

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

«На правах рукопису»

УДК _____

ДО ЗАХИСТУ ДОПУЩЕНО

Завідувач кафедри

_____ Дмитро ЛАНДЕ

«__» _____ 20__ р.

Дипломна робота
на здобуття ступеня бакалавра
за освітньо-професійною програмою «Системи, технології та математичні
методи кібербезпеки»
спеціальності 125 «Кібербезпека»

на тему: Оцінка стану кіберзахисту університету

Виконав (-ла): здобувач (-ка) вищої освіти **IV** курсу, групи ФБ-23
(шифр групи)

Тарасенко Ангеліна Віталіївна
(прізвище, ім'я, по батькові)

(підпис)

Керівник: к.т.н., доцент, доцент кафедри Інформаційної безпеки

Гальчинський Леонід Юрійович
(посада, науковий ступінь, вчене звання, ім'я, прізвище)

(підпис)

Рецензент _____
(посада, науковий ступінь, вчене звання, науковий ступінь, ім'я, прізвище) (підпис)

Засвідчую, що у цій дипломній роботі немає
запозичень з праць інших авторів без відповідних
посилань.

Здобувач вищої освіти _____
(підпис)

Київ – 2026 року

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

Рівень вищої освіти – перший (бакалаврський)

Спеціальність – 125 «Кібербезпека»

Освітньо-професійна програма «Системи, технології та математичні методи кібербезпеки»

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ Дмитро ЛАНДЕ
(підпис)

«19» червня 2026 р.

ЗАВДАННЯ
на дипломну роботу здобувачу вищої освіти
Тарасенко Ангеліни Віталіївної
(прізвище, ім'я, по батькові)

1. Тема роботи Оцінка стану кіберзахисту університету

керівник роботи Гальчинський Леонід Юрійович, к.т.н., доцент, доцент кафедри Інформаційної безпеки

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «29» травня 2026 р. № 2001-с

2. Термін подання роботи здобувачем вищої освіти «11» червня 2026 р.

3. Вихідні дані до роботи: дослідницькі статті у сфері управління ризиками інформаційної безпеки та документація зі стандартів інформаційної безпеки

4. Зміст (дипломної роботи) пояснювальної записки (перелік завдань, які потрібно

розробити): огляд типової інфраструктури, ландшафту загроз та поширених вразливостей інформаційної безпеки освітнього сектору, огляд існуючих підходів та стандартів оцінки стану кіберзахисту, оцінка стану кіберзахисту університету.

5. Перелік графічного (ілюстративного) матеріалу (із зазначенням обов'язкових креслеників, плакатів, презентацій тощо): презентація

6. Дата видачі завдання 21 листопада 2025 р.

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів дипломної роботи	Примітка
1	Вибір теми дипломної роботи, формування завдання та мети дослідження	21.11.2025 – 22.12.2025	Виконано
2	Опрацювання літературних джерел	22.12.2025 – 20.02.2026	Виконано
3	Ознайомлення з типовою мережною інфраструктурою університету	23.02.2026 – 13.03.2026	Виконано
4	Ознайомлення з типовими вразливостями та загрозами освітнього сектору	16.03.2026 – 03.04.2026	Виконано
5	Ознайомлення із наявними дослідженнями у частині оцінки стану захищеності університетів	06.04.2026 – 17.04.2026	Виконано
6	Проходження переддипломної практики	20.04.2026 – 17.05.2026	Виконано
7	Доопрацювання структури сформованого комбінованого фреймворку оцінки стану захищеності університету	17.05.2026 – 22.05.2026	Виконано
8	Проведення опитування експертів та аналіз результатів	22.05.2026 – 01.06.2026	Виконано
9	Оцінка стану захищеності університету	01.06.2026 – 04.06.2026	Виконано
10	Оформлення дипломної роботи	04.06.2026 – 08.06.2026	Виконано
11	Передзахист дипломної роботи	11.06.2026	Виконано
12	Захист дипломної роботи	19.06.2026	Виконано

Здобувач вищої освіти

(підпис)

Ангеліна ТАРАСЕНКО

(Власне ім'я, ПРИЗВИЩЕ)

Керівник роботи

(підпис)

Леонід ГАЛЬЧИНСЬКИЙ

(Власне ім'я, ПРИЗВИЩЕ)

РЕФЕРАТ

Дипломна робота містить: 73 сторінки, 15 ілюстрацій, 11 таблиць, 32 джерела літератури.

Метою роботи є розробка підходу до оцінки поточного стану кіберзахисту університету та визначення пріоритетних напрямів розвитку функції ІБ.

Об'єктом досліджень є стан кіберзахисту інформаційної інфраструктури університету.

Предметом дослідження є підхід до оцінки стану кіберзахисту.

Методом дослідження є опрацювання літературних джерел за вибраною темою, дослідження існуючих методів оцінки стану кіберзахисту ЗВО та розробка фреймворку оцінки стану кіберзахисту.

Робота містить опис процесу оцінки стану кіберзахисту університету, а саме створення комбінованого фреймворку, створення опитувальника для множини експертів, проведення опитування, узгодження оцінок експертів та визначення пріоритетних напрямів для розвитку функції інформаційної безпеки ЗВО.

Ключові слова: ландшафт загроз, вразливості, оцінка стану кіберзахисту, фреймворк, стандарт.

ABSTRACT

The work includes 73 pages, 15 illustrations, 11 tables, and 32 references.

The purpose of the work is to develop an approach for assessing the current cybersecurity posture of a university and identifying priority areas for the development of its information security function.

The object of the study is the university's information infrastructure.

The subject of the study is an approach to cybersecurity posture assessment.

The research method includes the analysis of scientific and technical literature on the selected topic, the study of existing approaches to assessing the cybersecurity posture of higher education institutions, and the development of a cybersecurity assessment framework.

The paper contains description of the university cybersecurity posture assessment process, including the development of a combined assessment framework, the creation of a questionnaire for a group of experts, conducting the expert survey, reconciling expert assessments, and determining priority areas for the further development of the university's information security function.

Keywords: threat landscape, vulnerabilities, cybersecurity posture assessment, framework, standard.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ.....	7
ВСТУП	10
1 ЛАНДШАФТ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОСВІТНЬОГО СЕКТОРУ	13
1.1 Особливості інформаційної інфраструктури закладів вищої освіти	13
1.2 Основні вразливості та вектори кібератак на інфраструктуру ЗВО	17
1.3 Проблеми забезпечення інформаційної безпеки ЗВО.....	24
1.4 Мотивація для розробки спеціалізованого підходу до оцінки інформаційної безпеки ЗВО	27
Висновки до розділу 1	29
2 РОЗРОБКА ПІДХОДУ ДО ОЦІНЮВАННЯ РІВНЯ КІБЕРБЕЗПЕКИ ЗВО	32
2.1 Обґрунтування вибору опорних стандартів та структури оцінювання.	32
2.2 Формування критеріїв та показників оцінювання рівня кібербезпеки ЗВО	38
2.3 Модель експертного оцінювання	45
Висновки до розділу 2	47
3 ПРАКТИЧНЕ ЗАСТОСУВАННЯ РОЗРОБЛЕНОГО ПІДХОДУ	49
3.1 Формування опитувальника.....	49
3.2 Консолідація оцінок експертів.....	54
3.3 Узгодження оцінок експертів	56
3.4 Обробка результатів оцінки стану захищеності згідно із запропонованим підходом.....	62
Висновки до розділу 3	65
ВИСНОВКИ.....	67
ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	70

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ЗВО – заклад вищої освіти

ІБ – інформаційна безпека

СУІБ – система управління інформаційною безпекою

ІІІ – штучний інтелект

NIST CSF – Cybersecurity Framework Національного інституту стандартів і технологій США (англ. *National Institute of Standards and Technology Cybersecurity Framework*)

ISO/IEC – Міжнародна організація зі стандартизації / Міжнародна електротехнічна комісія (англ. *International Organization for Standardization / International Electrotechnical Commission*)

ISMS – система управління інформаційною безпекою (англ. *Information Security Management System*)

BYOD – використання власних пристроїв для доступу до корпоративних ресурсів (англ. *Bring Your Own Device*)

ІоТ – Інтернет речей (англ. *Internet of Things*)

DDoS – розподілена атака відмови в обслуговуванні (англ. *Distributed Denial of Service*)

SIS – система управління даними студентів (англ. *Student Information System*)

LMS – система управління навчанням (англ. *Learning Management System*)

MIS – інформаційна система управління (англ. *Management Information System*)

PDCA – цикл безперервного вдосконалення «Плануй–Виконуй–Перевірй–Дій» (англ. *Plan–Do–Check–Act*)

MFA – багатофакторна автентифікація (англ. *Multi-Factor Authentication*)

PAM – управління привілейованими обліковими записами (англ. *Privileged Access Management*)

VPN – віртуальна приватна мережа (англ. *Virtual Private Network*)

TLS – протокол захисту транспортного рівня (англ. *Transport Layer Security*)

IPS – система запобігання вторгненням (англ. *Intrusion Prevention System*)

EDR – засіб виявлення та реагування на інциденти на кінцевих пристроях (англ. *Endpoint Detection and Response*)

IoC – індикатор компрометації (англ. *Indicator of Compromise*)

SOC – центр моніторингу кібербезпеки (англ. *Security Operations Center*)

AD – служба каталогів Active Directory

LDAP – протокол доступу до служби каталогів (англ. *Lightweight Directory Access Protocol*)

IRP – план реагування на інциденти (англ. *Incident Response Plan*)

CSIRP – план реагування на інциденти комп'ютерної безпеки (англ. *Computer Security Incident Response Plan*)

BCP – план забезпечення безперервності діяльності (англ. *Business Continuity Plan*)

DRP – план аварійного відновлення (англ. *Disaster Recovery Plan*)

RTO – цільовий час відновлення (англ. *Recovery Time Objective*)

RPO – цільова точка відновлення (англ. *Recovery Point Objective*)

CERT – команда реагування на комп'ютерні інциденти (англ. *Computer Emergency Response Team*)

GV – домен управління (англ. *Govern*)

ID – домен ідентифікації (англ. *Identify*)

PR – домен захисту (англ. *Protect*)

DE – домен виявлення (англ. *Detect*)

RS – домен реагування (англ. *Respond*)

RC – домен відновлення (англ. *Recover*)

ВСТУП

Актуальність роботи:

Інформаційні технології стали фундаментом функціонування абсолютної більшості компаній, установ та організацій світу. З цієї причини питання інформаційної безпеки є як ніколи актуальним та потребує особливої уваги. ЗВО не є виключенням. Протягом тривалого часу цифровізація освітнього середовища в Україні відбувалася нерівномірно та часто супроводжувалася використанням застарілого програмного забезпечення, технічного обладнання й недостатнім рівнем захисту інформаційних систем. У багатьох випадках впровадження цифрових сервісів здійснювалося без комплексного підходу до забезпечення кібербезпеки, що створило значну кількість потенційних вразливостей у внутрішній інформаційній інфраструктурі ЗВО.

Після 2020 року більшість освітніх закладів здійснили стрімкий перехід до дистанційного навчання, хмарних сервісів, електронного документообігу та онлайн-платформ для організації освітнього процесу. Така трансформація дозволила забезпечити безперервність навчання, однак водночас суттєво розширила поверхню потенційних кібератак. Значна кількість сервісів, користувачів та інтегрованих інформаційних систем створила складне цифрове середовище, у межах якого традиційні підходи до захисту інформації часто виявляються недостатньо ефективними. Особливо вразливими залишаються системи контролю доступу, механізми захисту персональних даних студентів та працівників, а також засоби моніторингу й реагування на кіберінциденти. Додатковим фактором ризику є низький рівень кібергігієни користувачів, що створює сприятливі умови для реалізації атак соціальної інженерії, фішингу та компрометації облікових записів.

На відміну від комерційних організацій, ЗВО поєднують у собі відкритість інформаційного середовища, велику кількість користувачів із різним рівнем доступу та обмежені ресурси для впровадження комплексних засобів захисту. Це створює складну модель кіберзахисту, у межах якої традиційні механізми оцінювання ризиків та захищеності не завжди дозволяють об'єктивно визначити реальний рівень зрілості системи інформаційної безпеки. Крім того, постійне зростання кількості кібератак на освітній сектор, зокрема атак із використанням соціальної інженерії, шкідливого програмного забезпечення та компрометації облікових даних, підсилює потребу у впровадженні структурованих підходів до оцінювання кіберзахищеності ЗВО.

Актуальність роботи полягає в тому, що більшість освітніх організацій не мають єдиної методології оцінки поточного стану захищеності інформаційної інфраструктури. Як наслідок, в умовах обмежених ресурсів та нестачі кадрів у функції інформаційної безпеки ЗВО, проблема пріоритизації розвитку процесів ІБ постає гостро. Наведені проблеми призводять до необхідності розробки підходу до оцінки стану захищеності, що враховував би особливості інформаційної інфраструктури ЗВО, ландшафту загроз та обмеження у ресурсах для розвитку функції ІБ.

Метою роботи є розробка підходу для оцінки поточного стану кіберзахисту університету та визначення пріоритетності напрямів розвитку функції ІБ.

Об'єктом дослідження є інформаційна інфраструктура університету.

Предметом дослідження є підхід до оцінки стану кіберзахисту.

Методом дослідження є опрацювання літературних джерел за вибраною темою, дослідження існуючих методів оцінки стану кіберзахисту ЗВО та розробка фреймворку оцінки стану кіберзахисту.

Практичне значення отриманих результатів полягає у можливості використання розробленого підходу для оцінки стану кіберзахисту навчального закладу.

1 ЛАНДШАФТ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОСВІТНЬОГО СЕКТОРУ

1.1 Особливості інформаційної інфраструктури закладів вищої освіти

Сучасні заклади вищої освіти є складними інформаційно-телекомунікаційними середовищами, які поєднують велику кількість програмних, апаратних та мережевих компонентів, необхідних для забезпечення освітньої, наукової, адміністративної та комунікаційної діяльності. На відміну від більшості корпоративних організацій, інфраструктура ЗВО орієнтована не лише на підтримку внутрішніх бізнес-процесів, але й на забезпечення відкритого доступу до інформаційних ресурсів для великої кількості користувачів із різним рівнем технічної підготовки та різними правами доступу. Така специфіка формує особливий ландшафт кіберризиків, який суттєво відрізняється від традиційних корпоративних мереж.

