програм кібербезпеки та брак кваліфікованого персоналу.

Людський фактор залишається найбільш непередбачуваним елементом системи безпеки. За статистикою галузевих досліджень, близько дев'яноста п'яти відсотків успішних кібератак починаються саме з фішингових

повідомлень, спрямованих на співробітників організації [8]. Вразливості цієї категорії включають низький рівень обізнаності персоналу щодо кіберзагроз, схильність до методів соціальної інженерії, недотримання політик безпеки через незручність або нерозуміння їх важливості, внутрішні загрози від незадоволених або недобросовісних працівників, помилки при конфігурації систем через недостатню кваліфікацію.

Для комплексної оцінки рівня вразливості об'єкта критичної інфраструктури доцільно використовувати інтегральний показник, що враховує внесок кожної категорії з відповідними ваговими коефіцієнтами:

$$IV = \alpha \times TV + \beta \times OV + \gamma \times HV \quad (1.2)$$

де IV - інтегральний показник вразливості (Integrated Vulnerability), TV - оцінка технічних вразливостей (Technical Vulnerabilities), OV - оцінка організаційних вразливостей (Organizational Vulnerabilities), HV - оцінка вразливостей людського фактору (Human Vulnerabilities). Вагові коефіцієнти α, β та γ визначаються відповідно до специфіки об'єкта та складають 0.5, 0.3 та 0.2 згідно з рекомендаціями міжнародних стандартів [12]. Такий розподіл відображає пріоритетність технічних вразливостей через їх безпосередній вплив на можливість компрометації систем.

Оцінка інтегрального показника здійснюється за шкалою від нуля до ста балів із такою інтерпретацією результатів. Значення від нуля до двадцяти свідчить про критичний рівень вразливості, що потребує термінових заходів та може вимагати тимчасового обмеження функціональності системи. Діапазон від двадцяти одного до сорока балів відповідає високому рівню вразливості з необхідністю пріоритетних дій протягом найближчих тижнів. Значення від сорока одного до шістдесяти характеризує середній рівень із плановими покращеннями у квартальному горизонті. Діапазон від шістдесяти одного до вісімдесяти відповідає низькому рівню вразливості, а від вісімдесяти одного до ста - мінімальному рівню, що потребує лише підтримки досягнутого стану.

1.2. Підходи до аудиту та оцінювання кіберзахищеності об'єктів критичної інфраструктури

Концептуальні основи аудиту кібербезпеки

Аудит кібербезпеки об'єктів критичної інфраструктури являє собою систематичний процес незалежного оцінювання відповідності впроваджених систем захисту встановленим вимогам, стандартам та найкращим практикам галузі [13]. На відміну від традиційного аудиту інформаційних технологій, який фокусується переважно на корпоративних системах, аудит критичної інфраструктури має враховувати специфіку промислових систем управління, де порушення функціонування може мати катастрофічні наслідки для життя людей та навколишнього середовища.

Ключова відмінність полягає у пріоритизації атрибутів безпеки відповідно до типу системи. Класична тріада CIA визначає три основні атрибути: конфіденційність (Confidentiality), цілісність (Integrity) та доступність (Availability). Для корпоративних інформаційних систем традиційно найважливішою є конфіденційність даних, оскільки витік комерційної інформації може завдати значних фінансових та репутаційних збитків. Натомість для промислових систем управління найвищий пріоритет має доступність, оскільки зупинка технологічного процесу може призвести до аварій, екологічних катастроф або загрози життю людей. Порівняння пріоритетів для різних типів систем наведено в таблиці 1.2.

Таблиця 1.2

Пріоритетність атрибутів безпеки для різних типів систем

Тип системи	1-й пріоритет	2-й пріоритет	3-й пріоритет
Корпоративні IT	Конфіденційність (C)	Цілісність (I)	Доступність (A)
Промислові OT	Доступність (A)	Цілісність (I)	Конфіденційність (C)
Гібридні системи КІ	Доступність (A)	Цілісність (I) = Конфіденційність (C)	-

Концептуальна модель аудиту кіберзахищеності об'єктів критичної інфраструктури базується на кількох фундаментальних принципах. Перший принцип передбачає адаптацію тріади CIA до специфіки об'єкта, де для операційних технологій послідовність пріоритетів змінюється на AIC: доступність, цілісність, конфіденційність. Це означає, що при виборі засобів захисту перевагу слід надавати тим, які не впливають на безперервність функціонування системи.

Другий принцип передбачає побудову багаторівневого захисту за моделлю Defense in Depth, яка походить з військової доктрини та передбачає створення множинних бар'єрів на шляху зловмисника. Модель охоплює сім рівнів захисту від політик та процедур на найвищому рівні до захисту даних на найнижчому, що ілюструє рисунок 1.1. Кожен рівень має власні засоби захисту та контролі, а компрометація одного рівня не повинна автоматично призводити до компрометації наступних.

Рис. 1.1 Модель багаторівневого захисту (Defense in Depth)

На рівні політик та процедур формується стратегічна основа кібербезпеки організації. Фізична безпека забезпечує захист приміщень та обладнання від несанкціонованого фізичного доступу. Периметр мережі включає міжмережеві екрани, системи виявлення та запобігання вторгнень, VPN-шлюзи для захищеного віддаленого доступу. Внутрішня мережа захищається через

сегментацію, VLAN та внутрішні міжмережеві екрани. На рівні хостів впроваджуються антивірусний захист, системи контролю додатків та управління конфігураціями. Рівень додатків передбачає безпечну розробку, тестування на вразливості та контроль доступу до функцій. Найнижчий рівень даних захищається шифруванням, системами запобігання витоку даних та резервним копіюванням.

Третій принцип полягає у застосуванні ризик-орієнтованого підходу, який дозволяє раціонально розподіляти обмежені ресурси та концентрувати зусилля на найбільш критичних напрямках. Рівень ризику визначається як добуток трьох складових:

$$R = T \times V \times I \quad (1.3)$$

де R - рівень ризику (Risk), T - ймовірність реалізації загрози (Threat probability) в діапазоні від нуля до одиниці, V - ступінь вразливості системи (Vulnerability) також від нуля до одиниці, I - потенційний вплив успішної атаки (Impact) за десятибальною шкалою. Такий підхід дозволяє кількісно оцінити та порівняти різні ризики для прийняття обґрунтованих управлінських рішень щодо пріоритизації заходів захисту.

Для візуалізації та пріоритизації ризиків використовується матриця оцінювання за шкалою 5×5, що наведена на рисунку 1.2. Матриця дозволяє класифікувати ризики за чотирма категоріями залежно від комбінації ймовірності та впливу. Низький ризик із показником від одного до п'яти потребує лише моніторингу. Середній ризик від шести до десяти вимагає щоквартального перегляду. Високий ризик від одинадцяти до п'ятнадцяти потребує негайних дій. Критичний ризик понад п'ятнадцять балів вимагає пріоритетного реагування та може потребувати тимчасового припинення операцій.

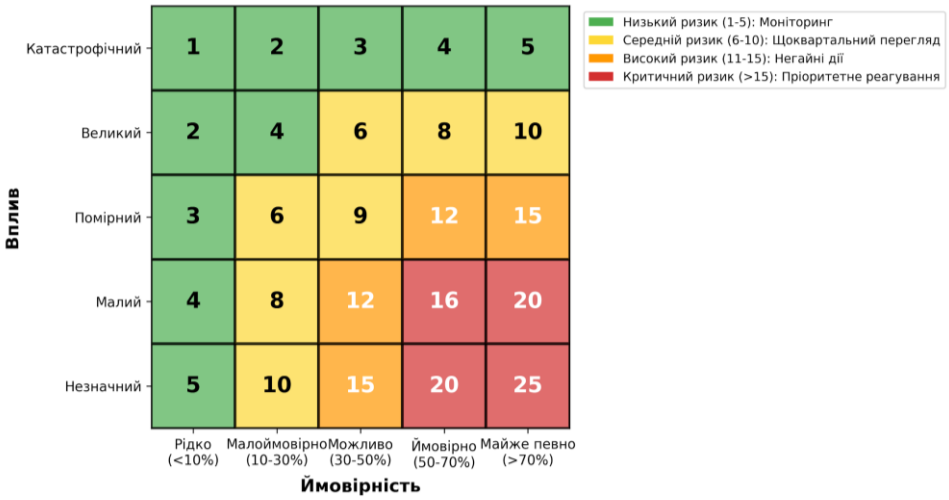

Рис. 1.2 Матриця оцінювання ризиків за шкалою 5×5

Методології та стандарти проведення аудиту

Серед сучасних методологій проведення аудиту кіберзахищеності особливе місце посідає NIST Cybersecurity Framework, який у 2024 році отримав суттєве оновлення до версії 2.0 [18]. Ключовою зміною стало додавання шостої функції Govern, яка охоплює питання управління кібербезпекою на стратегічному рівні організації та забезпечує інтеграцію кібербезпеки з бізнес-процесами.

Шість функцій NIST CSF 2.0 формують повний цикл управління кібербезпекою. Функція Govern встановлює та моніторить стратегію управління ризиками кібербезпеки організації, включаючи політики, процеси та процедури. Вона охоплює компоненти GV.RM для стратегії управління ризиками, GV.RR для визначення ролей та відповідальності, GV.PO для політик організації та GV.SC для управління ризиками ланцюга постачання. Функція Identify забезпечує розуміння організацією своїх активів, бізнес-середовища та ризиків кібербезпеки через інвентаризацію активів, оцінку ризиків та аналіз бізнес-контексту. Функція Protect впроваджує захисні заходи для забезпечення надання критичних послуг, включаючи контроль доступу, захист даних та підвищення обізнаності персоналу. Функція Detect розробляє та впроваджує відповідні заходи для виявлення подій безпеки через безперервний моніторинг та процеси виявлення аномалій. Функція Respond визначає дії щодо виявлених

подій безпеки, включаючи планування реагування, комунікації та пом'якшення наслідків. Функція Recover підтримує плани відновлення та своєчасне повернення до нормальних операцій після інциденту.

Оцінка зрілості за методологією NIST передбачає чотири рівні (Implementation Tiers), які відображають ступінь інтеграції практик кібербезпеки в діяльність організації. Характеристики кожного рівня наведено в таблиці 1.3.

Таблиця 1.3

Рівні зрілості за методологією NIST CSF 2.0

Рівень	Характеристика	Оцінка	Рекомендації
Рівень 1: Частковий	Реактивний підхід, відсутність формалізованих процесів, ad-hoc рішення	1-25 балів	Термінові дії
Рівень 2: Усвідомлення ризиків	Ризик-орієнтований підхід, часткова формалізація, обмежена обізнаність	26-50 балів	Покращення
Рівень 3: Повторюваний	Формальні процеси, регулярний моніторинг, документовані процедури	51-75 балів	Оптимізація
Рівень 4: Адаптивний	Проактивний підхід, безперервне вдосконалення, інтеграція з бізнесом	76-100 балів	Підтримка

Інтегральна оцінка за методологією NIST розраховується як середнє арифметичне показників за всіма шістьма функціями:

$$NIST_{Score} = \frac{GV + ID + PR + DE + RS + RC}{6} \quad (1.4)$$

де GV - оцінка функції Govern, ID - Identify, PR - Protect, DE - Detect, RS - Respond, RC - Recover. Кожна функція оцінюється за стобальною шкалою на основі аналізу відповідних підкатегорій та контролів.

Стандарт IEC 62443 спеціально розроблений для промислових систем автоматизації та контролю (Industrial Automation and Control Systems, IACS) і визначає комплексний підхід до забезпечення їх кібербезпеки [19]. На відміну від універсальних стандартів, IEC 62443 враховує специфіку промислового середовища, де безперервність операцій та безпека людей мають найвищий пріоритет.

Стандарт визначає чотири рівні безпеки (Security Levels), які відповідають різним рівням загроз. SL1 забезпечує захист від випадкових порушень та ненавмисних помилок. SL2 захищає від простих умисних атак з використанням базових інструментів та методів. SL3 протидіє складним атакам з використанням спеціалізованих інструментів та глибоких знань системи. SL4 забезпечує захист від атак державного рівня з необмеженими ресурсами та можливостями. Для більшості об'єктів критичної інфраструктури рекомендується досягнення рівня SL3, тоді як SL4 застосовується для особливо важливих об'єктів національного значення.

Серцевиною стандарту є сім базових вимог (Foundational Requirements), кожна з яких деталізується через системні вимоги (System Requirements). Структура базових вимог наведена в таблиці 1.4.

Таблиця 1.4

Базові вимоги (Foundational Requirements) стандарту IEC 62443-3-3

FR	Назва вимоги	Опис	Кількість SR
FR1	Identification & Authentication	Ідентифікація та автентифікація	13 вимог (SR 1.1-1.13)
FR2	Use Control	Контроль використання	12 вимог (SR 2.1-2.12)
FR3	System Integrity	Цілісність системи	9 вимог (SR 3.1-3.9)
FR4	Data Confidentiality	Конфіденційність даних	3 вимоги (SR 4.1-4.3)
FR5	Restricted Data Flow	Обмеження потоків даних	4 вимоги (SR 5.1-5.4)
FR6	Timely Response	Своєчасне реагування	2 вимоги (SR 6.1-6.2)
FR7	Resource Availability	Доступність ресурсів	8 вимог (SR 7.1-7.8)

Розрахунок відповідності стандарту IEC 62443 здійснюється за формулою з урахуванням вагових коефіцієнтів системних вимог:

$$IEC_{Compliance} = \frac{\Sigma(FR_i \times w_i)}{\Sigma w_i} \times 100\% \quad (1.5)$$

де FR_i - оцінка виконання і-ї системної вимоги (0 - не виконано, 1 - виконано), w_i - вага вимоги, яка залежить від цільового рівня безпеки та критичності вимоги. Для рівня SL3 більшість вимог мають вагу 2 або 3, тоді як для SL2 переважають ваги 1 та 2.

Цільовий рівень безпеки для конкретного об'єкта визначається як максимум із трьох значень:

$$Target_{SL} = \max(SL_{Threats}, SL_{Regulatory}, SL_{Business}) \quad (1.6)$$

де SL_Threats - рівень безпеки, необхідний для протидії актуальним загрозам на основі аналізу ландшафту загроз, SL_Regulatory - рівень, що вимагається регуляторними документами для даного типу об'єктів, SL_Business - рівень, визначений бізнес-вимогами та толерантністю до ризику організації.

Архітектура промислових систем управління традиційно описується за допомогою моделі Purdue, яка визначає шість рівнів від фізичного процесу до корпоративної мережі, що проілюстровано на рисунку 1.3. Ключовим елементом моделі є чітке розмежування зон IT та OT через демілітаризовану зону (DMZ) на третьому рівні. Така архітектура забезпечує контрольований обмін даними між корпоративними та промисловими системами при мінімізації ризиків проникнення загроз з корпоративної мережі до систем управління технологічними процесами.

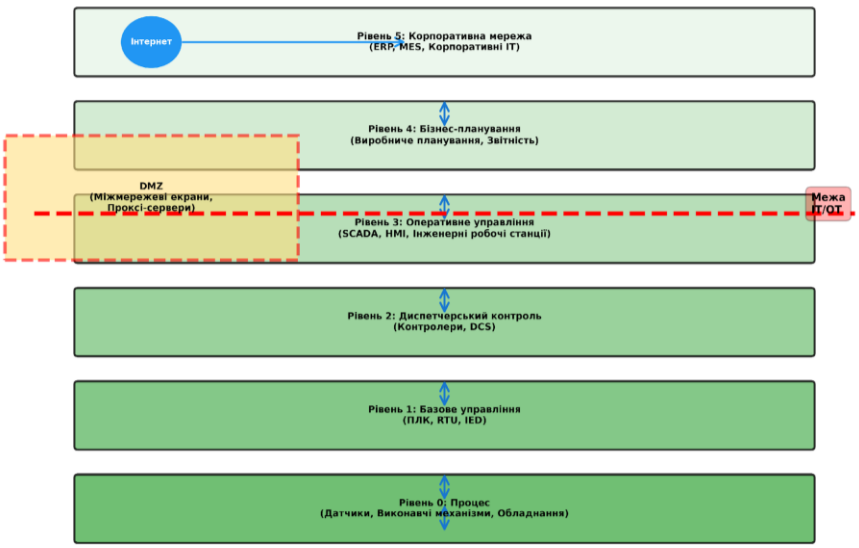

Рис. 1.3 Архітектура промислових систем управління (модель Purdue)

Фази проведення аудиту кіберзахищеності

Повний цикл аудиту кіберзахищеності об'єкта критичної інфраструктури складається з п'яти послідовних фаз, кожна з яких має специфічні цілі, методи

та результати. Правильне планування та виконання кожної фази є критичним для досягнення достовірних результатів аудиту.

Фаза планування та підготовки займає від десяти до п'ятнадцяти відсотків загального часу аудиту. На цьому етапі визначається обсяг та межі аудиту (scope), формується команда аудиторів з необхідними компетенціями, узгоджується методологія та критерії оцінювання, розробляється детальний план аудиту з графіком робіт, підготовлюється необхідна документація включаючи форми опитування та чек-листи. Результатом фази є затверджений план аудиту з чітко визначеними цілями, обсягом, ресурсами та термінами.

Фаза збору інформації потребує від двадцяти п'яти до тридцяти відсотків часу та є найбільш інформаційно насиченою. Вона включає документальний аналіз існуючих політик, процедур, архітектурних схем та попередніх звітів. Проводиться інтерв'ювання ключового персоналу включаючи керівництво, адміністраторів систем та операторів. Виконується технічне сканування мережевої інфраструктури, при цьому для промислових систем переважно використовуються пасивні методи, що не впливають на роботу обладнання. Збираються дані про конфігурації систем, журнали подій та інциденти безпеки.

Фаза аналізу та тестування є найбільш трудомістким етапом, що займає від тридцяти до тридцяти п'яти відсотків часу. На цьому етапі проводиться Gap Analysis - порівняння поточного стану з вимогами стандартів та найкращими практиками. Виконується оцінка вразливостей (Vulnerability Assessment) з використанням методології CVSS для визначення критичності. Проводиться тестування ефективності контролів безпеки через перевірку їх фактичного функціонування. Для некритичних систем може проводитися тестування на проникнення (Penetration Testing) для виявлення реальних векторів атак.

Фаза оцінки ризиків потребує від п'ятнадцяти до двадцяти відсотків часу та спрямована на систематизацію виявлених проблем. Проводиться інтегральна оцінка ризиків з урахуванням ймовірності та впливу кожної загрози. Будується матриця ризиків для візуалізації та комунікації результатів керівництву.

Виконується пріоритизація виявлених вразливостей та формуються рекомендації щодо їх усунення з урахуванням наявних ресурсів та обмежень.

Фаза звітування займає від десяти до п'ятнадцяти відсотків загальної тривалості аудиту. Готується Executive Summary для вищого керівництва з ключовими висновками та рекомендаціями. Розробляється детальний технічний звіт з описом всіх виявлених проблем та доказами. Формується матриця відповідності вимогам стандартів (Compliance Matrix). Розробляється план усунення недоліків (Remediation Plan) з термінами та відповідальними особами.

Метрики та ключові показники ефективності аудиту

Для вимірювання ефективності процесу аудиту та стану кібербезпеки об'єкта використовуються спеціалізовані метрики та ключові показники ефективності (KPI). Ці показники дозволяють об'єктивно оцінити якість проведеного аудиту, поточний рівень захищеності та прогрес у впровадженні рекомендацій.

Показник охоплення аудиту (Audit Coverage) визначає повноту перевірки критичних активів організації:

$$Audit_{Coverage} = \left(\frac{Audited_{Assets}}{Total_{CriticalAssets}}\right) \times 100\% \qquad (1.7)$$

Цільове значення цього показника має становити не менше дев'яноста п'яти відсотків для критичних активів. Нижче значення свідчить про наявність непокритих зон, які можуть містити невиявлені вразливості та ризики.

