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: “ МЕТОДИКА ЗАСТОСУВАННЯ ФРЕЙМВОРКУ NIST CSF 2.0 ДЛЯ ОЦІНКИ РІВНЯ КІБЕРЗРІЛОСТІ ОБ’ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ”

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

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

_____ Іван КРИВОВ’ЯЗ
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД-41

Іван КРИВОВ’ЯЗ
Ім’я, ПРІЗВИЩЕ

Керівник: Юрій ЩАВІНСЬКИЙ
к.т.н., доцент Ім’я, ПРІЗВИЩЕ

Рецензент: Юрій ПЕПА
к.т.н., доцент Ім’я, ПРІЗВИЩЕ

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут кібербезпеки та захисту інформації

Кафедра управління кібербезпекою та захистом інформації

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УКБЗІ
_____ Світлана ЛЕГОМІНОВА
“____”_____2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Кривов’язу Івану Ярославовичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “ Методика застосування фреймворку NIST CSF 2.0 для оцінки рівня кіберзрілості об’єктів критичної інфраструктури ”,
керівник кваліфікаційної роботи ЩАВІНСЬКИЙ Юрій, к.т.н., доцент
(ПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологійвід “24“ лютого 2025 р. №56.

2. Строк подання кваліфікаційної роботи “12” травня 2025р.

3. Вихідні дані до кваліфікаційної роботи: *нормативно-правові документи оцінювання об’єктів критичної інфраструктури, методи оцінювання рівня кіберзрілості, фреймворк NIST CSF.*

4. Перелік питань, які мають бути розроблені:
4.1. Дослідити структуру та функціональні можливості фреймворку NIST CSF 2.0 у контексті оцінки кіберзрілості.
4.2. Розробити методику оцінювання рівня кіберзахисту на основі NIST CSF з урахуванням специфіки критичної інфраструктури.
4.3. Провести тестову оцінку кіберзрілості підприємства з використанням визначеної методики.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “5“ березня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2025	Виконано
2.	Збір та аналіз літератури.	29.03.2025	Виконано
3.	Дослідження структури та функціональних можливостей фреймворку NIST CSF 2.0 у контексті оцінки кіберзрілості	08.04.2025	Виконано
4.	Розробка методики оцінювання кіберзрілості об’єктів критичної інфраструктури на основі фреймворку NIST CSF 2.0 та її адаптація до національного контексту.	15.04.2025	Виконано
5.	Тестування методики на умовному об’єкті, аналіз результатів та формування обґрунтованих рекомендацій щодо підвищення кіберзахисту.	22.04.2025	Виконано
6.	Формулювання висновків за результатами проведеного дослідження.	29.04.2025	Виконано
7.	Оформлення роботи.	06.05.2025	Виконано
8.	Оформлення презентації.	09.05.2025	Виконано
9.	Отримання рецензії на роботу.	12.06.2025	Виконано
10.	Захист в ДЕК.	__.06.2025	

Здобувач вищої освіти _____ Іван КРИВОВ’ЯЗ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Юрій ЩАВІНСЬКИЙ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

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

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

Направляється здобувач Кривов'яз І.Я. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: " Методика застосування фреймворку NIST CSF 2.0 для оцінки рівня кіберзрілості об'єктів критичної інфраструктури "

Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувач КРИВОВ'ЯЗ Іван у кваліфікаційній роботі дослідив методику застосування фреймворку NIST CSF 2.0 для оцінки кіберзрілості об'єктів критичної інфраструктури. У роботі проаналізовано ключові функції фреймворку, проведено огляд нормативно-правового поля України у сфері кіберзахисту об'єктів критичної інфраструктури, розроблена методика оцінювання а також розглянуто реалістичний сценарій застосування методики на умовному об'єкті телекомунікаційного сектору.

КРИВОВ'ЯЗ Іван продемонстрував глибоке розуміння методології кіберзахисту, вміння працювати з сучасними фреймворками, аналітичне мислення, здатність до самостійного дослідження і формулювання практичних висновків. Здобувач проявив себе як відповідальний і підготовлений виконавець, що володіє навичками дослідження в галузі кібербезпеки.

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

Керівник кваліфікаційної роботи _____ Юрій ЩАВІНСЬКИЙ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____"_____2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Кривов'яз І.Я. допускається до захисту даної роботи в Екзаменаційній комісії.

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

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувача вищої освіти КРИВОВ'ЯЗА Івана
на тему " Методика застосування фреймворку NIST CSF 2.0 для оцінки рівня кіберзрілості об'єктів критичної інфраструктури"

Актуальність. В умовах зростання масштабів і складності кібератак на критичну інфраструктуру, питання системної оцінки рівня її захищеності набуває особливого значення. Використання фреймворків управління кіберризиками, зокрема оновленого NIST Cybersecurity Framework 2.0, дозволяє структурувати процеси безпеки, оцінити рівень кіберзрілості організацій та сформувати обґрунтовані рекомендації щодо підвищення стійкості до загроз.

У цьому контексті тема роботи є вкрай актуальною, особливо з урахуванням українських реалій – постійних кібератак на об'єкти критичної інфраструктури під час збройної агресії.

Позитивні сторони.

1. У роботі системно представлено структуру та можливості застосування NIST CSF 2.0, включно з аналізом функцій, профілів, рівнів зрілості та їх адаптацією до українського нормативного поля.
2. Розроблено та апробовано практичну методику оцінки кіберзрілості, яка враховує специфіку критичної інфраструктури, результати апробації дозволяють зробити висновок про її ефективність.
3. Дослідження містить достатній огляд сучасної нормативної бази, аналіз загроз та обґрунтовані рекомендації для вдосконалення кіберзахисту об'єктів критичної інфраструктури.

Недоліки.

Доцільно було б розширити дослідження в напрямку автоматизації процесу оцінки кіберзрілості з використанням інструментів типу CSF Assessment Tools або GRC-рішень та більшої уваги до метрик ефективності в контексті кіберзахисту.

Однак, вищезгадані зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на високому науково-практичному рівні та заслуговує оцінки "відмінно". Здобувач КРИВОВ'ЯЗ Іван заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент:
к.т.н., доцент _____ Юрій ПЕПА
підпис Ім'я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена розробці та обґрунтуванню методики застосування фреймворку NIST Cybersecurity Framework 2.0 для оцінки рівня кіберзрілості об’єктів критичної інфраструктури (ОКІ) України. Робота складається зі вступу, чотирьох основних розділів, висновків, списку використаних джерел. Загальний обсяг становить 72 аркуші, з яких 8 аркушів займають перелік умовних скорочень та список використаних джерел.

Метою роботи є розробка та обґрунтування методики застосування фреймворку NIST Cybersecurity Framework 2.0 для оцінки рівня кіберзрілості об’єктів критичної інфраструктури з метою підвищення рівня їхньої захищеності від сучасних кіберзагроз.

Об’єктом дослідження є управління кібербезпекою об'єктів критичної інфраструктури та оцінка їхнього рівня кіберзрілості відповідно до вимог та рекомендацій NIST CSF 2.0.

Предмет дослідження – методи оцінки рівня кіберзрілості об’єктів критичної інфраструктури на основі фреймворку NIST CSF 2.0.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи системного аналізу, моделювання загроз, аналізу нормативних вимог.

Як результат, у роботі сформовано методику оцінки кіберзрілості на основі фреймворку NIST CSF 2.0, проведено її апробацію на умовному об’єкті критичної інфраструктури, виявлено ключові недоліки в системі кіберзахисту та надано практичні рекомендації щодо їх усунення.

Галузь застосування. Результати дослідження можуть бути використані підприємствами критичної інфраструктури, державними регуляторами та аудиторськими структурами під час оцінювання рівня кіберзрілості, розробки політик кіберзахисту та побудови систем управління інформаційною безпекою.

Ключові слова: КІБЕРЗРІЛІСТЬ, КІБЕРБЕЗПЕКА, КРИТИЧНА ІНФРАСТРУКТУРА, ФРЕЙМВОРК, МЕТОДИКА ОЦІНКИ.

ABSTRACT

The qualification work is devoted to the development and substantiation of the methodology for applying the NIST Cybersecurity Framework 2.0 to assess the level of cyber maturity of critical infrastructure facilities (CIF) in Ukraine. The paper consists of an introduction, four main sections, conclusions, and a list of references. The total volume is 66 pages, of which 5 pages are occupied by the list of abbreviations and references.

The purpose of the study is to develop and substantiate the methodology for applying the NIST Cybersecurity Framework 2.0 to assess the level of cyber maturity of critical infrastructure facilities in order to increase their level of protection against modern cyber threats.

The object of the study is to manage the cybersecurity of critical infrastructure facilities and assess their cyber maturity level in accordance with the requirements and recommendations of NIST CSF 2.0.

The subject of the study is the methods for assessing the level of cyber maturity of critical infrastructure based on the NIST CSF 2.0.

Research methods. To solve the above scientific task, the paper uses the methods of system analysis, threat modeling, and analysis of regulatory requirements.

As a result, the paper developed a methodology for assessing cyber maturity based on the NIST CSF 2.0 framework, tested it on a conditional critical infrastructure facility, identified key shortcomings in the cyber defense system and provided practical recommendations for their elimination.

Field of application. The results of the study can be used by critical infrastructure enterprises, government regulators and auditors in assessing the level of cyber maturity, developing cyber defense policies and building information security management systems.

Keywords: CYBER MATURITY, CYBERSECURITY, CRITICAL INFRASTRUCTURE, FRAMEWORK, ASSESSMENT METHODOLOGY.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

CSF	Cybersecurity Framework
KPI	Key Performance Indicator
NIST	National Institute of Standards and Technology
SIEM	Security Information and Event Management
ДССЗЗІ	Державна служба спеціального зв’язку та захисту інформації України
ІБ	Інформаційна безпека
ІС	Інформаційна система
ІТ	Інформаційні технології
КІІ	Критична інформаційна інфраструктура
КМУ	Кабінет Міністрів України
НБУ	Національний банк України
ОКІ	Об’єкт критичної інфраструктури
РНБО	Рада національної безпеки і оборони України
ПЗ	Програмне забезпечення

ВСТУП

Актуальність теми. В умовах зростаючих кіберзагроз та гібридної війни, що триває, критична інфраструктура України постійно перебуває під ризиком цілеспрямованих кібератак. Сектори енергетики, зв'язку, транспорту, охорони здоров’я, урядування та інші є не лише технологічно уразливими, а й стратегічно важливими для національної безпеки. Тому питання кіберстійкості ОКІ стає пріоритетом державної політики, галузевого регулювання та практичного управління безпекою на підприємствах.

У зв’язку з цим виникає потреба у впровадженні системного, стандартизованого підходу до оцінки стану кібербезпеки, який дозволить виявляти слабкі місця, визначати рівень кіберзрілості організації та формулювати дієві кроки для його підвищення. Одним із найбільш ефективних інструментів, який для цього використовують у світі, є фреймворк NIST Cybersecurity Framework 2.0, що є офіційно рекомендований до застосування й в Україні. Його універсальна структура, гнучкість у застосуванні та відповідність міжнародним стандартам робить NIST CSF доцільним вибором для побудови сучасних програм управління ризиками інформаційної безпеки на ОКІ.

Метою роботи є розробка та обґрунтування методики застосування фреймворку NIST CSF 2.0 для оцінки рівня кіберзрілості об’єктів критичної інфраструктури з метою виявлення слабких місць і підвищення загального рівня їх кіберстійкості.

Об’єктом дослідження є управління кібербезпекою об'єктів критичної інфраструктури та оцінка їхнього рівня кіберзрілості відповідно до вимог та рекомендацій NIST CSF 2.0.

Предмет дослідження **–** методи оцінки рівня кіберзрілості об’єктів критичної інфраструктури на основі фреймворку NIST CSF 2.0.

Для досягнення мети в роботі необхідно виконати наступні **завдання**:

1. Провести аналіз стану кібербезпеки об’єктів критичної інфраструктури, визначити основні загрози та ризики, а також дослідити існуючі нормативно-

правові вимоги та стандарти (NIST, ISO 27001, NIST 800-53, CIS Controls тощо).

2. Дослідити фреймворк NIST CSF 2.0, його структуру, функціональні області, категорії та методи оцінки кіберзрілості організацій. Порівняти NIST CSF з іншими моделями кібербезпеки та обґрунтувати його доцільність у застосуванні для критичної інфраструктури.

3. Розробити методику оцінки рівня кіберзрілості об’єктів критичної інфраструктури на основі NIST CSF 2.0, визначити ключові критерії, алгоритм проведення оцінювання та можливі інструменти автоматизації аналізу.

4. Застосувати розроблену методику на тестовому або реальному об’єкті, провести оцінку кіберзрілості, проаналізувати отримані результати та виявити слабкі місця у системі безпеки.

5. Розробити рекомендації щодо покращення рівня кібербезпеки, засновані на результатах оцінки, та сформувати пропозиції щодо впровадження NIST CSF 2.0 у систему управління інформаційною безпекою організації.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи системного аналізу, моделювання загроз, аналізу нормативних вимог.

Практичне значення одержаних результатів. Запропонована методика може бути використана в організаціях, що відносяться до ОКІ, для проведення самооцінки рівня кіберзрілості, формування цільових профілів безпеки та вдосконалення систем управління кіберризиками відповідно до NIST CSF 2.0.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції “Стратегії кіберстійкості: управління ризиками та безперервність бізнесу” 27 лютого 2025 року.

Розділ 1 АНАЛІЗ СТАНУ КІБЕРБЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

1.1 Поняття та класифікація об'єктів критичної інфраструктури

Критична інфраструктура – це сукупність об'єктів, систем, мереж і послуг, безперебійне функціонування яких є життєво важливим для національної безпеки, економічної стабільності, здоров'я населення та суспільного добробуту.

Дане визначення закріплене в низці міжнародних та національних документів. Згідно з Директивою Ради Європейського Союзу 2008/114/ЕС, критичною інфраструктурою вважаються активи, системи чи частини яких є життєво важливими для підтримки ключових соціальних функцій, здоров'я, безпеки, економічного чи соціального добробуту громадян [1, 2]. В Україні це поняття визначене в Законі України "Про критичну інфраструктуру" [2], а також деталізується в постановах КМУ та інших Законах України [3, 4].

Класифікація ОКІ відбувається за галузевою ознакою, серед основних зазвичай виділяють:

- урядування та надання найважливіших публічних (адміністративних) послуг;
- енергозабезпечення;
- водопостачання;
- продовольче забезпечення;
- охорона здоров'я;
- інформаційні послуги;
- електронні комунікації;
- фінансові послуги;
- транспортне забезпечення;
- оборона, державна безпека;
- правопорядок;

- цивільний захист населення та територій, служби порятунку;
- космічна діяльність, космічні технології та послуги;
- хімічна промисловість;
- дослідницька діяльність.

Для визначення рівня вимог щодо забезпечення захисту ОКІ відповідно до рівня їх важливості у межах секторів критичної інфраструктури здійснюється категоризація відповідно до категорій критичності [2]:

- І категорія критичності - особливо важливі об’єкти, які мають загальнодержавне значення, значний вплив на інші об’єкти критичної інфраструктури та порушення функціонування яких призведе до виникнення кризової ситуації державного значення;
- ІІ категорія критичності - життєво важливі об’єкти, порушення функціонування яких призведе до виникнення кризової ситуації регіонального значення;
- ІІІ категорія критичності - важливі об’єкти, порушення функціонування яких призведе до виникнення кризової ситуації місцевого значення;
- ІV категорія критичності - необхідні об’єкти, порушення функціонування яких призведе до виникнення кризової ситуації локального значення.

Особливу увагу привертає критична інформаційна інфраструктура (КІІ) – це ті елементи критичної інфраструктури, які базуються на ІТ або забезпечують функціонування інформаційних систем. До КІІ зазвичай відносять інформаційні системи урядових установ, банків, операторів мобільного зв'язку, транспортних хабів, медичних установ тощо [4].