Кампусові мережі університетів зазвичай охоплюють десятки навчальних корпусів, гуртожитків, адміністративних будівель, бібліотек, дослідницьких лабораторій, спортивних та медичних об'єктів, які об'єднуються в єдину інформаційну систему. У сучасних умовах інформаційна інфраструктура ЗВО забезпечує функціонування систем дистанційного навчання, електронного документообігу, корпоративної пошти, наукових обчислювальних ресурсів, систем контролю доступу, відеоспостереження, хмарних сервісів та багатьох інших інформаційних платформ. Водночас така інфраструктура повинна підтримувати, у випадку нашого університету, одночасну роботу десятків тисяч користувачів та значної

кількості пристроїв, що створює суттєве навантаження як на мережеву, так і на серверну інфраструктуру.

Для аналізу особливостей побудови інформаційної інфраструктури ЗВО в даній роботі за основу взято схему телекомунікаційної мережі Національного технічного університету України «КПІ ім. Ігоря Сікорського», яка є одним із найбільших прикладів кампусової мережі закладу вищої освіти в Україні [1]. Мережа охоплює десятки навчальних корпусів та гуртожитків, об'єднаних високошвидкісними магістральними каналами передачі даних.

Оригінальна схема мережі містить велику кількість окремих вузлів, комутаторів, каналів зв'язку та допоміжних елементів, однак для цілей даного дослідження така деталізація є надмірною. У межах роботи було побудовано спрощену модель мережевої інфраструктури ЗВО, яка дозволяє виділити ключові структурні компоненти інформаційної системи університету без надлишкової технічної деталізації.

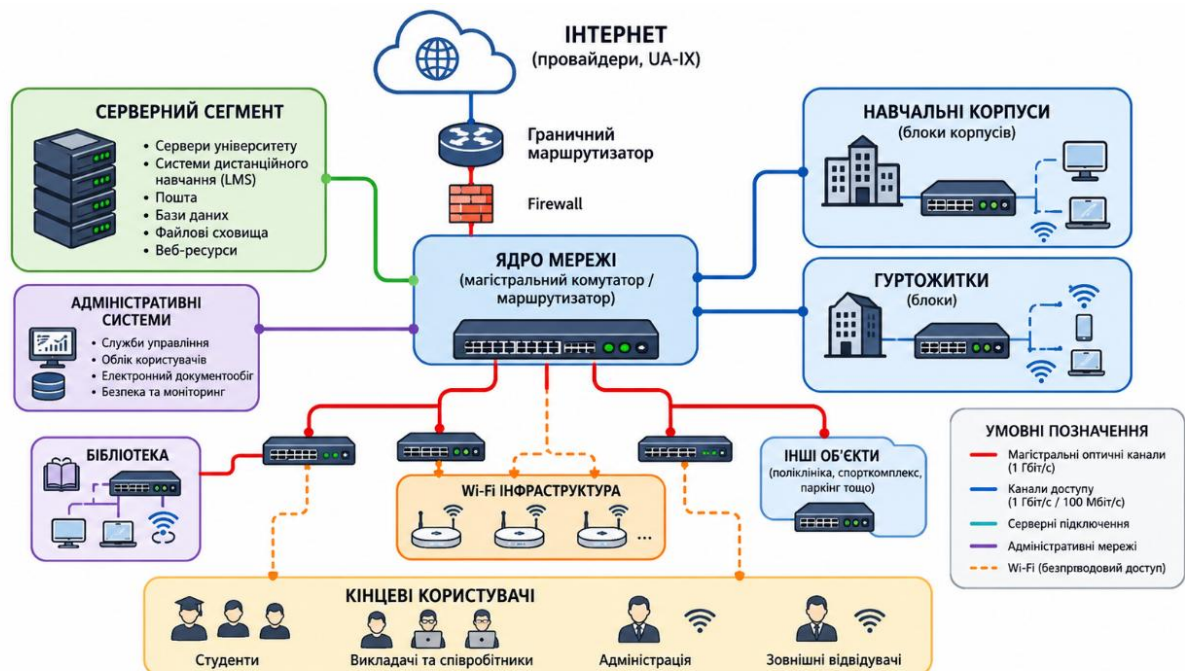


Рисунок 1.1 – Спрощена схема мережі університету

Наведена мережа зазвичай розділяється на ієрархію сегментів із різним режимом доступу до чутливої інформації університету. Таким чином, гостьові

мережі взагалі не мають доступу до такого роду інформації, а ректорат має найбільш повний рівень доступу відносно усього університету.

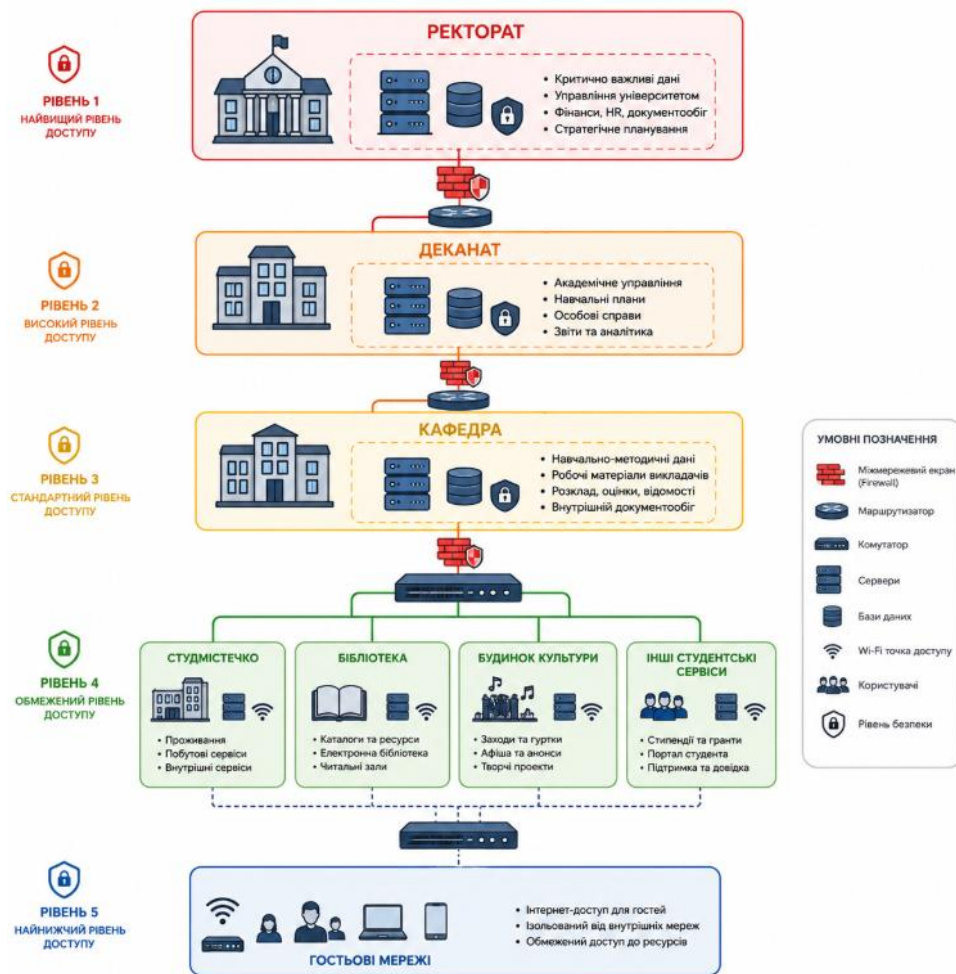


Рисунок 1.2 – Ієрархія сегментів університетської мережі

Спрощена схема інформаційної інфраструктури університету включає декілька основних компонентів: ядро мережі, серверний сегмент, навчальні корпуси, гуртожитки, бездротову інфраструктуру та зовнішні канали доступу до мережі Інтернет. Такий підхід відповідає класичній багаторівневій архітектурі кампусових мереж, яка широко використовується у сучасних закладах вищої освіти.

Центральним елементом архітектури є ядро мережі (core layer), яке забезпечує маршрутизацію та розподіл трафіку між усіма сегментами університетської інфраструктури. До нього підключаються серверні ресурси, локальні мережі корпусів, гуртожитків та інші інформаційні сервіси.

Використання централізованого ядра дозволяє забезпечити високу пропускну спроможність мережі та централізоване адміністрування ресурсів. Важливим компонентом інфраструктури є серверний сегмент, у якому розміщуються системи дистанційного навчання, корпоративна пошта, бази даних, файлові сховища та вебресурси університету. У великих ЗВО також можуть використовуватись спеціалізовані обчислювальні ресурси для наукових досліджень. Окрему роль відіграють локальні мережі навчальних корпусів та гуртожитків, які забезпечують доступ користувачів до централізованих ресурсів та мережі Інтернет. При цьому саме сегменти гуртожитків є одними з найбільш складних із точки зору інформаційної безпеки через велику кількість користувацьких пристроїв та низький рівень централізованого контролю.

Суттєвою особливістю сучасних ЗВО є використання технології BYOD (Bring Your Own Device), відповідно до якої користувачі підключають до мережі власні ноутбуки, смартфони та інші пристрої. Це значно ускладнює контроль мережевого середовища та підвищує ризики поширення шкідливого програмного забезпечення й компрометації облікових записів. Зокрема, дослідження університетів Великої Британії засвідчило, що частка університетів, які здійснюють сегрегацію Wi-Fi мереж для студентів і персоналу окремо від гостьових мереж, скоротилась із 92% у 2022 році до 77% у 2023 році [2]. Водночас тільки 16% університетів підтримують повний і точний реєстр активів мережі, що робить контроль підключених пристроїв вкрай ускладненим [2].

Важливою особливістю сучасних кампусів є масштабне впровадження пристроїв Інтернету речей (IoT). Розумні аудиторії, системи контролю доступу, камери відеоспостереження, сенсори навколишнього середовища та підключені системи управління інфраструктурою значно розширюють периметр мережі університету. За даними IoT Analytics, кількість активних глобальних IoT-підключень зросла на 18% у 2022 році та досягла 14,3 мільярда

одиниць [3]. При цьому IoT-пристрої на кампусах часто мають слабкі механізми аутентифікації, рідко оновлюються та не мають стандартизованих протоколів захисту, що перетворює їх на потенційні точки входу для зломисників. Скомпрометовані IoT-пристрої можуть використовуватись для розширення атак на критичну інфраструктуру університету або для організації DDoS-атак.

Ще однією особливістю інформаційної інфраструктури ЗВО є інтеграція з глобальними мережами та зовнішніми сервісами. Університети активно використовують хмарні платформи, міжнародні наукові ресурси та сервіси відеоконференцій. Для цього великі ЗВО часто мають власні канали зв'язку та публічні IP-адреси, що фактично робить університет окремим великим мережевим оператором. При цьому залежність від сторонніх постачальників програмного забезпечення та хмарних сервісів формує додатковий вектор ризику: за даними звіту Verizon DBIR 2024, у 15% порушень безпеки було задіяно третіх сторін, включаючи вразливості стороннього програмного забезпечення та інші проблеми ланцюжка поставок, що на 68% більше порівняно з попереднім роком [4].

1.2 Основні вразливості та вектори кібератак на інфраструктуру ЗВО

1.2.1 Типові вразливості мережі університету

Через типово високий рівень складності мережевої інфраструктури університету, що включає велику кількість користувачів, складні взаємозв'язки між кампусними інформаційними системами та численну кількість сегментів мережі, що потребують різний рівень доступу, управління вразливостями такої мережі постає складною задачею. Згідно з дослідженням компанії Heimdal, авторитетного данського постачальника систем кіберзахисту, до основних вразливостей мережевої інфраструктури, які

притаманні і ЗВО також, відносяться використання застарілого або невчасно оновленого програмного забезпечення, слабка сегментація мережі, помилки конфігурації мережевого обладнання, недостатньо захищені Wi-Fi мережі, використання однофакторної автентифікації, слабкі паролі, а також незахищені користувацькі та IoT-пристрої [5].

Ці вразливості є характерними і для типової інфраструктури закладів вищої освіти. Через загальну культуру відкритості та високий рівень доступності інформаційних ресурсів університети активно використовують політику BYOD під час надання студентам і працівникам доступу до внутрішніх сервісів. Водночас користувацькі пристрої зазвичай не контролюються на належному рівні з боку адміністрації. Освітні заклади, як правило, не висувають чітких вимог щодо захисту особистих пристроїв, хоча саме вони часто є основною точкою входу до мережі університету. У разі втрати такого пристрою або його компрометації, за відсутності належних внутрішніх механізмів захисту, під загрозою опиняється вся інформаційна інфраструктура ЗВО.

Важливою системною вразливістю ЗВО є також недостатній рівень управління активами. Дослідження, проведене на основі аналізу даних британських університетів, засвідчило, що лише 16% закладів підтримують повний та точний реєстр своїх активів [6]. Це суттєво ускладнює виявлення несанкціонованих пристроїв у мережі, оцінку актуального стану захищеності та своєчасне усунення вразливостей. Без повного розуміння того, які пристрої підключені до мережі, неможливо ефективно керувати поверхнею атаки.

Дослідження структури атак у секторі освіти за даними Sophos «The State of Ransomware in Education 2024» показало, що в 2024 році найпоширенішою першопричиною успішних атак стала експлуатація вразливостей програмного забезпечення — 42% випадків. Компрометація облікових даних спостерігалась у 23% атак, тоді як шкідливі електронні листи та фішинг склали 21% та 11% відповідно [7]. Таким чином, несвоєчасне

оновлення програмного забезпечення та слабка пароліна гігієна залишаються основними вразливостями, якими користуються зловмисники під час атак на ЗВО.

Окрему увагу слід приділити вразливостям, пов'язаним безпосередньо з користувачами мережевої інфраструктури університету. Рівень кібергігієни студентів та працівників ЗВО часто залишається недостатнім, що суттєво підвищує ризик реалізації атак із використанням людського фактора. Користувачі можуть встановлювати неавторизоване програмне забезпечення, переходити за підозрілими посиланнями, використовувати ненадійні зовнішні сервіси або передавати облікові дані стороннім ресурсам, створюючи потенційні точки компрометації інформаційної інфраструктури. Незважаючи на те, що в багатьох закладах вищої освіти проводяться навчальні заходи та тренінги з підвищення обізнаності у сфері інформаційної безпеки, рівень практичних знань і реальної готовності користувачів до протидії кіберзагрозам у більшості випадків системно не оцінюється. У результаті навіть необережні дії окремих користувачів можуть створювати ризик компрометації окремих сегментів або всієї мережевої інфраструктури університету.