Оцінка відповідності за результатами gap-аналізу показує ступінь виконання вимог обраного стандарту:

$$Gap_{Compliance} = \left(\frac{Compliant_{Controls}}{Total_{Controls}}\right) \times 100\% \qquad (1.8)$$

Ефективність впроваджених контролів безпеки визначається як відношення кількості контролів, що функціонують належним чином, до загальної кількості впроваджених контролів:

$$Control_{Effectiveness} = \left(\frac{Effective_{Controls}}{Total_{Controls}}\right) \times 100\% \qquad (1.9)$$

Цільове значення ефективності контролів має досягати щонайменше вісімдесяти п'яти відсотків. Нижчі значення свідчать про проблеми з впровадженням, конфігурацією або супроводом засобів захисту.

Середній час встановлення патчів (Mean Time to Patch, MTTP) є важливим операційним показником, що відображає оперативність реагування на виявлені вразливості:

$$MTTP = \frac{\Sigma(Patch_{Date} - Discovery_{Date})}{Vulnerabilities_{Count}} \quad (1.10)$$

Рекомендоване значення MTTP не повинно перевищувати чотирнадцяти днів для критичних вразливостей, тридцяти днів для вразливостей високого рівня та дев'яноста днів для вразливостей середнього рівня.

Комплексна оцінка ризику з урахуванням множинних загроз та їх вагових коефіцієнтів розраховується за формулою:

$$Risk_{Score} = \Sigma(P_i \times I_i \times w_i) \quad (1.11)$$

де P_i - ймовірність реалізації і-ї загрози, I_i - потенційний вплив, w_i - ваговий коефіцієнт загрози, що визначається її значимістю для організації.

Залишковий ризик після впровадження заходів захисту дозволяє оцінити ефективність застосованих контролів:

$$Residual_{Risk} = Initial_{Risk} \times (1 - Control_{Effectiveness}) \quad (1.12)$$

Показник відповідності регуляторним вимогам є критичним для об'єктів критичної інфраструктури:

$$Compliance_{Rate} = \left(\frac{Compliant_{Requirements}}{Total_{Requirements}}\right) \times 100\% \quad (1.13)$$

Інтерпретація результатів: значення від дев'яноста до ста відсотків свідчить про відмінний стан відповідності, від вісімдесяти до вісімдесяти дев'яти - добрий стан із незначними недоліками, від сімдесяти до сімдесяти дев'яти - задовільний стан, що потребує покращень, нижче сімдесяти відсотків - незадовільний стан, що може призвести до санкцій регулятора.

1.3. Нормативно-правові та міжнародні стандарти для оцінювання рівня кіберзахищеності об'єктів критичної інфраструктури

Міжнародні стандарти кібербезпеки

Міжнародна система стандартизації у сфері кібербезпеки критичної інфраструктури представлена кількома ключовими документами, що взаємно доповнюють один одного та формують комплексну основу для побудови системи захисту. Вибір конкретних стандартів залежить від галузевої специфіки об'єкта, регуляторних вимог та бізнес-контексту організації.

Стандарт ISO/IEC 27001 у редакції 2022 року встановлює вимоги до систем управління інформаційною безпекою (ISMS) та є найбільш універсальним документом у цій сфері [24]. Оновлена версія містить дев'яносто три контролі, організовані у чотири категорії: тридцять сім організаційних контролів охоплюють політики, ролі, відповідальність та управління активами; тридцять чотири технологічні контролі включають захист мережі, криптографію та безпеку додатків; вісім людських контролів стосуються навчання, дисципліни та awareness-програм; чотирнадцять фізичних контролів забезпечують захист периметру та обладнання.

Процес сертифікації за ISO 27001 складається з дев'яти етапів: gap-аналіз тривалістю два-чотири тижні, розробка документації ISMS протягом двох-трьох місяців, впровадження контролів за три-шість місяців, внутрішній аудит протягом двох-чотирьох тижнів, Stage 1 audit (документаційний) тривалістю один-два дні, Stage 2 audit (впровадження) за два-п'ять днів, отримання сертифікату протягом чотирьох-шести тижнів, щорічні наглядові аудити та ресертифікація кожні три роки.

Стандарт ISO/IEC 27005:2022 визначає процес управління ризиками інформаційної безпеки та включає п'ять етапів: встановлення контексту, ідентифікація ризиків, аналіз ризиків, оцінка ризиків та обробка ризиків. Базова формула оцінки ризику за цим стандартом:

$$R = I \times P \quad (1.14)$$

де R - рівень ризику, I - вплив (Impact) за шкалою від одного до п'яти, P - ймовірність (Probability) також за шкалою від одного до п'яти. Обробка ризику може здійснюватися чотирма способами: модифікація через впровадження контролів, утримання при прийнятному рівні ризику, уникнення через відмову від ризикованої діяльності, розподіл через страхування або передачу третій стороні.

Американський стандарт NIST SP 800-53 у п'ятій редакції містить найбільш повний каталог контролів безпеки, організованих у двадцять сімейств. Стандарт визначає три базові рівні: LOW із ста двадцятьма п'ятьма контролями для систем низької критичності, MODERATE із трьомастами двадцятьма п'ятьма контролями для більшості державних систем, та HIGH із чотирмастами двадцятьма одним контролем, рекомендований для систем критичної інфраструктури. Особливо важливими для промислових систем є сімейства Access Control із двадцятьма п'ятьма контролями, Contingency Planning із тринадцятьма контролями, Incident Response із десятьма контролями, Physical and Environmental Protection із двадцятьма трьома контролями та System and Information Integrity із двадцятьма трьома контролями.

Для енергетичного сектору Північної Америки застосовуються обов'язкові стандарти NERC CIP (Critical Infrastructure Protection), які включають тринадцять стандартів від CIP-002 до CIP-014. Ключові вимоги охоплюють ідентифікацію критичних активів (CIP-002), управління безпекою (CIP-003), періодичну оцінку вразливостей (CIP-010) та управління ризиками ланцюга постачання (CIP-013). За порушення вимог передбачені штрафи до одного мільйона доларів на день.

Європейські директиви та регламенти

Європейське регулювання у сфері кібербезпеки критичної інфраструктури зазнало суттєвих змін із прийняттям директиви NIS2 у 2022 році, яка замінила попередню директиву NIS1 від 2016 року [28]. Порівняння ключових аспектів двох директив наведено в таблиці 1.5.

Таблиця 1.5

Порівняння директив NIS1 та NIS2

Аспект	NIS1 (2016)	NIS2 (2022)
Охоплення секторів	7 секторів	18 секторів (включно з держуправлінням)
Категорії суб'єктів	OES (оператори essential services)	Essential + Important entities
Штрафні санкції	Визначаються державами-членами	До €10M або 2% глобального обороту
Термін звітування	72 години	24 години (early warning), 72 години (повний)
Supply chain	Обмежені вимоги	Обов'язкове управління ризиками
Відповідальність керівництва	Не визначена	Персональна відповідальність топ-менеджменту

Директива NIS2 значно розширила коло суб'єктів регулювання, включивши вісімнадцять секторів замість семи. Нові сектори охоплюють виробництво, поштові послуги, управління відходами, виробництво продуктів харчування, цифрові провайдери та державне управління. Організації поділяються на дві категорії: essential entities (суттєві суб'єкти) та important entities (важливі суб'єкти), з різними вимогами та санкціями.

Стаття 21 директиви NIS2 встановлює одинадцять обов'язкових заходів з кібербезпеки: політики аналізу ризиків та безпеки інформаційних систем, управління інцидентами включаючи запобігання та реагування, безперервність бізнесу та управління кризовими ситуаціями, безпека ланцюга постачання, безпека при придбанні та розробці систем, політики оцінки ефективності заходів кібербезпеки, базові практики кібергігієни та навчання персоналу, політики використання криптографії, безпека людських ресурсів та політики контролю доступу, використання багатофакторної автентифікації та захищених комунікацій.

Для essential entities максимальний штраф становить десять мільйонів євро або два відсотки глобального річного обороту. Для important entities - сім мільйонів євро або 1.4 відсотка обороту. Крім того, директива вводить персональну відповідальність керівництва організації за невиконання вимог кібербезпеки.

Для фінансового сектору Європейський Союз прийняв регламент DORA (Digital Operational Resilience Act), який набуває чинності у січні 2025 року [29]. Регламент встановлює п'ять ключових вимог: створення повноцінної системи управління ризиками інформаційно-комунікаційних технологій (ICT risk management framework), впровадження процесів управління інцидентами та звітування, проведення тестування цифрової стійкості включаючи Threat-Led Penetration Testing (TLPT) для системно важливих установ, управління ризиками третіх сторін та постачальників ІСТ-послуг, участь в обміні інформацією про загрози та вразливості.

Національне законодавство України

Національне законодавство України у сфері захисту критичної інфраструктури активно розвивається, враховуючи як міжнародний досвід, так і специфічні виклики воєнного часу. Базовим документом є Закон України «Про критичну інфраструктуру» від 16 листопада 2021 року № 1882-IX [31].

Закон визначає одинадцять секторів критичної інфраструктури України: енергетика включаючи електроенергетику, нафтогазовий комплекс та атомну енергетику; хімічна промисловість; транспорт усіх видів; інформаційно-комунікаційні технології; електронні комунікації та зв'язок; банківський та фінансовий сектор; охорона здоров'я; забезпечення життєдіяльності населення включаючи водопостачання та теплопостачання; харчова промисловість та агропромисловий комплекс; оборонно-промисловий комплекс; космічна галузь.

Критерії віднесення об'єктів до критичної інфраструктури визначені статтею 6 Закону та включають масштаб потенційних наслідків порушення функціонування, наявність міжгалузевої залежності від об'єкта, кількість споживачів послуг або продукції та державне значення об'єкта для забезпечення національної безпеки.

Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII визначає суб'єктів забезпечення кібербезпеки [26]. До них належать Державна служба спеціального зв'язку та захисту інформації України (ДССЗЗІ) як головний орган, Національна поліція

для розслідування кіберзлочинів, Служба безпеки України та Головне управління розвідки для протидії кібершпигунству, Національний банк України для фінансового сектору.

Постанова Кабінету Міністрів України № 518 від 19 червня 2024 року «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» конкретизує мінімальні технічні та організаційні вимоги [22]. Документ встановлює чіткі терміни впровадження заходів: організаційні вимоги включаючи призначення відповідальних осіб, розробку політик та проведення аудитів мають бути виконані протягом шести місяців; технічні вимоги включаючи сегментацію мережі, впровадження моніторингу, антивірусного захисту та резервного копіювання - протягом дванадцяти місяців; вимоги щодо персоналу включаючи навчання та перевірку надійності - протягом шести місяців; система управління інцидентами включаючи план реагування та формування команди - протягом дев'яти місяців.

Показник відповідності вимогам Постанови КМУ № 518 розраховується з урахуванням вагових коефіцієнтів різних категорій вимог:

$$Compliance_{Score} = \frac{\Sigma(C_i \times W_i)}{\Sigma W_i} \times 100\% \qquad (1.16)$$

де C_i - виконання і-ї вимоги (0 - не виконано, 1 - виконано), W_i - вага вимоги за шкалою від одного до п'яти, де п'ять відповідає критичним вимогам з найвищим пріоритетом.

Гармонізація стандартів при проведенні аудиту

При проведенні аудиту об'єктів критичної інфраструктури, що підпадають під дію кількох стандартів та регуляторних документів одночасно, виникає необхідність гармонізації вимог для уникнення дублювання зусиль та забезпечення комплексного покриття. Матриця відповідності ключових контролів основним стандартам наведена в таблиці 1.6.

Таблиця 1.6

Матриця відповідності ключових контролів стандартам

Контроль	ISO 27001	IEC 62443	NIST CSF	NIS2
Багатофакторна автентифікація	5.17, 8.5	SR 1.5	PR.AC-7	Ст. 21(j)
Сегментація мережі	8.20, 8.22	SR 5.1	PR.AC-5	Ст. 21
Управління патчами	8.8	SR 3.3	PR.IP-12	Ст. 21
Безперервний моніторинг	8.15, 8.16	SR 6.1	DE.CM-1	Ст. 21
Управління інцидентами	5.24-5.28	SR 6.2	RS.RP-1	Ст. 23
Резервне копіювання	8.13	SR 7.3	PR.IP-4	Ст. 21(c)

Інтегрований набір контролів для комплексного аудиту формується як об'єднання вимог усіх застосовних стандартів із застосуванням принципу найсуворіших вимог у випадку розбіжностей:

$$Unified_{ControlSet} = \bigcup(ISO27001 \cup IEC62443 \cup NIST \cup NIS2) \quad (1.17)$$

Практична реалізація гармонізації передбачає кілька кроків. Спочатку визначаються всі застосовні стандарти та регуляторні вимоги для конкретного об'єкта. Потім будується матриця відповідності, що зіставляє контролі різних стандартів. Далі формується єдиний перелік контролів із вибором найсуворіших вимог. Нарешті проводиться оцінка відповідності за єдиним переліком із формуванням звітів для кожного стандарту окремо.

Висновки до розділу 1

Досліджено теоретичні основи оцінювання рівня кіберзахищеності об'єктів критичної інфраструктури (ОКІ) та проаналізовано сучасний стан нормативно-правового забезпечення у цій сфері. Встановлено, що питання комплексної оцінки кіберзахищеності ОКІ набуває особливої актуальності в умовах зростання кількості та складності кібератак на критичну інфраструктуру України.

- Вивчено сутність та класифікацію об'єктів критичної інфраструктури відповідно до Закону України «Про критичну інфраструктуру».

Виокремлено 11 секторів КІ (енергетика, транспорт, ІКТ, банківський сектор, охорона здоров'я та інші) та встановлено критерії віднесення об'єктів до категорій критичності. Обґрунтовано, що специфіка кожного сектору визначає унікальні вимоги до оцінювання кіберзахищеності.

- Проаналізовано таксономію вразливостей об'єктів критичної інфраструктури. Систематизовано вразливості за категоріями: технічні (застаріле програмне забезпечення, відсутність оновлень, слабкі паролі), організаційні (недостатня обізнаність персоналу, відсутність політик безпеки), архітектурні (незахищені протоколи, відсутність сегментації мережі) та специфічні для промислових систем (вразливості SCADA/ICS).
- Визначено концептуальні основи та методології аудиту кібербезпеки ОКІ. Проаналізовано відмінності між аудитом відповідності (compliance audit), технічним аудитом та аудитом ризиків. Обґрунтовано доцільність комбінованого підходу, що поєднує всі три типи для отримання комплексної оцінки. Детально розглянуто фази проведення аудиту: планування, збір інформації, аналіз, оцінка та формування звіту.
- Систематизовано міжнародні стандарти кібербезпеки, застосовні до ОКІ: ISO/IEC 27001 (система управління інформаційною безпекою), IEC 62443 (безпека промислових систем автоматизації), NIST Cybersecurity Framework (управління кіберризиками). Проаналізовано європейські директиви NIS та NIS2, що встановлюють вимоги до кібербезпеки операторів основних послуг.
- Досліджено національне законодавство України у сфері кібербезпеки КІ: Закон «Про основні засади забезпечення кібербезпеки України», Закон «Про критичну інфраструктуру», НД ТЗІ та галузеві нормативні акти. Виявлено необхідність гармонізації національних вимог з міжнародними стандартами та розробки практичних методик оцінювання кіберзахищеності.
- Встановлено, що існуючі підходи до оцінювання кіберзахищеності ОКІ переважно зосереджені на перевірці відповідності нормативним вимогам

та не забезпечують комплексної кількісної оцінки рівня захищеності. Обґрунтовано необхідність розробки системи ключових показників ефективності (KPI) та ризиків (KRI) для об'єктивного вимірювання стану кіберзахищеності.

РОЗДІЛ 2 ФОРМУВАННЯ СИСТЕМИ КЛЮЧОВИХ ПОКАЗНИКІВ KPI ТА KRI

2.1 Методологія побудови системи ключових показників ефективності та ризиків (KPI/KRI) для оцінювання рівня кіберзахищеності об'єктів критичної інфраструктури

2.1.1 KPI

Захист конфіденційних даних має ключове значення для будь-якої компанії. Будь-яка витока інформації може призвести до руйнівних наслідків: шкода репутації, фінансові втрати, втрата ринкових позицій, відтік клієнтів тощо. Внутрішня система кібербезпеки повинна забезпечувати надійний захист даних, а також бути проактивною – вчасно виявляти та запобігати кібератакам.

Для відстеження рівня кібербезпеки необхідно мати чек-лист та аналізувати KPI. Ключові показники ефективності (KPI) є ефективним способом вимірювання успіху та результативності будь-якої програми, включаючи кібербезпеку. Без аналізу роботи системи кібербезпеки неможливо оцінити реальний стан безпеки та рівень захисту [1].

Кіберзлочинці динамічно розвиваються та постійно винаходять нові і більш складні методи атак. Відповідно змінюються процеси та технології для їх запобігання. Важливо регулярно оцінювати ефективність інструментів захисту та вчасно замінювати та/або оновлювати застарілі засоби.

Аналіз ключових показників ефективності (KPI), ключових показників ризику (KRI) та заходів безпеки дозволяє отримати повну картину роботи команди безпеки, зрозуміти, що працює, а що не працює, та вжити відповідних заходів. Метрики надають кількісну інформацію, яку можна легко скласти у звіт та поділитися з усіма зацікавленими сторонами.

Важливість та переваги KPI [2]

KPI відіграють вирішальну роль у досягненні організаційного успіху та покращенні продуктивності. Ось деякі ключові переваги використання KPI:

- Вимірювані цілі: KPI забезпечують спосіб встановлення конкретних, вимірюваних цілей, які узгоджуються з організаційними завданнями. Чітко визначаючи, як виглядає успіх, організації можуть зосередити свої зусилля та відстежувати прогрес.
- Стратегічне узгодження: KPI гарантують, що дії та активності узгоджені із загальними стратегічними пріоритетами. Відстежуючи правильні метрики, організації можуть залишатися на правильному шляху та вносити корективи за необхідності.
- Моніторинг ефективності: KPI дозволяють організаціям контролювати продуктивність та відстежувати прогрес з часом. Регулярний перегляд KPI може допомогти виявити тенденції, закономірності та сфери для покращення. Це дозволяє організаціям приймати обґрунтовані рішення та вживати коригувальних заходів у разі потреби.
- Прийняття рішень на основі даних: Використовуючи KPI, організації можуть приймати рішення на основі даних, спираючись на об'єктивні вимірювання, а не на припущення чи інтуїцію. Це покращує точність та ефективність процесів прийняття рішень.
- Підвищення ефективності: KPI виділяють сфери неефективності або вузькі місця в процесах, дозволяючи організаціям виявляти можливості для покращення. Зосереджуючись на цих сферах, організації можуть підвищити ефективність, знизити витрати та оптимізувати ресурси.
- Підзвітність та прозорість: KPI створюють культуру підзвітності, забезпечуючи чіткі очікування та метрики для вимірювання продуктивності. Це сприяє прозорості та дає змогу окремим особам та командам брати на себе відповідальність за свої обов'язки.

Приклади KPI

KPI можуть значно відрізнятися залежно від галузі, організації та конкретних цілей. Ось деякі приклади часто використовуваних KPI:

- Дохід: Вимірює загальний дохід, отриманий організацією за певний період.
- Задоволеність клієнтів: Оцінює рівень задоволеності серед клієнтів та їхнє сприйняття продуктів або послуг організації.
- Коефіцієнт конверсії продажів: Вимірює відсоток потенційних клієнтів або можливостей, які призводять до продажу.
- Показник плинності кадрів: Обчислює відсоток працівників, які залишають організацію протягом певного періоду часу.
- Трафік веб-сайту: Відстежує кількість відвідувачів та переглядів сторінок на веб-сайті.
- Доставка вчасно: Вимірює відсоток замовлень або проєктів, доставлених вчасно.
- Індекс Net Promoter Score: Оцінює лояльність клієнтів та готовність рекомендувати організацію іншим.
- Показник інцидентів безпеки: Обчислює кількість інцидентів або нещасних випадків з безпекою на визначену одиницю роботи або часу.