У практичному сенсі визначення об’єктів КІІ також супроводжується оцінкою їхньої вразливості до зовнішніх і внутрішніх загроз, що дозволяє формувати стратегії забезпечення кіберзахисту які і КІІ так і ОКІ вцілому [5].

1.2 Аналіз основних загроз та ризиків у сфері кібербезпеки критичної інфраструктури

ОКІ стикаються як із традиційними фізичними загрозами (терористичні акти, диверсії, природні катастрофи), так і з широким спектром кіберзагроз. В останні роки кібернетична складова загроз набуває все більшого значення [6], оскільки ОКІ все глибше інтегруються з інформаційними системами та мережами (концепція Industry 4.0, Інтернет речей, автоматизовані системи управління тощо). З розвитком цифрових технологій та інтеграцією все нових інформаційних систем ОКІ дедалі частіше стають цілями кіберзлочинців, хактивістів і злочинних груп, що фінансуються урядами країн. Такий динамічній зріст призводить до змін в характері загроз – від традиційних DDoS-атак до складних цілеспрямованих атак (APT) та використання вразливостей нульового дня (zero-day vulnerabilities) [7]. Нижче розглянемо найбільш характерні кіберзагрози та атаки, на які слід звертати увагу при захисті критичних систем:

- APT на промислові системи. Державні чи організовані хакерські групи часто обирають ОКІ як мішень для складних, багатоступеневих атак типу Advanced Persistent Threat. Такі атаки можуть тривати місяцями, вони включають попередню розвідку, проникнення у внутрішню мережу, пошук шляхів до промислових систем керування (SCADA/ICS) і внесення деструктивних змін. Як приклад російські атаки BlackEnergy та Industroyer на енергосистему України (2015-2016) [8]. Метою таких APT-кампаній є не крадіжка даних, а саме порушення функціонування об’єкта (виведення з ладу, пошкодження обладнання, зупинка технологічного процесу)[9].

- Деструктивні атаки типу “wipe” та саботаж. На відміну від традиційних кібератак, що націлені на отримання вигоди (грошей, даних), існує клас атак на знищення, характерний для військових та терористичних дій. У контексті війни росії проти України фіксуються шкідливі програми-вайпери (наприклад, HermeticWiper, IsaacWiper)[10], які знищують дані та виводять з ладу IT-системи організацій. Якщо такі програми потрапляють до мереж критичних підприємств,

вони можуть зірвати роботу автоматизованих систем, стерти резервні копії, “цеглиною” перетворити мережеве обладнання. Наприклад, у випадку атаки на телеком-оператора Київстар у грудні 2022 року [9], хакери (група Sandworm) зруйнували частину інфраструктури ядра мережі. Метою було як психологічний ефект (позбавити населення зв’язку), так і збір розвідданих та спроба викрадення інформації, але наслідком став фактичний саботаж критичного сервісу.

- Атаки типу DDoS (розподілені відмови в обслуговуванні). Хоча DDoS-атаки і не проникають усередину систем, для критичних сервісів вони надзвичайно небезпечні тим, що можуть зробити послугу недоступною для споживачів [11]. Наприклад, DDoS на DNS-сервери провайдера може відключити інтернет-зв’язок у цілому регіоні, або атака на веб-портал держпослуг паралізує доступ громадян до ключових електронних сервісів. Ворог активно застосовує DDoS-атаки проти українських відомств і компаній з початку війни, щоб порушити їх роботу. Для захисту від DDoS критичні вузли потребують наявності резервних каналів, систем розподілу навантаження і фільтрації трафіку.

- Кібершпигунство та викрадення даних. ОКІ володіють цінною інформацією: технологічною (про режими роботи обладнання, мережеві схеми), комерційною (контракти, плани), персональною (дані клієнтів або співробітників), яка може бути цікава як державним розвідкам, так і конкурентам чи криміналітету [12]. Тому спостерігається значна кількість спроб проникнення до мереж ОКІ з метою викрадення даних або встановлення бекдорів. Часто першою фазою масштабної атаки є саме розвідка – зловмисники компрометують окремі вузли мережі, витягають важливі відомості (наприклад, схеми мереж, списки користувачів, паролі), і згодом використовують цю інформацію для наступних, ще небезпечніших дій.

- Шкідливе програмне забезпечення та програми “вимагачі”. Різноманітні віруси, трояни та інші типи malware постійно сканують інфраструктуру на вразливі місця. Якщо звичайна компанія в разі ураження вірусом може втратити гроші чи дані, то для критичної інфрастуктури наслідки можуть бути фізичними

– зупинка процесу, аварія. Останніми роками особливо поширилися атаки здирницьких програм (ransomware), коли зловмисники шифрують дані і вимагають викуп [13].

•Інсайдерські загрози. Значний ризик становлять не лише зовнішні, а й внутрішні порушники – працівники або підрядники, що мають доступ до систем. Недобросовісний або завербований інсайдер може навмисно пошкодити систему, викрасти критичні дані або впровадити шкідливий код. Часто інсайдерські дії поєднуються з людськими помилками та нехтуванням правилами безпеки. Наприклад, працівник може відкрити фішинговий лист і заразити мережу, або підключити несанкціонований носій в критичний сегмент мережі. В умовах віддаленої роботи питання контролю дій користувачів і їх обізнаності у кібергігієні стало ще важливішим. Для протидії цим загрозам організації впроваджують політики розмежування доступів, моніторингу активностей користувачів (Privileged Access Management, аудит логів) та програми підвищення обізнаності персоналу [7, 14].

•Атаки на ланцюги постачання. Критична інфраструктура залежить від численних постачальників обладнання, програмного забезпечення, сервісів. Вразливості або компрометація в компанії-постачальника можуть призвести до того, що атакуючі отримають “чорний хід” у систему ОКІ через легітимні оновлення чи довірені зв’язки. Відомим прикладом є злам компанії SolarWinds (2020), коли через оновлення ПЗ було уражено сотні організацій, у тому числі урядових. В умовах ОКІ це може проявлятись і через взаємодію з операторами зв’язку, хмарними сервісами, виробниками промислових АСУ – якщо ті скомпрометовані, клієнт також під ударом. Тому зараз велика увага приділяється безпеці ланцюгів постачання (Supply Chain Security): оцінці кіберзрілості контрагентів, включенню вимог з кібербезпеки у договори, моніторингу підозрілої активності з боку підключених сторонніх систем.

•Інші загрози. Серед інших актуальних загроз для ОКІ можна відзначити: підробку чи підрив GPS/GNSS сигналів (важливо для транспорту і енергомереж), несанкціоноване втручання у бездротові сенсори та контролери, криптографічні

атаки на застарілі протоколи зв’язку, ураження вірусами IoT-пристроїв (камер, датчиків, смарт-компонентів інфраструктури) та ін. Кожен сектор має специфічні загрози – наприклад, для енергетики критичні автоматизовані релейні захисти (атака на них може знеструмити мережу), для залізниці – системи сигналізації і стрілочного переводу, для водоканалу – АРМи технологів тощо [15].

Окрім атак, слід враховувати і природні загрози та аварії, які можуть мати негативний вплив на стан кіберзахисту. Зокрема, воєнні дії в Україні призводять до прямих фізичних ушкоджень ОКІ (ракетні удари по об’єктах, пошкодження інфраструктури тощо). Це, у свою чергу, призводить до втрати доступності систем, аварійних відключень, перевантаження мереж. Тому питання підготовки та підтримки актуальних сценаріїв забезпечення кіберстійкості ОКІ мають враховувати і такі комплексні випадки, коли фізичні та кіберінциденти розвиваються одночасно. Таким чином, ландшафт загроз для критичної інфраструктури є вкрай широкий і динамічний [16]. Для адекватного реагування необхідна система управління ризиками, що дозволяє ідентифікувати найімовірніші та найнебезпечніші загрози, впроваджувати багаторівневий захист, здійснювати своєчасне реагування на інциденти та мати плани відновлення. Одним із інструментів для побудови такої системи є впровадження структурованих фреймворків кібербезпеки, що задають “каркас” необхідних процесів і заходів. Передусім для ОКІ в різних країнах рекомендовано застосування стандартів на кшталт NIST, ISO 27000, COBIT, а також галузевих вимог.

1.3 Огляд нормативно-правових актів та стандартів кібербезпеки

Основою правового поля кібербезпеки в Україні є Закон № 2163-VIII “Про основні засади забезпечення кібербезпеки України” від 05.10.2017. Цей закон заклав базові принципи та механізми державної кібербезпеки: розподілив ролі між суб’єктами, визначив поняття критичної інформаційної інфраструктури і

вимоги до її захисту. На виконання цього Закону було затверджено низку підзаконних актів, зокрема: Порядок віднесення об’єктів до ОКІ (постанова КМУ № 1109), створено Національний координаційний центр кібербезпеки при РНБО, прийнято в 2021 році Стратегію кібербезпеки України, яка особливу увагу приділяє захисту критичних інформаційних ресурсів.

У 2021 році ухвалено спеціалізований Закон України “Про критичну інфраструктуру” № 1882-IX. Він визначив правові та організаційні основи функціонування системи захисту ОКІ, встановив категорії критичності, порядок формування Реєстру ОКІ та координаційні механізми. Згідно із цим Законом, центральним органом з питань захисту критичної інфраструктури є ДССЗЗІ, яка здійснює нормативне регулювання, веде Реєстр, координує оцінку уразливостей тощо. Галузеві органи (міністерства, відомства) відповідають за ідентифікацію та категоризацію об’єктів у своїх секторах. Закон також передбачає розробку державної системи моніторингу стану безпеки критичної інфраструктури та реагування на інциденти (вочевидь, у перспективі – Національна мережа ситуаційних центрів).

Інші закони, дотичні до захисту ОКІ, включають: Закон “Про захист інформації в інформаційно-телекомунікаційних системах” (визначає вимоги до захисту інформації і відповідальність за порушення); Закон “Про електронні комунікації” (містить положення щодо обов’язків операторів зв’язку із забезпечення кібербезпеки та стійкості мереж); Закон “Про основні засади забезпечення кібербезпеки України” (як згадано вище, визначає загальну політику); Закон “Про оборонні закупівлі”, що в частині кібербезпеки регулює закупівлю засобів захисту для критичних потреб; Закон “Про санкції”, який використовується для блокування програмних продуктів з держави-агресора, що теж є елементом кібербезпеки критичних систем (наприклад, заборона антивірусів Kaspersky на ОКІ). Важливими також є накази профільних органів – наприклад, стандарти технічного захисту інформації ДСТСЗІ, документи НБУ щодо кібербезпеки в банківському секторі, галузеві вимоги до операторів енергетики тощо.

Нормативні вимоги часто відсилають до галузевих стандартів, які є практичними інструментами побудови систем захисту. Серед найбільш відомих міжнародних стандартів, що застосовуються для ОКІ: сімейство стандартів ISO/IEC 27000 (система управління інформаційною безпекою – ISMS; зокрема ISO 27001:2022 та набір заходів ISO 27002:2022); стандарти для промислових систем ISA/IEC 62443 [17]; рекомендації NIST SP 800-53 Rev.5 (каталог з ≈1000 контролів безпеки для систем різного класу); стандарти COBIT 2019 (фреймворк IT-управління з компонентами кібербезпеки); керівні принципи CIS Critical Security Controls та інші [18].

В багатьох випадках ці стандарти не конкуренти, а є доповненнями один одного. Саме тому все ширше впроваджується фреймворк NIST CSF, який інтегрує найкращі практики різних стандартів у єдину рамку. Більше того, NIST CSF має спеціальні профілі для різних секторів – наприклад, для енергетики, охорони здоров'я, виробництва – що враховують галузеву специфіку. Використання фреймворків дозволяє ОКІ дотримуватися принципу "безперервного процесу кібербезпеки": постійно оцінювати свій стан, зіставляти із кращими світовими практиками і вдосконалювати заходи захисту. У наступному розділі докладно розглянемо структуру та можливості NIST CSF версії 2.0 – як одного з центральних елементів сучасної методології оцінки кіберзрілості організацій.

1.4 Роль фреймворків у забезпеченні кібербезпеки критичної інфраструктури

Фреймворки кібербезпеки є структурованими інструментами, що дозволяють організація систематизувати процеси керування кіберризиками та адаптуватися до нових викликів та загроз. Вони забезпечують послідовний підхід до виявлення вразливостей, оцінювання ризиків і впровадження засобів контролю, охоплюючи всі аспекти управління кібербезпекою. Дотримання загальновизнаного фреймворку стандартизує процеси захисту в різних

підрозділах, зменшує неоднозначність у прийнятті рішень та забезпечує цілісний огляд стану безпеки. Це дозволяє ефективніше визначати пріоритетні напрями розвитку і розподіляти ресурси, покращує готовність до інцидентів та масштабованість програм безпеки. Прийняття визнаного фреймворку також демонструє зацікавленим сторонам (керівництву, клієнтам, регуляторам) відданість організації належній кібербезпеці, що підсилює довірчі відносини між сторонами.

Україна, як частина світової спільноти, активно переймає найкращі практики кібербезпеки, зокрема впроваджує відомі міжнародні фреймворки для захисту своєї критичної інфраструктури. У сфері державної політики кібербезпеки роль фреймворків постійно зростає – це відображено в стратегічних документах і конкретних заходах органів, відповідальних за кіберзахист. Залучення України до стандартів NIST стало можливим завдяки як внутрішнім реформам, так і підтримці міжнародних партнерів. Ще у 2018 році за підтримки Посольства США було здійснено офіційний переклад NIST CSF українською мовою, що став основою для поширення цього фреймворку серед українських фахівців. Національний координаційний центр кібербезпеки (НКЦК) при РНБО та ДССЗЗІ у своїх публікаціях неодноразово наголошували на важливості впровадження міжнародних стандартів. Зокрема, у серпні 2020 РНБО започаткувала платформу співпраці з провідними світовими постачальниками кіберрішень, де одним із пріоритетів було названо узгодження національних практик із кращими світовими стандартами кібербезпеки.

Особливий прогрес спостерігається з 2021 року після ухвалення нової Стратегії кібербезпеки України. Нормативна база почала враховувати NIST CSF як інструмент підвищення кіберстійкості критичної інфраструктури. Так, постановою Кабінету Міністрів України №518 від 24.03.2023 р. було запроваджено обов’язкові аудити кібербезпеки об’єктів критичної інфраструктури з періодичністю раз на 2–3 роки (залежно від категорії критичності). Цей нормативний акт офіційно визнав декілька способів підтвердження належного рівня захисту, серед яких поруч із традиційною

побудовою комплексної системи захисту інформації (КСЗІ) та впровадженням системи управління інформаційною безпекою (ISMS за ISO 27001) з'явився новий підхід – аудит на відповідність вимогам NIST CSF з подальшим повторним аудитом після реалізації рекомендацій. Іншими словами, уряд дозволив використовувати NIST CSF як критерій оцінки кібербезпеки критичних об'єктів, що є значним визнанням цього фреймворку на державному рівні. Це рішення, ухвалене за поданням ДССЗЗІ, фактично заклало правові підвалини для масштабного впровадження CSF в різних секторах.

На початку 2025 року ДССЗЗІ видала наказ №54 (від 30.01.2025), яким затверджено базові заходи кіберзахисту та методичні рекомендації щодо їх здійснення на основі NIST CSF версії 2.0. Цей наказ офіційно імплементує оновлений фреймворк у практику як державних, так і приватних структур. Наказ передбачає, що до кожного заходу безпеки надаються методичні вказівки та приклади реалізації, а також рекомендації щодо формування профілю кіберзахисту організації для самооцінки. Впровадження CSF 2.0 національним регулятором має на меті підвищити зрілість управління кіберризиками в Україні, привести наші стандарти у відповідність з міжнародними та адаптувати кіберзахист до сучасних технологій. Важливо, що CSF 2.0 інтегрується з іншими стандартами (ISO/IEC 27001, COBIT, NIST Risk Management Framework тощо) і враховує нові виклики (наприклад, безпека штучного інтелекту, хмарних сервісів) [19]. Це означає, що українські організації, виконуючи вимоги наказу, одночасно наближаються до світового рівня і можуть легше співставити свої досягнення з загальноприйнятими метриками кібербезпеки.