1.2.2 Основні вектори кібератак на освітній сектор

За даними DeepStrike, одного зі світових лідерів у сфері penetration testing та аналізу кіберзагроз, освітній сектор наразі є найбільш атакованою галуззю, випереджаючи навіть банківський сектор та державні установи [8]. На момент проведення дослідження у 2025 році заклади освіти в середньому зазнавали майже 4500 кібератак щотижня. За даними Check Point Software, ще у першому кварталі 2023 року середня кількість атак на один університет складала 2507 на тиждень — на 15% більше порівняно з аналогічним періодом 2022 року [9].

Подібні показники демонструють, що освітній сектор більше не розглядається зловмисниками як другорядна або менш цінна ціль. Навпаки,

сучасні університети стали повноцінними об'єктами систематичних кібератак, інтенсивність яких співставна або навіть перевищує рівень атак на критичну інфраструктуру та фінансові організації. При цьому атаки на ЗВО мають не поодинокий характер, а є постійним процесом, що включає автоматизоване сканування мереж, brute-force атаки, фішингові кампанії, спроби експлуатації відомих вразливостей та компрометацію облікових записів користувачів.

Про масштаб проблеми свідчить і звіт Verizon Data Breach Investigations Report (DBIR) 2024, у якому було проаналізовано 30 458 інцидентів безпеки у всьому світі. Відповідно до цього звіту, освітній сектор зафіксував 1780 інцидентів (17% від загальної кількості) та 1537 підтверджених витоків даних (14%), що вивело освіту до п'ятірки найбільш скомпрометованих галузей у світі [4]. Порівняно з попереднім роком кількість підтверджених витоків збільшилась на 258%, а обсяги розкритих даних зросли на 545% [10].

Згідно з результатами опитування [11], проведеного Департаментом науки, інновацій та технологій Великої Британії, близько 91% закладів вищої освіти країни повідомили про кібератаки або кіберінциденти протягом 2025 року. При цьому приблизно 40% університетів зазнали негативних наслідків у результаті успішної реалізації атак. Подібні показники є значно вищими, ніж середні значення для більшості інших секторів економіки.

Основними цілями кібератак на освітній сектор є інформаційні системи, що містять персональні, фінансові та академічні дані студентів і працівників, а також сервіси, критичні для забезпечення безперервності освітнього процесу [8]. До найбільш привабливих для зловмисників ресурсів належать student information systems (SIS), системи дистанційного навчання, корпоративна електронна пошта, сервери зберігання даних, а також сторонні хмарні сервіси та програмні платформи, які використовуються університетами. Основною причиною зацікавленості атакуючих є велика концентрація чутливої інформації: персональних даних студентів та працівників, номерів соціального

страхування, медичної інформації, фінансових даних, інформації про академічну успішність, а також результатів наукових досліджень [8].

Згідно з результатами опитування керівництва британських закладів вищої освіти [11], найбільш поширеним способом реалізації кібератак на університети залишався фішинг — його зазначили 97% респондентів, чий установи зазнали кіберінцидентів. Другим за поширеністю типом атак стали impersonation attacks (атаки уособлення), які передбачають видавання зловмисника за довірену особу або організацію з метою отримання доступу до інформаційних ресурсів чи облікових даних; про такі інциденти повідомили 68% опитаних. Крім того, 42% респондентів зазначили випадки зараження інформаційних систем різними видами шкідливого програмного забезпечення, а 36% — атаки типу denial-of-service, спрямовані на порушення доступності цифрових сервісів університету. Також частина закладів повідомила про випадки неавторизованого доступу до внутрішніх систем та ресурсів університету, що було відзначено 14% опитаних [11].

Як видно із представленої статистики, найбільш популярним способом реалізації кібератаки є фішинг. Це пояснюється простотою створення подібних кампаній, їх легким масштабуванням та високою ефективністю. З урахуванням можливостей штучного інтелекту, що стрімко розвивається, такі атаки тепер можуть стати більш персоналізованими під конкретного користувача та його досвід, що робить фішинг тільки небезпечнішим [12]. Дослідники зафіксували зростання кількості фішингових листів на 1265% після масового поширення генеративних ШІ-інструментів [13].

Значну загрозу для ЗВО становлять також атаки з використанням програм-вимагачів (ransomware). За даними Malwarebytes, 2023 рік став найгіршим за кількістю зафіксованих ransomware-атак на освітній сектор: загальна кількість зросла на 105% — із 129 у 2022 році до 265 у 2023 році. У вищій освіті зростання склало 70% — з 68 до 116 атак [14]. Попри деяке зниження кількості зафіксованих атак у 2024 році (116 підтверджених

випадків у всьому світі), у першій половині 2025 року знову зафіксовано зростання на 23%, а середній розмір вимоги викупу в освітньому секторі склав 556 000 доларів США [15]. За даними Sophos, середня вартість відновлення після ransomware-атаки для університетів у 2024 році склала 4,02 млн доларів — майже вчетверо більше порівняно з 2023 роком [7].

Окремо слід виділити атаки на ланцюжок постачання програмного забезпечення, які можуть одночасно вразити велику кількість університетів. Прикладом такої атаки стало використання вразливості в ПЗ MOVEit Transfer у 2023 році. Угрупування C10p скористалось цією вразливістю для проникнення до систем сотень організацій, серед яких і ряд вищих навчальних закладів. Зокрема, Університет штату Колорадо зазнав витоку персональних даних близько 19 000 осіб [16, 17]. Атаки на ПЗ такого рівня є особливо небезпечними, оскільки не вимагають індивідуального проникнення до кожного університету та використовують довіру до стороннього постачальника.

Подібна ситуація повторилась у 2024 році з системою PowerSchool — платформою управління даними учнів, якою користуються понад 60 мільйонів студентів та 10 мільйонів вчителів. Зловмисник, використавши скомпрометовані облікові дані субпідрядника технічної підтримки, отримав доступ до бази даних платформи та виплатив 2,85 млн доларів у вигляді викупу [18]. Цей випадок наочно демонструє, наскільки критичним є ризик третіх сторін для університетів, що використовують зовнішні освітні платформи.

Наочним прикладом масштабних наслідків атак на сторонні освітні платформи є інцидент травня 2026 року, коли хакерське угруповання ShinyHunters здійснило кібератаку на платформу управління навчанням Canvas, якою користуються близько 9 000 навчальних закладів у США, Канаді та Австралії. Внаслідок атаки університети були змушені переносити іспити, студенти втратили доступ до навчальних матеріалів, а зловмисники вимагали

викуп у біткоїнах, погрожуючи оприлюднити викрадені персональні дані студентів і викладачів [19].

Таким чином, кіберзагрози для закладів вищої освіти доцільно поділити на дві великі групи: зовнішні та внутрішні.

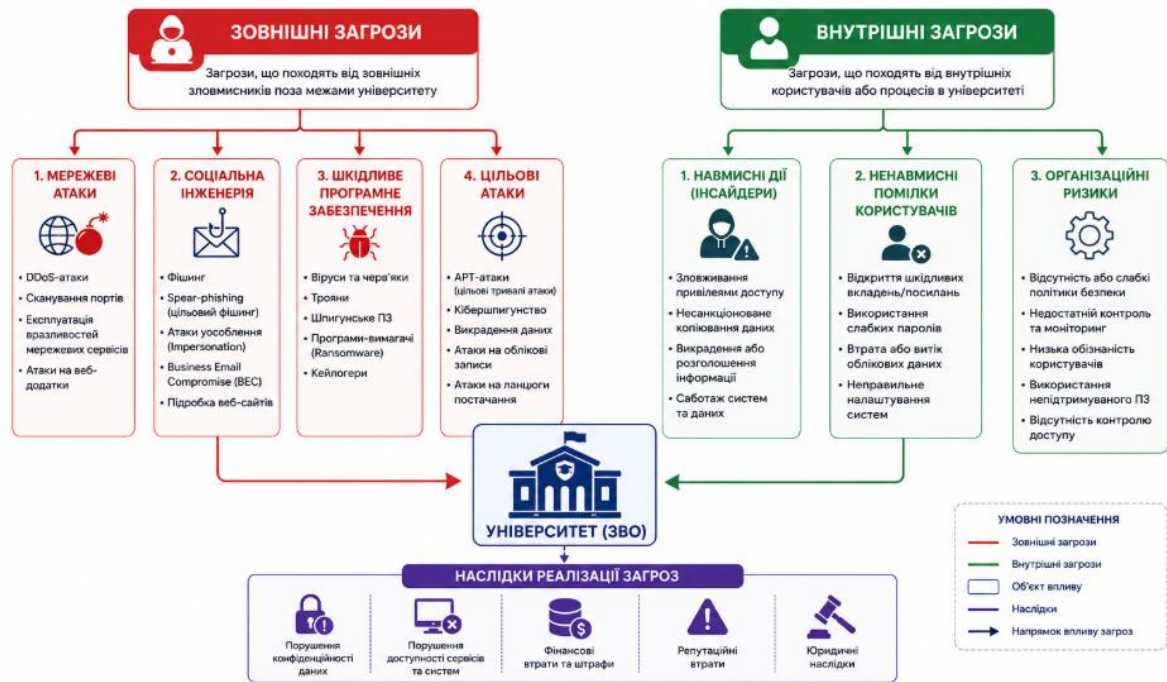


Рисунок 1.3 – Схема опису внутрішніх та зовнішніх загроз

До зовнішніх загроз належать атаки, що здійснюються особами або групами, які не мають легітимного доступу до інформаційної інфраструктури університету. До таких загроз можна віднести фішингові кампанії, програми-вимагачі, шкідливе програмне забезпечення, DDoS-атаки, експлуатацію вразливостей інформаційних систем та кібершпигунство.

Внутрішні загрози пов'язані з діяльністю легітимних користувачів університетської мережі — студентів, викладачів, адміністративного персоналу або підрядників. Такі загрози можуть бути як навмисними (інсайдерські атаки, зловживання привілеями доступу, викрадення інформації), так і ненавмисними, що виникають внаслідок помилок користувачів, низького рівня кібергігієни, використання слабких паролів, встановлення несанкціонованого програмного забезпечення або відкриття

шкідливих вкладень. Саме поєднання зовнішніх атак із внутрішніми слабкими місцями користувачів найчастіше призводить до успішної компрометації інформаційної інфраструктури ЗВО.

1.3 Проблеми забезпечення інформаційної безпеки ЗВО

Сучасні ЗВО функціонують в умовах постійного впливу як технічних, так і організаційних кіберзагроз. У зв'язку з цим доцільним є аналіз поточного стану інформаційної безпеки закладів вищої освіти та основних проблем, з якими вони стикаються під час побудови системи управління інформаційною безпекою.

У дослідженні MJBAS від 2021 – середземноморського журналу фундаментальних і прикладних наук, - було проведено оцінювання рівня відповідності систем управління інформаційною безпекою закладів вищої освіти вимогам стандарту ISO/IEC 27001 [20]. Для проведення оцінювання використовувався стандартизований опитувальник ISO27001 assessment questionnaire, а респондентами виступали директори Management Information System (MIS) підрозділів закладів вищої освіти. Основною метою дослідження було визначення рівня готовності ЗВО до впровадження повноцінної Системи управління інформаційною безпекою (СУІБ) та виявлення найбільш проблемних компонентів інформаційної безпеки університетського середовища.

Результати дослідження показали, що більшість університетів загалом усвідомлюють важливість інформаційної безпеки та мають базові елементи управління кіберзахистом. Зокрема, 100% досліджуваних закладів підтвердили наявність визначеної сфери застосування СУІБ, підтримки з боку керівництва, визначення ролей та відповідальностей, а також врахування ризиків та можливостей під час впровадження систем інформаційної безпеки [20]. Водночас ЗВО, де проводилися дослідження, продемонстрували суттєві

проблеми у практичній реалізації процесів управління інформаційною безпекою.

Однією з найбільш проблемних сфер виявилася відсутність повноцінного risk treatment process. Згідно з результатами опитування [20], жоден із досліджуваних ЗВО не продемонстрував повної відповідності вимогам Information Security Risk Treatment, а також Monitoring, Measurement and Evaluation, Internal Audit, Management Review та Corrective Action and Continual Improvement доменів ISO27001 [21]. Це свідчить про те, що в багатьох університетах інформаційна безпека існує переважно на рівні декларативних політик або окремих технічних заходів, однак відсутній системний процес безперервного моніторингу, аудиту та вдосконалення СУІБ. Фактично значна частина закладів не реалізує повноцінний PDCA-підхід (Plan-Do-Check-Act), який лежить в основі ISO/IEC 27001 [21].

Окрему проблему становить недостатній рівень operational planning and control. Лише 20% опитаних закладів підтвердили наявність повноцінного операційного планування та контролю процесів інформаційної безпеки [20]. Подібний результат свідчить про відсутність централізованого підходу до управління змінами, контролю конфігурацій, реагування на інциденти та документування процедур безпеки. У контексті університетської інфраструктури це створює значні ризики, оскільки навіть незначні зміни в конфігурації систем або мережі можуть призводити до появи нових вразливостей та порушення безпеки критичних сервісів.

Також суттєві проблеми були виявлені у сфері awareness and communication та ISMS resources and competence [20]. Результати опитування демонструють, що значна частина університетів не має достатнього кадрового та ресурсного забезпечення для підтримки системи управління інформаційною безпекою. Це може бути пов'язано як із недостатнім фінансуванням освітнього сектору, так і з дефіцитом кваліфікованих фахівців у сфері кібербезпеки. Крім того, у багатьох ЗВО питання інформаційної

безпеки досі розглядається переважно як технічна задача ІТ-відділу, а не як окремий управлінський процес на рівні всієї організації. У результаті навчання користувачів, оцінювання рівня їхньої обізнаності та формування культури кібербезпеки часто здійснюються нерегулярно або формально.

Дослідження також показало недостатній рівень документування процесів інформаційної безпеки. Лише 70% закладів підтвердили відповідність вимогам щодо документації інформації [20]. Відсутність актуальної документації, процедур реагування на інциденти, регламентів резервного копіювання та політик доступу суттєво ускладнює централізоване управління безпекою інформаційної інфраструктури. Особливо критично це для великих університетів із розподіленою мережею, де різні факультети або підрозділи можуть використовувати власні інформаційні системи без єдиних підходів до забезпечення безпеки.