Це лише кілька прикладів, і організації можуть визначити свій власний унікальний набір KPI на основі своїх стратегічних цілей та галузевих еталонів.

Критика та суперечки

Хоча KPI широко використовуються та визнані цінними інструментами, існує певна критика та суперечки, пов'язані з їх впровадженням:

- Надмірний акцент на числових метриках: Критики стверджують, що надмірна увага до числових метрик може призвести до вузького прийняття рішень та нехтування іншими важливими аспектами продуктивності та організаційного здоров'я.
- Неузгодженість зі стратегією: Якщо KPI не узгоджені зі стратегічними пріоритетами організації, вони можуть стимулювати поведінку,

яка суперечить довгостроковим цілям. Важливо регулярно переглядати та оновлювати KPI, щоб забезпечити їхню релевантність та узгодженість.

- Складність вимірювання комплексних концепцій: Деякі організаційні цілі, такі як інновації або залученість працівників, важко виміряти точно. KPI можуть не повністю відображати багатовимірну природу цих концепцій.
- Маніпуляції та зловживання: У деяких випадках працівники або команди можуть маніпулювати KPI для досягнення короткострокових вигод або виконання цільових показників без фактичного покращення загальної продуктивності.

Щоб пом'якшити цю критику та суперечки, організації повинні ретельно розробляти та впроваджувати свої KPI, враховуючи ширший контекст та застосовуючи збалансований підхід.

Підсумовуючи, Ключові показники ефективності (KPI) є важливими інструментами для організацій для вимірювання їхнього прогресу та продуктивності. Визначаючи та відстежуючи правильні метрики, організації можуть узгоджувати свою діяльність зі стратегічними цілями, контролювати прогрес та приймати рішення на основі даних. Хоча існують виклики та суперечки, пов'язані з використанням KPI, їхні переваги переважають недоліки, коли вони впроваджуються обдумано та відповідно до стратегії організації.

Ключові показники ефективності кібербезпеки:

- Рівень готовності – визначення кількості справних та оновлених пристроїв, сканування на вразливості та управління ними;
- Неідентифіковані пристрої у внутрішніх мережах – виявлення вторгнень у мережу (працівники можуть підвищувати кіберризики та становити загрозу, використовуючи власні пристрої та погано налаштовані IoT-пристрої);
- Спроби вторгнення – кількість спроб зловмисників отримати несанкціонований доступ;
- Інцидент безпеки – кількість порушень інформаційних активів та/або порушень мережі;

- Середній час виявлення (MTTD) – це середній час, необхідний для ідентифікації загрози після її першого потрапляння в середовище. Він відображає наскільки ефективними є ваша логіка виявлення, охоплення журналювання та процеси кореляції сигналів на практиці. Низький MTTD обмежує час, який зловмисник має для бічного переміщення, вилучення даних або експлуатації інших систем.

Щоб обчислити MTTD, віднімiть час початкового компрометування від часу виявлення для кожного інциденту, а потім усередніть це:

$$MTTD = \frac{\sum(\text{Час виявлення} - \text{Час порушення})}{\text{Кількість інцидентів}}, \quad (2.1)$$

Наприклад, якщо три порушення були виявлені через 40, 25 і 35 хвилин після компрометування, MTTD становить:

$$MTTD = \frac{40 + 25 + 35}{3} = 33{,}3\text{хвилин}, \quad (2.2)$$

Команди можуть відстежувати MTTD через централізовані конвеєри журналювання та оповіщення, часто посилені безперервним моніторингом експозиції загроз (CTEM). Постійно високий MTTD вказує на сліпі зони у видимості або неправильно розставлені пріоритети сигналів і повинен ініціювати покращення в інженерії виявлення, логіці кореляції або картуванні аналізу загроз [4].

- Середній час усунення (MTTR) – MTTR вимірює середній час, необхідний для повного стримування та усунення загрози після її виявлення. Він відображає реальну гнучкість вашого життєвого циклу реагування на інциденти, від сортування до пом'якшення наслідків і відновлення. Високий MTTR безпосередньо корелює з тривалим періодом ризику для бізнесу та вищими витратами на інциденти.

Щоб обчислити MTTR, віднімiть час виявлення від часу завершення повного усунення для кожного інциденту, а потім візьміть середнє значення:

$$MTTR = \frac{\sum(\text{Час усунення} - \text{Час виявлення})}{\text{Кількість інцидентів}}, \quad (2.3)$$

Наприклад, якщо три загрози були усунені через 60, 45 і 75 хвилин після виявлення:

$$MTTR = \frac{60 + 45 + 75}{3} = 60 \text{ хвилин}, \quad (2.4)$$

Організації, які відстежують це через хронології інцидентів у програмах СТЕМ або системах тікетів, можуть виявити повторювані вузькі місця, такі як затримки в передачі відповідальності або етапах затвердження. Низький MTTR – це не лише швидкість; він відображає зрілість у виконанні плейбуків, комунікації та валідації після інциденту.

- Середній час стримування показує час реагування компанії та здатність оцінювати стан її кібербезпеки;
- Рейтинги безпеки – оцінка ризиків кібербезпеки, виявлення показників інформаційної безпеки, які потребують уваги;
- Середній рейтинг безпеки третіх сторін;
- Частота встановлення патчів – час на впровадження патчів безпеки додатків та/або виправлення вразливостей високого ризику;
- Контроль доступу та аналіз доступу (який користувач має права адміністратора);
- Оцінка ризиків третіх сторін та потенційних вразливостей;
- Час реагування третьої сторони на інцидент. Інцидент безпеки – це успішна кібератака. Однак ціллю також може бути компанія, до якої кіберзлочинці намагаються отримати доступ через третю сторону. Чим довше партнер реагує на інцидент, тим більша ймовірність того, що компанія постраждає від витоку даних.

Не існує загального рішення щодо того, які метрики використовувати. Кожна компанія обирає KPI та KRI залежно від сфери діяльності, потреб компанії, правил, настанов, бачення ризиків керівництвом тощо. Важливо, щоб обрані метрики були зрозумілими для всіх, включаючи нетехнічних фахівців, відображали поточну ситуацію та допомагали приймати рішення щодо кібербезпеки компанії.

2.1.2 KRI

Ключові показники ризику (KRI) – це критичні метрики, які використовуються керівниками служб безпеки та командами управління ризиками для моніторингу та вимірювання рівня кіберризиків [3].

KRI можна використовувати для відстеження змін у профілі ризиків вашої організації, отримання інформації про вразливості в апараті безпеки або цифровому середовищі, а також для підтримки постійного моніторингу ризиків між аудитами безпеки.

KRI часто плутають з ключовими показниками ефективності (KPI), але між ними є різниця. KRI дозволяють відстежувати та кількісно оцінювати кіберризик, щоб ви могли швидко вжити коригувальних заходів. KPI, з іншого боку, вимірює ефективність безпеки, прогрес у досягненні цілей та тенденції з плином часу.

Розглянемо п'ять KRI, які ви повинні відстежувати, щоб зрозуміти потенційні ризики, з якими стикається ваша організація.

1. Обсяг вашої поверхні атаки

Важливим KPI є знання того, де ризик прихований у вашому цифровому середовищі. Але оскільки ваш бізнес розширюється в хмару, охоплюючи бізнес-підрозділи, географічні регіони та віддалені локації, може бути складно виявити та перевірити ваш цифровий слід, ідентифікувати потенційний ризик та визначити пріоритети усунення.

Одним із способів отримання цього розуміння є використання інструменту виявлення та звітності, такого як сканування поверхні атаки. Ця технологія автоматично та безперервно веде облік ваших цифрових активів, далеко за межами традиційного периметра мережі. Результати представлені у вигляді інформаційних панелей, активи визначаються за місцезнаходженням, а зони концентрованого ризику виділяються, щоб ви могли швидко вжити заходів щодо їх усунення.

KRI для моніторингу включають:

- Раніше невідомі екземпляри хмарних сервісів або тіньові IT та стан ризику цих активів.
- Бізнес-підрозділи, дочірні компанії або віддалені офіси, які не дотримуються корпоративних політик безпеки.
- Профіль ризику критичних цифрових активів, таких як хмарний екземпляр, який зберігає конфіденційні дані.
- Зони найвищого рівня ризику.

2. Наявність шкідливого програмного забезпечення

Наявність шкідливого програмного забезпечення у вашій мережі є сильним індикатором ймовірності порушення, а отримання видимості активності шкідливих програм є важливим для зменшення рівня кіберризиків вашої організації. Але розробники шкідливого ПЗ володіють навичками створення зловмисного програмного забезпечення, яке може залишатися невиявленим традиційними антивірусними програмами та інструментами сканування.

Хоча жодна організація не є імунною до шкідливого ПЗ, ви можете використовувати потужні аналітичні дані Bitsight, щоб виявити машини, які вже можуть бути скомпрометовані. Ви також можете ідентифікувати поведінку користувачів, яка може призвести до проникнення шкідливого ПЗ у вашу мережу, та класифікувати рівень ризику для вашого бізнесу.

KRI шкідливого ПЗ для моніторингу включають:

- Викриття облікових даних співробітників у даркнеті (хакери використовують цю інформацію для проникнення у вашу мережу та встановлення шкідливого ПЗ).
- Випадки завантаження співробітниками скомпрометованих файлів.
- Кількість машин, уражених шкідливим ПЗ або ботнетами.

3. Незакриті патчами та неправильно налаштовані системи

Погана гігієна безпеки у вигляді систем без патчів та неправильно налаштованих систем є значним індикатором ризику. Коли Bitsight проаналізував сотні випадків програм-вимагачів, щоб оцінити відносну

ймовірність того, що організація стане ціллю програм-вимагачів, ми виявили, що:

- Підприємства з частотою встановлення патчів, які отримали оцінки D або F, мали більш ніж у 7 разів вищу ймовірність стати жертвою порівняно з організаціями з оцінкою A.
- Компанії з оцінкою C або нижче в конфігураціях TLS/SSL майже в 4 рази частіше стають жертвами програм-вимагачів.
- Лише 10% організацій досягли оцінки A за досконаліть у продуктивності безпеки.

Щоб покращити ці показники, використовуйте Bitsight для безперервного та автоматичного моніторингу вашої цифрової інфраструктури на предмет вразливостей та прогалин у безпеці.

KRI гігієни безпеки для моніторингу включають:

- Ефективність сертифікатів TLS/SSL: Bitsight аналізує сертифікати, щоб визначити, чи підписані вони з використанням безпечного алгоритму.
- Конфігурації TLS/SSL: Виявлення серверів з неправильно налаштованими бібліотеками протоколів безпеки та слабкими стандартами шифрування.
- Частота встановлення патчів: Виявлення систем, на які впливають критичні вразливості, та швидкість встановлення патчів вашою організацією.
- Та інше.

4. Ризики третіх сторін

Ризик третіх сторін є однією з провідних причин витоків даних. Але може бути важко визначити, чи ведете ви бізнес з постачальником високого ризику. Це пояснюється тим, що традиційні методи оцінки та вимірювання стану безпеки ваших постачальників фіксують лише миттєвий погляд на ризик. Вони також є дорогими, трудомісткими та вимагають від вас довіри до слова ваших постачальників.

Кращим способом виявлення ризику у вашому ланцюгу постачання є безперервний та автоматичний моніторинг ефективності безпеки вашого пулу постачальників – від початку співпраці і протягом усього періоду відносин.

KRI ризиків третіх сторін для моніторингу включають:

- Наявність та серйозність вразливостей безпеки в IT-інфраструктурах ваших постачальників.
- Історична ефективність безпеки ваших постачальників (минуле порушення може добре вказувати на їхній поточний стан безпеки).
- Будь-які зміни у стані безпеки ваших постачальників протягом строку дії їхніх контрактів.

5. Фінансові втрати

Оскільки середня вартість витоку даних наразі становить 44,35 мільйона доларів, рада директорів та вище керівництво повинні розуміти фінансові втрати вашої організації. Тільки тоді вони зможуть приймати більш обґрунтовані рішення щодо управління кіберризиками та визначати пріоритети нових технологічних інвестицій для захисту вашої організації.

Однак необхідні значні ресурси та експертиза для збору необхідних даних та моделювання різних сценаріїв – таких як фінансовий вплив атаки програм-вимагачів або витоку даних. І цей процес не є легко повторюваним.

Але з Bitsight Financial Quantification ви можете змоделювати фінансові втрати вашої організації в умовах сотень тисяч кіберподій.

KRI, які ви можете змоделювати, включають фінансовий вплив:

- Відмови в обслуговуванні, крадіжки даних, вимагання, порушень конфіденційності та інших типів атак.
- Кіберінцидентів у вашому цифровому ланцюгу постачання.
- Невідповідності стандартам та нормам кібербезпеки та ймовірних штрафів і зборів.

KRI є критичною частиною будь-якої програми управління ризиками кібербезпеки і повинні бути тісно пов'язані з KPI. Наприклад, якщо ви виявите постійні KRI в усій вашій організації, такі як системи без патчів, відповідним

KPI може бути вимірюване покращення вашої частоти встановлення патчів протягом певного періоду часу.

KRI та KPI будуть відрізнятися залежно від організації, але які б метрики ви не обрали, обов'язково використовуйте технології та автоматизацію, щоб ви могли легко збирати та аналізувати дані, відстежувати тенденції та швидко усувати проблеми.

Рис. 2.1 Відмінняіть між показниками ефективності та ризиків

2.2 Визначення основних метрик для оцінки рівня кіберзахищеності об’єктів критичної інфраструктури

У 2025 році метрики кібербезпеки стали важливими для оцінки ефективності кіберзахисту компанії. Ці метрики та Ключові показники ефективності (KPI) виходять за рамки відстеження інвестицій; вони пропонують розуміння моделей загроз, ефективності реагування на інциденти та вразливостей системи завдяки досягненням в аналітиці на основі штучного інтелекту.

Ці метрики є критично важливими для повідомлення стану кібербезпеки зацікавленим сторонам, демонструючи рентабельність інвестицій та надійність заходів безпеки. В епоху зростаючої цифрової залежності вони відіграють ключову роль у стратегічному прийнятті рішень, підкреслюючи готовність компанії до еволюціонуючих кіберзагроз[5].

Метрики кібербезпеки - це не просто числові дані; вони відображають адаптивність та готовність компанії в динамічному ландшафті цифрових загроз, підкреслюючи важливість відстеження та постійного вдосконалення стратегій кібербезпеки.

Метрики інформаційної безпеки - це інструменти, які використовуються для оцінки та вимірювання продуктивності та сили кібербезпеки організацій. Ці потужні метрики можуть надати бізнесу критично важливі точки даних, щоб допомогти їм розробляти стратегії та визначати пріоритети в областях, де їхні існуючі кібер-процедури слабкі, і де вони повинні виділити більше часу та витрат для зміцнення своєї кібер-позиції.

Ви не можете керувати тим, що не можете виміряти. Оскільки кіберзагрози постійно еволюціонують і стають все важче виявляти, вам потрібно мати заходи для оцінки ефективності ваших програм кібербезпеки. Бенчмаркінг кібербезпеки є важливим способом контролю ваших зусиль у сфері безпеки. Вам потрібно відстежувати метрики кібербезпеки з двох важливих причин: Можливість приймати обґрунтовані рішення щодо кібербезпеки та комунікація з бізнес-зацікавленими сторонами.

Відстеження KPI та KRI є критично важливим для розуміння ефективності ваших стратегій кібербезпеки. Ці дані надають історичну перспективу, допомагаючи вам бачити тенденції та зміни у вашій позиції кібербезпеки з часом. Без цих метрик прийняття рішень у кібербезпеці стає спекулятивним, а не заснованим на доказах. Наявність міцного фундаменту даних дозволяє більш стратегічне та проактивне планування кібербезпеки, виходячи за межі реактивних заходів до більш попереджувального підходу в боротьбі з кіберзагрозами.

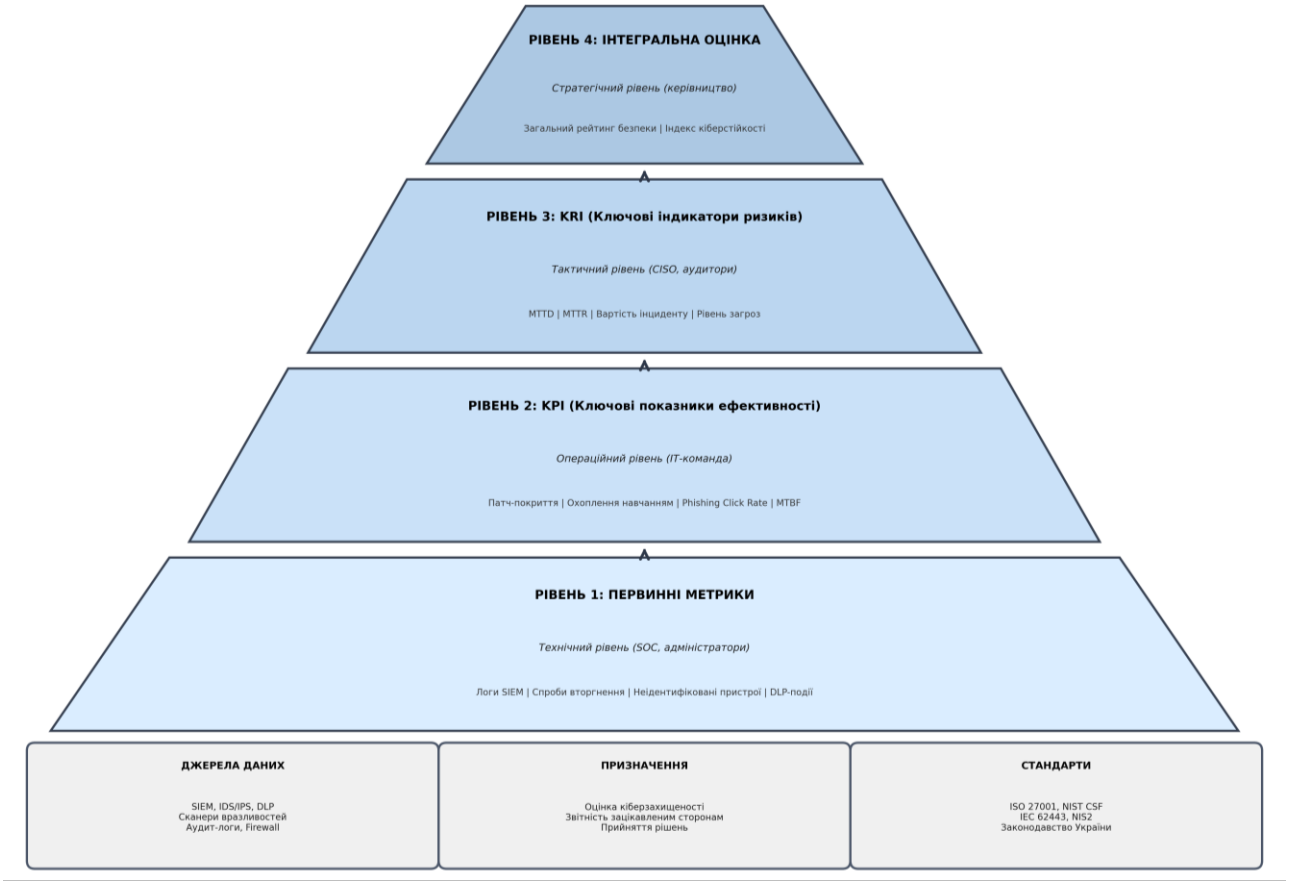

Рис.2.2 Ієрархічна модель системи показників KPI/KRI

Точні метрики кібербезпеки є важливими для повідомлення стану вашої кібербезпеки зацікавленим сторонам. Ці метрики дозволяють вам представити чітку картину стану мережевої інфраструктури та обґрунтувати бюджет та ресурси, виділені на ініціативи кібербезпеки. При звітуванні нетехнічним членам організації, таким як члени ради директорів або керівництво, добре підібрані KPI можуть ефективно ілюструвати ландшафт кібербезпеки. Цей аспект розповіді про звітність з кібербезпеки є життєво важливим, особливо при висвітленні загальної позиції кібербезпеки організації.