Висновки до розділу 1

У першому розділі було проведено комплексний аналіз теоретичних, нормативних і практичних аспектів, що стосуються функціонування та захисту ОКІ в контексті кібербезпеки. Сформульовано узагальнене визначення критичної інфраструктури як сукупності об'єктів і систем, безперебійне

функціонування яких є життєво важливим для держави, суспільства й економіки. Особливу увагу приділено КІІ, яка становить основу цифрової стійкості країни в умовах зростаючих кіберзагроз.

Проаналізовано галузеву класифікацію ОКІ та систему категоризації об’єктів за рівнями критичності, що дозволяє встановлювати пріоритети для впровадження заходів захисту залежно від масштабу потенційного впливу інцидентів. Окремо розглянуто динамічний та багаторівневий характер кіберзагроз, які впливають на ОКІ, зокрема: APT-атаки, деструктивні програми типу “вайперів”, атаки на ланцюги постачання, DDoS, шпигунство, інсайдерські загрози та програми-вимагачі. Підкреслено, що сучасні загрози мають як технічний, так і організаційний характер, часто комбінуються з фізичними атаками, і потребують системної багаторівневої протидії.

У ході аналізу нормативної бази окреслено ключові положення українського законодавства у сфері кібербезпеки ОКІ, зокрема Закони України “Про критичну інфраструктуру” та “Про основні засади забезпечення кібербезпеки України”, а також підзаконні акти, що регламентують категоризацію, аудит, захист інформації та управління ризиками. Особливу увагу приділено інтеграції міжнародних стандартів у національну практику – ISO 27001, NIST SP 800-53, COBIT, CIS Controls – які доповнюють правові вимоги перевіреними інструментами для організації процесів безпеки.

На завершення розділу проаналізовано роль фреймворків як інструментів стандартизації, систематизації та вдосконалення процесів кіберзахисту ОКІ. Визначено, що використання структурованих фреймворків, зокрема NIST Cybersecurity Framework, дає змогу забезпечити цілісний підхід до управління кіберризиками, визначати поточний та цільовий стан безпеки, планувати покращення і вимірювати прогрес. Показано, що Україна поступово інтегрує NIST CSF у нормативну та практичну площину, що підтверджується відповідними рішеннями РНБО, ДССЗЗІ та КМУ, а також публікацією офіційних методичних рекомендацій на основі CSF 2.0.

Розділ 2 ФРЕЙМВОРК NIST CSF 2.0 ЯК ІНСТРУМЕНТ ОЦІНКИ РІВНЯ КІБЕРЗРІЛОСТІ

2.1 Огляд фреймворку NIST CSF 2.0: структура, функції, категорії

NIST Cybersecurity Framework – це нормативний документ та набір рекомендацій, розроблений NIST (США) для управління кібербезпекою на основі ризик-орієнтованого підходу. Поява CSF в 2014 році була відповіддю на потребу підвищити рівень захисту критичних секторів, однак згодом його застосування стало універсальним. Оновлена версія CSF 2.0 опублікована 26 лютого 2024 р [20]. стала першою великою ревізією фреймворку за десятиліття. Розробники розширили сферу його дії, додавши нові компоненти та більше ресурсів для допомоги організаціям у впровадженні [21]. CSF 2.0 зберігає наступність із попередньою версією 1.1 (2018) [22], але включає важливі доповнення:

- Шість основних функцій (Functions) замість п’яти. Додано нову функцію Govern (Управління) до існуючих Identify (Ідентифікація), Protect (Захист), Detect (Виявлення), Respond (Реагування), Recover (Відновлення). Це підкреслює роль управлінських процесів і керівництва у побудові ефективної кібербезпеки, про що докладніше нижче.
- Розширена увага до управління ризиками постачальників та ланцюгів поставок. В CSF 2.0 значно докладніше розглянуто аспекти оцінки ризиків, пов’язаних із взаємодією організацій з третіми сторонам. Додано рекомендації щодо моніторингу безпеки постачальників, проведення аудитів кібербезпеки підрядників тощо.
- Інтеграція з новими технологічними викликами. Фреймворк враховує сучасні тренди – перехід у хмарні середовища, масове впровадження IoT-пристроїв, використання штучного інтелекту. Додано кращі практики щодо безпеки хмарних сервісів та IoT, а також рекомендації з оцінки ризиків впровадження інновацій. Це робить CSF релевантним для

сьогоднішніх умов цифрової трансформації.

- Наголос на показниках ефективності та кіберзрілості. CSF 2.0 пропонує організаціям використовувати метрики для оцінювання стану безпеки та прогресу в часі. Зокрема, передбачається розробка KPI (ключових показників ефективності) з кібербезпеки і інтеграція їх в загальну систему менеджменту організації. Також фреймворк заохочує визначення цільового рівня кіберзрілості і відстеження його досягнення через профілі та рівні [20, 21].
- Більше інструментів підтримки впровадження. Одночасно з релізом CSF 2.0, NIST представив цілий набір ресурсів: довідковий посібник (Quick Start Guide) [20] для малих підприємств, приклади реалізації для певних галузей, інтерактивний онлайн-інструмент CSF 2.0 Reference Tool та каталог інформативних посилань (mapping) на інші стандарти. Це допомагає новим користувачам швидко розпочати роботу з фреймворком, а досвідченим – інтегрувати його з існуючими стандартами і системами.
- Фреймворк складається з трьох основних компонентів: Core (Ядро), Implementation Tiers (Рівні впровадження) та Profiles (Профілі). Ці компоненти забезпечують різні “виміри” або аспекти застосування фреймворку:
- Core – по суті, це базова структура з шести функцій (Functions), що розбиті на категорії та підкатегорії. Ядро описує вихідні цільові стани або результати (outcomes) кібербезпеки, яких організація повинна досягати. Іншими словами, Core відповідає на питання “Що ми повинні робити, щоб ефективно управляти кіберризиками?” – без прив’язки до конкретних технологій чи методів (“що” замість “як”). На рис. 2.1 зображено оновлене ядро NIST CSF 2.0.

Рис. 2.1 Ядро NIST CSF 2.0

- Implementation Tiers – шкала з чотирьох рівнів, що характеризують зрілість кібербезпекових практик організації, тобто наскільки глибоко і послідовно організація впровадила процеси управління кіберризиками. Фактично виступають критеріями кіберзрілості в рамках CSF. Рівні описані від Partial (частковий) до Adaptive (адаптивний).
- Profiles – це модель представлення стану кібербезпеки організації, яка формується шляхом вибору релевантних підкатегорій Core та порівняння поточного профілю (Current Profile) з цільовим (Target Profile). Профіль дозволяє адаптувати фреймворк до конкретних потреб бізнесу та оцінити прогалини: наприклад, які підкатегорії ще не реалізовані чи реалізовані не повністю. Профілі можуть бути галузевими (industry profiles) або індивідуальними для окремої організації.

NIST CSF 2.0 містить шість функцій верхнього рівня: Govern, Identify, Protect, Detect, Respond та Recover. Всі функції разом охоплюють повний життєвий цикл управління кіберризиками – від стратегічного керування до відновлення після інцидентів. Логіка така, що ефективна програма кібербезпеки

має виконувати заходи за всіма шістьма напрямами. Розглянемо зміст кожної функції (включаючи їх трактування у контексті критичної інфраструктури):

- Govern (Управління). Нова функція, додана в CSF 2.0, яка фокусується на належному управлінні кібербезпекою на рівні організації. Мета функції – інтегрувати кібербезпеку в корпоративне управління і культуру, визнати її як невід'ємну частину управління ризиками підприємства. Для ОКІ це означає, що вищі керівники (топ-менеджмент, власники) повинні активно залучатися до питань безпеки, приймати обґрунтовані рішення щодо ризиків, призначати відповідальних за захист систем, контролювати виконання вимог законодавства і стандартів.
- Identify (Ідентифікація). Ця функція зосереджується на визначенні активів, бізнес-середовища та ризиків, які є основою побудови системи захисту. Організація повинна знати, що саме вона захищає і від чого. Основні категорії тут: управління активами (склад і критичність апаратних засобів, програм, даних; для ОКІ – також фізичних об'єктів), розуміння бізнес-середовища (місце організації у ланцюгах поставок, залежності від інших, законодавчі вимоги), оцінка ризиків (ідентифікація загроз і вразливостей, проведення аналізу ризиків), стратегія управління ризиками (підходи до прийняття, зниження чи передання ризику), управління поставками і сторонніми залежностями (якщо актив чи процес залежить від зовнішньої організації, це має бути враховано).
- Protect (Захист). Ця функція охоплює впровадження заходів захисту, які необхідні для забезпечення кібербезпеки і зниження ризиків, виявлених на етапі Identify. Задача Protect – зробити так, щоб уразливості були мінімізовані, а загрозам було важче реалізуватися. Заходи Protect повинні враховувати безпеку і класичних IT-систем (серверів, робочих станцій) і промислових (PLC, RTU, промислові мережі). Важливо також підготувати плани безперервності: резервне живлення, дублюючі канали зв'язку, резервні ЦОД – ці аспекти теж можна віднести до функції Protect, оскільки вони зменшують вразливість до атак (наприклад, на енергопостачання).

- Detect (Виявлення). Невід'ємною частиною кібербезпеки є своєчасне виявлення інцидентів і аномалій у роботі систем. Функція Detect включає: безперервний моніторинг та аналіз подій (використання систем збору логів, SIEM, SOC), виявлення аномалій та подій (налаштовані правила кореляції, розпізнавання нетипових дій у мережі чи системах), процедури оголошення про події (хто і як повідомляє про виявлені інциденти), використання загрозової розвідки (threat intelligence) – оновлення сигнатур, IoC (індикаторів компрометації), отримання інформації про нові атаки з зовнішніх джерел. Для ОКІ ця функція особливо критична, адже своєчасне виявлення кібератаки може запобігти фізичним аваріям.
- Respond (Реагування). Дана функція визначає набір заходів для ефективного реагування на виявлені інциденти, з метою локалізувати і мінімізувати їх вплив. Основні аспекти: планування реагування (наявність заздалегідь розроблених планів реагування на інциденти, IRP), зв'язок та оповіщення (налагоджена схема внутрішніх та зовнішніх комунікацій під час інциденту – кого повідомити, взаємодія з держорганами, CERT), аналіз (проведення розслідування інциденту, з'ясування причини та обсягу), стримування (дії з локалізації – відключення уражених вузлів, ізоляція сегментів мережі), усунення наслідків (видалення шкідливого ПЗ, закриття вразливостей) і покращення (витяг уроків, оновлення планів і заходів).
- Recover (Відновлення). Фінальні функція, яка охоплює дії з відновлення систем і сервісів після інциденту, а також заходи для запобігання повторення подібного в майбутньому. Для ОКІ функція Recover змикається з поняттям стійкості (resilience): наприклад, компанія повинна мати можливість заживити споживачів від резервних схем за лічені години, переключити трафік на інші вузли або швидко розгорнути тимчасові точки зв'язку у разі масштабного збою. У контексті кібербезпеки це означає заздалегідь підготуватися до відновлення: мати актуальні резервні копії, запасне мережеве обладнання, запасні ліцензійні ключі для ПЗ, контракти з постачальниками на екстрену підтримку. Після

подолання наслідків інциденту організація має проаналізувати, що спрацювало, а що ні, та оновити свої плани реагування і відновлення. NIST CSF 2.0 вказує, що увага до функції Recover підвищує загальну кіберстійкість організації і готовність до майбутніх атак.

На рис 2.2 зображено декомпозицію ключових 6 функцій ядра NIST CSF 2.0.

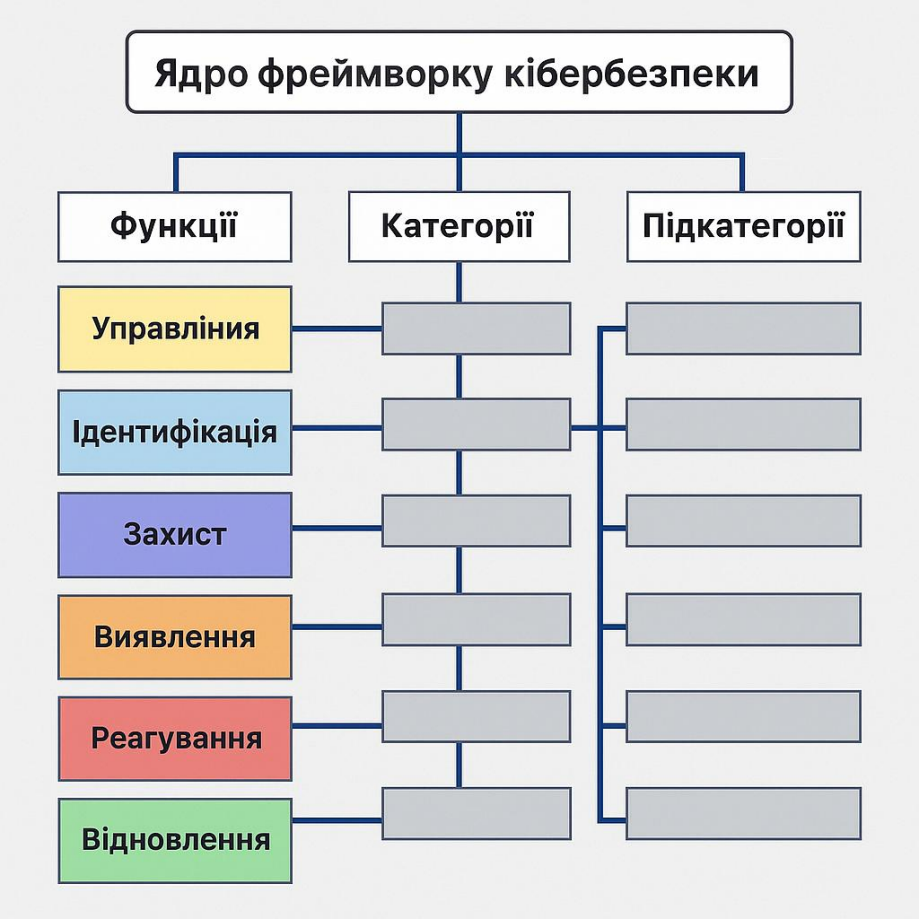

Рис. 2.2 Функції NIST CSF 2.0

Отже, шість функцій CSF охоплюють повний спектр діяльності з кібербезпеки – від стратегічного управління до технічного реагування. Важливо розуміти, що функції не є покроковим процесом, вони здійснюються одночасно і безперервно. Фреймворк часто зображають у вигляді колеса або циклу, де всі функції взаємопов’язані. Тобто, реалізувавши заходи Protect, ми повинні паралельно налаштувати Detect, після Respond та Recover обов’язково

повертаємося до Govern та Identify для оновлення ризик-аналізу. Це безперервний цикл PDCA (Plan-Do-Check-Act) у сфері кібербезпеки [23].