Однак найбільш проблемним компонентом системи інформаційної безпеки досліджуваних ЗВО виявилася саме недостатня зрілість процесів контролю та оцінювання ефективності функціонування СУІБ. Жоден із університетів, що брали участь у дослідженні, не мав повноцінно реалізованих механізмів *monitoring, measurement and evaluation*, а також процесів *corrective action and continual improvement* [20]. Фактично заклади не здійснювали системного контролю за результативністю функціонування власної системи управління інформаційною безпекою та не мали організованого підходу до її постійного вдосконалення. У випадках, коли окремі заходи кіберзахисту все ж модернізувалися, такі зміни здебільшого мали несистемний характер і не базувалися на формалізованому аналізі ризиків або оцінюванні реального стану захищеності інфраструктури. Унаслідок цього ресурси часто розподілялися неефективно та не спрямовувалися на найбільш критичні або вразливі компоненти інформаційної системи університету. Таким чином, у значної частини ЗВО інформаційна безпека досі має переважно реактивний характер: заходи захисту впроваджуються вже після виникнення інцидентів

або появи суттєвих проблем, а не на основі безперервного моніторингу, аналізу ризиків та проактивного управління кіберзагрозами.

1.4 Мотивація для розробки спеціалізованого підходу до оцінки інформаційної безпеки ЗВО

Проведений аналіз особливостей інформаційної інфраструктури закладів вищої освіти, типових вразливостей університетських мереж та основних векторів кібератак на освітній сектор демонструє, що сучасні ЗВО функціонують у середовищі постійного впливу значної кількості кіберзагроз. Відкритість мережевої інфраструктури, використання BYOD-політики, велика кількість користувачів із різним рівнем доступу, інтеграція із зовнішніми сервісами та складна структура інформаційних систем формують специфічний ландшафт ризиків, який суттєво відрізняється від традиційних корпоративних інформаційних систем. При цьому статистика кібератак на освітній сектор свідчить про те, що університети вже давно стали повноцінними цілями систематичних атак з боку кіберзлочинців.

Водночас результати досліджень стану інформаційної безпеки ЗВО демонструють, що більшість університетів, навіть усвідомлюючи важливість кіберзахисту, стикаються із суттєвими труднощами під час побудови ефективної системи управління інформаційною безпекою. Особливо критичною проблемою виявилася відсутність системного контролю за ефективністю функціонування СУІБ, механізмів постійного моніторингу, аудиту та вдосконалення заходів захисту. У багатьох випадках інформаційна безпека реалізується фрагментарно та реактивно, а ресурси спрямовуються на усунення вже наявних інцидентів, а не на проактивне управління ризиками. Це створює ситуацію, у якій університет фактично не має можливості об'єктивно оцінити власний рівень захищеності та визначити найбільш критичні проблеми інформаційної безпеки.

Однак сама по собі наявність окремих стандартів та фреймворків інформаційної безпеки не вирішує даної проблеми. Міжнародні стандарти, такі як ISO/IEC 27001 [21] або NIST Cybersecurity Framework [22], пропонують загальні підходи до побудови систем управління інформаційною безпекою, проте не враховують повною мірою специфіку освітнього середовища. На відміну від комерційних організацій, заклади вищої освіти змушені одночасно підтримувати високий рівень відкритості інформаційних ресурсів, забезпечувати доступ великої кількості користувачів та працювати в умовах обмеженого фінансування і дефіциту спеціалізованих кадрів у сфері кібербезпеки. Крім того, типовою проблемою ЗВО є децентралізація інформаційної інфраструктури, коли окремі факультети, кафедри або підрозділи можуть використовувати власні інформаційні системи та сервіси без єдиного централізованого підходу до забезпечення безпеки.

У таких умовах особливо важливим стає не лише впровадження окремих засобів захисту, а й формування механізму об'єктивного оцінювання поточного стану інформаційної безпеки університету. Саме оцінювання дозволяє визначити найбільш критичні вразливості інфраструктури, оцінити зрілість процесів управління безпекою, встановити пріоритетність розподілу ресурсів та сформуванню основу для подальшого вдосконалення СУІБ. Без наявності структурованого підходу до оцінки кіберзахищеності університет фактично не здатний визначити, які компоненти його інформаційної системи потребують першочергового посилення та наскільки ефективними є вже впроваджені заходи захисту.

Таким чином, виникає необхідність у розробці спеціалізованого підходу до оцінювання рівня інформаційної безпеки ЗВО, який би враховував специфіку освітнього сектору, характерні для нього ризики, організаційні обмеження та типові проблеми побудови системи кіберзахисту. Такий підхід повинен дозволяти не лише формально оцінити відповідність окремим вимогам стандартів інформаційної безпеки, а й забезпечувати можливість

визначення реального рівня зрілості системи захисту університету та пріоритетних напрямів її подальшого розвитку.

Висновки до розділу 1

Виходячи з результатів проведеного аналізу, можна зробити такі висновки:

- Сучасні заклади вищої освіти є складними інформаційно-телекомунікаційними середовищами, що поєднують велику кількість користувачів, мережових сегментів, інформаційних систем та зовнішніх сервісів. Відкритість освітнього середовища та необхідність забезпечення доступності ресурсів формують специфічний ландшафт кіберризиків, який суттєво відрізняється від традиційних корпоративних мереж.
- Типова інфраструктура ЗВО характеризується наявністю низки поширених вразливостей, серед яких використання застарілого програмного забезпечення, недостатня сегментація мережі, слабкий контроль користувацьких пристроїв, помилки конфігурації мережевого обладнання та недостатній рівень кібергігієни користувачів. Особливу проблему створює використання політики BYOD, яка значно ускладнює централізований контроль мережевого середовища.
- Освітній сектор є однією з найбільш атакованих галузей сучасної цифрової інфраструктури. Основними цілями кібератак на ЗВО виступають системи дистанційного навчання, корпоративна пошта, student information systems, файлові сховища та інші сервіси, що містять персональні, фінансові та академічні дані студентів і працівників.
- Найбільш поширеними векторами кібератак на заклади вищої освіти є фішинг-кампанії, атаки соціальної інженерії, шкідливе програмне забезпечення, експлуатація вразливостей, атаки відмови в обслуговуванні та компрометація облікових записів користувачів. Значна частина таких атак

базується на експлуатації людського фактору та недостатнього рівня обізнаності користувачів у сфері кібербезпеки.

- Аналіз результатів досліджень стану інформаційної безпеки ЗВО показав, що більшість університетів мають базові елементи систем управління інформаційною безпекою, однак стикаються із суттєвими проблемами у практичній реалізації процесів СУІБ. Найбільш критичними проблемами виявилися відсутність системного моніторингу, внутрішнього аудиту, оцінювання ефективності заходів захисту та механізмів постійного вдосконалення системи інформаційної безпеки.
- У значної частини закладів вищої освіти інформаційна безпека досі має переважно реактивний характер. Заходи кіберзахисту часто впроваджуються після виникнення інцидентів або появи критичних проблем, а не на основі проактивного аналізу ризиків та постійного контролю стану захищеності інформаційної інфраструктури.
- Існуючі міжнародні стандарти та фреймворки інформаційної безпеки пропонують загальні підходи до побудови систем управління інформаційною безпекою, однак не враховують повною мірою специфіку освітнього середовища, відкритість університетських мереж, децентралізацію інфраструктури, використання BYOD-політики та обмежені ресурси ЗВО.
- В умовах обмеженого фінансування та значної кількості потенційних вразливостей особливо важливим стає формування механізму пріоритизації заходів кіберзахисту. Без структурованого підходу до оцінювання стану інформаційної безпеки університет фактично не здатний об'єктивно визначити найбільш критичні ризики, оцінити зрілість процесів кібербезпеки та ефективно розподіляти ресурси між компонентами інформаційної інфраструктури.
- Проведений аналіз підтверджує необхідність розробки спеціалізованого підходу до оцінювання рівня інформаційної безпеки закладів вищої освіти, який би враховував специфіку освітнього сектору, характерні для нього

кіберризиках, організаційні обмеження та дозволяв визначати пріоритетні напрями вдосконалення системи кіберзахисту ЗВО.

2 РОЗРОБКА ПІДХОДУ ДО ОЦІНЮВАННЯ РІВНЯ КІБЕРБЕЗПЕКИ ЗВО

2.1 Обґрунтування вибору опорних стандартів та структури оцінювання

2.1.1 Проблематика вибору опорного стандарту

Заклади вищої освіти функціонують в умовах постійного впливу значної кількості кіберзагроз, однак водночас мають суттєві організаційні та ресурсні обмеження у сфері кібербезпеки. Для більшості ЗВО характерними є недостатній рівень фінансування систем кіберзахисту, дефіцит кваліфікованих фахівців з інформаційної безпеки, використання застарілого програмного забезпечення, низький рівень кібергігієни користувачів та складність централізованого контролю мережевої інфраструктури через використання політики використання особистих пристроїв та децентралізованих інформаційних систем. При цьому освітній сектор залишається однією з найбільш атакованих галузей, а основними векторами атак є фішинг, компрометація облікових записів, експлуатація вразливостей та шкідливе програмне забезпечення. У таких умовах основною задачею системи оцінювання кібербезпеки стає не лише формальна перевірка відповідності окремим вимогам безпеки, а й визначення найбільш критичних вразливостей, оцінювання зрілості процесів кіберзахисту та формування пріоритетів для ефективного розподілу обмежених ресурсів ЗВО.

Проведення оцінки стану кіберзахисту університету саме за визначеним стандартом або фреймворком пояснюється необхідністю систематизації процесу внутрішнього контролю ефективності функції інформаційної безпеки та потребою в єдності підходів між підрозділами, відповідальними за її підтримку. Таким чином, керівництво зможе бачити цілісну картину

поточного стану інформаційної безпеки ЗВО та визначати пріоритетні напрями її вдосконалення.

ISO/IEC 27001 [21] є одним із найбільш поширених стандартів у сфері інформаційної безпеки та добре підходить для формалізації процесів управління, управління ризиками, аудитів та побудови СУІБ. Однак у контексті закладів вищої освіти його використання у чистому вигляді має ряд суттєвих обмежень. Стандарт орієнтований переважно на побудову формалізованої системи управління інформаційною безпекою, що потребує значних організаційних ресурсів, стабільного фінансування та наявності кваліфікованих фахівців із кібербезпеки. Для багатьох ЗВО, які функціонують в умовах обмеженого бюджету та дефіциту спеціалістів, повноцінне впровадження всіх процесів СУІБ є складною задачею. Крім того, ISO/IEC 27001 недостатньо фокусується на специфічних проблемах освітнього середовища, зокрема низькому рівні кібергігієни користувачів, використанні політики використання особистих пристроїв, відкритості мережевої інфраструктури та необхідності постійного моніторингу великої кількості користувацьких пристроїв. Стандарт також не забезпечує достатньої деталізації оцінювання фактичного рівня технічної захищеності мережі та ефективності технічних і організаційних заходів захисту.

Водночас NIST CSF 2.0 [22] є значно більш придатним для оцінювання зрілості процесів кіберзахисту та кіберстійкості організації, оскільки фреймворк орієнтований на практичні аспекти управління кібербезпекою та дозволяє оцінювати здатність організації виявляти, реагувати та відновлюватися після кібератак. Це є особливо актуальним для ЗВО, які постійно перебувають під впливом фішингових кампаній, атак із використанням шкідливого програмного забезпечення та компрометації облікових записів користувачів. Однак NIST CSF 2.0 має менш формалізований характер та не забезпечує достатньої деталізації управлінських процесів, аудитів, управління документацією та механізмів

постійного вдосконалення, що ускладнює використання фреймворку як основи для побудови повноцінної СУІБ у великих університетських середовищах.

Важливо зазначити, що NIST CSF 2.0, оновлений у лютому 2024 року, отримав шосту функцію — «Govern» (Управління), яка значно розширила функціональність фреймворку в частині управлінської складової [23]. Ця функція охоплює питання кібербезпекової стратегії, організаційних ролей і відповідальностей, управління ризиками та відповідності вимогам, що робить NIST CSF 2.0 суттєво ближчим до ISO/IEC 27001 за своїм охопленням управлінських аспектів [23]. Водночас принципова відмінність між двома підходами зберігається: ISO/IEC 27001 визначає, що саме необхідно впровадити, тоді як NIST CSF допомагає організації обрати як це зробити, зосереджуючись на найбільш критичних заходах захисту. Для ЗВО з обмеженими ресурсами ця гнучкість NIST CSF є перевагою, однак одночасно може призводити до неповноти охоплення заходів, якщо організація не має достатнього досвіду у сфері кібербезпеки.

Результати систематичного огляду наукових публікацій щодо стратегій кіберзахисту ЗВО, проведеного у 2024 році [24], підтверджують, що жоден зі стандартів у чистому вигляді не є достатнім для закладів вищої освіти. Дослідники зазначають, що аналізовані стандарти не орієнтовані на специфіку ЗВО та потребують суттєвих адаптацій для практичного впровадження. При цьому більшість наукових праць не описують повноцінного процесу управління ризиками, а функції, які відповідають потребам ЗВО, включають насамперед ідентифікацію загроз, захист та виявлення інцидентів. Це свідчить про те, що потреба у спеціалізованому підході є визнаною проблемою не лише на практиці, а й у науковій спільноті.

Водночас практичні дослідження підтверджують, що для університетів, які перебувають на початковому або середньому рівні зрілості кіберзахисту, оптимальною стратегією може бути поетапний підхід: початкове

використання NIST CSF як практичної «дорожньої карти» для пріоритизації заходів захисту з подальшим переходом до більш формалізованих процесів управління. ISO/IEC 27001 краще підходить для організацій із вже усталеними процесами, готових до формального управління, тоді як NIST CSF — для тих, хто ще формує базові засади кіберзахисту. При цьому реалізація ISO/IEC 27001 займає від 6 до 18 місяців та потребує від 10 000 до 50 000 доларів США на консультації, тоді як NIST CSF є безкоштовним та може впроваджуватися поступово. Зважаючи на обмежені бюджети більшості університетів, цей фактор має суттєве практичне значення.

Слід також окремо зупинитися на проблемі недостатності будь-якого єдиного фреймворку з точки зору відповідності вимогам нормативно-правового регулювання. Оскільки вимоги відповідності часто вузько орієнтовані на конкретні сфери (наприклад, захист персональних даних або контроль доступу), університети можуть не помічати вразливостей за межами конкретного стандарту. Крім того, вимоги оновлюються рідко та не встигають за темпами розвитку нових кіберзагроз, внаслідок чого організація може формально відповідати стандарту, але залишатися вразливою до нових атак. Інвестиції в заходи, які не відповідають реальному профілю ризиків установи, призводять до неефективного витрачання ресурсів.

Таким чином, жоден із розглянутих стандартів або фреймворків не дозволяє одночасно врахувати низький рівень кібергігієни користувачів, дефіцит ресурсів, необхідність визначення пріоритетності заходів захисту, постійний вплив кібератак та потребу у системному контролі ефективності процесів кібербезпеки. Це зумовлює необхідність формування комбінованого підходу.