У сучасному взаємопов'язаному бізнес-середовищі бенчмаркінг кібербезпеки виходить за межі вашої організації. Оскільки значна кількість компаній зазнають порушень через відносини з третіми сторонами, необхідно встановлювати бенчмарки не лише для вашої організації, але й для третіх і четвертих сторін, підключених до вашої мережі. Майже 98% організацій мають

відносини принаймні з однією третьою стороною, яка зазнала порушення протягом останніх двох років, тому вже недостатньо забезпечувати безпеку лише вашої власної організації; компанії, з якими ви ведете бізнес, повинні відповідати аналогічним стандартам.

Нижче наведено приклади чітких метрик кібербезпеки та KPI, які ви можете легко відстежувати та представляти своїм бізнес-зацікавленим сторонам.

1. Рівень готовності

Оцінка рівня готовності до кібератак є ключовою метрикою. Вона оцінює готовність вашої організації до обробки та пом'якшення загроз кібербезпеки.

Оновлення пристроїв та програмного забезпечення: Відстежуйте відсоток пристроїв та програмного забезпечення, які повністю пропатчені та оновлені. Регулярні оновлення є фундаментальною частиною підтримки надійного захисту від нових загроз.

Постійна відповідність оновленням: Визначте, наскільки послідовно оновлюються ваші пристрої та програмне забезпечення. Постійна відповідність оновленням гарантує, що ви не просто реагуєте на загрози, а проактивно їх запобігаєте.

Виявлення вразливостей високого ризику: Підрахуйте кількість вразливостей високого ризику, виявлених у вашій системі. Ця метрика допомагає у визначенні пріоритетів, які вразливості потрібно усунути спочатку, забезпечуючи ефективний розподіл ресурсів для пом'якшення найкритичніших ризиків.

2. Неідентифіковані пристрої у внутрішній мережі

Наявність неідентифікованих пристроїв, таких як особисті пристрої співробітників або нерозпізнані IoT-пристрої, становить значний ризик. Ці

пристрої часто не мають належних заходів безпеки та можуть стати точками входу для кібератак.

Підрахунок пристроїв: Кількісно визначте кількість неідентифікованих пристроїв, підключених до вашої мережі. Це допомагає зрозуміти масштаб потенційного ризику.

Журнал інвентаризації пристроїв: Встановіть, чи підтримує ваша організація всеосяжний журнал усіх пристроїв, підключених до мережі. Детальна інвентаризація допомагає у відстеженні та управлінні доступом до мережі, забезпечуючи кращий контроль над безпекою мережі.

Протокол безпеки для нових пристроїв: Оцініть, чи існують протоколи для виявлення нових пристроїв та оцінки безпеки. Проактивні заходи для нових пристроїв можуть значно пом'якшити ризики, пов'язані з несанкціонованими або вразливими пристроями у вашій мережі.

3. Спроби вторгнення

Моніторинг та кількісна оцінка спроб вторгнення є важливими для розуміння інтенсивності та частоти кіберзагроз, з якими стикається ваша організація. Регулярне відстеження цих спроб допомагає в оцінці стійкості ваших заходів кібербезпеки.

Підрахунок спроб порушення: Документуйте кількість разів, коли зловмисники намагалися порушити ваші мережі. Ця метрика надає уявлення про рівень зацікавленості з боку кіберзлочинців.

Аналіз частоти: Оцініть частоту цих несанкціонованих спроб. Вони спорадичні чи слідують певному шаблону? Розуміння шаблону може допомогти у прогнозуванні та підготовці до майбутніх атак - і потенційно виявленні мотивацій або особистостей хакерів.

Ідентифікація джерела: Виявіть звичайні джерела або методи цих спроб вторгнення. Ця інформація є критично важливою для посилення вашого захисту кібербезпеки проти найбільш поширених векторів атак, спрямованих на вашу організацію.

Сигнали розвідки загроз, на які вжито заходів, також можуть надати цінну інформацію. Ця метрика відстежує, скільки сповіщень розвідки загроз ваша команда фактично переглядає - і, що важливіше, на скільки з них вони діють.

4. Ефективність запобігання втраті даних

Оцінка продуктивності систем запобігання втраті даних (DLP) є критично важливою для вимірювання їхньої ефективності у захисті конфіденційної інформації. Ця метрика оцінює здатність системи ефективно запобігати несанкціонованому доступу до даних або витокам.

Коефіцієнт запобігання інцидентам: Розрахуйте співвідношення успішно припинених інцидентів з даними до загальної кількості спроб. Це співвідношення пропонує кількісний показник ефективності вашої системи DLP.

Час відгуку: Оцініть час відгуку системи DLP на потенційні порушення даних. Швидший час відгуку може значно зменшити ризик та вплив витоків даних.

Хибні спрацьовування та пропуски: Відстежуйте частоту хибних спрацьовувань та пропусків. Висока частота хибних сповіщень може вказувати на надмірну чутливість, тоді як пропущені інциденти вказують на прогалини в системі. Збалансування точності з реагуванням є ключем до ефективної стратегії DLP.

Охоплення класифікації даних: Ця метрика вимірює, скільки даних вашої організації точно позначені на основі їхньої конфіденційності - як PHI, PII або фінансові записи.

5. Середній час між відмовами (MTBF)

MTBF є важливою метрикою для оцінки надійності та довговічності ваших систем кібербезпеки. Вона обчислює середній часовий інтервал між двома послідовними відмовами системи або компонента.

Оцінка надійності: MTBF надає еталон для оцінки надійності вашої інфраструктури кібербезпеки. Більший MTBF вказує на більш надійні та стійкі системи.

Прогнозоване обслуговування: Відстежуючи MTBF, організації можуть прогнозувати потенційні відмови системи та планувати обслуговування проактивно, мінімізуючи простої та збої.

Аналіз тенденцій продуктивності: Аналіз тенденцій MTBF з часом допомагає у виявленні шаблонів та областей для покращення. Якщо MTBF скорочується з часом, це може вказувати на застарілу інфраструктуру або збільшені зовнішні загрози, сигналізуючи про потребу в оновленнях або посилених заходах безпеки.

6. Середній час виявлення (MTTD)

MTTD є ключовою метрикою, яка кількісно визначає середню тривалість часу, необхідного вашій команді кібербезпеки для виявлення потенційного інциденту безпеки. Це критично важливо для оцінки реагування та пильності ваших операцій безпеки.

Ефективність виявлення: MTTD допомагає оцінити, наскільки ефективно та швидко ваші системи кібербезпеки та команда можуть ідентифікувати загрози. Коротший MTTD означає швидше виявлення, що дозволяє швидше реагувати для пом'якшення ризиків.

Покращення стратегій відгуку: Аналізуючи MTTD, ви можете визначити області для покращення у ваших методологіях виявлення загроз. Це може призвести до вдосконалень у ваших інструментах моніторингу безпеки, системах сповіщень або навчанні команди.

Бенчмаркінг відносно галузевих стандартів: Порівняння вашого MTTD з галузевими еталонами може надати уявлення про можливості виявлення вашої організації відносно конкурентів.

7. Середній час підтвердження (MTTA)

MTTA відіграє критичну роль в оцінці ефективності реагування організації на інциденти кібербезпеки. Вона вимірює середню тривалість між початковим виявленням інциденту та тим, коли він офіційно підтверджується або реєструється вашою командою.

Готовність до реагування: MTTA є показником готовності вашої команди та здатності почати усувати проблеми кібербезпеки. Нижчий MTTA свідчить про швидке визнання та початкову обробку потенційних загроз, що є життєво важливим для ефективного управління інцидентами.

8. Середній час стримування (MTTC)

MTTC є критично важливою метрикою в кібербезпеці, яка вказує на ефективність, з якою ваша команда може контролювати або обмежувати вплив порушення безпеки або загрози після її виявлення.

Ефективність стримування: Вимірювання MTTC відображає, наскільки швидко ваша команда безпеки може ізолювати та пом'якшити загрозу, мінімізуючи її потенційну шкоду. Нижчий MTTC свідчить про ефективні стратегії стримування та надійні протоколи реагування на інциденти.

9. Середній час усунення (MTTR)

MTTR - або Середній час усунення/відновлення - це життєво важлива метрика в кібербезпеці, що використовується для вимірювання швидкості, з якою організація може виявити, відреагувати та повністю відновитися після інциденту безпеки.

Ефективність усунення: Ця метрика оцінює ефективність та швидкість вашої команди кібербезпеки в усуненні та відновленні після загроз. Коротший MTTR означає більш ефективний процес реагування та відновлення, що має вирішальне значення для мінімізації впливу кіберінцидентів.

10. Дні до встановлення патча (частота усунення вразливостей)

Однією з фундаментальних метрик кібербезпеки є частота усунення вразливостей, або дні до встановлення патча, яка вимірює, наскільки швидко організація усуває виявлені вразливості. Вона оцінює ефективність систем та процесів управління патчами. Висока частота встановлення патчів вказує на

проактивний підхід до усунення вразливостей, мінімізуючи вікно експозиції та зменшуючи потенційну поверхню атаки.

Кіберзлочинці часто експлуатують затримки між випусками патчів та впровадженням. Вимірювання цього є хорошим способом зрозуміти ефективність вашої команди після порушення кібербезпеки.

11. Навчання з питань обізнаності про кібербезпеку

Ця метрика оцінює ефективність освітніх програм та заходів, спрямованих на підвищення знань та практик співробітників щодо кіберзагроз та запобігання.

Охоплення та інклюзивність навчання: Життєво важливо забезпечити, щоб навчання з кібербезпеки охоплювало всі рівні організації, від співробітників початкового рівня до вищого керівництва.

12. Кількість повідомлених інцидентів кібербезпеки

Звітування про інциденти демонструє, що ваші співробітники та інші зацікавлені сторони розпізнають проблеми у вашій мережі та вживають заходів для їх вирішення. Це також означає, що ваше навчання працює.

13. Рейтинги безпеки

Часто найлегшим способом повідомлення метрик нетехнічним колегам є зрозуміла оцінка. Рейтинги безпеки SecurityScorecard дають вашій компанії літерну оцінку від A до F за 10 категоріями безпеки (безпека мережі, стан DNS, частота встановлення патчів, оцінка cubit, безпека кінцевих точок, репутація IP, безпека веб-додатків, розмови хакерів, витік облікових даних та соціальна інженерія). На основі цих 10 факторів вам потім присвоюється загальна оцінка.

14. Управління доступом (і коефіцієнт успішності автентифікації користувачів)

Управління доступом як метрика кібербезпеки стосується контролю, практик та процесів, створених та впроваджених організацією для управління контролем доступу користувачів до систем та мереж.

Частота перегляду привілейованого доступу відстежує, як часто ваша організація перевіряє облікові записи користувачів високого рівня - таких як

адміністратори, системні інженери та сервісні облікові записи - щоб переконатися, що їхній доступ все ще необхідний і безпечний.

Коефіцієнт успішності автентифікації користувачів оцінює ефективність та результативність механізмів автентифікації, таких як паролі, багатофакторна автентифікація (MFA) або біометрія.

15. Відповідність політиці безпеки

Відповідність політиці безпеки стосується здатності організації узгоджувати практики безпеки, процедури та контролі з встановленими політиками та стандартами безпеки.

16. Нелюдський трафік (NHT)

Забезпечення того, щоб ваш бізнес не відстежував трафік ботів як метрику, є ключем до розуміння успіху бізнес-операцій та зусиль. Нелюдський трафік - це метрика кібербезпеки, яка стосується частини мережевого або веб-трафіку, що походить з автоматизованих джерел, а не від користувачів-людей.

17. Моніторинг вірусних інфекцій

Постійний моніторинг вірусних інфекцій - це KPI кібербезпеки, що стосується постійного нагляду за додатками, системами та кінцевими точками для моніторингу наявності вірусів, шкідливого ПЗ або зловмисного коду.

18. Успішність фішингових атак

Успішність фішингових атак стосується рівня успіху кіберзлочинців або загрозливих факторів у досягненні своїх зловмисних цілей через обман користувачів за допомогою фішингових спроб.

Phishing Click Rate також є критично важливою метрикою кібербезпеки. Це оцінює, наскільки успішно користувачі виявляють і уникають фішингових спроб.

19. Вартість одного інциденту

Вартість одного інциденту в метриках кібербезпеки стосується суми грошей та фінансового впливу, пов'язаного з кожним інцидентом безпеки на організацію.

20. Відповідність аудиту безпеки

Аудит відповідності безпеці допоможе вашому бізнесу виділити області, де ви можете відставати з точки зору ефективності програмного забезпечення, яке ви зараз використовуєте.

2.3. Інтегральна оцінка стану безпеки за результатами аудиту

Аналіз ризику включає в себе дві основні складові:

- аналіз у вузькому розумінні цього слова як процес розкладання явища на окремі елементи та кількісну оцінку кожного з них;
- синтез отриманих результатів та інтегральну оцінку.

Весь спектр діяльності підприємства розкладається на окремі види ризику з урахуванням властивої йому специфіки, наприклад майнові, особистої та цивільної відповідальності. Далі детально розглядаються ризики, характерні для окремих підрозділів підприємства, будівель, установок, систем та технологічних процесів. Кожен з них може бути розкладений на окремі події, ймовірність яких розраховується виходячи з минулого досвіду або на основі побудови ланцюжка послідовних кроків, що ведуть від вихідних інцидентів до головних подій. Кожен такий ланцюжок називається сценарієм.

Для конкретної системи або процесу існує свій набір головних подій. Наприклад, для промислової установки це можуть бути відмова обладнання різного ступеня тяжкості - від дрібних неполадок до серйозних пошкоджень, аварія, що призводить до руйнування установки, або з вибухом, пожежею тощо. Кожна головна подія характеризується певним розміром збитку та ймовірністю виникнення, що розраховуються на основі методів, які розглядалися в попередніх розділах.

Набір головних подій може бути безперервним за розміром збитку, однак на практиці ми маємо справу з дискретною вибіркою з окремих ситуацій, які відомі або з минулої історії діяльності підприємства, отримані теоретичним шляхом на основі сценарного підходу. Найбільш простий набір з трьох сценаріїв - це так звані песимістичний, середній та оптимістичний прогнози. Іноді цього буває достатньо для грубої інтегральної оцінки ризику.

Для того щоб краще уявити собі, що ж таке набір сценаріїв, розроблених або відібраних зі статистичних даних, згадаємо відоме з теорії ймовірностей поняття функції розподілу випадкової величини. У даному випадку як

випадкова величина виступає розмір збитку, а сама функція розподілу представлена дискретною вибіркою.

Інтегральна оцінка ризику – це отримання із сукупності головних подій деяких кількісних параметрів, які можуть охарактеризувати розглянутий ризик у цілому, не оперуючи окремими ситуаціями.

Найбільш важливими з точки зору планування процесу управління є середні та граничні характеристики ризику. Середнє значення величини збитку дає нам знання того, які збитки понесе підприємство в середньому за тривалий проміжок часу. Це важливо для стратегічного планування.

У якості граничної характеристики ризику можна використовувати максимальне значення величини збитку для даної системи. Наприклад, для промислового підприємства максимальною величиною майнового збитку є вартість його основних та оборотних фондів. Однак застосування такої характеристики непродуктивно, особливо для великих підприємств. Дійсно, ймовірність повного руйнування індустріального комплексу, що включає в себе десятки цехів та інших виробничих будівель, вкрай мала, хоча на практиці такі випадки й траплялися. Брати як орієнтир для прийняття рішень з управління ризиком такі маловірогідні події недоцільно.

Більш правильним було б використання поняття максимально прийнятної величини збитку в купі з максимально допустимою величиною ймовірності її виникнення. Зміст останнього поняття полягає в тому, що за відправну точку приймається деяке дуже мале значення ймовірності виникнення великих збитків, а події з ймовірністю менше заданої взагалі не беруться до розрахунку.

Стандарти безпеки, які існують у розвинених країнах, визначають допустимий рівень ймовірності виникнення аварійних ситуацій у промисловості рівним від 0,001 до 0,0001%. Щоб наочно уявити собі ці величини, зазначимо, що події з ймовірністю 0,001% відбуваються раз на 100 000 років. Даному значенню ймовірності відповідає деяке порогове значення збитку, зміст якого полягає в тому, що події з більш великими збитками

відбуваються з частотою менше ніж 0,001%. Це і буде максимально прийнятне значення величини збитку.

Розглянута характеристика, як уже зазначалося, є суб'єктивною в тому сенсі, що її конкретне значення залежить від сприйняття ризику керівництвом підприємства. Чим більш консервативною є політика в галузі управління ризиком, тим нижче допустимий рівень ймовірності несприятливих подій, і тим більше витрати на проведення заходів зі зниження рівня ризику.

Максимально прийнятне значення величини збитку дає нам орієнтир щодо того, яких граничних збитків слід очікувати від окремої несприятливої події або сукупності таких подій протягом тривалого проміжку часу.

Як відомо, гнучкі методи управління дають можливість досягти поставлених стратегічних цілей завдяки ефективному використанню наявних ресурсів, вмінню управлінців швидко реагувати на зміни у зовнішньому середовищі, інтуїтивно відчувати напрямок дій, бути персонально відповідальним за результати реалізації проєкту або плану розвитку, а також своєчасно реагувати на вплив тих чи інших факторів ризику. Стратегія гнучкої системи управління, на думку автора, повинна базуватися на системі ключових параметрів оцінки ризиків, яка може являти собою універсальну методику, придатну практично будь-якому промисловому підприємству. Вивчення основних методів кількісної оцінки ризиків показує, що при окремому використанні певного методу менеджмент не отримує повних даних про ступінь впливу ризиків, що впливає на гнучкість розвитку підприємства. Тому в сучасних умовах потрібен комбінований принцип використання методів, оскільки в даному випадку з'являється можливість усунення недоліків одного методу за рахунок використання інших. У статті пропонується новий інтегральний підхід до оцінки ступеня ризику, який базується на комплексному застосуванні методів кількісного аналізу, а саме нормативного методу, методу дерева відмов, методу експертних оцінок та статистичного методу. Застосування елементів статистичного методу дозволяє виявити ситуації ризику, але не ідентифікує конкретні ризики в діяльності підприємства, а

розглядає ризик як єдину величину. Це обумовлює використання методу дерева відмов, який здатний виявити зовнішні ризики підприємства. Але цей метод не в змозі оцінити величину ризиків, що вказує на необхідність використання інших методів. У цьому випадку метод експертних оцінок допоможе оцінити ризики, що виникають у зовнішньому середовищі і не залежать від діяльності підприємства. Нормативний же метод допоможе оцінити всю сукупність ризиків, що виникають на мікрорівні і впливають на гнучкий розвиток у цілому [1–8]. Умовно запропоновану інтегральну методику кількісного оцінювання ступеня ризику можна розділити на три блоки:

перший блок – комплексна оцінка зовнішніх ризиків підприємства;

другий блок – комплексна оцінка внутрішніх ризиків підприємства;

третій блок – зведення результатів та отримання інтегрального показника ризиків гнучкого функціонування підприємства. Загальний алгоритм запропонованого методу оцінки складається з чотирьох етапів (Таблиця. 2.1).