2.2 Методологія оцінки рівня кіберзрілості за NIST CSF 2.0

Поняття “кіберзрілість” (cybersecurity maturity) означає рівень розвиненості та ефективності процесів кібербезпеки в організації. Оцінка кіберзрілості – це діагностика, наскільки компанія відповідає кращим практикам, чи встановлені всі необхідні процеси, чи працюють вони системно, а не від випадку до випадку. NIST CSF добре підходить як основа для такої оцінки, оскільки має чітко визначені вимоги (через функції/категорії/підкатегорії) та шкалу зрілості (tiers) [22]. Методологія оцінки кіберзрілості за CSF зазвичай включає такі ключові кроки [24]:

- Визначення сфери оцінки (Scope). На першому етапі вирішується, що саме оцінюємо: всю організацію цілком, певний підрозділ, окрему ІС чи процес. Для ОКІ доцільно брати максимально широке охоплення – весь об’єкт або підприємство, щоб оцінити його захищеність у комплексі.
- Збір інформації про поточний стан (Current Profile). Використовуючи структуру CSF Core, необхідно зібрати дані про реалізацію кожної підкатегорії у компанії. Для цього застосовують: опитувальники/анкети (їх часто складають у формі питань по кожній підкатегорії, напр. “Чи має організація актуальний перелік апаратних і програмних активів?” відповіді – так/ні/частково/не застосовується), інтерв’ю з фахівцями (CISO, IT-служба, служба безпеки, керівники підрозділів – щодо процесів, які вони виконують), аналіз документів (політик, інструкцій, звітів аудиту), технічне тестування (результати пенетеста, сканування вразливостей, оцінки конфігурацій). Весь цей масив інформації структуризується відповідно до функцій та категорій CSF. Результат – формування поточного профілю (Current Profile), тобто опису: які підкатегорії виконуються, які ні, на якому рівні.

- Оцінка рівня впровадження (Tier). Спираючись на зібрані дані, експерти визначають, на якому Tier перебуває організація в розрізі кожної з шести функцій, або загалом. Для обґрунтування рівня використовуються критерії з NIST та відповідність підкатегоріям. Якщо більшість вимог підкатегорій певної функції виконані лише частково і несистемно – це Tier 1-2; якщо майже всі виконані на постійній основі – Tier 3; якщо присутні передові практики – Tier 4.
- Визначення цільового профілю і рівня (Target Profile & Tier). Спільно з керівництвом організації приймається рішення, якого рівня прагне досягти організація. Цільовий профіль може включати впровадження тих підкатегорій CSF, що наразі не виконуються.
- Виявлення прогалин (Gap Analysis). Порівнюється поточний профіль з цільовим. В результаті формується список слабких місць та недоліків, що потребують уваги.
- Рекомендації та план вдосконалення. На основі виявлених прогалин розробляються рекомендації – що слід зробити, щоб досягти бажаного рівня кіберзрілості. Це фактично дорожня карта (roadmap) з кібербезпеки: які політики розробити, яке обладнання закупити, яке ПЗ впровадити, який персонал найняти чи навчити. Кожна рекомендація прив’язується до конкретної підкатегорії CSF.
- Формування звіту та кіберпрофілю організації. Результати оцінки оформлюються у вигляді звіту, що містить: опис поточного стану по кожній функції CSF, присвоєні рівні зрілості, перелік виявлених недоліків і рекомендації з їх усунення. Такий звіт стає відправною точкою для керівництва при плануванні інвестицій в кібербезпеку
- Подальший моніторинг і повторні оцінки. Кіберзрілість – не статичний параметр, методологія передбачає періодичні переоцінки (наприклад, щорічно або після суттєвих змін), що дозволяє відслідковувати динаміку: чи зросте рівень кіберзрілості (тобто рекомендації виконуються), чи ні.

Однією з важливих переваг методики є те , що NIST CSF дозволяє гнучко підійти до оцінки рівня кіберзрілості: не всі підкатегорії однаково застосовні до різних організацій. Наприклад, якщо в компанії немає розробки власного ПЗ [21], то підкатегорія про безпечну розробку може бути не застосовною. Цю гнучкість передбачено у принципах CSF: організація сама формує свій профіль і визначає пріоритетні напрямки розвитку.

2.3 Порівняльний аналіз NIST CSF з іншими фреймворками кібербезпеки (ISO 27001, NIST 800-53, COBIT)

Щоб краще зрозуміти місце NIST CSF серед інших підходів, розглянемо його порівняння з трьома широко визнаними фреймворками/стандартами: ISO/IEC 27001:2022, NIST SP 800-53 Rev.5 та COBIT 2019.

1. NIST CSF та ISO 27001.

ISO 27001 є сертифікаційним стандартом, а NIST CSF – добровільним керівництвом [25]. Тобто, ISO задає мінімум обов'язкових вимог, яких компанія має дотриматися, щоб отримати сертифікат відповідності. NIST CSF же більш гнучкий: він не призначений для сертифікації, немає чітких меж відповідності – це інструмент самооцінки та вдосконалення.

За змістом NIST CSF і ISO 27001 значною мірою узгоджені: обидва використовують ризик-орієнтований підхід, охоплюють схожі області контролю. Наприклад, функції CSF "Protect/Detect/Respond" відповідають розділам A.5–A.8, A.13–A.17 ISO 27001. Функція "Identify" відповідає вимогам ISO щодо оцінки ризиків та управління активами. Нова функція "Govern" відображає вимоги ISO про лідерство керівництва, політики, організацію процесів – тобто те, що власне і є змістом побудови ISMS.

2. NIST CSF та NIST 800-53.

NIST SP 800-53 "Security and Privacy Controls for Information Systems" – це об'ємний каталог детальних контролів (близько 1000) для інформаційних систем, що традиційно застосовується в урядових органах США [26]. SP 800-53

задає низку сімейств контролів (Access Control, Audit and Accountability, Incident Response, System and Communications Protection тощо) з докладними вимогами. По суті, 800-53 – це опис що конкретно робити (наприклад, “AC-2: Створити процедури управління обліковими записами користувачів, включно з створенням, деактивацією...”), тоді як NIST CSF – методичні рамки: він описує яких результатів досягти (“Управління доступом до активів здійснюється належним чином”).

Отже, CSF – є високорівневий і встановлює ключові результати, 800-53 – нижчого рівня і перелічує засоби досягнення цих результатів. В самій структурі CSF є “Informative References”, що в рамках підкатегорій напряму посилаються на конкретні вимоги SP 800-53 Rev.5. Наприклад, CSF підкатегорія PR.DS-1 “Дані в стані спокою захищені” відповідає цілої низці контролів SP 800-53: SC-28 (Protection of Information at Rest), MP-4 (Media Storage), тощо.

3. NIST CSF та COBIT 2019.

COBIT (Control Objectives for Information and related Technology) – це фреймворк для управління та забезпечення контролю над IT-процесами підприємства, розроблений ISACA [27]. COBIT охоплює широку область IT-діяльності: від стратегічного вирівнювання IT цілям бізнесу до управління проектами, обслуговування, і, зокрема, безпеки. COBIT 2019 визначає 40 цілей управління (Governance and Management Objectives) по доменах Evaluate/Direct/Monitor та Plan/Build/Run/Monitor. Кожна ціль містить компоненти процесів, практик, показників і моделі зрілості.

COBIT може бути корисним на рівні великих корпорацій, що хочуть сформувати структурний підхід до керуванняи всіма IT-активами (включно з безпекою). Але для безпосередньої оцінки кібербезпеки конкретного об’єкта CSF дасть більш прикладний фокус. Проте, якщо організація вже впроваджує COBIT, її безпековий компонент тісно пов’язаний з CSF. Тобто, COBIT – це фреймворк, який накриває в тому числі і практики CSF, гармонійно їх доповнюючи і вбудовуючи в загальну систему управління.

2.4 Критерії визначення рівня кіберзрілості об’єкта критичної інфраструктури

Для характеристики рівня кіберзрілості та культури управління ризиками NIST CSF застосовує поняття Implementation Tiers – рівні впровадження або ступені зрілості кібербезпеки організації [22]. Існує чотири таких рівні: Tier 1 – Partial (частковий), Tier 2 – Risk Informed (ризик-інформований), Tier 3 – Repeatable (відтворюваний) та Tier 4 – Adaptive (адаптивний) (Рис. 2.3). Ці рівні відображають поступову еволюцію підходів до керування кібербезпекою – від неформалізованих, реактиваних реакцій на загрози до гнучких, проактивних і безперервно удосконалюваних процесів. Важливо, що Implementation Tiers описують зрілість практик керування кіберризиками, але офіційно NIST застерігає, що вони не є прямою оцінкою зрілості чи вимогою досягти найвищого рівня для всіх організацій. Кожна організація повинна обрати той рівень (або комбінацію рівнів для різних функцій), який відповідає її цілям, регуляторним вимогам та ресурсам, і при цьому забезпечує прийнятний рівень зниження ризиків. Нижче наведено характеристику кожного рівня кіберзрілості та приклади типових організацій на цих рівнях:

- Tier 1 (Partial / Частковий). Кібербезпека впроваджена фрагментарно, несистемно. Процеси здебільшого реактивні. Формалізовані політики або відсутні, або лише на папері. Управління ризиками як практика практично не застосовується – ризики можуть усвідомлюватися на індивідуальному рівні, але не оцінюються та не керуються організаційно. Компанія на цьому рівні часто діє після факту: усуває наслідки інцидентів, але не проактивно запобігає їм. Для критичної інфраструктури такий рівень є неприйнятно низьким, адже залишає багато вразливостей, що потенційно можуть використовуватись зловмисниками.
- Tier 2 (Risk Informed / Обізнаний про ризики). Організація усвідомлює значення кібербезпеки і враховує результати процесів управління ризиками в своїй діяльності. Присутні базові політики кібербезпеки,

визначено відповідальних. Кібербезпека інтегрована у деякі ключові процеси – наприклад, нові проєкти IT проходять оцінку ризиків, критичні активи визначені і для них впроваджено заходи захисту. Проте реалізація не всеосяжна: присутні підрозділи або процеси, де питання безпеки не охоплені повністю. Управління ризиками здійснюється нерегулярно і не за єдиною методикою. В цілому – організація знає про свої основні вразливості і загрози та намагається їх вирішувати, але зрілість ще середня.

- Tier 3 (Repeatable / Повторюваний). Кібербезпекові практики стандартизовані, задокументовані і впроваджені на постійній основі. Існують встановлені процедури, які виконуються регулярно і послідовно (тобто repeatable – можуть повторюватися з однаковим результатом). Управління кіберризиками інтегроване у більшість бізнес-процесів: при плануванні нової системи обов'язково проводиться аналіз ризиків, є процес управління змінами з оцінкою впливу на безпеку, регулярно проводяться аудити і моніторинг. Персонал навчений та обізнаний зі своїми ролями. Кібербезпека розглядається як частина культури організації. На цьому рівні також налагоджується міжорганізаційна координація: компанія може обмінюватися інформацією про загрози з галузевими центрами (ISAC), враховує ризики постачальників. Tier 3 – це хороший рівень зрілості, бажаний для більшості критичних організацій.
- Tier 4 (Adaptive / Адаптивний). Вищий рівень, при якому організація проактивно і динамічно керує кібербезпекою, постійно вдосконалюючи свої процеси, спираючись на передовий досвід та нові технології. Кібербезпекова програма не лише дотримується процедур, а й адаптується на основі отриманих даних: активно аналізуються інциденти, проводиться самооцінка, впроваджуються інноваційні рішення. Ризик-менеджмент є частиною прийняття рішень на найвищому рівні. Організація швидко реагує на зміни в ландшафті загроз – наприклад, миттєво застосовує заходи з усунення при появі критичних вразливостей, має розгорнуті засоби розвідки загроз і вміє передбачати потенційні атаки. Такий рівень

характерний для провідних компаній або структур, для яких кібербезпека – один з напрямів конкурентної переваги. Для OKI Tier 4 є цільовим ідеалом, до якого варто прагнути, хоча практично його досягнення може бути складним через ресурсні обмеження і високу складність.

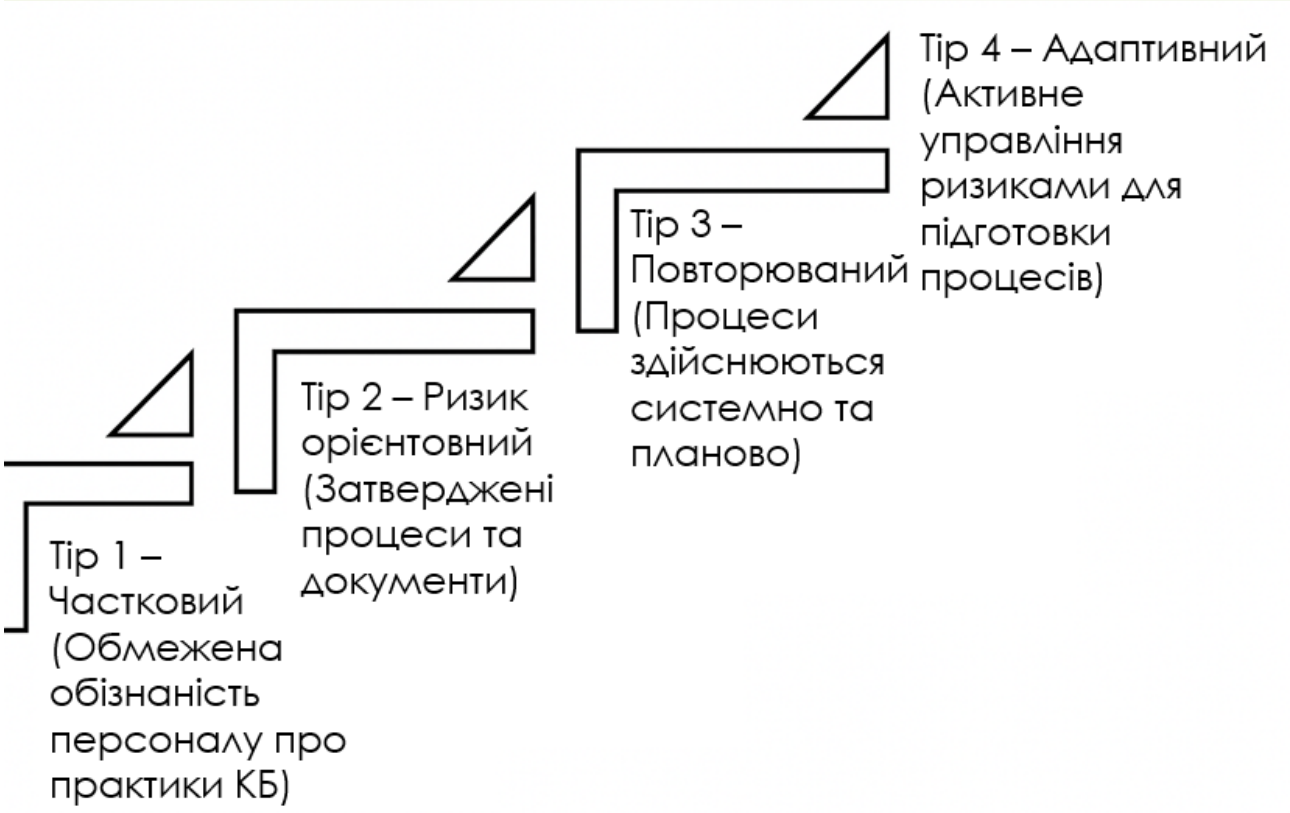

Рис. 2.3 Рівні відповідності NIST CSF 2.0

У контексті оцінки кіберзрілості ці Implementation Tiers є узагальненими рівнями, які можна виставити організації в цілому або окремим функціям/процесам. NIST CSF рекомендує визначати як поточний Tier, так і бажаний цільовий Tier для своєї програми кібербезпеки.

Варто зауважити, що на відміну від формальних моделей зрілості як, наприклад, CMMI або, де є чіткі сертифікаційні вимоги на кожен рівень, CSF Tiers носять рекомендаційний характер і їх оцінювання дещо суб’єктивне.