2.1.2 Розробка структури комбінованого фреймворку

За основу структури розроблюваного фреймворку оцінювання рівня кіберзахищеності закладів вищої освіти було обрано NIST Cybersecurity

Framework 2.0, оскільки він пропонує зрозумілу, логічно структуровану та процесно-орієнтовану модель управління кібербезпекою. Фреймворк базується на шести функціональних доменах — Govern, Identify, Protect, Detect, Respond та Recover — які охоплюють повний життєвий цикл управління кіберризиками організації та дозволяють комплексно оцінювати як організаційні, так і технічні аспекти кіберзахисту. Однією з ключових переваг NIST CSF є те, що його функції не є жорстко регламентованими етапами, а розглядаються як взаємопов'язані та постійно діючі процеси, що формують безперервну культуру операційної стійкості організації.

Додатковою перевагою NIST CSF 2.0 є деталізація кожного функціонального домену через систему категорій та підкатегорій, що дозволяє більш структуровано проводити оцінювання стану кібербезпеки.

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Cybersecurity Supply Chain Risk Management	GV.SC
	Roles, Responsibilities, and Authorities	GV.RR
	Policies, Processes, and Procedures	GV.PO
	Oversight	GV.OV
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

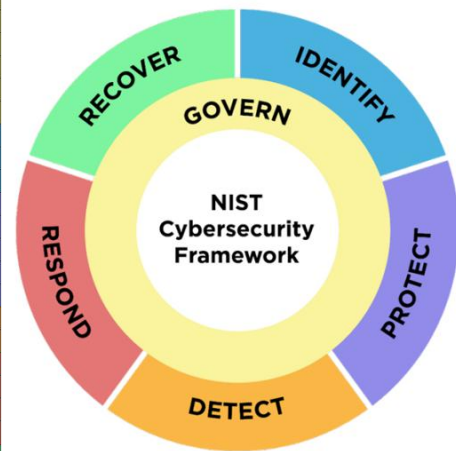


Рисунок 2.1 – Домени NIST CSF 2.0 та їхні категорії

Домен Identify орієнтований на формування розуміння інформаційного середовища організації та включає категорії, пов'язані з інвентаризацією активів, оцінюванням ризиків, управлінням залежностями від зовнішніх сервісів та визначенням критичних компонентів інфраструктури. Це дозволяє оцінювати рівень контролю над інформаційними ресурсами організації, розуміння потенційних ризиків та загальний рівень видимості інформаційного середовища.

Домен Protect фокусується на реалізації механізмів захисту та охоплює процеси контролю доступу, підвищення обізнаності користувачів, захисту даних, управління конфігураціями та використання технічних засобів кіберзахисту. У свою чергу домени Detect, Respond та Recover охоплюють процеси моніторингу, аналізу інцидентів, реагування та відновлення після кібератак, що є особливо важливим для сучасних ЗВО в умовах постійного зростання кількості кібератак на освітній сектор.

Домен Govern при цьому забезпечує стратегічний та управлінський рівень функціонування всієї системи кібербезпеки, формуючи основу для координації процесів управління ризиками, контролю ефективності заходів захисту та інтеграції кібербезпеки у загальну систему управління організацією.

Однак навіть після введення домену Govern фреймворк NIST CSF все ще залишається переважно операційно-орієнтованим підходом та у меншій мірі фокусується на формалізації СУІБ-процесів, аудитів, документації та механізмів постійного покращення, які є критично важливими саме для великих децентралізованих середовищ закладів вищої освіти.

Для більшості ЗВО характерними залишаються такі проблеми, як недостатній контроль ефективності процесів кібербезпеки, відсутність формалізованих процедур управління інформаційною безпекою, хаотичний розподіл ресурсів, низька зрілість управлінських процесів та недостатня регламентація відповідальностей між структурними підрозділами університету. У таких умовах використання лише NIST CSF 2.0 не дозволяє повною мірою оцінити зрілість системи управління інформаційною безпекою університету. Саме тому для деталізації управлінських категорій, механізмів управління ризиками, політик безпеки, аудитів та постійного покращення у межах даної роботи додатково використовуються положення ISO/IEC 27001, який значно краще формалізує організаційні аспекти побудови СУІБ. Таким чином, у межах роботи формується комбінований підхід, у якому NIST CSF

2.0 використовується як основний структурний каркас фреймворку оцінювання, а ISO/IEC 27001 — як джерело управлінських критеріїв оцінювання інформаційної безпеки ЗВО.

2.2 Формування критеріїв та показників оцінювання рівня кібербезпеки ЗВО

2.2.1 Розробка моделі критеріїв фреймворку

Таблиця 2.1 – Структура фреймворку

Домен NIST	Категорія NIST	Основний стандарт	Що саме використовується
Govern (GV)	Organizational Context (GV.OC)	ISO/IEC 27001	Context of organization, scope of ISMS
	Risk Management Strategy (GV.RM)	ISO/IEC 27001	Risk management methodology
	Cybersecurity Supply Chain Risk Management (GV.SC)	ISO/IEC 27001	Third-party and supplier security management
	Roles, Responsibilities, and Authorities (GV.RR)	ISO/IEC 27001	Roles and responsibilities
	Policies, Processes, and Procedures (GV.PO)	ISO/IEC 27001	Security policies and procedures
	Oversight (GV.OV)	ISO/IEC 27001	Internal audit, management review, continual improvement
Identify (ID)	Asset Management (ID.AM)	ISO/IEC 27001	Asset inventory and ownership
	Risk Assessment (ID.RA)	ISO/IEC 27001	Risk identification and evaluation
	Improvement (ID.IM)	ISO/IEC 27001	Improvement and corrective actions
Protect (PR)	Identity Management, Authentication, and Access Control (PR.AA)	ISO/IEC 27001	Access control, authentication management
	Awareness and Training (PR.AT)	ISO/IEC 27001	Security awareness and training
	Data Security (PR.DS)	ISO/IEC 27001	Data protection and information handling
	Platform Security (PR.PS)	ISO/IEC 27001	Secure configuration and system protection
	Technology Infrastructure Resilience (PR.IR)	ISO/IEC 27001	Infrastructure protection and resilience

Кінець таблиці 2.1

Detect (DE)	Continuous Monitoring (DE.CM)	NIST CSF	Security monitoring and detection processes
	Adverse Event Analysis (DE.AE)	NIST CSF	Event analysis and anomaly detection
Respond (RS)	Incident Management (RS.MA)	NIST CSF + ISO/IEC 27001	Incident management procedures
	Incident Analysis (RS.AN)	NIST CSF	Incident analysis
	Incident Response Reporting and Communication (RS.CO)	ISO/IEC 27001	Communication and reporting procedures
	Incident Mitigation (RS.MI)	NIST CSF	Mitigation and containment
Recover (RC)	Incident Recovery Plan Execution (RC.RP)	NIST CSF + ISO/IEC 27001	Recovery planning and restoration
	Incident Recovery Communication (RC.CO)	ISO/IEC 27001	Recovery communication procedures

Вибір ISO/IEC 27001 як основного джерела критеріїв для домену Govern зумовлений тим, що саме даний стандарт найбільш детально формалізує процеси побудови та підтримки СУІБ. Категорії Organizational Context, Risk Management Strategy, Roles and Responsibilities, Policies та Oversight безпосередньо пов'язані з управлінськими процесами, управлінням ризиками, аудитами та постійним покращенням, що є критично важливими для ЗВО. Як було показано у першому розділі, однією з головних проблем університетів є низька зрілість процесів управління інформаційною безпекою, відсутність централізованого контролю ефективності СУІБ та хаотичний розподіл ресурсів. У такому контексті ISO/IEC 27001 дозволяє оцінювати не лише наявність окремих заходів захисту, а й рівень організаційної зрілості системи кібербезпеки загалом.

Категорії домену Identify також значною мірою базуються на положеннях ISO/IEC 27001, оскільки стандарт приділяє суттєву увагу процесам управління активами, ідентифікації ризиків та оцінюванню критичності інформаційних ресурсів. Для ЗВО це особливо важливо через складність та децентралізованість інформаційної інфраструктури, велику кількість інформаційних систем і постійне використання BYOD-пристроїв та зовнішніх сервісів. Без належної інвентаризації активів та оцінювання ризиків

університет фактично не здатний визначити найбільш критичні компоненти мережі та пріоритетні напрями посилення кіберзахисту.

Для домену Protect також використовуються переважно положення ISO/IEC 27001, оскільки стандарт містить значну кількість controls, пов'язаних із управлінням доступом, захистом даних, навчанням користувачів та базовими технічними механізмами захисту інформаційної інфраструктури. У контексті ЗВО це особливо важливо через високий рівень залежності безпеки від людського фактора, низьку кібергігієну користувачів та активне використання особистих пристроїв для доступу до внутрішніх сервісів університету. Використання ISO/IEC 27001 у межах категорій Protect дозволяє оцінювати як технічний рівень захисту систем, так і рівень формалізації процесів контролю доступу та захисту інформації.

У свою чергу домени Detect, Respond та Recover значною мірою базуються саме на NIST CSF, оскільки даний фреймворк є більш процесно-орієнтовним у питаннях операційної безпеки та краще описує процеси моніторингу, виявлення кіберінцидентів, реагування на атаки та відновлення після них. Для сучасних ЗВО, які постійно перебувають під впливом phishing-кампаній, malware-атак та компрометації облікових записів, здатність своєчасно виявляти інциденти та мінімізувати їх наслідки є не менш важливою, ніж превентивний захист. Саме тому категорії Continuous Monitoring, Incident Analysis, Incident Mitigation та Recovery Planning базуються переважно на підходах NIST CSF. Водночас окремі категорії, пов'язані із процесами реагування, комунікацією та управлінням процедурами відновлення у частині управління та організації, додатково доповнюються положеннями ISO/IEC 27001 для забезпечення більш формалізованого підходу до управління інцидентами та постійного покращення.

2.2.2 Модель оцінки стану захищеності за розробленим фреймворком

Для оцінювання рівня кіберзахищеності ЗВО у межах розробленого фреймворку використовується модель оцінювання, побудована на основі підходів NIST CSF 2.0 [20]. Кожна вимога у межах фреймворку оцінюється за шкалою від 0 до 4, де значення відображає рівень зрілості відповідного процесу або механізму захисту — від його повної відсутності до повноцінної реалізації із постійним вдосконаленням.

Таблиця 2.2 – Шкала оцінювання фреймворку

Оцінка	Значення
0	Процес відсутній
1	Процес реалізований частково
2	Процес реалізований базово
3	Процес реалізований повністю
4	Процес реалізований та постійно вдосконалюється

Використання єдиної шкали оцінювання дозволяє уніфікувати оцінювання як організаційних, так і технічних критеріїв без необхідності використання складних механізмів нормалізації або окремих моделей оцінювання для різних типів вимог. Такий підхід також спрощує подальшу інтерпретацію результатів та дозволяє безпосередньо порівнювати рівень зрілості різних компонентів системи кібербезпеки університету.

На першому етапі оцінювання визначаються оцінки окремих вимог фреймворку. Експерт обирає значення від 0 (процес відсутній) до 4 (процес реалізований та постійно вдосконалюється) для кожного критерію визначеного домену, після чого обраховується загальна оцінка домену, що буде представлятися середньоарифметичним із усіх наданих оцінок по категорії:

$$S_k = \frac{\sum_{i=1}^n x_i}{n} \quad (2.1)$$

де:

S_k – загальна оцінка категорії

x_i – оцінка вимоги

n – кількість вимог у категорії

На другому етапі, коли всі категорії були оцінені, розраховується загальна оцінка всього домену за схожим принципом:

$$S_d = \frac{\sum_{i=1}^m S_k}{m} \quad (2.2)$$

де:

S_k – загальна оцінка категорії

x_i – оцінка вимоги

m – кількість категорій у домені

Описаний підхід дозволяє сформувати профіль кіберзахищеності ЗВО та визначити рівень зрілості окремих напрямів забезпечення інформаційної безпеки. Саме подібний підхід використовується в більшості сучасних моделей оцінювання, побудованих на основі NIST CSF або ISO/IEC 27001. Однак отримання оцінок окремих категорій та доменів саме по собі не вирішує одну з ключових проблем закладів вищої освіти — проблему пріоритизації заходів кіберзахисту. Як було показано у першому розділі, більшість університетів функціонують в умовах обмеженого фінансування, дефіциту кваліфікованих фахівців та значної кількості ризиків. У таких умовах практично неможливо забезпечити однаково високий рівень зрілості всіх компонентів системи інформаційної безпеки, а спроби рівномірного розподілу ресурсів часто призводять до їх неефективного використання.

Крім того, різні напрями кібербезпеки мають неоднаковий вплив на загальну кіберстійкість університету. Наприклад, недостатній рівень захисту облікових записів користувачів або механізмів контролю доступу може створювати значно більші ризики для ЗВО, ніж недосконалість окремих процедур відновлення після інцидентів. Таким чином, для формування практичних рекомендацій щодо вдосконалення системи кібербезпеки доцільно враховувати не лише поточний рівень зрілості окремих напрямів, а й

їх відносну важливість для забезпечення загальної кіберстійкості університету.

З цією метою у межах розробленого фреймворку пропонується використовувати систему вагових коефіцієнтів, яка дозволяє враховувати специфіку інформаційної інфраструктури ЗВО та пріоритетність окремих напрямів кіберзахисту.

Таблиця 2.3 – Вагові коефіцієнти пріоритизації доменів

Домен	Вага
Govern	0.15
Identify	0.15
Protect	0.25
Detect	0.20
Respond	0.15
Recover	0.10

На відміну від традиційного підходу, де всі напрями оцінюються як рівнозначні, використання вагових коефіцієнтів дозволяє адаптувати результати оцінювання до реальних умов функціонування університетів та спростити процес прийняття управлінських рішень щодо розподілу обмежених ресурсів на заходи кібербезпеки.

Визначення вагових коефіцієнтів доменів фреймворку базується на аналізі двох ключових чинників: відносного внеску кожного домену у запобігання кіберінцидентам та економічності інвестицій у відповідні напрями захисту. Відповідно до звіту IBM Cost of a Data Breach 2024, організації, що застосовували штучний інтелект та автоматизацію саме у превентивних заходах захисту (домен Protect), скорочували середні витрати від порушень на 2,22 млн доларів — найбільший показник економії серед усіх напрямів кіберзахисту [25]. Це підтверджує пріоритетність домену «Protect» та обґрунтовує присвоєння йому найвищого вагового коефіцієнта (0,25). Водночас той самий звіт зафіксував, що організації, які самостійно виявляли витоки власними засобами виявлення (домен Detect), витрачали в середньому майже на 1 млн доларів менше порівняно з тими, у яких факт витоку розкривав

сам зловмисник [25]. Це свідчить про те, що своєчасне виявлення інцидентів має суттєвий прямий вплив на обмеження їхніх наслідків, що обґрунтовує другу за величиною вагу домену «Detect» (0,20).