Таблиця 2.1

Етапи інтегрального методу оцінки ризиків

Етап 1	Етап 2	Етап 3	Етап 4
Статистичний аналіз ступеня ризику	Використання дерева відмов	Експертна оцінка	Оцінка внутрішніх ризиків

На першому етапі розраховуються основні показники статистичного методу дослідження – середньоквадратичне відхилення та коефіцієнт варіації. Перший показник оцінки ступеня ризику характеризує його якісну сторону і показує, як відхиляється фінансовий результат підприємства від його середнього очікуваного значення; другий – говорить про інтенсивність ризику і дозволяє виявити в яку ризикову область потрапляє підприємство. Оцінити ступінь ризику за допомогою запропонованих показників – означає зробити ризики зіставними між собою. Використання дерева відмов – це другий етап запропонованого методу. На цьому етапі дерево відмов дає можливість

визначити сукупність зовнішніх ризиків, впливаючих на діяльність підприємства та його гнучкий розвиток. Дерево відмов зображається таким чином:

- На вершині дерева відмов розміщують найважливішу подію. Так, наприклад, на гнучкий розвиток підприємства впливає найголовніша подія - недоотримання чистого прибутку або навіть збиток. Ця подія є фундаментальною.
- Крона дерева уособлює шляхи реалізації події, але також містить певну умову, яка пов’язує вихідну та основну події. Як умова можуть застосовуватися «і» або «або». Таким чином, дерево відмов дає змогу визначити всі варіанти, що призводять до основної події, тобто ризики, які спричиняють зменшення прибутку або отримання збитків.
- Третім етапом методики є метод експертних оцінок для визначення ступеня зовнішнього ризику. На цьому етапі запропонованої комплексної оцінки ми переходимо до безпосереднього визначення ймовірності реалізації виявлених зовнішніх ризиків. Для цього залучаються експерти, які займаються вивченням цієї проблеми.

В основу цього етапу оцінювання рівня ризиків покладена методика, що передбачає поділ ризиків за характером їх впливу на прості та складні. Варто зазначити, що в цьому випадку складні ризики становлять собою синтез простих, які характеризуються певними подіями, тому їх необхідно аналізувати окремо.

Запропонуємо таку послідовність експертного оцінювання зовнішнього ризику таблиця 2.2.

Таблиця 2.2

Послідовність експертного оцінювання зовнішнього ризику

Етап	Опис етапу	Пояснення	Формула - Критерій
1	Визначення зовнішніх ризиків	Виконується у рамках другого етапу комплексної оцінки	
2	Оцінка вірогідності певного ризику	Необхідно оцінити вірогідність ризиківза системою оцінки	0,00-0,25 - ризик розглядається як несуттєвий 0,25-0,50 – ризик скоріше за все не реалізується 0,50-0,70 – про наступ рмзику нічоко конкретного сказати неможна 0,70-0,85 – ризик скоріше за все реалізується 0,85-1,00 – ризик реалізується найбільш вірогідно
3	Сортування ризиків по рівням	Сортування ризиків по рівням, визначающі важливість кожної групи відповідного рівня, тобто встановлення приоритету кожної групи ризиікв	
4	Визначення питомої ваги ризику	Оцінюється питома вага простого ризтку по всьому діапазону ризиків	S_i-звичайний ризик i-номер виду ризику, i=1,2,3…n Q_j-група приоритету j-загальне число приоритетів j=1,2,3…k (k<n) W_j-вага приритетної групи ризику W_{sj}-вага звичайних ризиків по групам приоритету Q_j, W_j>0, $\sum W_j = 1$ C_j-кількість ризиків, Що входять до приоритетних груп Q_j

Продовження таблиці 2.2

Етап	Опис етапу	Пояснення	Формула - Критерій
5	Розрахунок ваги кожного простого ризтку в інтервалі від 0 до 1	Перший та останній рівень сортування мають максимальні та мінімальні значення. Відносення ваги ризиків першого та останнього приоритетів = f, тобто в скільки разів перший приоритет вагоміше останнього	$\frac{W_I}{W_j} = f$
6	Визначення ваги групи з найменщим приоритетом		$W_j = \frac{2}{k(f+1)}$
7	Визначення ваги всіх інших груп приоритетів		$W_j = \frac{W_k((k-j)f + j - 1)}{k-1}$
8	Розрахунок ваги простих ризиків, присутніх в приоритетній групі	Всі прості ризики однієї приоритетної групи мають онакову вагу, тобто якщо приоритет завчасно не встановлюється, то всі вони мають однакову вагу	$W_{si} = \frac{W_j}{C_j}$
9	Визначення комплексного показника зовнішніх ризиків		$r = \sum W_i P_i$, P_i –середня вірогідність реалізації ризику

Таким чином, значення комплексного показника може набувати значення від 0 до 1

Таблиця 2.3

Шкала градації ризикових зон комплексного показника

0,0 – 0,25	Зона мінімального ризику
0,25 – 0,50	Зона допустимого ризику
0,50 – 0,75	Зона критичного ризику
0,75 – 1,0	Зона катострофічного ризику

Результати запропонованої оцінки дають змогу визначити зону зовнішнього ризику як на макро-, так і на мезорівнях. Цей метод допомагає здійснити узагальнювальне оцінювання.

Четвертий етап включає повноцінну оцінку внутрішніх ризиків компанії. Існує багато різних методик оцінювання. Пропонуємо проводити аналіз таких підсистем підприємства: рентабельність, операційна система, обслуговування боргу, майновий стан і управління активами, ліквідність, структура активів.

Показники рентабельності відображають загальну картину роботи підприємства в цілому й характеризують, наскільки сьогодні підприємство може бути гнучким. Дані операційного аналізу оцінюють динаміку прибутку підприємства. Доповненням до них слугує аналіз операційних витрат, що здійснюється з метою оцінки динаміки частки різних видів витрат у структурі сукупних витрат підприємства.

Показники обслуговування боргу демонструють, яка частина прибутку або грошового потоку поглинається процентними та (або) іншими фіксованими витратами (платежами). Ця група показників характеризує можливості підприємства розраховуватися за своїми зобов’язаннями.

Коефіцієнти майнового стану підприємства характеризують стан його основних засобів та ступінь їх зношення.

Що стосується коефіцієнтів ліквідності, ці параметри відображають можливість підприємства в оперативному режимі перетворити активи на гроші. Вивчаючи показники ліквідності, управлінець здатен оцінити достатність або нестачу оборотних активів для покриття поточних боргів, а саме короткострокової кредиторської заборгованості.

Показники ефективності управління активами відображають тенденції у використанні ресурсів підприємства. Використовуючи ці показники, можна визначити, наскільки розмір певних видів активів у балансі відповідає фактичній або плановій фінансово-господарській діяльності підприємства, а також оцінити результати й ефективність його поточної основної виробничої

діяльності. Крім того, ці показники дозволяють оцінити ефективність використання підприємством власних коштів.

Коефіцієнти структури капіталу зазвичай відображають ступінь можливого ризику банкрутства підприємства у зв'язку з використанням кредитів і позик.

Важливо зазначити, що розрахунок запропонованих показників сам по собі майже неінформативний і не відображає, наскільки гнучким може бути підприємство в умовах впливу ризиків. Певні висновки можна зробити лише за умови проведення їх просторово-часового аналізу або шляхом порівняння розрахованих величин із нормативними значеннями.

Тому наступним кроком є порівняння отриманих раніше показників з еталонними. Так, наявні значення показників, які були розраховані для конкретного підприємства, порівнюють із нормативними, а за ступенем відхилення роблять висновки про величину ризику.

Крім того, різні показники можуть свідчити про різний рівень ризику. У зв'язку з цим визначають діапазон значень для кожного з коефіцієнтів. Як і у статистичному аналізі, можна виділити чотири ризикові зони: мінімального ризику (відхилення в межах 25 % від нормативу), допустимого ризику (відхилення в межах 50 %), критичного ризику (відхилення в межах 75 %) і катастрофічного ризику (відхилення понад 75 %).

Важливою групою показників, для яких пропонуємо змінити зазначені зони ризиків, є показники рентабельності, оскільки вони характеризують не окрему сферу функціонування підприємства, а всю його діяльність у цілому. Для показників рентабельності відхилення в межах 25 % від нормативу буде відповідати зоні критичного ризику; понад 25 % - зоні катастрофічного ризику.

Також для деяких показників нормативні значення не встановлені, тому в цих випадках орієнтуються на позитивні або негативні зміни в динаміці.

Для того щоб звести отримані результати до порівняльного вигляду, їх ранжують, присвоюючи певний бал. Присвоєння балів пропонується здійснювати, виходячи з відповідності отриманого значення показника певній

зоні ризику, а також його значенню в динаміці. Під час порівняння з нормативом 1 бал відповідає показникам зони мінімального ризику, 2 бали - зони допустимого ризику, 3 бали - зони критичного ризику, 4 бали - зони катастрофічного ризику.

Під час характеристики показників у динаміці бали розподіляються таким чином: 1 - значення коефіцієнта змінилося на краще або залишилося на попередньому рівні, що відповідав гнучкому розвитку підприємства; 2 - значення коефіцієнта дещо погіршилося або залишилося на попередньому цілком позитивному рівні; 3 - значення коефіцієнта суттєво погіршилося; 4 - значення коефіцієнта значно погіршилося і свідчить про наявність серйозних проблем у підприємства.

В обох випадках між балами існує чітка логічна градація, і вони мають однаковий інтервал: кожен наступний бал характеризує наступний за логікою рівень - від мінімальної точки до максимальної.

Визначивши групи фінансових показників, нормативні значення, а також розрахувавши зони їх коливань, можна визначити, у якій ризиковій зоні перебуває та чи інша підсистема функціонування підприємства, а також підприємство в цілому. Таким чином, показник рівня ризику внутрішньої підсистеми підприємства виявляє слабкі місця його гнучкого розвитку та розраховується за формулою:

$$П_{п} = \frac{\sum Б_{і}}{n}, \quad (2.5)$$

$П_{п}$ – ризик підсистеми підприємства; $Б_{і}$ – бальне значення показника в межах групи; n – кількість характеристик у групі.

Нормована комплексна оцінка внутрішнього ризику підприємства як системи є середньозваженим значенням рівнів ризику всіх підсистем і визначається за такою формулою:

$$К_{вп} = \sum П_{п}\, q, \quad (2.6)$$

$К_{вп}$ – нормована комплексна оцінка внутрішніх ризиків підприємства; q – питома вага групи ризику.

На цьому етапі ми можемо отримати комплексний показник внутрішнього ризику підприємства, який дає змогу ранжувати досліджувані підприємства між собою за рівнем їхнього ризику і, відповідно, гнучкості розвитку. Таким чином, у результаті реалізації запропонованої методики ми можемо отримати комплексні показники зовнішніх і внутрішніх ризиків.

Проте в окремих випадках підприємству для вибору стратегії гнучкого розвитку необхідно мати єдиний інтегральний показник, що характеризував би всю сукупність ризиків компанії. Для отримання такого показника насамперед потрібно пронормувати значення комплексного показника зовнішнього ризику підприємства за запропонованою раніше методикою відповідності нормованих значень певному числу.

Інтегральний показник ризику підприємства (**I**) визначатиметься як зважена сума нормованих комплексних значень показників зовнішнього та внутрішнього ризиків підприємства:

$$I = q_з \times WP + q_в \times К_{вп}, \qquad (2.7)$$

WP – нормовані значення комплексного показника зовнішніх ризиків; $q_з/q_в$ – відповідно ваги зовнішнього та внутрішнього ризиків.

Підсумовуючи, зазначимо, що запропонований метод інтегральної оцінки ступеня ризиків дає змогу виявити ризикову ситуацію на підприємстві шляхом аналізу динаміки основних показників його діяльності та надати швидку оцінку ризикової ситуації за допомогою статистичного методу. Методи дерева відмов і експертних оцінок конкретизують зовнішні ризики, з якими стикається підприємство в процесі своєї діяльності, а застосування нормативного методу може показати, які саме внутрішні ризики є найбільш небезпечними й потребують зниження в межах стратегії гнучкого розвитку.

Інтегральний показник оцінювання ступеня ризиків дасть змогу підприємствам не лише обрати загальну стратегію управління ризиками, але й в

оперативному періоді здійснювати заходи щодо вдосконалення гнучкого розвитку в цілому.

Висновки до розділу 2

Обґрунтовано методологію формування системи ключових показників ефективності (KPI) та ризиків (KRI) для оцінювання рівня кіберзахищеності об'єктів критичної інфраструктури. Розроблено інтегральну методику оцінки, що базується на комбінованому застосуванні кількісних методів аналізу.

Визначено теоретичні засади системи ключових показників у контексті кіберзахисту ОКІ. Встановлено, що KPI дозволяють оцінити результативність заходів захисту та відповісти на запитання «Наскільки добре ми захищені?», тоді як KRI орієнтовані на виявлення та моніторинг потенційних загроз і дають відповідь на запитання «Які ризики нам загрожують?». Обґрунтовано необхідність інтеграції обох груп показників для забезпечення комплексної оцінки.

Запропоновано класифікацію KPI кібербезпеки ОКІ за категоріями: технічні показники захищеності (рівень готовності систем, ефективність антивірусного захисту, покриття резервним копіюванням, MTBF); часові показники реагування (MTTD - середній час виявлення, MTTA - середній час підтвердження, MTTC - середній час стримування, MTTR - середній час усунення); організаційні показники (рівень зрілості СУІБ, охоплення навчанням, відповідність політикам).

Систематизовано категорії KRI для ОКІ: показники вразливостей (кількість критичних вразливостей, коефіцієнт експозиції, індекс застарілості); показники загроз (інтенсивність атак, успішність фішингових атак, наявність шкідливого ПЗ); показники поверхні атаки (тіньові ІТ-активи, відхилення від політик); показники третіх сторін (рейтинги постачальників, вразливості ланцюга постачання); показники фінансового впливу (потенційні збитки, вартість простою).

Визначено основні принципи вибору метрик для ОКІ: релевантність галузевій специфіці та ключовим бізнес-процесам; вимірюваність та відтворюваність результатів; зрозумілість для технічних фахівців та керівництва; оперативність збору даних; збалансованість охоплення всіх аспектів кібербезпеки.

Запропоновано базовий набір із 20 метрик кібербезпеки для ОКІ, адаптованих до вимог українського законодавства та міжнародних стандартів (NIST CSF, ISO 27001, IEC 62443). Для кожної метрики визначено формулу розрахунку, цільові значення та методи вимірювання з урахуванням галузевої специфіки.

Розроблено інтегральну методику оцінювання стану кіберзахищеності ОКІ, що базується на комбінованому застосуванні чотирьох методів: статистичного аналізу (середньоквадратичне відхилення, коефіцієнт варіації), методу дерева відмов (ідентифікація зовнішніх ризиків), експертних оцінок (визначення ймовірностей та ваг), нормативного методу (порівняння з еталонними значеннями).

Обґрунтовано формулу розрахунку інтегрального показника кіберзахищеності: $I = q\text{з} \times WP + q\text{в} \times \text{Квп}$, де WP - нормований показник зовнішніх ризиків, Квп - комплексна оцінка внутрішніх ризиків, qз та qв - ваги відповідних компонентів. Розроблено шкалу градації ризикових зон (мінімальний, допустимий, критичний, катастрофічний ризик) з рекомендованими заходами для кожної зони.

РОЗДІЛ 3. РЕАЛІЗАЦІЯ ВПРОВАДЖЕННЯ СИСТЕМИ КЛЮЧОВИХ ПОКАЗНИКІВ ЕФЕКТИВНОСТІ ТА РИЗИКІВ (KPI/KRI) ДЛЯ ОЦІНЮВАННЯ РІВНЯ КІБЕРЗАХИЩЕНОСТІ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В ПРОЦЕСІ АУДИТУ

3.1. Характеристика досліджуваного об'єкта

Загальна інформація про підприємство

Для дослідження обрано ТОВ "Трител" - українську компанію, що спеціалізується на створенні телекомунікаційних мереж спеціального призначення, розробці криптографічних засобів захисту та їх серійному виробництві. Компанія віднесена до критичної інфраструктури у двох секторах: інформаційно-комунікаційних технологій та електронних комунікацій.

Діяльність регулюється ліцензіями ДССЗЗІ (криптографічний та технічний захист інформації) та спецдозволом СБУ для роботи з державною таємницею. Така багаторівнева система дозволів підкреслює стратегічну важливість для національної безпеки.

Таблиця 3.1

Загальна характеристика об'єкта дослідження

Параметр	Значення
Сервери (всього)	42 (18 фізичних + 24 віртуальних)
Робочі станції	165
Комутатори	28
Маршрутизатори	8
Міжмережеві екрани	6
Персонал	185 осіб
Річний оборот	120 млн грн
Бюджет кібербезпеки	4.8 млн грн/рік

Компанія має 8 сертифікованих виробів ДССЗЗІ, ще 3 на стадії сертифікації. Виробничі потужності (2400 м²) включають 3 акредитовані лабораторії. Річна потужність - до 5000 пристроїв. ІТ-інфраструктура: 42

сервери (18 фізичних, 24 віртуальних), 165 робочих станцій, 28 комутаторів, 8 маршрутизаторів, 6 міжмережевих екранів.

Бюджет кібербезпеки - 4.8 млн грн/рік (4% від IT-бюджету). Центр моніторингу працює 8 год/день, 5 днів/тиждень.

Архітектура інформаційних систем

Інформаційна інфраструктура має чотири сегменти:

- Корпоративна мережа: Active Directory, Exchange, файлові сервери, 1C:Enterprise, 92 станції Windows 10/11
- Мережа досліджень: GitLab, Jenkins, Jira, Confluence, 8 серверів, 45 станцій
- Виробнича мережа: системи управління виробництвом, контролю якості, програматори, тестові стенди
- Режимна мережа: ізольована, 28 станцій, криптомодулі, без інтернет-доступу

Периметр захищено Fortinet FortiGate, Suricata IDS/IPS, VPN. Внутрішня сегментація через VLAN, контроль доступу 802.1X.

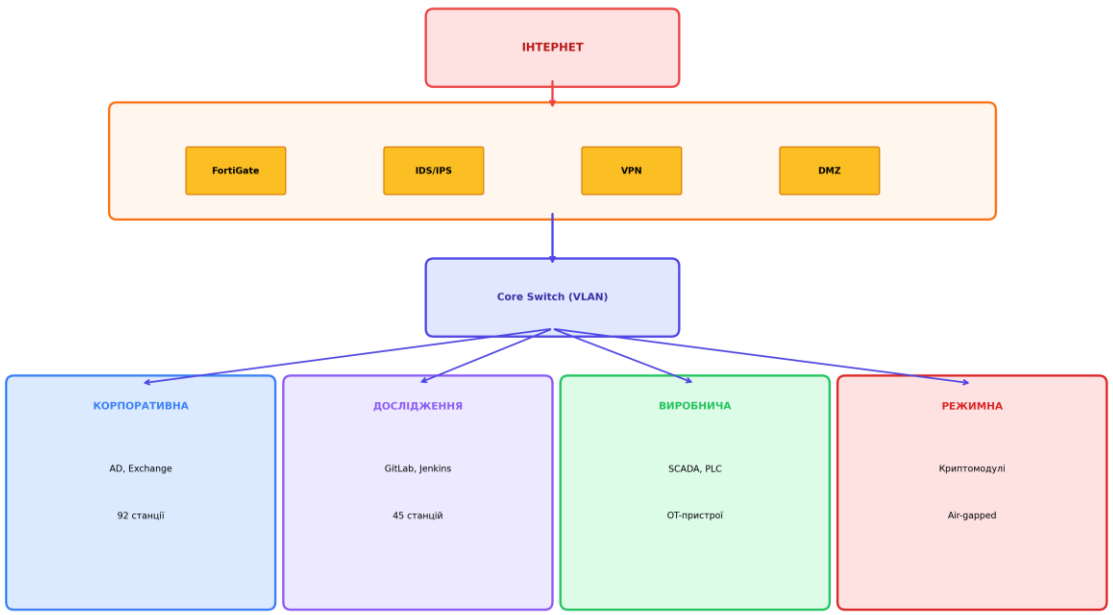

Рис.3.1 Мережева архітектура ТОВ «Трител»

3.2. Проведення аудиту кібербезпеки

Методологія аудиту

Аудит проводився згідно комбінованої методології: ISO/IEC 27001:2022, ISA/IEC 62443, НД ТЗІ України, NIST CSF. Використовувався гібридний підхід: аналіз документації, інтерв'ю персоналу, технічне тестування, сканування вразливостей, тестування на проникнення.