Важливо зазначити, що кіберзрілість організації в контексті NIST CSF визначається за сукупністю кількісних і якісних критеріїв, що відображають

наскільки глибоко й ефективно кібербезпека інтегрована в управлінські та операційні процеси. На основі Implementation Tiers і профілів можна виділити такі ключові критерії визначення рівня зрілості:

- Формалізація процесів та політик: Чи існують офіційно затверджені політики, стандарти і процедури кібербезпеки? На низьких рівнях зрілості (Tier 1) практики є реактивними, несистемними, тоді як вищі рівні (Tier 3–4) характеризуються наявністю формалізованих процесів, документованих та регулярно перегляданих.
- Інтеграція управління ризиками: Наскільки кібербезпека інтегрована в загальну систему управління ризиками підприємства і підтримку бізнес-цілей? На зрілих рівнях кіберризики розглядаються керівництвом нарівні з фінансовими та операційними ризиками; рішення ухвалюються з урахуванням кіберризиків і толерантності до них. На нижчих рівнях ця інтеграція слабка або відсутня (кібербезпека не зв’язана з бізнес-завданнями).
- Повнота охоплення та повторюваність: Чи охоплюють заходи кібербезпеки всю організацію (всі підрозділи, системи) чи тільки окремі частини? Чи виконуються ключові процеси (оцінки вразливостей, моніторинг, навчання) на регулярній основі? Вищі рівні передбачають організаційно-широкий підхід та повторювані, сталІ процеси (наприклад, регулярні сканування, планові навчання). Натомість Tier 1–2 – це фрагментарне охоплення та епізодичні дії (нерегулярні оцінки, випадкове навчання персоналу).
- Обмін інформацією і координація: Наскільки ефективно організація ділиться інформацією про кіберзагрози та інциденти внутрішньо і з зовнішніми структурами? Зрілі організації мають налагоджений обмін: всередині між відділами (напр., ІТ і бізнес регулярно обмінюються даними про ризики), а також із партнерами, галузевими центрами обміну інформацією, постачальниками. Низькозрілі – зазвичай “замкнені”, інформація про інциденти не документується і не поширюється навіть в

середині компанії.

- Управління ланцюгом постачання (supply chain): Врахування кібербезпеки постачальників, підрядників та зовнішніх сервісів. На початкових рівнях організація не усвідомлює або не відстежує ризики ланцюга постачання. На середніх – усвідомлює ризики, але діє випадково, без системності. На найвищому – запроваджено механізми для постійного моніторингу постачальників, включно з вимогами безпеки в контрактах, обміном даними про інциденти з ними тощо.
- Моніторинг та наявність метрик оцінки: Використання метрик та показників для оцінки кібербезпеки. Більш зрілі програми впроваджують ключові показники ефективності та ризику (KPI, KRI) для кібербезпеки, які регулярно доповідаються керівництву. Наприклад, метрики на кшталт кількості вчасно встановлених оновлень, середнього часу виявлення інциденту, кількості заблокованих атак тощо – усе це слугує індикаторами прогресу. На рівні Tier 4 керівники очікують отримувати такі показники поряд з іншими бізнес-метриками, щоб розуміти поточний стан безпеки і ефективність заходів. Якщо організація ще не визначила і не відстежує жодних метрик кібербезпеки – це ознака низької зрілості.
- Культура та навченість персоналу: Людський фактор – важлива ознака зрілості. На зрілих рівнях кібербезпека є частиною культури: співробітники усвідомлюють її важливість, регулярно проходять тренінги, існують програми підвищення обізнаності. Персонал має чітко визначені ролі й обов’язки в кібербезпеці, і володіє необхідними знаннями та навичками. На початкових рівнях навчання проводиться рідко або формально, обізнаність низька, відповідальні за безпеку не визначені чітко.

Перераховані індикатори дають комплексне уявлення про кіберзрілість ОКІ. Зазначений перелік не є вичерпним, проте може слугувати надійною основою для проведення первинної або періодичної оцінки рівня кіберзрілості організації. У процесі поглибленого аналізу можуть бути враховані й інші

аспекти, такі як технічна архітектура, відповідність галузевим стандартам, результати зовнішніх аудитів, рівень автоматизації безпекових процесів, статистика процесів управління інцидентами тощо. Важливо адаптувати критерії до контексту конкретної організації, враховуючи масштаб, галузь, регуляторні вимоги.

Висновки до розділу 2

У другому розділі було здійснено глибокий аналіз структури, принципів функціонування та методологічних особливостей фреймворку NIST Cybersecurity Framework версії 2.0, який є одним з найбільш визнаних та адаптивних підходів до побудови та оцінки системи управління кібербезпекою, зокрема в контексті ОКІ.

Оновлений CSF 2.0 включає шість функцій верхнього рівня – Govern, Identify, Protect, Detect, Respond і Recover – що відображає повний життєвий цикл управління кіберризиками. Особливістю нової версії є посилення ролі управлінських процесів, інтеграція з новими технологічними реаліями (хмарні сервіси, IoT, AI), а також акцент на вимірювання кіберзрілості та використання допоміжних ресурсів для впровадження. Таким чином, CSF 2.0 не лише задає напрямки роботи, але й підтримує організації у впровадженні з урахуванням галузевої специфіки та рівня підготовки.

Методологія оцінки рівня кіберзрілості за CSF 2.0 передбачає структурований підхід: від визначення області охоплення до формування поточного профілю, оцінки рівня впровадження (Implementation Tier), аналізу прогалин і визначення цільового стану. Застосування профілів CSF дає змогу адаптувати фреймворк до специфіки конкретної організації, оцінити прогрес у реалізації заходів безпеки, а також розробити обґрунтовану дорожню карту підвищення зрілості.

Порівняльний аналіз NIST CSF з іншими стандартами (ISO/IEC 27001, NIST SP 800-53, COBIT) продемонстрував його взаємодоповнюючий характер.

CSF забезпечує високу гнучкість і зручність адаптації, надає високорівневу структуру та дозволяє інтегруватися з детальними наборами контролів або управлінськими фреймворками. Таким чином, CSF може слугувати “оболонкою” для об’єднання вимог різних стандартів у єдиній моделі оцінки та вдосконалення кібербезпеки.

Завершальним елементом розділу стало вивчення чотирьох рівнів зрілості (Implementation Tiers), які дозволяють класифікувати організацію за ступенем інтеграції кібербезпеки у її діяльність. Від часткового (Tier 1) до адаптивного (Tier 4) рівня ці тири відображають прогрес у системності, повторюваності та динамічності безпекових практик. Для об’єктів критичної інфраструктури доцільним є прагнення до Tier 3 або вище, що гарантує надійність та стійкість до складних загроз.

У сукупності, другий розділ надав цілісне уявлення про потенціал CSF 2.0 як практичного інструменту для оцінки й підвищення рівня кіберзрілості критично важливих організацій. Це створює підґрунтя для розробки авторської методики оцінювання на основі CSF 2.0, яку буде реалізовано у наступному розділі.

Розділ 3 РОЗРОБКА МЕТОДИКИ ОЦІНКИ КІБЕРЗРІЛОСТІ ЗА NIST CSF 2.0

3.1 Обґрунтування вибору методики оцінки

При підборі та розробці методики оцінки кіберзрілості варто враховувати наступні принципи (Рис. 3.1):

- Комплексність. Методика повинна охоплювати всі ключові аспекти кібербезпеки критичного об’єкта – від управлінських процесів до технічних засобів захисту, від профілактики до реагування і відновлення. Для цього якнайкраще підходить модель функцій NIST CSF 2.0, що забезпечує комплексний підхід до оцінки програм захисту.
- Адаптованість. Хоча фреймворк NIST CSF універсальний, його слід “адаптувати” до особливостей критичної інфраструктури. Це означає врахувати, що оцінка має охоплювати не лише IT, а й операційні технології, які для ОКІ є ядром діяльності.
- Використання існуючих інструментів та даних. Оцінка кіберзрілості не повинна базуватися лише на суб’єктивних інтерв’ю – необхідно підтверджувати відповіді об’єктивними даними. Методикою передбачено використання автоматизованих інструментів, які вже є або можуть бути впроваджені на підприємстві: систем моніторингу подій, сканерів вразливостей, звітів антивірусів, систем управління конфігураціями тощо. Такі дані допоможуть, наприклад, оцінити фактичний рівень реалізації підкатегорій Detect чи Protect – на об’єктивній основі.
- Алгоритмічність і відтворюваність. Методика має бути описана чітким алгоритмом. Це потребує стандартизованих опитувальників, методик підрахунку балів чи присвоєння рівнів.
- Практичність і зрозумілість результатів. Результати оцінки мають бути зрозумілими менеджменту об’єкту дослідження, щоб на їх основі приймати рішення. Також обов’язковим є формулювання конкретних

рекомендацій під подальші дії.

Рис. 3.1 Основні принципи методики оцінки рівня кіберзрілості

З урахуванням зазначених принципів, вибір методики на основі NIST CSF 2.0 є доцільним для оцінки рівня кіберзрілості ОКІ. Вона поєднує гнучкість і масштабованість із структурованістю та зрозумілою логікою, що робить її ефективним інструментом як для початкової оцінки, так і для системного вдосконалення кібербезпеки. Завдяки фокусу на результатах, фреймворк дозволяє адаптувати підхід до потреб конкретної організації – враховуючи її ресурси, технології, ризики та стратегічні пріоритети.

Крім того, методика легко інтегрується з іншими міжнародними стандартами ISO/IEC 27001, NIST 800-53, COBIT тощо, що сприяє уніфікації підходів до безпеки на міжорганізаційному або галузевому рівні. Важливо й те, що NIST CSF 2.0 підтримує принципи постійного поліпшення PDCA і дозволяє організаціям не просто досягати певного рівня, а й підтримувати та підвищувати його в динамічному середовищі загроз.

Таким чином, обраний підхід є не лише технічно виправданим, але й стратегічно вигідним – як з точки зору забезпечення кіберстійкості, так і в контексті відповідності законодавчим та регуляторним вимогам у сфері захисту критичної інформаційної інфраструктури.

3.2 Алгоритм проведення оцінки кіберзрілості об’єкта критичної інфраструктури

Більш детально розглянемо покроковий алгоритм, що може використовуватися групою аудиторів або внутрішньою комісією з кібербезпеки підприємства для проведення оцінки рівня кіберзрілості об’єкта критичної інфраструктури (Рис. 3.2).

1. Підготовка та визначення меж оцінки.

На даному етапі визначається склад команди оцінки. Визначається обсяг: які саме підрозділи і системи входять до оцінки. Для ОКІ доцільно охопити всі ключові служби: ІТ-службу, службу фізичної безпеки, відділ кадрів тощо. Визначаються часові рамки проведення оцінки і затверджуються опитувальники. На цьому ж кроці збираються попередні матеріали: актуальні політики з кібербезпеки, організаційна структура, наявні звіти попередніх аудитів або тестів на проникнення, результати останнього аналізу ризиків.

2. Анкетування та інтерв’ю.

Розробляється опитувальник за шістьма функціями NIST CSF, який складається з питань по відповідних категоріях. Кожне питання перевіряє реалізацію певної підкатегорії CSF. На кожен пункт опитувальника респонденти дають відповідь і наводять докази. Доказами можуть бути: документ (політика, звіт), журнали подій, фото з системи, усний опис процесу підтверджений іншими учасниками. Команда оцінки проводить інтерв’ю з керівниками напрямів (CIO, CISO, начальник виробництва, керівник служби безпеки і т.д.) за цими питаннями, уточнює відповіді, збирає посилання на докази.

3. Обробка результатів та визначення поточного профілю.

На цьому етапі команда оцінки обробляє всі зібрані відповіді та докази. Для кожної підкатегорії встановлюється підсумкова оцінка виконання від 1 до 4. Ці оцінки групуються за функціями, після чого здійснюється обчислення показників по функціях. На основі цього визначаються рівні Tier для функцій.

Але важливим аспектом є експертне судження: наприклад, якщо якась критична підкатегорія має 0, то навіть при високих балах інших ми не можемо сказати, що функція повністю на Tier 3. Тому команда обговорює і затверджує присвоєння Tier кожній з шести функцій CSF. Результатом кроку є формування поточного профілю безпеки.

4. Визначення цільового рівня кібербезпеки.

Спільно з керівництвом об’єкта проводиться сесія визначення цільового профілю. Результатом обговорень є розуміння, якого рівня прагне досягти організація з урахуванням зовнішніх і внутрішніх вимог. Для ОКІ, як правило, ставиться мета не нижче Tier 3.

5. Аналіз та розробка рекомендацій.

Порівнявши поточний і цільовий профіль, визначається список gap-ів: кожна підкатегорія з низьким виконанням, яку потрібно підвищити. Ці прогалини ранжуються за пріоритетом. Пріоритет можна визначати за двома факторами: критичність ризику (наскільки серйозну вразливість створює невиконання цієї вимоги) та складність усунення. Для кожного gap формується рекомендація: що конкретно слід зробити. Рекомендації бувають організаційні (прийняти політику, призначити відповідального, провести тренінги), технічні (впровадити рішення – брандмауер, DLP, SIEM; оновити обладнання), процесні (налагодити процес – управління оновленнями, резервне копіювання, моніторинг журналів) [14, 28].

6. Звіт і презентація результатів.

Готується підсумковий звіт оцінки кіберзрілості. В ньому викладається: коротко про методику, поточний рівень кібербезпеки, сильні сторони, вразливі місця і ризики, рекомендації і план покращення. Після фіналізації звіт передається на ознайомлення стороні дослідження та у разі відсутності зауважень затверджується. Даний документ стає дорожньою картою розвитку кібербезпеки об’єкта.

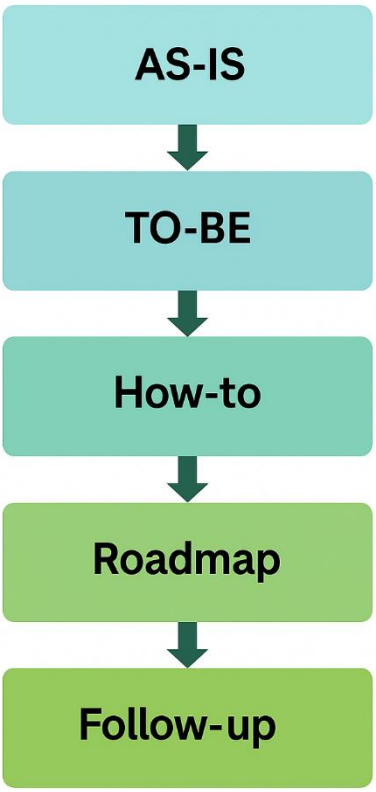

Рис. 3.2 Процес проведення оцінки кіберзрілості згідно NIST CSF 2.0

Варто зазначити, що після реалізації рекомендацій та витримування певної паузи (6-12 місяців) бажано повторити цикл оцінки, щоб оцінити прогрес і при необхідності скоригувати цілі.

3.3 Використання автоматизованих засобів аналізу

Особливістю підходу є активне використання автоматизованих засобів для інформування оцінки кіберзрілості. Розглянемо детальніше, які інструменти можуть бути залучені і як саме їх дані інтерпретувати:

- Система SIEM. Для критичного ОКІ важливо мати впроваджену Security Information and Event Management (наприклад, продукти типу IBM QRadar, Splunk, ArcSight, Elastic SIEM тощо) або хоча б накопичувати журнали подій у централізоване сховище і аналізувати їх . Дані, що можуть бути використаними при аналізі: число інцидентів за останній рік, середній час виявлення і середній час на реагування/усунення, покриття – які сегменти

мережі і системи моніторяться. Ці метрики допомагають оцінити функцію Detect та Respond. Наприклад, якщо інциденти фіксуються, але накопичуються невирішеними – значить, проблема з реагуванням, не вистачає людських ресурсів чи процесу ескалації.