Домени «Govern», «Identify» та «Respond» отримали однакові вагові коефіцієнти (0,15), що відображає їх рівнозначну роль у формуванні системи управління кібербезпекою, забезпеченні видимості активів та оперативному реагуванні на інциденти. Зокрема, дослідження IBM показало, що організації з тестованими планами реагування на інциденти мали середню вартість порушення на рівні 3,26 млн доларів — на 38% нижче, ніж у тих, де такого плану не було (5,29 млн доларів) [25]. Найменший ваговий коефіцієнт домену «Recover» (0,10) пояснюється тим, що механізми відновлення набувають значення вже після успішної реалізації атаки, тоді як інвестиції у попередні домени дозволяють запобігти самому факту інциденту або суттєво обмежити його масштаб. Це узгоджується з висновком аналітиків CompuNet, які встановили, що кожен долар, вкладений у превентивні заходи, дозволяє заощадити в середньому три долари на витратах відновлення [26]. Таким чином, запропонована система вагових коефіцієнтів відображає не довільне рішення авторів, а обґрунтовану ієрархію пріоритетів, підкріплену даними провідних галузевих досліджень.

Тоді загальний коефіцієнт пріоритетності можна розрахувати за формулою:

$$P_d = w_d \cdot (4 - S_d) \quad (2.3)$$

де:

w_d — ваговий коефіцієнт пріоритизації

S_d — оцінка домену

Запропонована формула враховує не лише поточний рівень зрілості окремого домену, а й його важливість для забезпечення загальної кіберстійкості ЗВО. Величина $(4 - S_d)$ відображає так званий дефіцит зрілості

домену, тобто відстань між поточним станом та максимально можливим рівнем реалізації процесів кібербезпеки. Чим нижчою є оцінка домену, тим більшим буде значення даного показника i , відповідно, тим більше уваги потребує відповідний напрям. Водночас множення на ваговий коефіцієнт w_d дозволяє врахувати різний вплив окремих доменів на загальний рівень захищеності університету. Таким чином, високий пріоритет отримують насамперед ті напрями, які одночасно мають значний вплив на кіберстійкість ЗВО та характеризуються низьким рівнем зрілості. Отриманий коефіцієнт пріоритетності може використовуватися як основа для планування заходів з підвищення рівня інформаційної безпеки та визначення напрямів, на які доцільно спрямовувати ресурси в першу чергу.

2.3 Модель експертного оцінювання

Оскільки значна частина критеріїв розробленого фреймворку описує організаційні та процесні аспекти інформаційної безпеки, їх оцінювання не може бути повністю автоматизованим та потребує залучення фахівців із відповідною експертизою. З цією метою для оцінювання рівня кіберзахищеності ЗВО використовується метод експертного оцінювання. У межах дослідження було залучено п'ятьох експертів, які мають освітній ступінь не нижче магістра за спеціальністю, пов'язаною з кібербезпекою, та безпосередньо залучені до забезпечення інформаційної безпеки університету або мають практичний досвід роботи з відповідними процесами. Обмеження кількості експертів до п'яти осіб зумовлене часовими рамками проведення дослідження та необхідністю забезпечення детального опрацювання усіх критеріїв фреймворку кожним учасником експертної групи.

Кожен експерт незалежно від інших проводить оцінювання всіх вимог фреймворку відповідно до шкали зрілості, наведеної у таблиці 2.2. Оскільки результати оцінювання формуються на основі суб'єктивних суджень фахівців,

виникає необхідність перевірки ступеня узгодженості отриманих оцінок. Для цього використовується коефіцієнт кореляції Пірсона, який є одним із найбільш поширених статистичних показників для визначення сили та напрямку взаємозв'язку між двома наборами даних. У контексті даного дослідження коефіцієнт Пірсона [18] використовується для оцінювання ступеня подібності оцінок, виставлених різними експертами. Значення коефіцієнта може змінюватися в межах від -1 до 1, де значення, близькі до 1, свідчать про високий рівень узгодженості оцінок експертів, значення, близькі до 0, вказують на відсутність помітного зв'язку між оцінками, а від'ємні значення свідчать про протилежний характер оцінювання.

Для кожної пари експертів коефіцієнт кореляції обчислюється за формулою:

$$r = \frac{\sum_{i=1}^n (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^n (x_i - \bar{x})^2 \sum_{i=1}^n (y_i - \bar{y})^2}} \quad (2.4)$$

де:

r – коефіцієнт кореляції Пірсона;

x_i, y_i – оцінки, надані двома експертами;

n – кількість оцінених вимог;

$\bar{x}, \bar{y}$ – середні значення оцінок відповідних експертів.

Отримані значення коефіцієнтів кореляції використовуються для визначення ступеня узгодженості оцінок експертів. Для кожного експерта розраховується середнє значення його кореляції з іншими учасниками експертної групи. На основі цього показника визначається ваговий коефіцієнт експерта:

$$W_i = \frac{k_i}{\sum_{i=1}^m k_i} \quad (2.5)$$

де:

W_i – ваговий коефіцієнт експерта;

k_i – середнє значення коефіцієнта кореляції експерта з іншими експертами;

m – кількість експертів.

Після визначення вагових коефіцієнтів виконується розрахунок фінальної оцінки кожної вимоги фреймворку як зваженого середнього експертних оцінок:

$$X = \sum_{i=1}^m W_i x_i \quad (2.6)$$

де:

X – фінальна оцінка вимоги;

x_i – оцінка, виставлена i -м експертом;

W_i – ваговий коефіцієнт відповідного експерта.

Отримані значення надалі використовуються для розрахунку оцінок категорій, доменів та інтегрального показника кіберзахищеності ЗВО відповідно до моделі оцінювання, наведеної у підрозділі 2.2.2. Використання групового експертного оцінювання дозволяє зменшити вплив індивідуальної суб'єктивності окремих експертів та підвищити об'єктивність фінальних результатів оцінювання.

Висновки до розділу 2

Виходячи з результатів проведеного аналізу, можна зробити такі висновки:

- Проведений аналіз показав, що існуючі стандарти та фреймворки інформаційної безпеки не враховують повною мірою специфіку закладів вищої освіти та їхні характерні обмеження, пов'язані з фінансуванням, кадровими ресурсами та особливостями інформаційної інфраструктури.
- Як основу структури розроблюваного підходу було обрано NIST CSF 2.0 завдяки його логічній доменній структурі та орієнтації на оцінювання зрілості процесів кіберзахисту, а положення ISO/IEC 27001 використано для деталізації управлінських, організаційних та ризик-орієнтованих аспектів інформаційної безпеки.
- У результаті сформовано комбінований фреймворк оцінювання, який охоплює всі основні напрями забезпечення кібербезпеки ЗВО та дозволяє комплексно оцінювати як організаційні, так і технічні складові системи захисту.
- Розроблена модель оцінювання базується на шкалі зрілості від 0 до 4 балів та дозволяє визначати оцінки окремих вимог, категорій і доменів, формуючи профіль кіберзахищеності університету.
- На відміну від більшості існуючих підходів, запропонований фреймворк додатково враховує проблему пріоритизації заходів кіберзахисту через використання вагових коефіцієнтів доменів та показника пріоритетності, що дозволяє більш ефективно розподіляти обмежені ресурси ЗВО.
- Для підвищення об'єктивності оцінювання запропоновано модель групового експертного оцінювання з перевіркою узгодженості думок експертів за допомогою коефіцієнта кореляції Пірсона та подальшим формуванням підсумкових оцінок критеріїв фреймворку.
- Розроблений підхід створює основу для проведення практичної оцінки рівня кібербезпеки закладу вищої освіти та визначення пріоритетних напрямів підвищення його кіберстійкості.

3 ПРАКТИЧНЕ ЗАСТОСУВАННЯ РОЗРОБЛЕНОГО ПІДХОДУ

3.1 Формування опитувальника

Для проведення оцінювання рівня кіберзахищеності ЗВО в межах розробленого фреймворку було обрано форму опитувальника. Такий підхід дозволяє стандартизувати процес збору інформації щодо стану реалізації вимог інформаційної безпеки та забезпечити можливість його застосування в організаціях різного масштабу. Кожна вимога фреймворку трансформується в окреме питання або групу питань, на які респонденти надають відповіді відповідно до визначеної шкали зрілості. У результаті формується набір оцінок, що може бути безпосередньо використаний для подальших розрахунків рівня зрілості категорій, доменів та загального стану кібербезпеки університету. Крім того, використання опитувальника забезпечує відтворюваність результатів та спрощує проведення повторних оцінювань для відстеження динаміки розвитку системи інформаційної безпеки.

Таблиця 3.1 – Опитувальник

Категорія	Питання	Оцінка (0 – 4)
1. Govern		
GV.OC Organizational Context	Наскільки чітко визначено та задокументовано організаційний контекст у сфері ІБ (внутрішні та зовнішні фактори, зацікавлені сторони, межі та область застосування СУІБ)?	
GV.OC Organizational Context	Чи враховуються вимоги зацікавлених сторін (студенти, викладачі, регулятори, партнери) при визначенні пріоритетів інформаційної безпеки університету?	
GV.RM Risk Management Strategy	Чи існує затверджена методологія управління ризиками ІБ (ризик-апетит, критерії прийнятності ризику, методи оцінювання) та чи застосовується вона системно?	

Продовження таблиці 3.1

GV.SC Supply Chain Risk Management	Як організована оцінка ризиків ІБ при залученні сторонніх постачальників (хмарні сервіси, LMS, CRM, аутсорс IT)?	
GV.RR Roles, Responsibilities & Authorities	Наскільки чітко визначено та задокументовано ролі і відповідальності у сфері ІБ між підрозділами університету (ІТ-відділ, юридичний, деканати, адміністрація)?	
GV.PO Policies, Processes & Procedures	Чи розроблено та затверджено політику інформаційної безпеки університету, і наскільки вона реально доступна та відома всьому персоналу?	
GV.PO Policies, Processes & Procedures	Чи охоплює внутрішня процесна документація ключові специфічні аспекти середовища університету: BYOD, хмарні сервіси, класифікація даних, парольна політика, дистанційний доступ?	
GV.OV Oversight	Чи проводяться внутрішні перевірки СУІБ та аналіз з боку керівництва, і яка їхня регулярність та формалізованість?	
2. Identify		
ID.AM Asset Management	Чи ведеться актуальний централізований реєстр інформаційних активів (сервери, програмне забезпечення, бази даних, мережеве обладнання) з визначеними власниками та класифікацією критичності?	
ID.AM Asset Management	Як університет контролює підключення BYOD-пристроїв та особистих девайсів до корпоративної мережі?	
ID.RA Risk Assessment	Наскільки регулярно проводиться оцінка ризиків ІБ університету, і чи задокументовано результати у вигляді реєстру ризиків?	
ID.RA Risk Assessment	Чи враховуються специфічні ризики університетського середовища при оцінюванні: BYOD, дистанційне навчання, хмарні сервіси, висока плинність користувачів (студенти), низька кібергігієна?	
ID.IM Improvement	Чи існує формалізований процес впровадження коригувальних дій за результатами аудитів, інцидентів та оцінок ризиків, із відстеженням їхнього виконання?	
3. Protect		

Продовження таблиці 3.1

PR.AA Identity Management & Access Control	Чи застосовується багатофакторна автентифікація (MFA) для доступу до критичних систем університету (корпоративна пошта, LMS, адміністративні системи, VPN)?	
PR.AA Identity Management & Access Control	Як організовано управління привілейованим доступом (PAM) та своєчасне відкликання прав при звільненні, відрахуванні або зміні ролі?	
PR.AA Identity Management & Access Control	Чи проводяться регулярні перегляди прав доступу (access review) для виявлення надлишкових або невикористовуваних прав, особливо для студентів та тимчасового персоналу?	
PR.AT Awareness & Training	Як часто проводяться навчання з кібербезпеки для співробітників та викладачів, і чи перевіряється засвоєння матеріалу?	
PR.AT Awareness & Training	Як часто проводяться симульовані фішингові кампанії серед користувачів університету, і чи передбачено обов'язкове навчання для тих, хто піддався?	
PR.AT Awareness & Training	Чи охоплюють програми підвищення обізнаності студентів (не лише персонал), та чи адаптовані вони до специфіки університетського середовища (BYOD, хмарні сервіси, соціальна інженерія)?	
PR.DS Data Security	Чи класифіковано інформаційні активи за рівнем конфіденційності (персональні дані, наукові дані, фінансова інформація), і чи застосовуються відповідні заходи захисту для кожної категорії?	
PR.DS Data Security	Як організовано резервне копіювання критичних даних університету (бази даних студентів, наукові матеріали, фінансові дані), і чи регулярно перевіряється можливість їх відновлення?	
PR.DS Data Security	Чи забезпечено шифрування даних університету в стані спокою (бази даних, файлові сховища) та при передачі (TLS, VPN для дистанційного доступу)?	
PR.PS Platform Security	Як організовано управління вразливістю та своєчасне встановлення оновлень безпеки на серверах, мережевому обладнанні та робочих станціях університету?	
PR.PS Platform Security	Чи застосовуються стандарти безпечної конфігурації (hardening baselines) для серверів, мережевого обладнання та кінцевих пристроїв, і чи контролюється їх дотримання?	