Аудит тривав 6 тижнів (жовтень-листопад 2025). Команда: 4 спеціалісти (керівник, експерт з мережевої безпеки, фахівець з безпеки додатків, експерт з організаційних заходів).

Етапи та інструменти

- Підготовчий етап: збір документації, визначення критичних активів.
- Інвентаризація:Nmap, OpenVAS.
- Аналіз конфігурацій: аудит AD, міжмережевих екранів, серверів.
- Виявлення вразливостей: Nessus, OpenVAS.
- Тестування на проникнення: Burp Suite, OWASP ZAP, Metasploit. Фішингові тести.

Виявлені вразливості

- Критичні вразливості: непропатчені системи (Windows Server 2012), слабкі паролі, відкриті порти, застарілі версії ПЗ.
- Організаційні недоліки: відсутність формалізованих процедур, неповне журналювання, застарілі політики.
- Фішинговий тест: 28% успішності атак.

Таблиця 3.2

Класифікація вразливостей

Категорія	Критичність	Кількість	Основні вразливості
Інфраструктурні	Висока	12	Застарілі ОС, непропатчені сервери
Управління доступом	Середня	18	Слабкі паролі, привілейовані акаунти
Мережеві	Середня	15	Відкриті порти, слабка сегментація
Застосунки	Висока	8	SQL-ін'єкції, XSS вразливості
Організаційні	Середня	22	Застарілі політики, відсутність процедур

3.3. Розрахунок показників ефективності (KPI)

Таблиця 3.3

Дані для розрахунку KPI

Показник	Фактичне	Цільове
Станцій із антивірусом	142	165
Пропатчених серверів	28	42
Час виявлення (T_середній)	12 год	4 год
Заблоковано атак	3340	-
Спроб вторгнень	4285	-
Систем з резервним копіюванням	39	42
Актуальних документів	26	36
Навчених співробітників	100	185
Час реагування (T_фактичний)	18 год	8 год
Час відновлення	6.2 год	4 год
Час простою (за рік)	114 год	-
Інцидентів за рік	42	-

Методологія розрахунку технічних KPI

Технічні показники ефективності розраховуються за наступними математичними формулами, розробленими у Розділі 2:

$$KPI_{\text{антивірус}} = \left(\frac{N_{\text{захищених}}}{N_{\text{загальна}}}\right) \times 100\%, \quad (3.1)$$

де $N_{\text{захищених}}$ - кількість робочих станцій з активним антивірусним захистом, $N_{\text{загальна}}$ - загальна кількість робочих станцій в організації.

Для ТОВ "Трител" розрахунок виглядає наступним чином:

$$KPI_{\text{антивірус}} = \left(\frac{142}{165}\right) \times 100\% = 86.06\% \quad (3.2)$$

Отримане значення 86.06% свідчить про неповне охоплення інфраструктури антивірусним захистом. Цільове значення для об'єктів критичної інфраструктури становить мінімум 95%. Таким чином, виявлено відхилення на 8.94%, що вимагає негайних коригувальних дій.

$$KPI_{\text{патчинг}} = \left(\frac{N_{\text{пропатчених}}}{N_{\text{критичних}}}\right) \times 100\%, \quad (3.3)$$

де N_пропатчених - кількість повністю пропатчених критичних серверів, N_критичних - загальна кількість критичних серверів.

Розрахунок для досліджуваного об'єкта:

$$KPI_{\text{патчинг}} = \left(\frac{28}{42}\right) \times 100\% = 66.67\% \quad (3.4)$$

Цей показник знаходиться значно нижче прийнятного рівня (90% для критичної інфраструктури). Відхилення становить 23.33%, що класифікується як критична вразливість, оскільки непропатчені системи піддають організацію значному ризику експлуатації відомих вразливостей.

$$KPI_{\text{виявлення}} = \frac{T_{\text{середній}}}{T_{\text{цільовий}}}, \quad (3.5)$$

де $T_{\text{середній}}$ - середній час від події безпеки до її виявлення (години), $T_{\text{цільовий}}$ - цільовий час виявлення згідно політики безпеки (години).

Фактичні дані для підприємства:

$$KPI_{\text{виявлення}} = \frac{12\text{год}}{4\text{год}} = 3.0 \quad (3.6)$$

Значення показника 3.0 означає, що фактичний час виявлення у три рази перевищує цільове значення. Це суттєво збільшує потенційний час, протягом якого зловмисник може діяти непоміченим у системі, що прямо впливає на масштаб можливих збитків.

$$KPI_{\text{екранування}} = \left(\frac{N_{\text{заблоковано}}}{N_{\text{спроб}}}\right) \times 100\%, \quad (3.7)$$

де $N_{\text{заблоковано}}$ - кількість успішно заблокованих атак міжмережевими екранами, $N_{\text{спроб}}$ - загальна кількість зареєстрованих спроб вторгнень за період.

На основі логів за останній місяць:

$$KPI_{\text{екранування}} = \left(\frac{3340}{4285}\right) \times 100\% = 77.95\% \quad (3.8)$$

Ефективність міжмережевих екранів 77.95% є задовільною, але нижчою за цільове значення 85%. Це свідчить про необхідність оптимізації правил фільтрації та актуалізації сигнатур атак.

$$KPI_{\text{резервування}} = \left(\frac{N_{\text{покритих}}}{N_{\text{критичних систем}}}\right) \times 100\%, \quad (3.9)$$

де $N_{\text{покритих}}$ - кількість систем з налаштованим резервним копіюванням, $N_{\text{критичних систем}}$ - загальна кількість критичних систем.

Розрахунок:

$$KPI_{\text{резервування}} = \left(\frac{39}{42}\right) \times 100\% = 92.86\% \quad (3.10)$$

Покриття резервним копіюванням 92.86% близьке до цільового значення 95%, що є позитивним результатом. Однак 3 критичні системи залишаються без захисту, що потребує виправлення.

Таблиця 3.4

Технічні показники ефективності з розрахунками

Показник	Формула розрахунку	Поточне	Цільове	Відхилення
Антивірусний захист	(142/165)×100%	86.06%	95%	-8.94%
Рівень пропатченості	(28/42)×100%	66.67%	90%	-23.33%
Час виявлення	12/4	3.0	1.0	+2.0
Ефективність екранів	(3340/4285)×100%	77.95%	85%	-7.05%
Резервне копіювання	(39/42)×100%	92.86%	95%	-2.14%

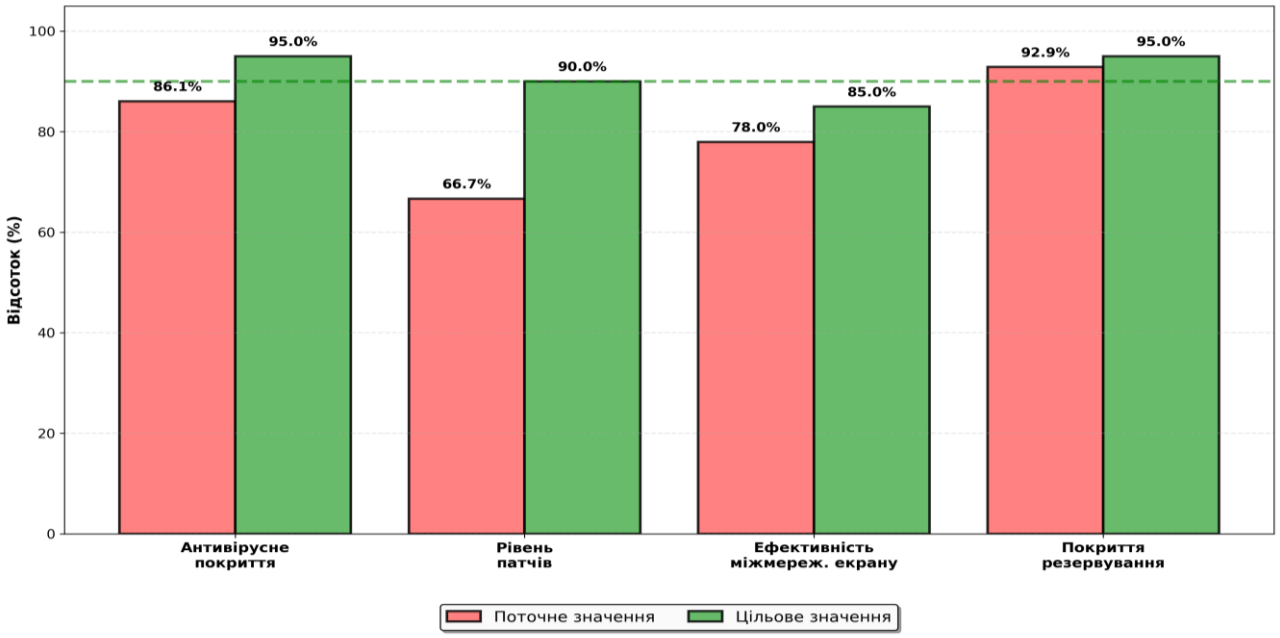

Рис.3.2 Відхилення технічних KRI від цільового значення

Організаційні показники з математичним апаратом

Для оцінки організаційної зрілості використовується багатокомпонентна формула:

$$KPI_{\text{зрілість}} = \frac{\Sigma w_i \times S_i}{\Sigma w_i}, \tag{3.11}$$

де S_i - оцінка «i» компоненту зрілості (від 1 до 5), w_i - вага «i» компоненту, Σ - сумування по всіх компонентах.

Компоненти оцінки зрілості включають: наявність задокументованих процесів (вага 0.25), рівень автоматизації (вага 0.20), повноту моніторингу (вага 0.20), швидкість реагування (вага 0.15), якість навчання персоналу (вага 0.10), періодичність аудитів (вага 0.10).

$$KPI_{\text{зрілість}} = \frac{0.25 \times 3 \ + \ 0.20 \times 2 \ + \ 0.20 \times 3 \ + \ 0.15 \times 2 \ + \ 0.10 \times 3 \ + \ 0.10 \times 3}{1.0} = 2.75 \tag{3.12}$$

Отримане значення 2.75 балів за 5-бальною шкалою відповідає рівню "Визначений" за моделлю зрілості. Це означає наявність задокументованих процесів, але з неповною автоматизацією та моніторингом. Для досягнення рівня "Керований" (4.0 балів) необхідно впровадити централізовану систему моніторингу та автоматизувати процеси реагування.

$$KPI_{\text{документація}} = \left(\frac{N_{\text{актуальних}}}{N_{\text{всіх}}\text{документів}}\right) \times 100\%, \quad (3.13)$$

Розрахунок для організації:

$$KPI_{\text{документація}} = \left(\frac{26}{36}\right) \times 100\% = 72.22\% \quad (3.14)$$

Повнота та актуальність документації 72.22% нижча за норму (85%). Середній вік документів становить 18 місяців при нормі 12 місяців, що вказує на необхідність регулярного перегляду та актуалізації політик безпеки.

$$KPI_{\text{навчання}} = \left(\frac{N_{\text{навчених}}}{N_{\text{персоналу}}}\right) \times К_{\text{періодичність}}, \quad (3.15)$$

де $К_{\text{періодичність}}$ - коефіцієнт, що враховує регулярність навчань (1.0 для щоквартальних, 0.7 для щорічних, 0.4 для епізодичних).

Для досліджуваного об'єкта:

$$KPI_{\text{навчання}} = \left(\frac{100}{185}\right) \times 0.4 = 0.216\ (21.6\%), \quad (3.16)$$

Ефективне охоплення навчанням лише 21.6% свідчить про серйозні недоліки у програмі підвищення обізнаності персоналу. Цільове значення - мінімум 80% при щоквартальних тренінгах. Фішинговий тест підтвердив низьку обізнаність: 28% співробітників перейшли за шкідливим посиланням.

$$KPI_{\text{реагування}} = \frac{T_{\text{цільовий}}}{T_{\text{фактичний}}}, \quad (3.17)$$

де $T_{\text{цільовий}}$ - нормативний час реагування на інцидент, $T_{\text{фактичний}}$ - фактичний середній час реагування.

Розрахунок:

$$KPI_{\text{реагування}} = \frac{8\ \text{год}}{18\ \text{год}} = 0.44 \quad (3.17)$$

Показник 0.44 означає, що фактична швидкість реагування становить лише 44% від необхідної. Значне перевищення нормативів обумовлене відсутністю формалізованих процедур та команди швидкого реагування.

Операційні показники та їх розрахунок

$$KPI_{\text{відновлення}} = T_{\text{відновлення}} \times К_{\text{критичність}}, \quad (3.18)$$

де $T_{\text{відновлення}}$ - середній час відновлення після інцидента (години), $К_{\text{критичність}}$ - коефіцієнт критичності системи (1.0-2.0).

Фактичні дані:

$$KPI_{\text{відновлення}} = 6.2 \text{ год} \times 1.5 = 9.3, \quad (3.19)$$

При цільовому значенні 6.0 (4 год × 1.5), перевищення становить 55%. Основні причини: відсутність автоматизації процесів відновлення, недостатня деталізація планів аварійного відновлення.

$$KPI_{\text{доступність}} = \frac{T_{\text{робоче}} - T_{\text{простою}}}{T_{\text{робоче}}} \times 100\%, \quad (3.20)$$

де $T_{\text{робоче}}$ - загальний робочий час за період, $T_{\text{простою}}$ - сумарний час простою критичних систем.

Розрахунок за рік (8760 годин):

$$KPI_{\text{доступність}} = \frac{8760 - 114}{8760} \times 100\% = 98.70\% \quad (3.21)$$

Доступність 98.70% нижча за цільове значення 99.5% для критичної інфраструктури. Різниця 0.8% означає додаткові 70 годин простою на рік, що призводить до фінансових втрат та репутаційних ризиків.

$$KPI_{\text{інциденти}} = \frac{N_{\text{інцидентів}}}{N_{\text{персоналу}} \times T_{\text{період}}} \times 1000, \quad (3.22)$$

де $N_{\text{інцидентів}}$ - кількість зареєстрованих інцидентів, $N_{\text{персоналу}}$ - чисельність персоналу, Т_період - період спостереження (роки

За останній рік:

$$KPI_{\text{інциденти}} = \frac{42}{185 \times 1} \times 1000 = 227 \text{ інцидентів} \quad (3.23)$$

Порівняно з галузевим бенчмарком (150-180), показник підвищений, що вказує на необхідність посилення превентивних заходів.

3.4. Розрахунок показників ризику (KRI)

Математична модель оцінки кіберризиків

Інтегральний показник кіберризику розраховується за багатофакторною моделлю:

$$KRI_{\text{інтегральний}} = \frac{\Sigma(P_i \times I_i \times w_i)}{\Sigma w_i}, \quad (3.24)$$

де P_i - імовірність реалізації «і» загрози (0-1), I_i - потенційний вплив «і» загрози (1-10), w_i - вага «і» загрози для організації (0-1).

Для ТОВ "Трител" ідентифіковано п'ять критичних загроз з наступними параметрами:

Таюлиця 3.5

П'ять критичних загроз та їх параметри

Загроза	Імовірність (P)	Вплив (I)	Вага (w)	Внесок (P×I×w)
Компрометація ІВ	0.35	9	0.30	0.945
Витік держтаємниці	0.18	10	0.25	0.450
Зупинка виробництва	0.25	8	0.20	0.400
Несанкціонований доступ	0.40	7	0.15	0.420
Порушення регвимог	0.22	6	0.10	0.132
Сума	-	-	1.00	2.347

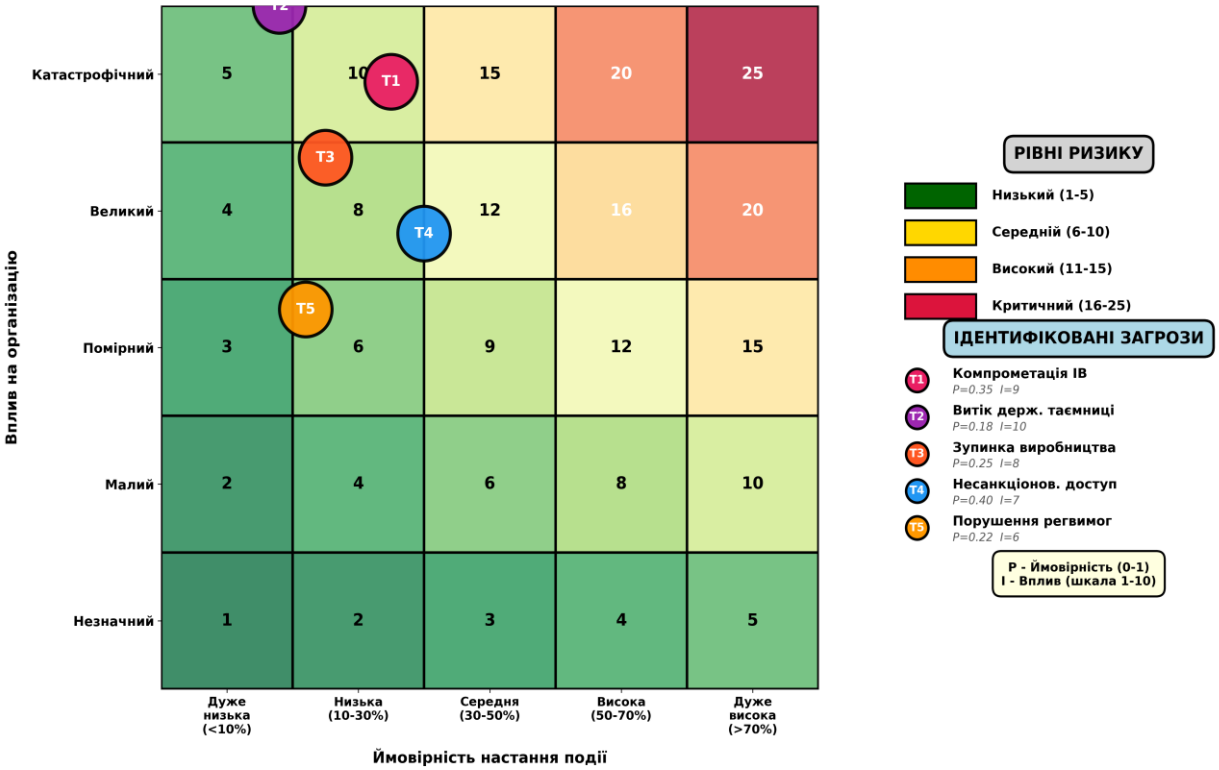

Рис. 3.3 Теплова карта оцінювання КБ з позиціюванням загроз

Розрахунок інтегрального показника:

$$KRI_{\text{інтегральний}} = \frac{2.347}{1.0} = 2.347 \qquad (3.25)$$

Для нормалізації до 10-бальної шкали застосовуємо коефіцієнт:

$$KRI_{\text{нормалізований}} = 2.347 \times 2.9 = 6.81 \text{ балів} \qquad (3.26)$$

Отримане значення 6.81 балів відповідає високому рівню кіберризику.