- Сканери вразливостей та управління конфігураціями. Інструменти як-от Nessus, Qualys, OpenVAS регулярно сканують IT-інфраструктуру на відомі вразливості. Дані, що можуть бути використаними при аналізі: кількість критичних і високих вразливостей; відсоток з них, закритих протягом нормативного терміну, типові категорії вразливостей. Якщо розгорнута система аналізу конфігурації (наприклад, SCAP-сканери чи модулі в тому ж Qualys), дивимось відповідність конфігурацій кращим практикам. Ця інформація дає зріз по функції Protect. Присутність великої кількості вразливостей в ІС або неналежне налаштування конфігурацій систем може свідчити про низьку зрілість у процесах Vulnerability Management.
- Системи контролю доступу та облікових записів. Корисні інструменти, що допомагають систематизувати та полегшити процеси аналізу даних з Active Directory або іншої Identity Management системи [29].
- Логи брандмауерів та IDS/IPS. Аналіз мережевого трафіку може вказати на наявність підозрілих подій: наприклад, спроби зв’язку з відомими шкідливими IP , сканування портів, аномально великий трафік.
- Антивірусні / EDR системи. Системи даного класу дають можливість централізовано відстежувати та аналізувати стан захищеності кінцевих точок всередині організації [30,31].
- Системи резервного копіювання. Використання систем резервного копіювання дозволяє перевіряти та контролювати чи всі критичні ІС копіюються, дані про останній успішний бекап, чи проводились тестові відновлення. Наявність систем даного класу значною мірою полегшує підтримку та аналіз виконання функції Recover [32,33].

Залучення цих даних не тільки підвищує точність оцінки, але і полегшує обґрунтування отриманих результатів при представлені керівництву.

Використання даних отриманих від автоматизованих інструментів дозволяє перейти від суб’єктивної оцінки до кількісної моделі зрілості. При цьому важливо, щоб такі інструменти самі були правильно налаштовані, інакше дані можуть привести до встановлення необ’єктивних оцінок рівня кіберзрілості процесів.

3.4 Приклади практичного застосування методики для оцінки кіберзрілості

Методика оцінки кіберзрілості на основі фреймворку NIST CSF 2.0 вже активно застосовується як у сфері державного управління, так і в приватному секторі [34]. Її гнучкість, адаптивність до галузевих особливостей і прозорість результатів робить її придатною для організацій з різним рівнем зрілості кібербезпеки. На практиці методика доводить свою ефективність у вирішенні цілого спектру завдань – від ідентифікації поточних недоліків до формування стратегічної дорожньої карти розвитку системи безпеки [35,36,37].

Застосування методики починається з визначення сфери охоплення оцінки: це може бути вся організація або окремий структурний підрозділ, сервіс, або технологічна платформа. Наприклад, у випадку IT-компаній – це може бути дата-центр або хмарна платформа, у промислових підприємств – виробничий кластер або система автоматизованого керування, у медичних установ – електронна система зберігання даних пацієнтів [38, 39].

Після визначення об’єкта оцінювання, формується робоча група, яка проводить збір інформації за допомогою адаптованих опитувальників, інтерв’ю та аналізу документів. При цьому використовуються як якісні, так і кількісні дані: описи політик, журнали подій, результати попередніх аудитів, конфігурації систем, журнали інцидентів, звіти від SIEM або сканерів вразливостей тощо. Це дозволяє мінімізувати суб’єктивність оцінки та зробити її максимально обґрунтованою.

Практичний досвід свідчить, що навіть у великих організаціях деякі

функції кібербезпеки можуть залишатися на початковому рівні зрілості (Tier 1 або Tier 2), тоді як інші – досягли стабільного функціонування (Tier 3). Наприклад, процес резервного копіювання може бути добре впроваджений, а от управління ризиками постачальників або формалізоване реагування на інциденти – слабо розвинені або відсутні. Методика CSF дозволяє зафіксувати цей дисбаланс та звернути на них увагу керівництва.

Одним із ключових практичних результатів є формування "поточного профілю" (Current Profile) організації, який містить пофункціональний аналіз зрілості: тобто стан реалізації заходів за функціями Govern, Identify, Protect, Detect, Respond, Recover. Це дозволяє не лише побачити загальний рівень кіберзрілості, а й розкласти його на складові, виявивши, де саме зосереджуються ризики. Наприклад, може з'ясуватись, що організація має засоби захисту, але не має належної системи реагування (відсутній план дій на випадок атаки, не проводяться тренування персоналу тощо), а це суттєво знижує загальну стійкість.

Після формування поточного профілю проводиться визначення цільового стану – тобто моделі, до якої організація прагне прийти з урахуванням галузевих стандартів, ресурсів, нормативних вимог та внутрішніх цілей. Це може бути, наприклад, рівень Tier 3 для всіх функцій або підвищення лише найбільш критичних із них.

Наступним етапом є побудова дорожньої карти розвитку – конкретного плану заходів, спрямованих на усунення виявлених прогалин. У практиці це найцінніша частина методики, адже на її основі керівництво приймає рішення про розподіл ресурсів, ініціацію проєктів з удосконалення ІБ, модернізацію інфраструктури чи зміну процедур.

Прикладом типових рекомендацій можуть бути:

- створення внутрішніх політик і призначення відповідальних за напрямки безпеки;
- впровадження централізованого журналювання і системи моніторингу подій (SIEM);

- регулярна оцінка ризиків для кожного сервісу;
- підвищення обізнаності персоналу;
- перевірка ефективності планів резервного копіювання та аварійного відновлення.

Крім цього, результати оцінки слугують основою для періодичного моніторингу прогресу. Через визначений проміжок часу (наприклад, пів року) може бути проведена повторна оцінка, яка дозволить оцінити, наскільки організація наблизилася до цільового рівня, та чи потрібні додаткові коригування.

Таким чином, у практичному застосуванні методика CSF 2.0 виконує кілька важливих функцій одночасно:

- є інструментом самодіагностики для внутрішнього аудиту;
- забезпечує структурований підхід до управління ризиками [40,41];
- допомагає підвищити прозорість комунікацій з керівництвом;
- формує єдину мову для обговорення питань безпеки між технічними фахівцями та менеджментом;
- дозволяє будувати систему безперервного вдосконалення на основі циклу PDCA (Plan – Do – Check – Act).

Усе це доводить, що методика NIST CSF 2.0 має високу практичну цінність і повинна розглядатися як базовий підхід при формуванні стратегії розвитку кібербезпеки ОКІ [42].

Висновки до розділу 3

У третьому розділі було представлено обґрунтування вибору методики оцінки кіберзрілості об’єктів критичної інфраструктури на основі фреймворку NIST CSF 2.0, розроблено чіткий алгоритм її застосування, а також проаналізовано можливості залучення автоматизованих інструментів та практичне значення реалізації методики.

NIST CSF 2.0 обрано як основу завдяки його комплексному, адаптивному та практично орієнтованому підходу. Методика дозволяє всебічно оцінити стан кібербезпеки – від управлінських процесів до технічного захисту та відновлення – і визначити рівень кіберзрілості організації за зрозумілою структурою з шести функцій.

Розроблений алгоритм оцінки охоплює ключові етапи: від підготовки та збору даних через опитування, інтерв'ю та аналіз наявної документації, до формування поточного профілю безпеки, визначення цільового рівня зрілості, розробки рекомендацій і презентації результатів керівництву. Методика дозволяє не лише фіксувати слабкі місця, але й формувати дорожню карту вдосконалення безпеки з урахуванням ризиків, ресурсів і організаційного контексту.

Залучення об'єктивних технічних джерел, таких як SIEM, сканери вразливостей, системи резервного копіювання та контролю доступу, підвищує точність і достовірність оцінки. Це забезпечує перехід від суто опитувального аналізу до кількісної, фактичної моделі оцінки кіберзрілості.

Узагальнений практичний досвід демонструє, що застосування CSF 2.0 дозволяє не лише виявити існуючі ризики, а й створити умови для системного розвитку системи кіберзахисту, інтегрувавши її у загальне корпоративне управління.

Таким чином, NIST CSF 2.0 є дієвим і сучасним інструментом для оцінки та підвищення рівня кіберзрілості, що є особливо важливим для об'єктів критичної інфраструктури в умовах зростання складності та частоти кіберзагроз.

Розділ 4 ПРАКТИЧНА РЕАЛІЗАЦІЯ МЕТОДИКИ ОЦІНКИ ТА РОЗРОБКА РЕКОМЕНДАЦІЙ

4.1 Проведення оцінки кіберзрілості на реальному або тестовому об’єкті

В якості тестового сценарію розглядається умовна українська компанія “УкрКом”, яка надає критично важливі комунікаційні послуги. Нехай це буде великий провайдер зв’язку, що забезпечує інтернет та телефонний зв’язок урядовим установам, силовим відомствам, стратегічним підприємствам і мільйонам приватних абонентів по всій країні, аналогічно реальним операторам на кшталт “Укртелеком”, “Київстар” тощо. Дана компанія є ОКІ (сектор інформаційно-комунікаційних послуг), а стабільність її роботи впливає на національну безпеку.

- Кібербезпекове середовище “УкрКом”: компанія має розгалужену мережу інфраструктури: десятки вузлів зв’язку (дата-центри, магістральні канали зв’язку), тисячі мережевих пристроїв (маршрутизатори, комутатори, базові станції), сервери та програми для підтримки роботи мережі. Також є корпоративна ІТ-інфраструктура (офісні мережі, ПК працівників, вебпортал). Персонал – кілька тисяч працівників по країні (інженери, оператори, служба підтримки, адміністрація). Компанія підпадає під державне регулювання: має виконувати вимоги регулятора зв’язку, стандарти з захисту мереж електрозв’язку, а також рекомендації НКЦК та ДССЗЗІ щодо критичної інформаційної інфраструктури [43].
- Виклики кібербезпеки: провайдер зв’язку – приваблива ціль для різних атак. Мета таких атак – масове відключення зв’язку, що має психологічний ефект на населення та ускладнює роботу органів влади, шпигунство або саботаж [44]. До основних загроз належать: проникнення в ядро мережі оператора (через мережеві пристрої або

підтримуючі системи), установка бекдорів для стеження, DDoS-атаки на вузли, компрометація акаунтів адміністрації мережі, атаки на DNS та маршрутизацію (BGP hijacking), шкідливі дії інсайдерів.

Компанія “УкрКом” усвідомлює ці ризики, тим більше що у 2022-2023 вже стикалася з кібератаками: були DDoS на її DNS-сервери, спроби фішингу співробітників.

Керівництво вирішило провести комплексну оцінку кіберзрілості за методикою NIST CSF 2.0, аби виявити слабкі місця і підготуватися до нових атак. Завдання – продемонструвати практичну реалізацію методики: як проводиться оцінка, які результати отримано, які рекомендації надано та як вони впроваджені у систему управління безпекою “УкрКом”.

4.2 Аналіз отриманих результатів та виявлення слабких місць у системі безпеки

Для початку робіт було створено робочу групу з фахівців компанії: голова – CISO “УкрКом”, члени – керівник департаменту мережевої безпеки, представник IT-департаменту, начальник відділу моніторингу мережі, представник служби внутрішнього аудиту. Також було прийнято рішення про охоплення всієї інфраструктури оператора для проведення повноцінної оцінки.

Наступним кроком було створено опитувальник , який базувався на шести функціях фреймворку NIST CSF 2.0 (Identify, Protect, Detect, Respond, Recover, Govern). Питання були адаптовані під специфіку “УкрКом” і охоплювали всі ключові напрямки: від інвентаризації активів до політик реагування на інциденти та процедур резервного копіювання. Паралельно було заплановано серію внутрішніх інтерв’ю з фахівцями, відповідальними за управління безпекою на різних рівнях. Під час інтерв’ю збиралася інформація про існуючі політики, рівень автоматизації захисту, процеси моніторингу, кадрову обізнаність, а також здійснювався аналіз наявної документації (регламенти, технічні паспорти систем, журнали подій).

У результаті проведеної оцінки кіберзрілості компанії “УкрКом” за фреймворком NIST CSF 2.0 було сформовано поточний профіль безпеки на основі шести функцій: Identify, Protect, Detect, Respond, Recover, Govern. Оцінювання охоплювало понад 100 результатів, згрупованих у категорії, кожна з яких аналізувалася через співбесіди з відповідальними працівниками, огляд документації, тестування процесів та інфраструктури. В результаті можемо стверджувати наступне:

- Сильні сторони.

Станом на момент оцінки “УкрКом” продемонструвала відносно високий рівень реалізації функції Protect, зокрема: функціонує сегментована мережева архітектура (сегментація ядра мережі та офісної IT-інфраструктури); реалізовано резервне копіювання критичних сервісів; використовується шлюзовий захист трафіку та антивірусні системи; обмежено привілеї користувачів за принципом мінімально необхідного доступу.

- Частково реалізовані або не реалізовані функції.

Попри наявність базових заходів кіберзахисту, в ході оцінки було виявлено ряд функцій фреймворку NIST CSF 2.0, які реалізовані частково або перебувають на низькому рівні зрілості. Це свідчить про наявність критичних зон, які потребують вдосконалення в межах функцій Identify, Detect, Respond, Recover та Govern.

Identify: Незважаючи на часткову інвентаризацію активів, компанія не має централізованого каталогу IT-ресурсів, який би включав повний перелік серверів, мережевого обладнання, програмного забезпечення та користувачів. Також відсутнє класифікування активів за критичністю, що ускладнює пріоритизацію захисту найважливіших елементів. Оцінка ризиків проводиться нерегулярно і не формалізована в єдиний процес, а ризик-профілі для окремих сервісів або бізнес-функцій відсутні. Крім того, не всі ролі і відповідальності в управлінні безпекою задокументовані – частина обов’язків виконується ситуативно. Також не враховуються ризики, пов’язані з постачальниками та контрагентами (supply chain risks), хоча компанія активно співпрацює з

зовнішніми провайдерами хмарних сервісів і обладнання.

Detect: В компанії відсутній єдиний центр моніторингу безпеки (SOC), тому інциденти фіксуються нецентралізовано, переважно на рівні окремих підрозділів або після звернень користувачів. Журналювання подій здійснюється вибірково: не всі вузли зв'язку або сервери передають лог-файли до центрального сховища. Також бракує інтегрованої SIEM-системи, що унеможливлює оперативну кореляцію подій з різних джерел [24]. Вразливості виявляються здебільшого реактивно – після інцидентів або у ході постфактум перевірок.

Respond: На момент оцінки в "УкрКом" не було затверджено формалізованого плану реагування на кіберінциденти. Відсутні визначені процедури внутрішньої та зовнішньої комунікації у випадку атак. Працівники не проходили навчання або тренування з моделювання надзвичайних ситуацій, таких як DDoS-атака чи витік даних [45]. Також не ведеться централізований облік інцидентів: зафіксовані випадки не документуються у єдиній базі для подальшого аналізу та вдосконалення заходів реагування.

Recover: Плани аварійного відновлення (Disaster Recovery) існують, однак не переглядалися понад два роки та не відображають актуальну мережеву топологію і зміни в інфраструктурі. Резервне копіювання критичних сервісів здійснюється, проте не супроводжується регулярними перевірками на працездатність резервних копій. Крім того, відсутній єдиний погоджений підхід до відновлення ключових функцій у разі масштабного інциденту, що створює ризик неузгоджених дій у кризовій ситуації [46].

Govern: Управління кібербезпекою на стратегічному рівні залишається недостатньо розвиненим. У структурі правління компанії не створено спеціалізованого комітету з питань кібербезпеки, що обмежує залучення топменеджменту до контролю за ІБ. Кіберризики не інтегровані у загальну систему управління корпоративними ризиками: вони розглядаються переважно в межах окремих технічних служб [47]. Також відсутня система внутрішніх індикаторів (KPI), що не дозволяє об'єктивно оцінювати динаміку стану

кібербезпеки та ефективність впроваджених заходів.

4.3 Розробка рекомендацій щодо покращення рівня кіберзахисту

На основі проведеної оцінки кіберзрілості компанії “УкрКом” було визначено низку слабких місць у реалізації функцій Identify, Detect, Respond, Recover та Govern за NIST CSF 2.0. Відповідно, сформовано обґрунтовані рекомендації для вдосконалення цих функцій, що враховують як вимоги й найкращі практики Cybersecurity Framework 2.0, так і реалії діяльності “УкрКом”. Рекомендації передбачають впровадження конкретних заходів, спрямованих на усунення виявлених недоліків та підвищення загального рівня кібербезпеки організації.