Продовження таблиці 3.1

PR.PS Platform Security	Чи контролюється встановлення несанкціонованого програмного забезпечення на корпоративних пристроях університету (application whitelisting / software inventory)?	
PR.IR Technology Infrastructure Resilience	Чи реалізовано належну сегментацію мережі університету між критичними сегментами (адміністративний, навчальний, гуртожитки, серверний, гостьовий Wi-Fi)?	
PR.IR Technology Infrastructure Resilience	Чи захищено периметр університетської мережі (firewall, IPS, антиспам, фільтрація вебтрафіку) та чи регулярно переглядаються правила безпеки?	
4. Detect		
DE.CM Continuous Monitoring	Чи ведеться централізований збір та зберігання логів з ключових систем університету (сервери, мережеве обладнання, корпоративна пошта, VPN, AD/LDAP)?	
DE.CM Continuous Monitoring	Як організовано моніторинг мережевого трафіку для виявлення аномалій (сканування портів, незвичайні з'єднання, ознаки ексфільтрації даних, lateral movement)?	
DE.CM Continuous Monitoring	Чи відстежується стан кінцевих точок (endpoint) на предмет індикаторів компрометації (IoC), підозрілих процесів та несанкціонованих змін (EDR/антивірус)?	
DE.CM Continuous Monitoring	Чи моніторяться привілейовані облікові записи та дії адміністраторів (PAM logging, UAM) для виявлення зловживань чи компрометації?	
DE.AE Adverse Event Analysis	Чи існує формалізований процес аналізу та кореляції подій безпеки, і хто відповідає за цю функцію (виділений SOC, ІБ-спеціаліст, ІТ-відділ)?	
DE.AE Adverse Event Analysis	Чи використовуються дані про актуальні загрози (threat intelligence) для налаштування правил виявлення та пріоритизації подій, специфічних для освітнього сектору?	
5. Respond		
RS.MA Incident Management	Чи існує затверджений план реагування на кіберінциденти (IRP/CSIRP), і чи регулярно він тестується?	

Кінець таблиці 3.1

RS.MA Incident Management	Як організовано класифікацію та пріоритизацію інцидентів ІБ з урахуванням їхнього впливу на освітній процес і критичність систем?	
RS.AN Incident Analysis	Чи проводиться post-incident аналіз (root cause analysis, lessons learned) після значущих інцидентів, і чи впроваджуються його результати у практику?	
RS.CO Incident Response Reporting & Communication	Чи визначено процедури комунікації під час інциденту: внутрішнє повідомлення керівництва, зовнішнє повідомлення регуляторів та суб'єктів персональних даних відповідно до законодавства?	
RS.MI Incident Mitigation	Чи мають фахівці університету технічні інструменти та задокументовані повноваження для оперативної ізоляції скомпрометованих систем та стримування інциденту?	
6. Recover		
RC.RP Incident Recovery Plan Execution	Чи розроблено план відновлення після інцидентів (BCP/DRP) із визначеними RTO та RPO для критичних систем (LMS, корпоративна пошта, студентські бази даних)?	
RC.CO Incident Recovery Communication	Чи визначено процедури комунікації в процесі відновлення після інциденту: повідомлення студентів і персоналу про статус відновлення сервісів, взаємодія з постачальниками та CERT?	

Запропонований опитувальник може використовуватися як у межах внутрішнього, так і зовнішнього аудиту. У випадку зовнішнього аудиту оцінювання проводиться незалежними експертами або аудиторськими організаціями, що дозволяє отримати більш об'єктивну оцінку стану кібербезпеки та зменшити вплив внутрішньої упередженості. Водночас залучення зовнішніх аудиторів потребує додаткових фінансових та організаційних ресурсів, які часто є обмеженими для закладів вищої освіти. Як було показано в першому розділі, однією з характерних проблем більшості ЗВО є недостатній рівень внутрішнього контролю ефективності процесів інформаційної безпеки та відсутність регулярного оцінювання їх зрілості.

Саме тому в межах даної роботи основний акцент робиться на можливості проведення самооцінювання шляхом заповнення опитувальника

відповідальними за інформаційну безпеку особами або власниками відповідних процесів. Такий підхід не потребує значних витрат, дозволяє регулярно здійснювати контроль стану кібербезпеки та створює основу для подальшого вдосконалення системи управління інформаційною безпекою університету.

3.2 Консолідація оцінок експертів

П'яти обраним експертам, що мають освіту у сфері кібербезпеки та захисту інформації, було запропоновано пройти наведений опитувальник та надати відповіді на питання за шкалою від 0 (процес не існує) до 4 (процес ефективний та постійно вдосконалюється). Таким чином, були отримані оцінки, наведені нижче.

Таблиця 3.2 – Результати опитування

Питання	Експерт				
Q#	A	B	C	D	E
Q1	2	2	3	2	3
Q2	3	3	1	1	2
Q3	2	0	4	2	1
Q4	1	1	2	1	2
Q5	2	3	2	3	3
Q6	2	2	2	1	3
Q7	1	0	3	1	1
Q8	1	2	3	1	1
Q9	2	2	2	3	2
Q10	1	1	1	1	1
Q11	0	2	0	1	1
Q12	1	3	2	1	2

Кінець таблиці 3.2

Q13	1	2	1	1	2
Q14	1	2	4	3	0
Q15	0	3	3	3	1
Q16	1	1	2	2	1
Q17	0	2	4	2	0
Q18	0	0	0	0	0
Q19	0	2	2	0	0
Q20	2	2	4	2	2
Q21	3	2	3	2	2
Q22	2	4	4	0	3
Q23	2	3	2	2	2
Q24	2	2	2	1	3
Q25	1	3	1	0	3
Q26	2	3	1	3	3
Q27	2	3	4	2	2
Q28	1	1	3	2	3
Q29	1	1	2	1	2
Q30	2	1	2	1	2
Q31	2	1	2	1	2
Q32	1	1	1	1	1
Q33	2	2	1	0	3
Q34	2	2	3	2	3
Q35	1	3	2	0	2
Q36	2	3	2	2	1
Q37	2	3	2	1	2
Q38	0	1	1	1	0
Q39	1	2	2	1	1
Q40	1	2	2	1	3

3.3 Узгодження оцінок експертів

Оскільки залучені до дослідження експерти мають різний рівень кваліфікації, науковий ступінь та практичний досвід у сфері кібербезпеки, виникає необхідність оцінити ступінь узгодженості їхніх суджень та визначити рівень довіри до отриманих оцінок. Для цього було використано підхід опорного експерта. В якості опорного експерта обирається фахівець (надалі експерт А), який має найвищий науковий ступінь та найбільший рівень експертизи серед учасників експертної групи. Передбачається, що його оцінки найбільш повно відображають професійне бачення стану інформаційної безпеки та можуть використовуватися як базис для порівняння оцінок інших експертів.

Для визначення ступеня узгодженості суджень кожного експерта з оцінками опорного експерта використовується коефіцієнт кореляції Пірсона. Вважається, що якщо значення коефіцієнта кореляції є меншим за 0,3, то рівень узгодженості оцінок такого експерта з оцінками опорного експерта є недостатнім. У такому випадку його оцінки не використовуються під час подальшого розрахунку підсумкових показників фреймворку, оскільки вони можуть суттєво спотворювати результати оцінювання.

Таблиця 3.3 – Узгодженість оцінок експертів із опорним експертом

Експерти	Кореляція
A-B	0.358401611
A-C	0.262700984
A-D	0.334366455
A-E	0.609748352

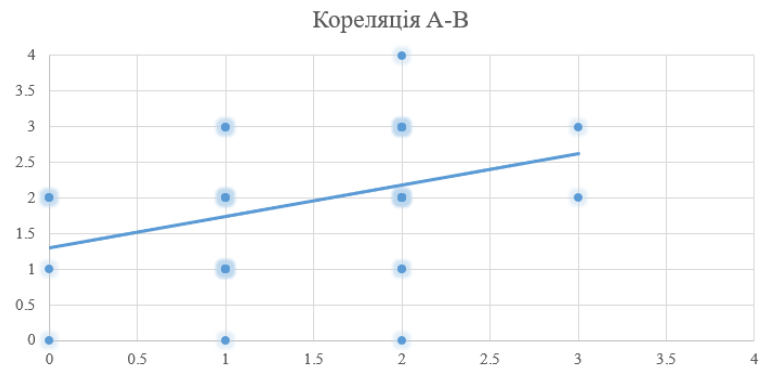


Рисунок 3.1 – Коефіцієнт кореляції Експертів А-В

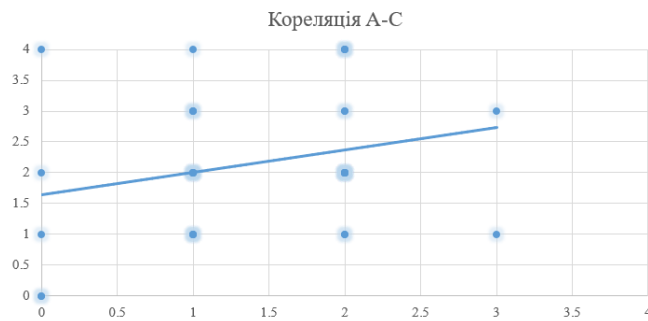


Рисунок 3.2 – Коефіцієнт кореляції Експертів А-С

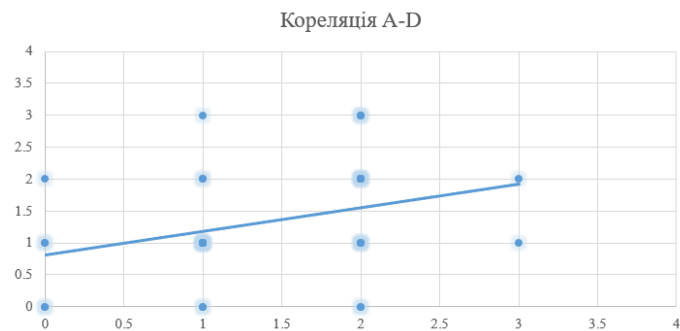


Рисунок 3.3 – Коефіцієнт кореляції Експертів А-Д

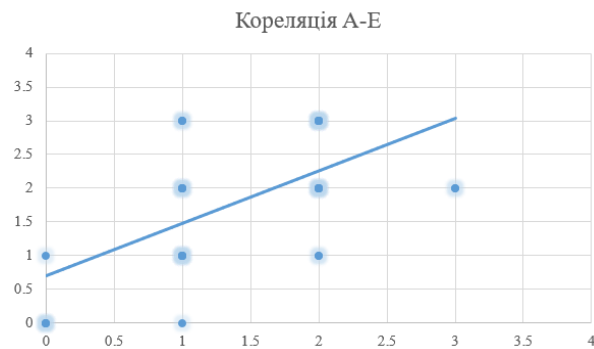


Рисунок 3.4 – Коефіцієнт кореляції Експертів А-Е

Як видно з отриманих результатів, коефіцієнт кореляції між оцінками опорного експерта А та експерта С виявився меншим за 0,3. Це свідчить про низький рівень узгодженості їхніх суджень щодо стану реалізації вимог фреймворку. Тому оцінки експерта С були виключені з подальшого аналізу.

Після виключення експертів, оцінки яких мають недостатній рівень узгодженості з опорним експертом, для решти експертів визначаються вагові коефіцієнти. Для опорного експерта значення коефіцієнта узгодженості приймається рівним 1, оскільки його оцінки використовуються як базові. Для інших експертів коефіцієнт k_i відповідає значенню кореляції Пірсона між їхніми оцінками та оцінками опорного експерта. Ваговий коефіцієнт кожного експерта розраховується за формулою (2.5).

Таким чином, вилучивши коефіцієнт кореляції експерта В, можна обрахувати суму коефіцієнтів:

$$\sum k_i = 1 + 0.3584 + 0.3344 + 0.6097 = 2.3025 \quad (3.1)$$

Як висновок, було отримано вагові коефіцієнти кожного обраного експерта.

Таблиця 3.4 – Вагові коефіцієнти експертів

Експерти	Вагові коефіцієнти
A	0.434307435
B	0.155656484
D	0.145217837
E	0.264818243

Тоді формула для розрахунку узгодженої оцінки середньозваженого експерта буде:

$$X = 0,4343x_A + 0,1557x_B + 0,1452x_D + 0,2648x_E \quad (3.2)$$

Для отримання інформації про стан інформаційної безпеки університету, необхідно таким чином обрахувати значення усіх наданих оцінок середньозваженого експерта.

Таблиця 3.5 – Узгоджені оцінки вимог

Питання	Загальна зважена оцінка
Q1	2.420474727
Q2	2.133433113
Q3	2.046494726
Q4	1.420474727
Q5	2.41003608
Q6	2.119600405
Q7	1.311312969
Q8	1.311312969
Q9	2.145217837
Q10	1
Q11	0.41003608
Q12	1.420474727
Q13	1.264818243
Q14	1.492586885
Q15	1.167441209
Q16	1.300874322
Q17	0.913061613
Q18	0
Q19	0.311312969
Q20	2.311312969
Q21	2.58996392
Q22	2.285695537
Q23	2
Q24	2.119600405

Кінець таблиці 3.5

Q25	1.384418648
Q26	2.254379596
Q27	2.311312969
Q28	1.986167292
Q29	1.420474727
Q30	1.854782163
Q31	1.854782163
Q32	1
Q33	1.818726084
Q34	2.420474727
Q35	1.27525689
Q36	1.735181757
Q37	1.854782163
Q38	0.300874322
Q39	1.155656484
Q40	1.68529297

Оцінки категорій розраховуються як середнє арифметичне оцінок окремих вимог, всередині цих категорій. Всі значення всередині категорій сумуються та діляться на їхню кількість. Таким чином були визначені оцінки категорій середньо зваженого експерта.

Таблиця 3.6 – Узгоджені оцінки категорій

Категорія	Оцінка
Organizational Context (GV.OC)	2.27695392
Risk Management Strategy (GV.RM)	2.046494726
Cybersecurity Supply Chain Risk Management (GV.SC)	1.420474727
Roles, Responsibilities, and Authorities (GV.RR)	2.41003608
Policies, Processes, and Procedures (GV.PO)	1.715456687

Кінець таблиці 3.6

Oversight (GV.OV)	1.311312969
Asset Management (ID.AM)	1.572608919
Risk Assessment (ID.RA)	0.915255404
Improvement (ID.IM)	1.264818243
Identity Management, Authentication, and Access Control (PR.AA)	1.320300805
Awareness and Training (PR.AT)	0.40812486
Data Security (PR.DS)	2.395657475
Platform Security (PR.PS)	1.834673018
Technology Infrastructure Resilience (PR.IR)	2.282846282
Continuous Monitoring (DE.CM)	1.779051586
Adverse Event Analysis (DE.AE)	1.409363042
Incident Management (RS.MA)	1.847865809
Incident Analysis (RS.AN)	1.735181757
Incident Response Reporting and Communication (RS.CO)	1.854782163
Incident Mitigation (RS.MI)	0.300874322
Incident Recovery Plan Execution (RC.RP)	1.155656484
Incident Recovery Communication (RC.CO)	1.68529297

Як фінальний крок, узгоджені оцінки доменів фреймворку обраховуються як середнє арифметичне оцінок категорій всередині них.