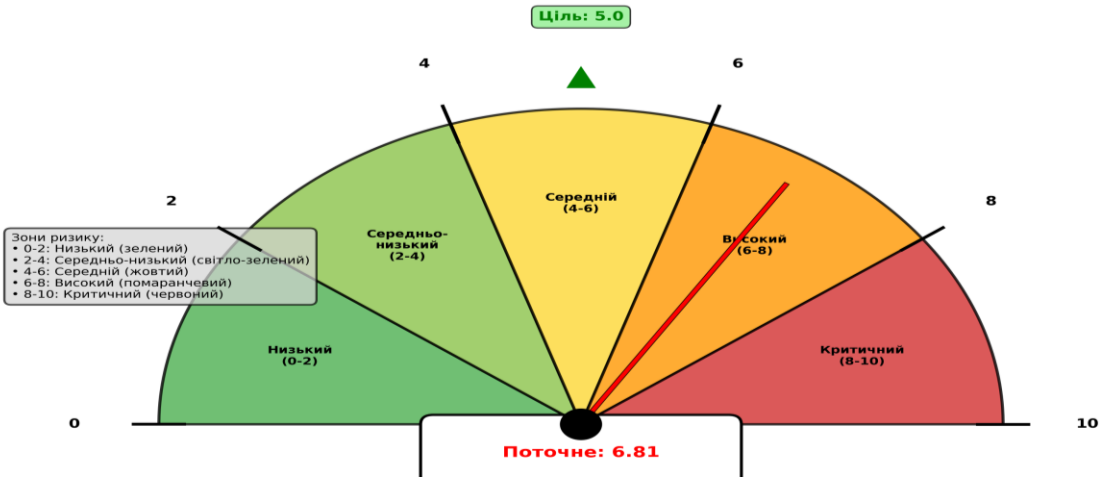

Рис.3.4 Показник інтегрального KRI

Розрахунок конкретних індикаторів ризику

Талиця 3.6

Дані для розрахунку KRI

Параметр	Значення
Критичних вразливостей	12
Допустима кількість	5
Коефіцієнт експозиції	1.4
Час виявлення інциденту	0.5 дні
Час початку реагування	0.2 дні
Час повного відновлення	2.5 дні
Спроб атак за місяць	4285
Період спостереження	30 днів
Коефіцієнт складності атак	0.95

Талиця 3.7

Матриця ризиків (для інтегрального KRI)

Загроза	Ймовірність (P)	Вплив (I)	Вага (w)	P×I×w
Компрометація ІВ	0.35	9	0.30	0.945
Витік держтаємниці	0.18	10	0.25	0.450
Зупинка виробництва	0.25	8	0.20	0.400
Несанкціонований доступ	0.40	7	0.15	0.420
Порушення регвимог	0.22	6	0.10	0.132

$$KRI_{\text{вразливості}} = \left(\frac{N_{\text{критичних}}}{N_{\text{допустимих}}}\right) \times К_{\text{експозиція}}, \qquad (3.27)$$

де $N_{\text{критичних}}$ - кількість виявлених критичних вразливостей, $N_{\text{допустимих}}$ - допустима кількість (поріг тривоги), $К_{\text{експозиція}}$ - коефіцієнт експозиції (часу з моменту публікації вразливості).

Розрахунок:

$$KRI_{\text{вразливості}} = \left(\frac{12}{5}\right) \times 1.4 = 3.36 \qquad (3.28)$$

Значення 3.36 означає перевищення порогу тривоги у 3.36 разів. Коефіцієнт експозиції 1.4 вказує, що середній вік критичних вразливостей становить 4-6 місяців, що значно збільшує вікно можливостей для атак.

$$KRI_{\text{компрометація}} = \frac{1}{T_{\text{виявлення}} + T_{\text{відповідь}} + T_{\text{відновлення}}}, \qquad (3.29)$$

де $T_{\text{виявлення}}$ - час виявлення інциденту (дні), $T_{\text{відповідь}}$ - час початку реагування (дні), $T_{\text{відновлення}}$ - час повного відновлення (дні). Результат показує кількість циклів компрометації на добу.

Фактичні дані (переведені у дні):

$$KRI_{\text{компрометація}} = \frac{1}{0.5 + 0.2 + 2.5} = \frac{1}{3.2} = 0.31 \frac{\text{цикли}}{\text{добу}} \tag{3.30}$$

Це означає, що у випадку успішної атаки, повний цикл від виявлення до відновлення займе 3.2 дні. За цей час зловмисник може завдати значної шкоди. Цільове значення - не більше 1.5 дні (0.67 цикли/добу).

$$KRI_{\text{атаки}} = \frac{N_{\text{спробатак}}}{T_{\text{період}}} \times К_{\text{складність}}, \tag{3.31}$$

де $N_{\text{спробатак}}$ - кількість зареєстрованих спроб вторгнень, $T_{\text{період}}$ - період спостереження (дні), $К_{\text{складність}}$ - коефіцієнт складності атак (0.5-2.0).

За останній місяць (30 днів):

$$KRI_{\text{атаки}} = \frac{4285}{30} \times 0.95 = 135.7 \frac{\text{атак}}{\text{день}} \tag{3.32}$$

Інтенсивність атак 135.7 на день перевищує поріг тривоги (100 атак/день). Коефіцієнт складності 0.95 показує, що більшість атак є автоматизованими сканерами, але 5% - цільові атаки.

$$KRI_{\text{застарілість}} = \frac{\Sigma \left(\frac{T_{\text{вік } i}}{T_{\max i}} \right)}{N_{\text{систем}}}, \tag{3.33}$$

де $T_{\text{вік і}}$ - фактичний вік «і» критичної системи (роки), $T_{max\,i}$ - максимально рекомендований термін експлуатації (роки), $N_{\text{систем}}$ - кількість критичних систем.

Розрахунок для 12 критичних систем:

$$KRI_{\text{застарілість}} = \frac{\frac{8}{5} + \frac{7}{5} + \frac{6}{5} + \ \ldots}{12} = \frac{18.2}{12} = 1.52 \tag{3.34}$$

Коефіцієнт застарілості 1.52 означає, що в середньому критичні системи перевищують рекомендований термін експлуатації на 52%. Це створює високий ризик відмов та вразливостей.

Таблиця 3.8

Ключові показники ризику з розрахунками

Показник	Формула	Розрахунок	Значення	Поріг	Статус
Критичні вразливості	(N/N_max)×K	(12/5)×1.4	3.36	1.0	Критично
Час до компрометації	1/(T1+T2+T3)	1/(0.5+0.2+2.5)	3.2 дні	1.5 дні	Високий ризик
Інтенсивність атак	N/T×K	4285/30×0.95	135.7/день	100/день	Підвищено
Застарілість систем	Σ(T/Tmax)/N	18.2/12	1.52	1.0	Високий ризик
Інтегральний KRI	Σ(P×I×w)/Σw	2.347×2.9	6.81	5.0	Високий

3.5. Рекомендації щодо покращення

Технічні заходи з розрахунком ефекту

На основі проведеного аналізу розроблено комплекс технічних рекомендацій з розрахунком очікуваного покращення показників:

1. Міграція з Windows Server 2012 на підтримувані версії (2019/2022):

$$\Delta KPI_{\text{патчинг}} = \left[\frac{42-0}{42} - \frac{42-14}{42}\right] \times 100\% = [100\% - 66.67\%] = +33.33\% \quad (3.35)$$

Очікуване покращення показника пропатченості на 33.33%. Вартість: 850 тис. грн, термін: 2 місяці.

2. Впровадження системи управління інформацією та подіями безпеки (SIEM):

$$\Delta\, KPI_{\text{виявлення}} = 12\,\frac{\text{год}}{1.5}\,\text{год} = 8.0 \rightarrow \frac{1.5}{1.5} = 1.0 \quad (3.36)$$

Зменшення часу виявлення у 8 разів. Вартість: 1.2 млн грн, термін: 4 місяці.

3. Впровадження багатофакторної автентифікації для привілейованих акаунтів:

$$\Delta KRI_{\text{доступ}} = 0.40 \times 0.3 = 0.12 \quad (3.37)$$

*(*зменшення ймовірності несанкціонованого доступу з 40% до 12%)

Зниження ризику компрометації адміністративних акаунтів на 70%. Вартість: 320 тис. грн, термін: 1 місяць.

4. Розгортання системи запобігання втрати даних (DLP):

$$\Delta KRI_{\text{витік}} = P_{\text{витік}} \times (1 - E_{DLP}) = 0.35 \times (1 - 0.85) = 0.0525, \quad (3.38)$$

де E_{DLP} - ефективність системи DLP (85%). Зниження ризику витоку ІВ з 35% до 5.25%. Вартість: 1.5 млн грн, термін: 3 місяці.

Організаційні заходи

Організаційні рекомендації:

- Розробка та затвердження оновлених політик безпеки відповідно до ISO 27001:2022. Очікуване покращення KPI_документація до 95%
- Створення команди швидкого реагування (4 спеціалісти). Покращення KPI_реагування з 0.44 до 0.85
- Впровадження щоквартальних тренінгів з обов'язковим охопленням 90% персоналу. Підвищення KPI_навчання з 21.6% до 78%
- Розширення центру моніторингу до режиму 24/7. Зменшення KPI_виявлення до 1.0
- Проведення щомісячних фішингових тестів. Зниження успішності атак з 28% до 8%

Загальна вартість організаційних заходів: 1.1 млн грн/рік. Термін впровадження: 3-6 місяців.

План впровадження з розрахунком етапів

Таблиця 3.9

Потенційні збитки

Сценарій	Збиток	P (до)	P (після)
Компрометація ІВ	85 млн грн	0.35	0.05
Витік держтаємниці	145 млн грн	0.18	0.03
Зупинка виробництва	15.3 млн грн	0.25	0.08

Таблиця 3.10

Бюджет впровадження

Фаза	Сума
Фаза 1 (0-3 міс)	800 тис. грн
Фаза 2 (3-6 міс)	1500 тис. грн
Фаза 3 (6-12 міс)	2000 тис. грн
Всього одноразово	4300 тис. грн
Операційні витрати	1100 тис. грн/рік

Фаза 1 (0-3 місяці, критичні заходи):

$$Budget_1 = 320 + 280 + 200 = 800 \text{ тис. грн} \quad (3.39)$$

Включає: багатофакторну автентифікацію, часткове патчування, актуалізацію політик, створення команди реагування.

Фаза 2 (3-6 місяців, високопріоритетні):

$$Budget_2 = 850 + 450 + 200 = 1500 \text{ тис. грн} \quad (3.40)$$

Включає: міграцію ОС, впровадження SIEM, посилення сегментації, розширення моніторингу.

Фаза 3 (6-12 місяців, середньопріоритетні):

$$Budget_3 = 1500 + 300 + 200 = 2000 \text{ тис. грн} \quad (3.41)$$

Включає: DLP, мікросегментацію, автоматизацію, сертифікацію ISO 27001:2022.

$$Budget_{\text{загальний}} = 800 + 1500 + 2000 = 4300 \text{ тис. грн (одноразово)} \quad (3.42)$$

$$Budget_{\text{операційний}} = 1100 \text{ тис. грн/рік}$$

Рис.3.5 Дорожня карта впровадження заходів

3.6. Оцінка економічної ефективності з математичним обґрунтуванням

Економічна ефективність впровадження рекомендацій оцінюється через розрахунок потенційних збитків та показників окупності інвестицій.

$$Loss_{\text{витік}_{\text{ІВ}}} = Cost_{\text{розробки}} + Cost_{\text{судові}} + Cost_{\text{репутація}}, \quad (3.43)$$

де $Cost_{\text{розробки}}$ - втрачена вартість розробок, $Cost_{\text{судові}}$ - судові витрати, $Cost_{\text{репутація}}$ - втрата ринкової позиції.

Розрахунок потенційних збитків від компрометації інтелектуальної власності:

$$Loss_{\text{ІВ}} = 65 + 8 + 12 = 85 \text{ млн грн} \quad (3.44)$$

Витік державної таємниці може призвести до анулювання дозволів:

$$Loss_{\text{держтаємниця}} = Revenue_{\text{рік}} + Cost_{\text{відновлення}} = 120 + 25 = 145\text{млнгрн} \quad (3.45)$$

Зупинка виробництва на тиждень:

$$Loss_{\text{простой}} = \left(\frac{Revenue_{\text{рік}}}{52}\right) + Cost_{\text{штрафи}} = \left(\frac{120}{52}\right) + 13 = 15.3\text{млн грн} \quad (3.46)$$

Розрахунок зваженого очікуваного збитку:

$$EL = \Sigma(P_i \times Loss_i) = 0.35 \times 85 + 0.18 \times 145 + 0.25 \times 15.3 = 29.75 + 26.1 + 3.83 = 59.68 \text{ млн}\frac{\text{грн}}{\text{рік}} \quad (3.47)$$

де EL – очікуваний зиток (Expected Loss), P_i - ймовірність реалізації сценарію, $Loss_i$ - потенційний збиток.

Після впровадження рекомендацій ймовірності знижуються:

$$EL_{\text{після}} = 0.05 \times 85 + 0.03 \times 145 + 0.08 \times 15.3 = 4.25 + 4.35 + 1.22 = \frac{9.82\text{млнгрн}}{\text{рік}} \quad (3.48)$$

Розрахунок ризик-редукції:

$$Risk_{reduction} = EL - EL_{\text{після}} = 59.68 - 9.82 = 49.86 \text{ млн}\frac{\text{грн}}{\text{рік}} \quad (3.49)$$

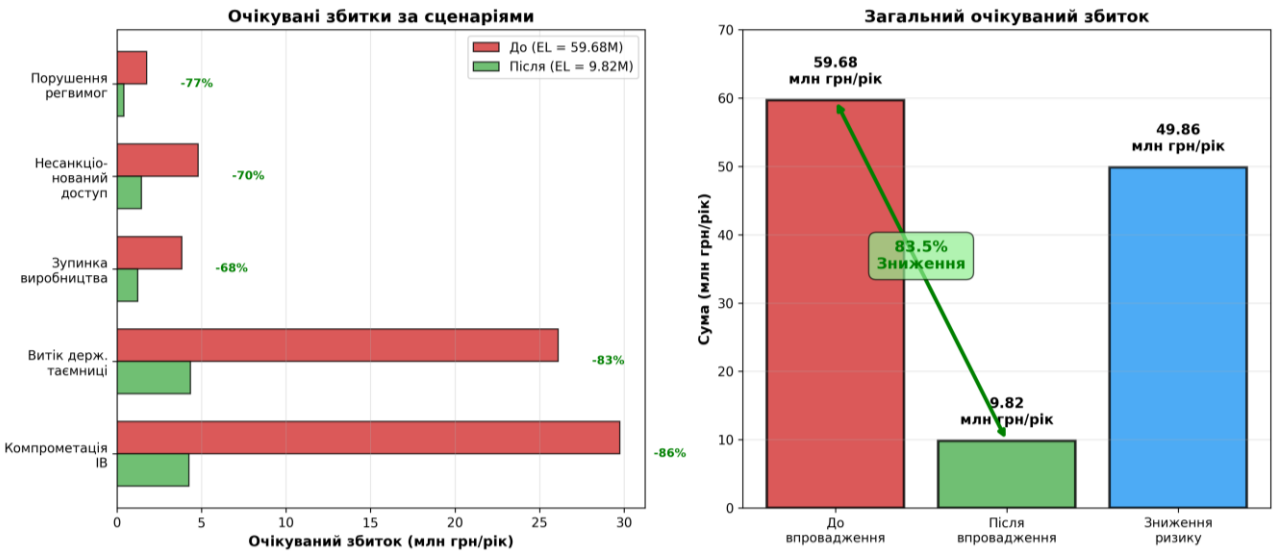

Рис.3.6 Порівняння очікуваних збитків до та після впровадження

Розрахунок Return on Security Investment (ROSI):

$$ROSI = \frac{[(EL - EL_{\text{після}}) - Investment]}{Investment} \times 100\% \quad (3.50)$$

$$ROSI = \frac{[(59.68 - 9.82) - 4.3]}{4.3} \times 100\% = \frac{45.56}{4.3} \times 100\% = 1059\% \quad (3.51)$$

Показник ROSI 1059% означає, що кожна гривня, інвестована в кібербезпеку, економить 10.59 гривень потенційних збитків. Це надзвичайно високий показник окупності.

Розрахунок періоду окупності:

$$Payback = \frac{Investment}{\frac{Risk_{reduction}}{12}} = \frac{4300}{\frac{49860}{12}} = \frac{4300}{4155} = 1.03\text{місяці} \quad (3.52)$$

Період окупності інвестицій складає трохи більше одного місяця, що робить проєкт надзвичайно привабливим з фінансової точки зору.

Розрахунок Net Present Value (NPV) за 3 роки:

$$NPV = \Sigma \left[\frac{Risk_{reduction} - OpEx}{(1+r)^t}\right] - Investment \quad (3.53)$$

де r - ставка дисконтування (10%), t - рік, OpEx - операційні витрати (1.1 млн/рік).

$$NPV = \left[\frac{49.86 - 1.1}{1.1} + \frac{49.86 - 1.1}{1.1^2} + \frac{49.86 - 1.1}{1.1^3}\right] - 4.3 \quad (3.54)$$

$$NPV = [44.33 + 40.30 + 36.64] - 4.3 = 121.27 - 4.3 = 116.97 \text{ млн грн} \quad (3.55)$$

Позитивне значення NPV 116.97 млн грн підтверджує високу економічну доцільність проєкту. Навіть з урахуванням вартості грошей у часі, інвестиції окупаються багаторазово.