- Функція Identify.

Для усунення виявленої невідповідностей в області ідентифікації активів і ризиків рекомендується впровадити комплексну систему обліку та класифікації інформаційних активів компанії. Йдеться про створення актуального реєстру апаратного і програмного забезпечення, даних, IT-інфраструктури, а також про визначення власників цих активів та їх критичності для бізнес-процесів [48]. Окрім цього, слід провести повномасштабну оцінку кіберризиків: виявити загрози та вразливості, що характерні для активів “УкрКом”, включно з ризиками, пов’язаними з ключовими постачальниками та партнерами. В результаті компанія зможе встановити пріоритети захисних заходів відповідно до своєї стратегії управління ризиками та бізнес-місії, усуваючи виявлену проблему недостатньої обізнаності про власні цифрові ресурси та найбільш уразливі місця [49].

- Функція Detect.

Для підвищення здатності своєчасно виявляти кібератаки та інші інциденти “УкрКом” слід запровадити сучасні засоби моніторингу і аналізу подій безпеки. Зокрема, рекомендується розгорнути систему централізованого збору і кореляції журналів безпеки (SIEM) та налаштувати безперервний

моніторинг мережевого трафіку на наявність аномалій [50]. Практика впровадження IDS/IPS (систем виявлення та запобігання вторгненням) допоможе автоматично відстежувати можливі ознаки компрометації в мережі, а використання SIEM – агрегувати журнали подій з різних систем для виявлення підозрілої активності. Такі інструменти забезпечують цілодобовий нагляд за IT-інфраструктурою та підвищують ймовірність раннього сповіщення про кіберінциденти [51]. Організації слід також визначити процедури реагування на виявлені аномалії: наприклад, створити регламенти для аналізу попереджень та ескалації інцидентів. Таким чином, “УкрКом” зможе мінімізувати час між початком атаки та її виявленням, що раніше було слабким місцем у системі кіберзахисту.

- Функція Respond.

Для ефективного реагування на інциденти компанії необхідно розробити і впровадити формалізований план реагування на кіберінциденти. Такий план має чітко визначати ролі та обов’язки учасників, а також описувати покрокові процедури локалізації, усунення та розслідування інциденту. Зокрема, документ повинен охоплювати заходи стримування атак (ізоляція уражених систем, відключення від мережі тощо) [52], методи усунення наслідків (поновлення систем із резервних копій, встановлення виправлень безпеки), порядок внутрішнього сповіщення керівництва і користувачів, а при необхідності – повідомлення відповідних зовнішніх сторін (наприклад, партнерів або регуляторів). Важливо також, щоб план містив вимоги до документування інцидентів та збереження доказів для подальшого аналізу і вдосконалення захисних заходів. Окрім розробки плану, необхідно регулярно його відпрацьовувати – проводити навчання персоналу і тренувальні імітації інцидентів, що дозволить виявити слабкі місця у реагуванні та підготувати працівників до реальних атак [53]. Виконання цих рекомендацій забезпечить “УкрКом” здатність оперативно локалізувати кіберінциденти і зменшувати їхній вплив на діяльність, що раніше було проблемним через відсутність чіткого плану дій при атаках.

- Функція Recover.

Враховуючи недоліки у сфері відновлення діяльності після інцидентів, компанії слід впровадити заходи для підвищення кіберстійкості та швидкого відновлення критичних сервісів. Насамперед, рекомендується розробити план відновлення (Disaster Recovery Plan), узгоджений із планом реагування: він має визначати стратегію повернення до нормальної роботи після кіберінциденту і містити конкретні процедури відновлення систем та даних [54]. План повинен включати пріоритетність відновлення – спершу поновлення найбільш критичних для бізнесу систем і сервісів – а також призначення відповідальних осіб за виконання відновлювальних робіт. Необхідно передбачити координацію між різними підрозділами (IT, інформаційна безпека, бізнес-керівники) під час ліквідації наслідків, аби дії були злагодженими [55]. Другим ключовим компонентом є система резервного копіювання: слід налаштувати регулярне резервування важливих даних і систем, зберігання резервних копій у захищеному середовищі та періодично тестувати їх відновлення. Це гарантуватиме цілісність і доступність даних у разі успішної атаки (наприклад, програми-вимагача) та мінімізує простої. Виконання плану відновлення потрібно відпрацьовувати на практиці – шляхом навчань і тестових сценаріїв – щоб упевнитися в його дієвості та готовності персоналу діяти за визначеним алгоритмом [56]. Також компанія має заздалегідь підготувати комунікаційний план на період відновлення: своєчасно інформувати зацікавлені сторони (керівництво, клієнтів, партнерів) про стан відновлювальних робіт та очікувані строки повного відновлення нормальної діяльності. Запропоновані заходи дозволять “УкрКом” підвищити готовність до кризових ситуацій і значно скоротити час простою після інцидентів у порівнянні з попереднім рівнем готовності.

- Функція Govern.

Окрему увагу приділено вдосконаленню функції кібербезпекового управління, яка в оновленому CSF 2.0 відіграє центральну роль в забезпеченні усіх інших напрямів. Для зміцнення цієї функції в “УкрКом” рекомендовано

впровадити цілісну систему управління кібербезпекою на рівні організації. Перш за все, необхідно сформувати офіційну стратегію кібербезпеки, яка визначатиме довгострокові цілі та пріоритети захисту інформації відповідно до бізнес-стратегії та ризик-апетиту компанії. має бути схвалена вищим керівництвом і інтегрована у загальну систему корпоративного управління ризиками, що забезпечить врахування кіберризиків поряд з іншими видами ризиків бізнесу. В рамках цієї стратегії компанія повинна запровадити політику управління ризиками постачальників (кібербезпека ланцюга поставок): проводити оцінювання кіберстійкості ключових постачальників, вимагати від них дотримання мінімальних стандартів безпеки та враховувати ризики контрагентів при укладенні договорів. Наступним кроком є удосконалення організаційної структури управління ІБ: призначення відповідальних осіб за напрям кібербезпеки на найвищому рівні та чітке розмежування ролей і зон відповідальності в сфері ІБ для всіх задіяних підрозділів. Відповідальні за безпеку повинні мати належні повноваження для реалізації захисних заходів і прямий зв’язок з керівництвом – це підвищить підзвітність та сприятиме постійному покращенню кібербезпеки завдяки регулярній оцінці результатів і ефективності заходів. Крім того, необхідно актуалізувати внутрішню нормативну базу з інформаційної безпеки: переглянути та оновити існуючі політики, стандарти й процедури у відповідності до виявлених прогалин. Зокрема, основна політика інформаційної безпеки має відобразити нові вимоги (щодо управління активами, реагування на інциденти, резервного копіювання, контролю доступу тощо) і встановити процес її періодичного перегляду в міру розвитку технологій, змін регуляторних вимог чи появи нових загроз. Вищий менеджмент “УкрКом” повинен здійснювати постійний нагляд за реалізацією кібербезпекової стратегії: передбачено регулярне заслуховування звітів про стан інформаційної безпеки, оцінку нових ризиків та за необхідності – коригування стратегії та ресурсів, виділених на кіберзахист. Реалізація цих рекомендацій дозволить усунути недоліки в управлінні ІБ, виявлені під час оцінки, та закладе основу для сталого підвищення кіберстійкості “УкрКом” у довгостроковій

перспективі.

4.4 Інтеграція результатів оцінки у систему управління інформаційною безпекою організації

Результати комплексної оцінки кіберзрілості за фреймворком NIST CSF 2.0 стали відправною точкою для трансформації підходів до управління інформаційною безпекою в компанії “УкрКом”. Після ідентифікації слабких сторін, керівництво організації визнало необхідність переходу від фрагментарних або реактивних рішень у сфері кіберзахисту до більш системного, інтегрованого та проактивного підходу. Це означало не просто впровадження окремих технічних засобів або процедур, а суттєве оновлення усієї системи управління інформаційною безпекою – від стратегічного рівня до операційних процесів. На рис. 4.1 зображено прогнозовані результати впливу впровадження рекомендованих компенсуючих заходів.

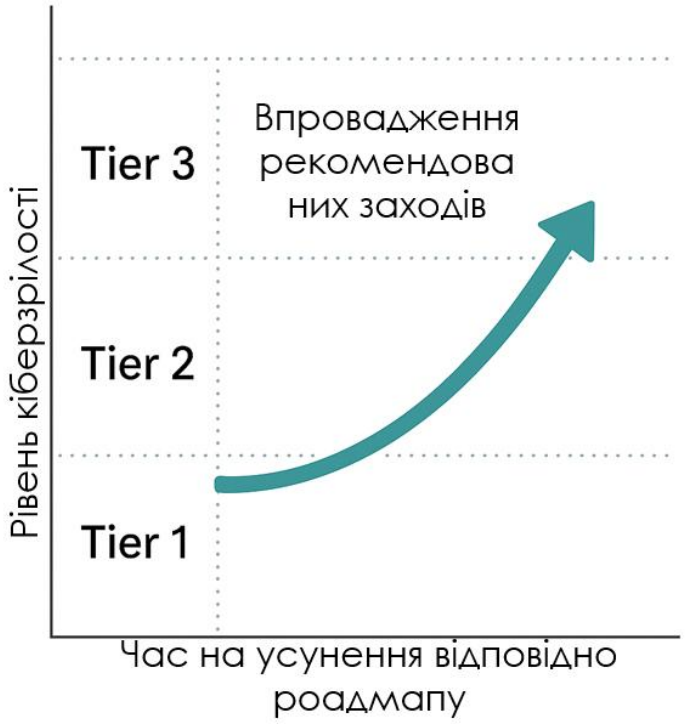

Рис. 4.1 Ядро NIST CSF 2.0

Інтеграція результатів оцінки передбачала, насамперед, переосмислення місця кібербезпеки у загальній моделі корпоративного управління. Кібербезпека перестала розглядатися як виключно технічна функція, і була визнана ключовим елементом забезпечення безперервності бізнесу, довіри клієнтів та стійкості організації до зовнішніх загроз. Це стало основою для включення інформаційної безпеки до стратегічних ініціатив компанії. Зокрема, нові завдання в сфері ІБ почали плануватися і реалізовуватися з урахуванням бізнес-цілей, а також були закладені в загальні політики управління ризиками, розвитку персоналу, взаємодії з партнерами тощо [57].

На практичному рівні інтеграція результатів оцінки означала налагодження систематичного підходу до управління всіма аспектами кібербезпеки. Організація почала поступово впроваджувати стандартизовані політики, процедури та регламенти, які базуються на результатах аналізу функцій NIST CSF. Наприклад, були розпочаті процеси з формалізації таких напрямів як управління активами, моніторинг подій, реагування на інциденти, резервне копіювання та відновлення. Але ці зміни не були реалізовані як одномоментні дії – натомість, компанія розробила поетапний план впровадження з урахуванням наявних ресурсів, рівня зрілості персоналу та важливості окремих процесів для стабільності сервісів.

Важливо, що в процесі інтеграції акцент робився не лише на змістовному наповненні заходів, але й на створенні відповідних умов для їх підтримки. Це включало призначення відповідальних осіб, оновлення посадових обов’язків, формування внутрішніх команд безпеки, а також залучення керівного складу до контролю за дотриманням політик та до прийняття рішень у сфері безпеки. У такий спосіб безпека перестала бути справою виключно фахівців з ІТ чи кіберзахисту – вона стала колективною відповідальністю, що підтримується культурою організаційної зрілості [58].

Окрему увагу компанія приділила створенню умов для сталого вдосконалення процесів безпеки. Результати оцінки були не просто враховані у моменті, а стали основою для побудови циклічного підходу до управління ІБ.

Регулярна переоцінка стану захищеності, аналіз інцидентів, визначення показників ефективності безпеки та коригування політик відповідно до нових викликів – усе це стало частиною операційної моделі компанії. Таким чином, кібербезпека перестала сприйматися як реакція на окремі інциденти і набула рис постійного, керованого і вимірюваного процесу [59].

У межах цієї трансформації “УкрКом” також почала переглядати свої зовнішні зобов’язання та взаємодію з партнерами. Зокрема, підхід до управління ризиками постачальників та контрагентів був змінений у бік більш вимогливого та контрольованого – із врахуванням кіберризиків у договорах, перевірках відповідності сторонніх систем вимогам безпеки тощо. Це дозволило знизити ризики, пов’язані з ланцюгами поставок, які раніше були поза фокусом уваги.

Зрештою, варто зазначити, що інтеграція результатів оцінки кіберзрілості в “УкрКом” не обмежилася організаційними та процедурними змінами. Вона також вплинула на загальний підхід до цифрової трансформації компанії. Усі подальші інноваційні проєкти, оновлення IT-інфраструктури, розгортання нових сервісів стали оцінюватися не лише з точки зору технічної доцільності або рентабельності, а й з позиції їх впливу на загальний рівень кіберстійкості організації. Це створило передумови для формування такої моделі розвитку компанії, в якій безпека є не перешкодою, а вбудованим компонентом успіху [60].

Отже, результати оцінки кіберзрілості, проведеної за методикою NIST CSF 2.0, стали каталізатором для побудови в “УкрКом” сучасної системи управління інформаційною безпекою. Ця система не лише враховує наявні ризики, а й здатна адаптуватися до динамічного середовища загроз, підтримуючи стратегічну стабільність організації в умовах зростаючих викликів у сфері національної та корпоративної кібербезпеки.

Висновки до розділу 4

У четвертому розділі кваліфікаційної роботи було практично реалізовано методику оцінки кіберзрілості за фреймворком NIST CSF 2.0 на прикладі умовної компанії критичної інфраструктури “УкрКом”, що надає телекомунікаційні послуги. Результатом оцінювання стало виявлення низки критичних прогалин у реалізації функцій Identify, Detect, Respond, Recover та Govern, які становлять потенційні вектори загроз для безперервної роботи підприємства. На основі виявлених недоліків було сформовано обґрунтовані рекомендації щодо підвищення рівня кіберзахисту, що охоплюють організаційні, процесні та технічні аспекти.

Подальша інтеграція результатів оцінки в систему управління інформаційною безпекою організації продемонструвала, що ефективне використання фреймворку NIST CSF 2.0 сприяє переходу компанії до цілісного, стратегічно орієнтованого підходу до кібербезпеки. Розпочаті процеси стандартизації, формалізації процедур, розбудови культури безпеки, а також включення питань ІБ у стратегічне управління створюють підґрунтя для сталого розвитку та підвищення кіберстійкості. Таким чином, фреймворк NIST CSF 2.0 довів свою практичну цінність як інструмент побудови системного захисту ОКІ в сучасному середовищі.

ВИСНОВКИ

У дипломній роботі було проведено дослідження проблематики оцінки рівня кіберзрілості ОКІ та запропоновано методику на основі фреймворку NIST Cybersecurity Framework версії 2.0, яка дозволяє реалізувати структурований, адаптивний і практико-орієнтований підхід до підвищення рівня кіберзахисту організацій.

У першому розділі проаналізовано поняття критичної інфраструктури, її галузеву класифікацію, систему категоризації за рівнем важливості, а також основні кіберзагрози, що стосуються ОКІ в сучасних умовах. Розглянуто ключові нормативно-правові акти України у сфері кібербезпеки та охарактеризовано роль міжнародних стандартів, які все активніше впроваджуються в національну практику. Показано, що застосування фреймворків, зокрема NIST CSF, дозволяє забезпечити безперервний і системний процес вдосконалення захисту.

У другому розділі здійснено аналіз структури, функцій та компонентів оновленого фреймворку NIST CSF 2.0. Розкрито його гнучкість, інтегрованість з іншими стандартами (ISO 27001, NIST SP 800-53, COBIT), а також визначено можливості його адаптації під галузеві й організаційні особливості. Описано методологію оцінки кіберзрілості організацій за допомогою механізмів профілювання та визначення рівнів впровадження (Tiers), що дозволяє не лише виявляти прогалини, але й будувати дорожні карти розвитку.

У третьому розділі розроблено власну методику оцінки кіберзрілості на основі CSF 2.0, яка охоплює підготовчий етап, збір і верифікацію даних, формування поточного профілю, виявлення прогалин, розробку рекомендацій та інтеграцію результатів в систему управління ІБ. Окрему увагу приділено використанню об’єктивних джерел даних – таких як SIEM, сканери вразливостей, резервні системи, журнали подій – що підвищує точність і надійність оцінки.

У четвертому розділі здійснено практичну реалізацію методики на умовному прикладі телекомунікаційної компанії “УкрКом”, яка класифікується як об’єкт критичної інфраструктури. Результати оцінки дозволили

ідентифікувати низку критичних недоліків у функціях Detect, Respond, Recover, Govern та Identify, що потенційно загрожують безперервній роботі підприємства. На основі цього були сформульовані конкретні рекомендації щодо вдосконалення політик, процедур, технічного забезпечення та управлінської моделі безпеки. Інтеграція результатів в управлінську систему організації продемонструвала перехід до системного підходу до кіберзахисту та забезпечила сталість змін через підтримку керівництва, розвиток процесної культури безпеки й побудову циклу безперервного покращення.

Узагальнюючи, можна стверджувати, що запропонована методика оцінки кіберзрілості за фреймворком NIST CSF 2.0 є ефективним, практичним інструментом для державних і приватних ОКІ. Вона дозволяє виявити ключові вразливості, встановити обґрунтовані цільові орієнтири та поступово досягати їх шляхом реалізації системних заходів. Методика сприяє не лише підвищенню технічного рівня безпеки, а й формуванню зрілої організаційної культури кіберстійкості – що є визначальним чинником захисту державних інтересів і сталого функціонування критичних сервісів в умовах зростання кіберзагроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Directive - 2008/114 - EN - EUR-Lex. EUR-Lex – Access to European Union law – choose your language. URL: https://eur-lex.europa.eu/eli/dir/2008/114/oj/eng (дата звернення: 10.05.2025).

2. Про критичну інфраструктуру. Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/laws/show/1882-20 (дата звернення: 10.05.2025).

3. Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави. Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/laws/show/563-2016 (дата звернення: 10.05.2025).

4. Про основні засади забезпечення кібербезпеки України. Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 10.05.2025).

5. Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури : Рішення Ради нац. безпеки і оборони України від 29.12.2016 : станом на 18 січ. 2017 р. URL: https://zakon.rada.gov.ua/laws/show/n0014525-16#Text (дата звернення: 10.05.2025).

6. ENISA Threat Landscape 2022 | ENISA. Home | ENISA. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022 (дата звернення: 10.05.2025).

7. Anderson J. L. Global cyberattacks increased 38% in 2022. Security Magazine | The business magazine for security executives. URL: https://www.securitymagazine.com/articles/98810-global-cyberattacks-increased-38-in-2022 (дата звернення: 10.05.2025).

8. Industrial Control Systems (ICS) Security | SANS Institute. Industrial Control Systems (ICS) Security | SANS Institute. URL: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf (дата звернення: 10.05.2025).

9. Russian hackers were in Kyivstar system for months - Reuters. LB.ua. URL: https://en.lb.ua/news/2024/01/04/25480_russian_hackers_were_kyivstar.html (дата звернення: 10.05.2025).

10. IsaacWiper and HermeticWizard: New wiper and worm targeting Ukraine. Award-winning news, views, and insight from the ESET security community. URL: https://www.welivesecurity.com/2022/03/01/isaacwiper-hermeticwizard-wiper-worm-targeting-ukraine/ (дата звернення: 10.05.2025).

11. Ukraine defence ministry website, banks, knocked offline. euronews. URL: https://www.euronews.com/2022/02/15/uk-ukraine-crisis-military-cyberattack (дата звернення: 10.05.2025).

12. Defending Ukraine: Early Lessons from the Cyber War - Microsoft On the Issues. Microsoft On the Issues. URL: https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war (дата звернення: 10.05.2025).

13. Guardian staff reporter. Colonial Pipeline confirms it paid $4.4m ransom to hacker gang after attack. the Guardian. URL: https://www.theguardian.com/technology/2021/may/19/colonial-pipeline-cyber-attack-ransom (дата звернення: 10.05.2025).

14. Kent K., Souppaya M. SP 800-92, Guide to Computer Security Log Management | CSRC. NIST Computer Security Resource Center | CSRC. URL:https://csrc.nist.gov/pubs/sp/800/92/final#:~:text=This%20publication%20seeks%20to%20assist%20organizations%20in%20understanding,maintaining%20effective%20log%20management%20practices%20throughout%20an%20enterprise. (дата звернення: 10.05.2025).

15. eIR MSU: Аналіз базової термінології і негативних наслідків кібератак на інформаційно-телекомунікаційні системи об’єктів критичної інфраструктури держави. URL: https://repository.mu.edu.ua/jspui/handle/123456789/5219 (дата звернення: 10.05.2025).

16. NIST Publishes SP 800-82, Revision 3 | CSRC. NIST Computer Security Resource Center | CSRC. URL: https://csrc.nist.gov/News/2023/nist-publishes-sp-800-82-revision. (дата звернення: 10.05.2025).

17. ISA/ IEC 62443-3-3:2013 - Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels. Interoperable Europe Portal. URL: https://interoperable-europe.ec.europa.eu/collection/ict-standards-procurement/solution/iec-62443-3-32013-industrial-communication-networks-network-and-system-security-part-3-3-system (дата звернення: 10.05.2025).

18. CIS Controls Version 8. CIS. URL: https://www.cisecurity.org/controls/v8 (дата звернення: 10.05.2025).

19. Безпека інформаційно-комунікаційних систем. DSpace :: ELAKPI :: Репозитарій КПІ ім. Ігоря Сікорського. URL: https://ela.kpi.ua/items/eba90ce5-b115-4467-b235-b3b5b6000ae0 (дата звернення: 10.05.2025). 18

20. NIST Cybersecurity Framework 2.0. NIST Technical Series Publications. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf (дата звернення: 10.05.2025).

21. Жилін А., Бєлявський В., Бакалинський О. NIST CSF 2.0: НОВИЙ ФРЕЙМВОРК З КІБЕРБЕЗПЕКИ ВІД НАЦІОНАЛЬНОГО ІНСТИТУТУ СТАНДАРТІВ І ТЕХНОЛОГІЙ США. Ukrainian Scientific Journal of Information Security. 2024. Т. 30, № 1. С. 73–76. URL: https://doi.org/10.18372/2225-5036.30.18606 (дата звернення: 10.05.2025).

22. Barrett M. P. Framework for Improving Critical Infrastructure Cybersecurity Version 1.1. NIST. URL: https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11 (дата звернення: 10.05.2025).

23. ДСТУ ISO/IEC 27005:2019 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2018, IDT). БУДСТАНДАРТ Online - нормативні документи будівельної галузі України. URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=85797 (дата звернення: 10.05.2025).

24. Brezavšček A., Baggia A. Recent Trends in Information and Cyber Security Maturity Assessment: A Systematic Literature Review. Systems. 2025. Т. 13, № 1. С. 52. URL: https://doi.org/10.3390/systems13010052 (дата звернення: 10.05.2025).

25. ISO/IEC 27001:2022. ISO. URL: https://www.iso.org/standard/27001 (дата звернення: 10.05.2025).

26. SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations | CSRC. NIST Computer Security Resource Center | CSRC. URL: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final (дата звернення: 10.05.2025).

27. COBIT | Control Objectives for Information Technologies | ISACA. ISACA. URL: https://www.isaca.org/resources/cobit (date of access: 10.05.2025).

28. STUDY OF THE CURRENT STATE OF SIEM SYSTEMS / T. Smirnova та ін. Cybersecurity: Education, Science, Technique. 2024. Т. 1, № 25. С. 6–18. URL: https://doi.org/10.28925/2663-4023.2024.25.618 (дата звернення: 10.05.2025).

29. NSA Jointly Releases Guidance for Mitigating Active Directory Compromises. National Security Agency/Central Security Service. URL: https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3917556/nsa-jointly-releases-guidance-for-mitigating-active-directory-compromises/ (дата звернення: 10.05.2025).

30. EXPLORING THE BENEFITS OF CROSS-IMPLEMENTING CYBERSECURITY STANDARDS TO COMBAT RANSOMWARE CYBER CRIMES / V. Dudykevych та ін. Cybersecurity: Education, Science, Technique. 2023. С. 226–237. URL: https://doi.org/10.28925/2663-4023.2023.22.226237 (дата звернення: 10.05.2025).

31. SP 800-61 Rev. 2, Computer Security Incident Handling Guide | CSRC. NIST Computer Security Resource Center | CSRC. URL: https://csrc.nist.gov/pubs/sp/800/61/r2/final (дата звернення: 10.05.2025).

32. SP 800-184, Guide for Cybersecurity Event Recovery | CSRC. NIST Computer Security Resource Center | CSRC. URL: https://csrc.nist.gov/pubs/sp/800/184/final (дата звернення: 10.05.2025).

33. Protecting Data from Ransomware. URL: https://cip.gov.ua/services/cm/api/attachment/download?id=57944 (дата звернення: 10.05.2025).

34. Applying NIST CSF 2.0: Risk management vs. maturity assessments. Responsible AI and Data Solutions | OneTrust. URL: https://www.onetrust.com/blog/applying-nist-csf-2-0-risk-management-vs-maturity-assessments/ (дата звернення: 10.05.2025).

35. Bernardo L., Malta S., Magalhães J. An Evaluation Framework for Cybersecurity Maturity Aligned with the NIST CSF. Electronics. 2025. Т. 14, № 7. С. 1364. URL: https://doi.org/10.3390/electronics14071364 (дата звернення: 10.05.2025).

36. Intel Use Case (NIST). Supplier.intel.com. URL: https://supplier.intel.com/static/governance/documents/The-cybersecurity-framework-in-action-an-intel-use-case-brief.pdf (дата звернення: 10.05.2025).

37. Success Story: Saudi Aramco. NIST. URL: https://www.nist.gov/cyberframework/success-stories/saudi-aramco (дата звернення: 10.05.2025).

38. Cyber Benchmark 2024: Progress in Cyber maturity continues, yet pace is slow. Wavestone. URL: https://www.wavestone.com/en/insight/cyber-benchmark-2024-progress-in-cyber-maturity-continues-yet-pace-is-slow/ (дата звернення: 10.05.2025).

39. NRI SecureTechnologies, Ltd. | Blog | NRI Secure. NRI SecureTechnologies | Managed Security Solutions. URL: https://www.nri-secure.com/blog/author/nri-secure (дата звернення: 10.05.2025).

40. NIST RMF. NIST Technical Series Publications. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1314.pdf#:~:text=The%20NIST%20RMF%20The%20RMF%20provides%20a,of%20organization%20regardless%20of%20size%20or%20sector. (дата звернення: 10.05.2025).

41. SP 800-161 Rev. 1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations | CSRC. NIST Computer Security Resource Center |

CSRC. URL: https://csrc.nist.gov/pubs/sp/800/161/r1/final (дата звернення: 10.05.2025).

42. Україна впроваджує норми NIST Cybersecurity Framework 2.0, підписано наказ. Інтернет журнал Кібербез. URL: https://cybersec.net.ua/normatyvni-dokumenty/793-ukraina-vprovadzhuie-naikrashchi-svitovi-praktyky-u-sferi-kiberbezpeky-ta-vprovadzhuie-normy-nist-cybersecurity-framework-20.html#:~:text=CSF%202,ризики,%20пов'язані%20з%20новітніми%20технологіями (дата звернення: 10.05.2025).

43. Consultant.net.ua. Законодавче забезпечення кібербезпеки в Україні. «Консультант». URL: https://consultant.net.ua/consultant-article/7309 (дата звернення: 10.05.2025).

44. ENISA Threat Landscape 2023 | ENISA. | ENISA. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 (дата звернення: 10.05.2025).

45. IBM X-Force reports evolving threat landscape amid shifting tactics, marking rise in stealth and identity exploits - Industrial Cyber. Industrial Cyber. URL: https://industrialcyber.co/reports/ibm-x-force-reports-evolving-threat-landscape-amid-shifting-tactics-marking-rise-in-stealth-and-identity-exploits/ (дата звернення: 10.05.2025).

46. ISO/IEC 27031:2011. ISO. URL: https://www.iso.org/standard/44374.html (дата звернення: 10.05.2025).

47. Mizrak F. Integrating cybersecurity risk management into strategic management: a comprehensive literature review. Pressacademia. 2023. URL: https://doi.org/10.17261/pressacademia.2023.1807 (дата звернення: 10.05.2025).

48. Edwardson R. D. Conducting a Comprehensive Asset Inventory: A Key Strategy for Assessing and Maintaining Device… Medium. URL: https://medium.com/o-m-n-i-navigating-the-new-cyber-era/conducting-a-comprehensive-asset-inventory-a-key-strategy-for-assessing-and-maintaining-device-a96c609919d6 (дата звернення: 10.05.2025).

49. NIST CSF to Define Risk Tolerances. Hyperproof. URL: https://hyperproof.io/nist-cybersecurity-framework/ (дата звернення: 10.05.2025).

50. Top Cybersecurity Trends and Strategies for Securing the Future | Gartner. Gartner. URL: https://www.gartner.com.au/en/cybersecurity/topics/cybersecurity-trends (дата звернення: 10.05.2025).

51. The Future of Security Automation. KPMG. URL: https://kpmg.com/us/en/articles/2025/future-of-security-automation.html (дата звернення: 10.05.2025).

52. NSA Jointly Releases Guidance for Mitigating Active Directory Compromises. National Security Agency/Central Security Service. URL: https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3917556/nsa-jointly-releases-guidance-for-mitigating-active-directory-compromises/#:~:text=This%20guidance%20addresses%20the%20most%20common%20techniques%20used,to%20mitigate%20it.%20Read%20the%20full%20report%20here. (дата звернення: 10.05.2025).

53. Dobbs M., Kotler I. Everyone Wants to Build a Cyber Range: Should You? | IBM. IBM - United States. URL: https://www.ibm.com/think/x-force/should-you-build-cyber-range (дата звернення: 10.05.2025).

54. Using ISO 27031 to Guide IT Disaster Recovery Alignment with ISO 22301. Riskonnect. URL: https://riskonnect.com/business-continuity-resilience/using-iso-27031-to-guide-it-disaster-recovery-alignment-with-iso-22301/ (дата звернення: 10.05.2025).

55. Business Continuity Planning for Operators | ENISA. Home | ENISA. URL: https://www.enisa.europa.eu/topics (дата звернення: 10.05.2025).

56. Miller J. A., Hannan E. What is a disaster recovery (DR) test. Search Disaster Recovery.URL:https://www.techtarget.com/searchdisasterrecovery/definition/disaster-recovery-DR-test (дата звернення: 10.05.2025).

57. Zero Trust Guidance Center. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/security/zero-trust/ (дата звернення: 10.05.2025).

58. 2025 Data Breach Investigations Report. Verizon Business. URL: https://www.verizon.com/business/resources/reports/dbir/ (дата звернення: 10.05.2025).

59. Cybersecurity Metrics & KPIs: What to Track in 2025. SentinelOne. URL: https://www.sentinelone.com/cybersecurity-101/cybersecurity/cybersecurity-metrics/ (дата звернення: 10.05.2025).

60. What Is Cybersecurity Mesh? Applications and Advantages | Fortinet. Fortinet. URL: https://www.fortinet.com/resources/cyberglossary/what-is-cybersecurity-mesh#:~:text=Gartner%20defines%20cybersecurity%20mesh%20architecture%20(CSMA)%20as%20“a,increasingly%20modular%20approaches%20consistent%20with%20hybrid%20multicloud%20architectures. (дата звернення: 10.05.2025).