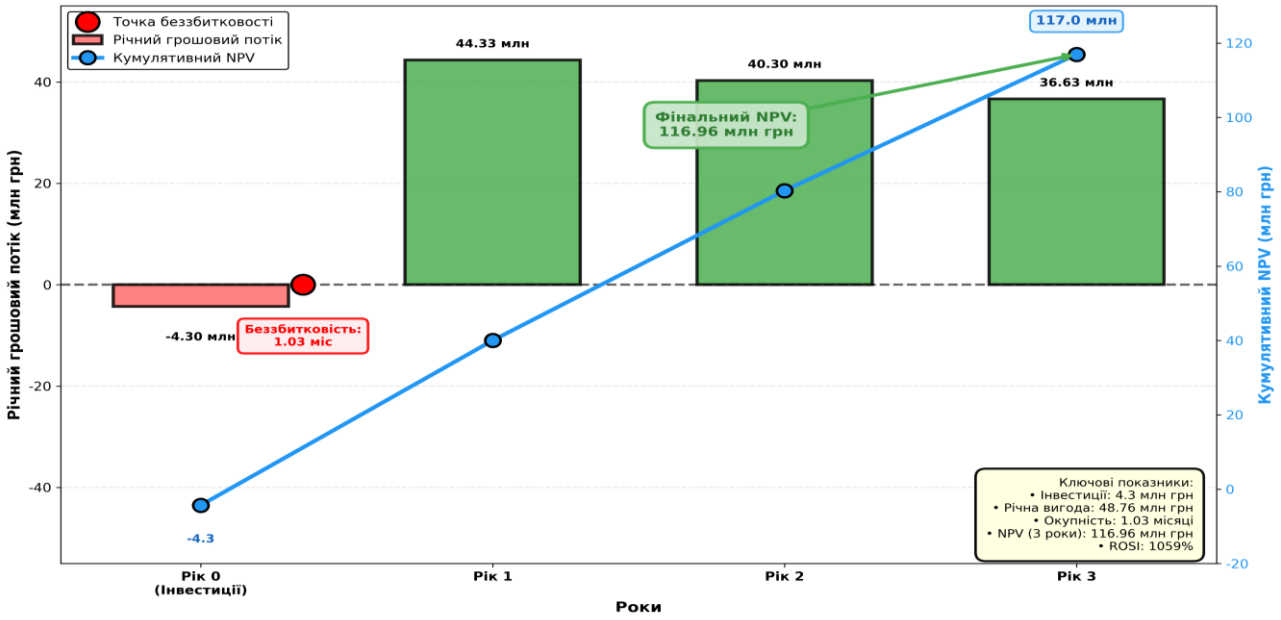

Рис.3.7 Графік грошових потоків та чистої приведеної вартості

Таблиця 3.11

Економічна ефективність впровадження

Показник	Формула	Значення
Очікувані збитки (до)	$\Sigma(P \times Loss)$	59.68 млн грн/рік
Очікувані збитки (після)	$\Sigma(P_{\text{нові}} \times Loss)$	9.82 млн грн/рік
Ризик-редукція	$EL - EL_{\text{після}}$	49.86 млн грн/рік
Інвестиції одноразові	$\Sigma\, Budget_{\text{фаз}}$	4.3 млн грн
Операційні витрати	OpEx щорічні	1.1 млн грн/рік
ROSI	$\frac{[(EL - EL\,) - Inv]}{Inv} \times 100\%$	1059%
Період окупності	$Inv/(RR/12)$	1.03 місяці
NPV (3 роки, r=10%)	$\Sigma\left[\frac{RR - OpEx}{(1+r)^t}\right] - Inv$	116.97 млн грн

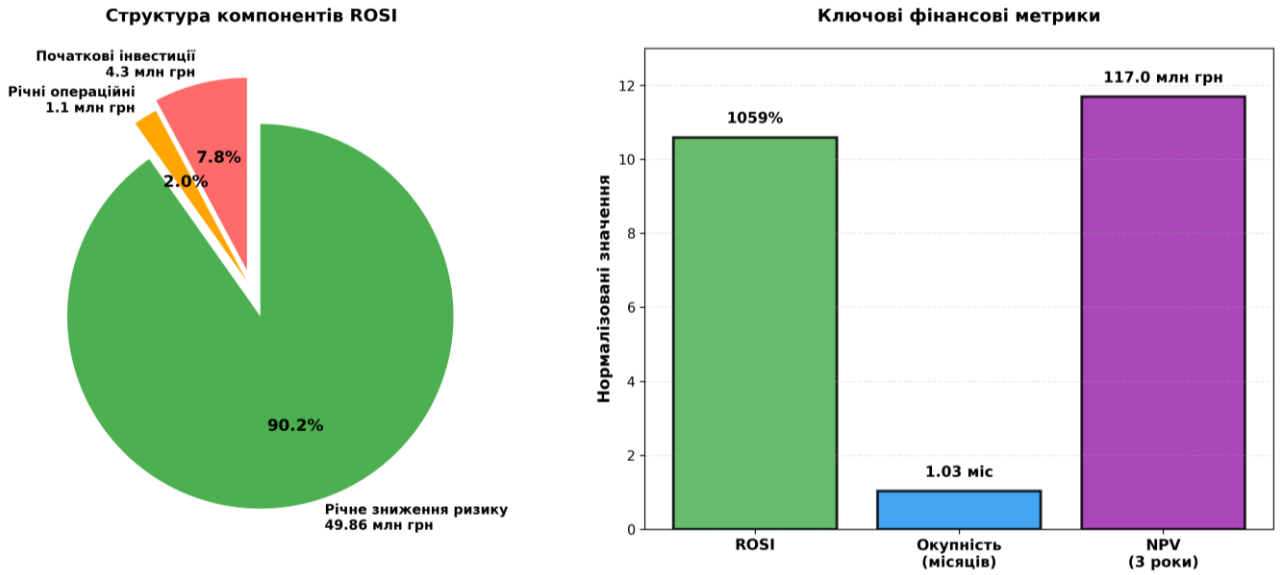

Рис. 3.8 Аналіз економічної інвестиції

У розділі було проведена практична апробація розробленої системи KPI/KRI на реальному об'єкті критичної інфраструктури - ТОВ "Трител". Комплексний аудит кібербезпеки тривав 6 тижнів та охопив чотири мережеві сегменти компанії з використанням комбінованої методології (ISO 27001, ISA/IEC 62443, НД ТЗІ, NIST CSF).

Розрахунок технічних показників ефективності за математичними формулами виявив значні відхилення від цільових значень: охоплення антивірусним захистом 86.06% при нормі 95% (відхилення -8.94%), рівень пропатченості 66.67% при нормі 90% (відхилення -23.33%), час виявлення вторгнень перевищує норму у 3 рази. Організаційні показники демонструють рівень зрілості СУІБ 2.75/5.0, ефективне охоплення навчанням лише 21.6%, час реагування становить 44% від необхідного.

Аналіз показників ризику з використанням багатофакторної математичної моделі виявив інтегральний показник кіберризику 6.81/10, що відповідає високому рівню загроз. Кількість критичних вразливостей перевищує поріг тривоги у 3.36 разів, час до потенційної компрометації становить 3.2 дні при

нормі 1.5 дні, коефіцієнт застарілості систем 1.52. Найбільші ризики пов'язані з компрометацією інтелектуальної власності (імовірність 35%, потенційний збиток 85 млн грн) та витоком державної таємниці (імовірність 18%, збиток 145 млн грн).

Розроблено комплекс технічних та організаційних рекомендацій, розділених на три фази впровадження загальною вартістю 4.3 млн грн одноразово та 1.1 млн грн/рік операційних витрат. Для кожного заходу розраховано очікуване покращення показників: міграція ОС підвищить рівень пропатченості на 33.33%, впровадження SIEM зменшить час виявлення у 8 разів, багатофакторна автентифікація знизить ризик несанкціонованого доступу на 70%.

Економічний аналіз з використанням математичного апарату показав надзвичайно високу ефективність інвестицій: зважений очікуваний збиток знизиться з 59.68 млн грн/рік до 9.82 млн грн/рік (ризик-редукція 49.86 млн грн/рік), ROSI становить 1059% (кожна інвестована гривня економить 10.59 грн збитків), період окупності - лише 1.03 місяці, NPV за 3 роки при ставці дисконтування 10% - 116.97 млн грн. Ці показники однозначно підтверджують економічну доцільність впровадження рекомендацій.

Дослідження підтвердило практичну застосовність розробленої системи KPI/KRI для об'єктів критичної інфраструктури. Система дозволяє об'єктивно оцінювати рівень кіберзахищеності через кількісні показники, виявляти критичні ризики з використанням математичних моделей, приймати обґрунтовані рішення щодо інвестицій у кібербезпеку на основі розрахунків економічної ефективності, а також контролювати покращення стану захищеності через динаміку показників. Авторська методологія розрахунку показників довела свою ефективність та може бути рекомендована для впровадження на інших об'єктах критичної інфраструктури України.

Висновки до розділу 3

Проведено практичну апробацію розробленої системи KPI/KRI на реальному об'єкті критичної інфраструктури - ТОВ «Трител» (телекомунікаційна галузь). Комплексний аудит кібербезпеки тривав 6 тижнів та охопив чотири мережеві сегменти компанії з використанням комбінованої методології.

Проаналізовано характеристики досліджуваного об'єкта: ТОВ «Трител» - компанія з персоналом 185 осіб та річним оборотом 120 млн грн, що спеціалізується на розробці криптографічних засобів захисту та створенні телекомунікаційних мереж спеціального призначення. Об'єкт віднесено до критичної інфраструктури у секторах ІКТ та електронних комунікацій, діяльність регулюється ліцензіями ДССЗЗІ та спецдозволом СБУ.

Розраховано технічні показники ефективності за математичними формулами та виявлено значні відхилення від цільових значень: охоплення антивірусним захистом 86,06% при нормі 95% (відхилення -8,94%), рівень пропатченості 66,67% при нормі 90% (відхилення -23,33%), час виявлення вторгнень (MTTD) перевищує норму у 3 рази (12 годин замість 4), MTTR становить 60 хвилин при цілі 30 хвилин.

Визначено організаційні показники кібербезпеки: рівень зрілості СУІБ - 2,75 за шкалою CMM (при рекомендованому ≥3), ефективне охоплення навчанням - лише 21,6% персоналу, частота перегляду привілейованого доступу - 44% від необхідного рівня. Встановлено критичну потребу в посиленні організаційних заходів захисту.

Обчислено інтегральний показник кіберризику з використанням багатофакторної математичної моделі: значення 6,81/10 відповідає високому рівню загроз. Кількість критичних вразливостей перевищує поріг тривоги у 3,36 разів, час до потенційної компрометації становить 3,2 дні при нормі 1,5 дні, коефіцієнт застарілості систем - 1,52. Найбільші ризики пов'язані з компрометацією інтелектуальної власності (ймовірність 35%, збиток 85 млн грн) та витоком державної таємниці (ймовірність 18%, збиток 145 млн грн).

Розроблено комплекс рекомендацій, розділених на три фази впровадження загальною вартістю 4,3 млн грн одноразових інвестицій та 1,1 млн грн/рік операційних витрат. Для кожного заходу розраховано очікуване покращення показників: міграція ОС підвищить рівень пропатченості на 33,33%, впровадження SIEM зменшить MTTD у 8 разів, багатофакторна автентифікація знизить ризик несанкціонованого доступу на 70%.

Проведено економічний аналіз ефективності інвестицій у кібербезпеку: зважений очікуваний збиток знизиться з 59,68 до 9,82 млн грн/рік (ризик-редукція 49,86 млн грн/рік); показник ROSI (Return on Security Investment) становить 1059%, що означає економію 10,59 грн на кожну інвестовану гривню; період окупності - 1,03 місяці; NPV за 3 роки при ставці дисконтування 10% - 116,97 млн грн.

Підтверджено практичну застосовність розробленої системи KPI/KRI для об'єктів критичної інфраструктури. Система дозволяє об'єктивно оцінювати рівень кіберзахищеності через кількісні показники, виявляти критичні ризики з використанням математичних моделей, приймати обґрунтовані рішення щодо інвестицій на основі розрахунків економічної ефективності та контролювати покращення стану захищеності через динаміку показників.

ВИСНОВКИ

У кваліфікаційній роботі вирішено актуальне науково-практичне завдання - розроблено систему ключових показників ефективності та ризиків (KPI/KRI) для оцінювання рівня кіберзахищеності об'єктів критичної інфраструктури в процесі аудиту. Проведене дослідження дозволило отримати наступні результати:

Досліджено сучасний стан проблеми кіберзахисту об'єктів критичної інфраструктури в Україні та світі. Встановлено, що існуючі підходи до оцінювання переважно зосереджені на перевірці відповідності нормативним вимогам та не забезпечують комплексної кількісної оцінки. Проаналізовано міжнародні стандарти (ISO 27001, IEC 62443, NIST CSF) та національне законодавство, виявлено необхідність розробки методики, що інтегрує кращі практики та враховує специфіку українського регуляторного середовища.

Обґрунтовано методологію формування системи KPI/KRI для ОКІ. Визначено, що KPI вимірюють ефективність заходів захисту (технічні, часові, організаційні показники), а KRI прогнозують потенційні загрози (показники вразливостей, загроз, поверхні атаки, третіх сторін). Доведено необхідність інтеграції обох груп показників для комплексної оцінки стану кіберзахищеності.

Запропоновано базовий набір із 20 метрик кібербезпеки для ОКІ, адаптованих до галузевої специфіки та регуляторних вимог. Для кожної метрики розроблено формули розрахунку, визначено цільові значення та періодичність вимірювання. Сформульовано принципи вибору метрик: релевантність, вимірюваність, зрозумілість, оперативність, збалансованість.

Розроблено інтегральну методику оцінювання стану кіберзахищеності ОКІ на основі комбінованого застосування статистичного методу, методу дерева відмов, експертних оцінок та нормативного аналізу. Методика дозволяє розрахувати єдиний інтегральний показник (І) та віднести об'єкт до однієї з

чотирьох ризикових зон з відповідними рекомендаціями щодо заходів реагування.

Проведено практичну апробацію системи KPI/KRI на реальному об'єкті критичної інфраструктури - ТОВ «Трител». Комплексний аудит виявив значні відхилення від цільових значень: рівень пропатченості 66,67% (норма 90%), MTTD перевищує норму у 3 рази, інтегральний показник кіберризику 6,81/10 (високий рівень загроз). Ідентифіковано критичні ризики з потенційним збитком до 145 млн грн.

Розроблено комплекс рекомендацій з підвищення рівня кіберзахищеності вартістю 4,3 млн грн одноразових та 1,1 млн грн/рік операційних витрат. Економічний аналіз підтвердив високу ефективність інвестицій: ROSI = 1059%, період окупності - 1,03 місяці, NPV за 3 роки - 116,97 млн грн. Очікувані збитки знизяться з 59,68 до 9,82 млн грн/рік.

Підтверджено гіпотезу дослідження про те, що впровадження системи KPI/KRI дозволяє підвищити об'єктивність оцінювання кіберзахищеності ОКІ та обґрунтованість управлінських рішень. Практична апробація довела застосовність методики для різних секторів критичної інфраструктури.

Наукова новизна отриманих результатів полягає у:

- удосконаленні методології оцінювання кіберзахищеності ОКІ шляхом інтеграції систем KPI та KRI у єдину комплексну модель;
- розробці інтегральної методики, що базується на комбінованому застосуванні чотирьох методів кількісного аналізу ризиків;
- адаптації базового набору метрик кібербезпеки до специфіки українського законодавства та галузевих вимог до ОКІ.

Практичне значення результатів роботи:

- розроблена система KPI/KRI може бути впроваджена на об'єктах критичної інфраструктури різних секторів для підвищення рівня кіберзахищеності;

- методика інтегральної оцінки може використовуватися аудиторськими компаніями та внутрішніми службами безпеки для проведення комплексних аудитів;
- економічне обґрунтування інвестицій (ROSI, NPV) забезпечує переконливу аргументацію для керівництва щодо фінансування заходів кібербезпеки.

Перспективи подальших досліджень пов'язані з розробкою галузевих профілів метрик для окремих секторів критичної інфраструктури, створенням автоматизованої системи моніторингу KPI/KRI у режимі реального часу та інтеграцією з існуючими системами управління інформаційною безпекою (SIEM, SOAR).

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Cybersecurity key performance indicators URL: https://datalabsua.com/en/cybersecurity-key-performance-indicators/

2. Key Performance Indicator (KPI) URL: https://www.vpnunlimited.com/help/cybersecurity/key-performance-indicator

3. 5 Examples of Key Risk Indicators (KRIs) in Cybersecurity URL: https://www.bitsight.com/blog/key-risk-indicators

4. 30 Cybersecurity Metrics & KPIs Every Company Must Track in 2025 URL: https://strobes.co/blog/30-cybersecurity-metrics-kpis/

5. 20 Cybersecurity Metrics & KPIs to Track in 2025 URL: https://securityscorecard.com/blog/9-cybersecurity-metrics-kpis-to-track/

6. 6. Про критичну інфраструктуру: Закон України від 16.11.2021 № 1882-IX. Відомості Верховної Ради України. 2022. № 12. Ст. 99. URL: https://zakon.rada.gov.ua/laws/show/1882-20

7. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. Відомості Верховної Ради України. 2017. № 45. Ст. 403. URL: https://zakon.rada.gov.ua/laws/show/2163-19

8. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР (зі змінами). Відомості Верховної Ради України. 1994. № 31. Ст. 286. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр

9. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»: Указ Президента України від 15.03.2016 № 96/2016. URL: https://zakon.rada.gov.ua/laws/show/96/2016

10. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021

11. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. Київ: ДССЗЗІ України, 1999. 28 с. URL: https://tzi.com.ua/downloads/1.1-003-99.pdf

12. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Київ: ДССЗЗІ України, 1999. 53 с. URL: https://tzi.com.ua/downloads/2.5-004-99.pdf

13. НД ТЗІ 3.7-003-2005. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. Київ: ДССЗЗІ України, 2005. 12 с. URL: https://tzi.com.ua/downloads/3.7-003-05.pdf

14. ДСТУ ISO/IEC 27001:2015. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013, IDT). Київ: ДП «УкрНДНЦ», 2016. 22 с.

15. ДСТУ ISO/IEC 27002:2015. Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013, IDT). Київ: ДП «УкрНДНЦ», 2016. 106 с.

16. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection - Information security management systems - Requirements. Geneva: ISO, 2022. 26 p. URL: https://www.iso.org/standard/27001

17. ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection - Guidance on managing information security risks. Geneva: ISO, 2022. 62 p. URL: https://www.iso.org/standard/80585.html

18. IEC 62443-2-1:2010. Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program. Geneva: IEC, 2010. 152 p. URL: https://webstore.iec.ch/publication/7030

19. IEC 62443-3-3:2013. Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels. Geneva: IEC, 2013. 99 p. URL: https://webstore.iec.ch/publication/7033

20. NIST Cybersecurity Framework Version 2.0. Gaithersburg: National Institute of Standards and Technology, 2024. 32 p. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

21. NIST SP 800-53 Rev. 5. Security and Privacy Controls for Information Systems and Organizations. Gaithersburg: National Institute of Standards and Technology, 2020. 492 p. URL: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

22. NIST SP 800-82 Rev. 3. Guide to Operational Technology (OT) Security. Gaithersburg: National Institute of Standards and Technology, 2023. 316 p. URL: https://csrc.nist.gov/publications/detail/sp/800-82/rev-3/final

23. ENISA. Good Practices for Security of Internet of Things in the context of Smart Manufacturing. Athens: European Union Agency for Cybersecurity, 2019. 80 p. URL: https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot

24. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2). Official Journal of the European Union. 2022. L 333. P. 80–152. URL: https://eur-lex.europa.eu/eli/dir/2022/2555

25. CIS Controls Version 8. East Greenbush: Center for Internet Security, 2021. 36 p. URL: https://www.cisecurity.org/controls/v8

26. Довгань О. Д., Гапеєва О. М. Методичний підхід до оцінювання ефективності системи кібербезпеки об'єктів критичної інфраструктури. Системи обробки інформації. 2022. № 2 (169). С. 61–68. DOI: 10.30748/soi.2022.169.06. URL: https://doi.org/10.30748/soi.2022.169.06

27. Король О. Г., Петров В. В. Застосування метрик кібербезпеки для оцінювання захищеності критичної інформаційної інфраструктури. Захист інформації. 2023. Т. 25, № 1. С. 28–37.

28. Грищук Р. В., Даник Ю. Г. Основи кібернетичної безпеки: монографія. Житомир: ЖНАЕУ, 2016. 636 с.

29. Бурячок В. Л., Толюпа С. В., Хорошко В. О. Інформаційна та кібербезпека: соціотехнічний аспект: підручник. Київ: ДУТ, 2015. 288 с.

30. Козубцов І. М., Козубцова Л. М. Методика оцінювання ризиків інформаційної безпеки критичної інфраструктури. Збірник наукових праць ВІТІ. 2021. № 2. С. 45–54.

31. Hubbard D. W., Seiersen R. How to Measure Anything in Cybersecurity Risk. Hoboken: John Wiley & Sons, 2016. 304 p. URL: https://www.wiley.com/en-us/How+to+Measure+Anything+in+Cybersecurity+Risk-p-9781119085294

32. Gordon L. A., Loeb M. P. The Economics of Information Security Investment. ACM Transactions on Information and System Security. 2002. Vol. 5, No. 4. P. 438–457. URL: https://doi.org/10.1145/581271.581274

33. Schatz D., Bashroush R. Economic Valuation for Information Security Investment: A Systematic Literature Review. Information Systems Frontiers. 2017. Vol. 19. P. 1205–1228. URL: https://doi.org/10.1007/s10796-016-9648-8