Таблиця 3.7 – Фіналізовані оцінки доменів

Домен	Оцінка
Govern	1.896642465
Identify	1.248109378
Protect	1.602997217
Detect	1.655822071
Respond	1.517313972
Recover	1.420474727

3.4 Обробка результатів оцінки стану захищеності згідно із запропонованим підходом

3.4.1 Графічне представлення поточного стану захищеності

Традиційно результати оцінювання кібербезпеки за NIST CSF 2.0 подаються у графічному вигляді у формі профілю зрілості, який дозволяє наочно відобразити поточний стан реалізації окремих напрямів кібербезпеки організації. Такий підхід спрощує інтерпретацію результатів оцінювання, дозволяє швидко виявити найбільш проблемні області та полегшує прийняття управлінських рішень щодо подальшого вдосконалення системи кіберзахисту. З огляду на це, у межах даного дослідження результати оцінювання також будуть представлені у графічному вигляді, що забезпечить можливість візуального порівняння рівня зрілості окремих доменів фреймворку та визначення пріоритетних напрямів розвитку системи інформаційної безпеки ЗВО.

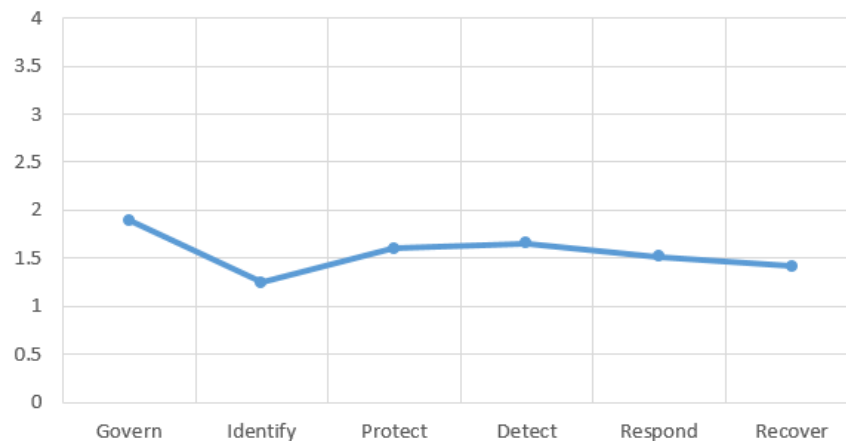


Рисунок 3.5 – Загальний стан захищеності університету за доменами фреймворку

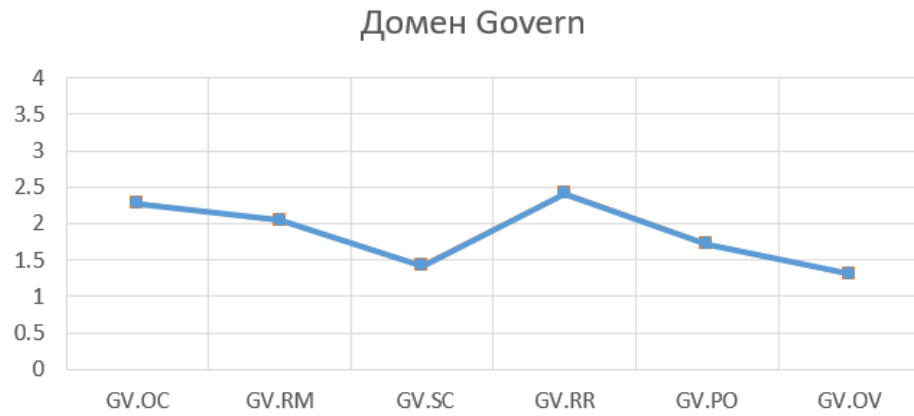


Рисунок 3.6 – Стан захищеності у домені Govern

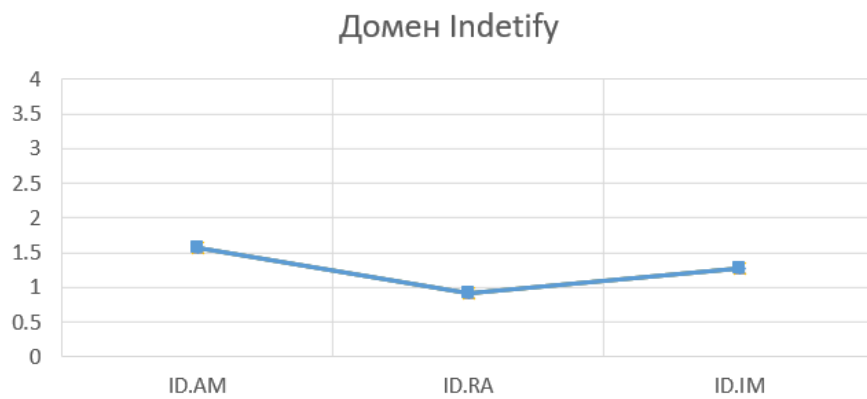


Рисунок 3.7 – Стан захищеності у домені Identify

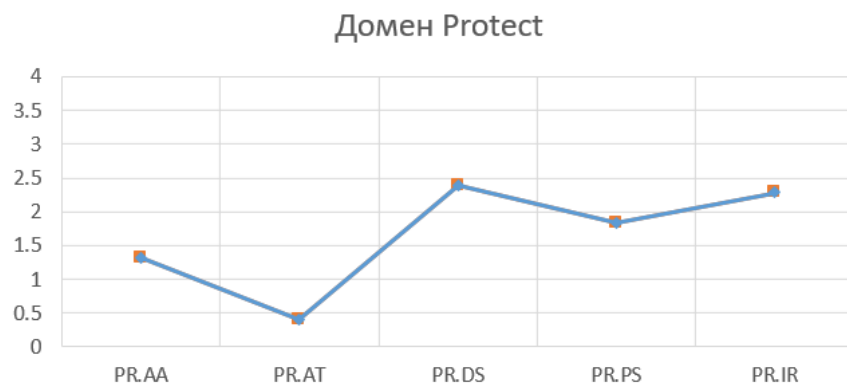


Рисунок 3.8 – Стан захищеності у домені Protect

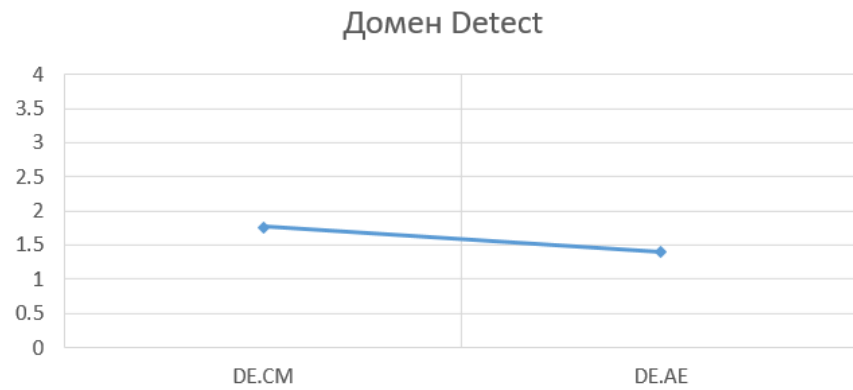


Рисунок 3.9 – Стан захищеності у домені Detect

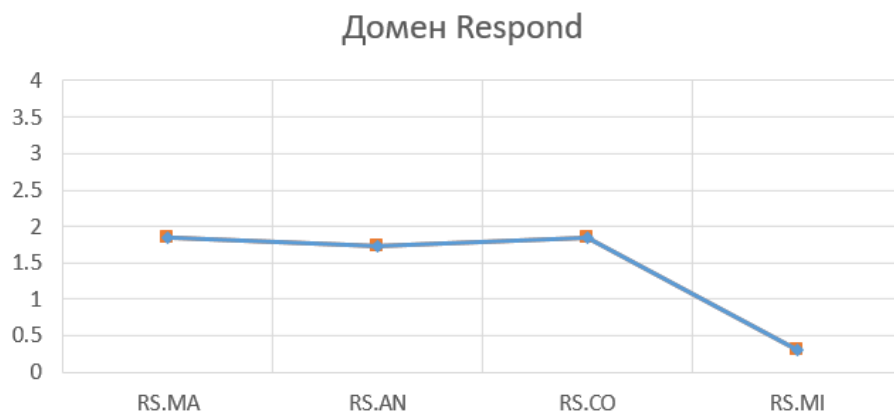


Рисунок 3.10 – Стан захищеності у домені Respond



Рисунок 3.11 – Стан захищеності у домені Recover

3.4.2 Визначення пріоритетності розвитку процесів ІБ

Після визначення поточного рівня зрілості кожного домену виникає необхідність встановити пріоритетність подальшого вдосконалення окремих

напрямів кібербезпеки. Для цього у межах розробленого підходу використовується коефіцієнт пріоритетності домену (2.3).

Такий підхід дозволяє враховувати одночасно як важливість відповідного напрямку кібербезпеки для забезпечення загальної кіберстійкості університету, так і рівень його фактичної реалізації. Відповідно, найбільші значення коефіцієнта пріоритетності отримуватимуть ті домени, які мають високу вагу та водночас демонструють низький рівень зрілості.

У межах даного дослідження за цільовий стан інформаційної безпеки приймається максимальний рівень зрілості, що відповідає оцінці 4 та характеризує повністю реалізовані процеси, які регулярно контролюються, аналізуються та постійно вдосконалюються. Визначення коефіцієнтів пріоритетності відносно цього цільового стану дозволяє сформулювати обґрунтовану послідовність розвитку системи кібербезпеки ЗВО.

Таким чином, була обрахована пріоритетність доменів в межах цього дослідження.

Таблиця 3.8 – Пріоритетність розвитку напрямів інформаційної безпеки

Домен	Оцінка домену	Ваговий коефіцієнт	Коефіцієнт пріоритетності	Пріоритет
Govern	1.897	0.15	0.316	5
Identify	1.248	0.15	0.413	3
Protect	1.603	0.25	0.599	1
Detect	1.656	0.20	0.469	2
Respond	1.517	0.15	0.372	4
Recover	1.420	0.10	0.258	6

Висновки до розділу 3

Виходячи з результатів проведеного дослідження, можна зробити такі висновки:

- Для практичного застосування розробленого фреймворку було сформовано спеціалізований опитувальник, який охоплює всі домени та категорії оцінювання та дозволяє проводити як зовнішній аудит, так і внутрішнє самооцінювання стану кібербезпеки закладу вищої освіти.
- Для підвищення об'єктивності результатів було використано групове експертне оцінювання з подальшою перевіркою узгодженості оцінок за допомогою коефіцієнта кореляції Пірсона. Це дозволило виключити неузгоджені експертні судження та сформувані підсумкові оцінки на основі середньозваженої думки експертної групи.
- Проведене оцінювання дозволило сформувати профіль кіберзахищеності університету та визначити рівень зрілості окремих доменів фреймворку. Отримані результати свідчать про наявність суттєвого потенціалу для вдосконалення більшості процесів інформаційної безпеки.
- Використання механізму пріоритизації дозволило визначити найбільш важливі напрями розвитку функції інформаційної безпеки. Найвищий пріоритет отримали домени Protect, Detect та Identify, що дає змогу обґрунтовано спрямовувати обмежені ресурси ЗВО на найбільш критичні напрями підвищення кіберстійкості.

ВИСНОВКИ

Дипломну роботу було виконано з метою розробки підходу до оцінки поточного стану кіберзахисту університету та визначення пріоритетних напрямів розвитку функції інформаційної безпеки.

В ході виконання роботи було досліджено особливості інформаційної інфраструктури закладів вищої освіти на прикладі телекомунікаційної мережі КПІ ім. Ігоря Сікорського. Встановлено, що сучасні університети є складними інформаційно-телекомунікаційними середовищами, які поєднують велику кількість користувачів, мережових сегментів та інтегрованих інформаційних систем, що формує специфічний ландшафт кіберризиків, суттєво відмінний від традиційних корпоративних мереж.

Проведено аналіз типових вразливостей та основних векторів кібератак на інфраструктуру закладів вищої освіти. Визначено, що освітній сектор є однією з найбільш атакованих галузей, а серед основних векторів атак — фішинг, компрометація облікових даних, програми-вимагачі та експлуатація вразливостей програмного забезпечення. Окремо встановлено, що використання BYOD-політики, низький рівень кібергігієни користувачів та недостатній контроль активів створюють значну кількість потенційних точок компрометації.

Здійснено огляд наявних підходів та стандартів оцінки стану кіберзахисту, зокрема ISO/IEC 27001 та NIST Cybersecurity Framework 2.0. Встановлено, що жоден із розглянутих стандартів у чистому вигляді не враховує повною мірою специфіку освітнього середовища, організаційні обмеження та кадровий дефіцит, характерні для більшості університетів.

На основі проведеного аналізу розроблено комбінований фреймворк оцінювання рівня кіберзахищеності ЗВО, у якому NIST CSF 2.0 використовується як основний структурний каркас із шістьма

функціональними доменами, а положення ISO/IEC 27001 — для деталізації управлінських та організаційних критеріїв оцінювання. Для кожного домену сформовано перелік критеріїв і визначено шкалу зрілості від 0 до 4 балів, а також запроваджено систему вагових коефіцієнтів доменів та коефіцієнт пріоритетності для обґрунтованого розподілу обмежених ресурсів ЗВО.

Розроблено спеціалізований опитувальник, що охоплює всі домени та категорії фреймворку та може застосовуватися як для внутрішнього самооцінювання, так і для зовнішнього аудиту. Проведено опитування п'яти експертів у сфері кібербезпеки, а узгодженість їхніх оцінок перевірено за допомогою коефіцієнта кореляції Пірсона. За результатами перевірки оцінки одного експерта було виключено через недостатній рівень узгодженості, а підсумкові оцінки сформовано на основі середньозваженої думки решти учасників.

На основі отриманих даних проведено оцінку стану кіберзахисту університету. Результати свідчать про загалом низький рівень зрілості процесів інформаційної безпеки в усіх доменах фреймворку. Найнижчі показники зафіксовано у доменах Identify та Protect, зокрема в категоріях управління ризиками, підвищення обізнаності користувачів та управління доступом.

Для університету, на прикладі якого проводилося оцінювання, з метою підвищення загального рівня кіберзахищеності було рекомендовано впровадження системи моніторингу та сканування зовнішніх і внутрішніх кіберзагроз. Таке рішення дозволить забезпечити своєчасне виявлення вразливостей, підозрілої активності та потенційних індикаторів компрометації як у зовнішньому периметрі мережі, так і у внутрішній інформаційній інфраструктурі. Впровадження подібного інструменту сприятиме підвищенню ефективності процесів виявлення інцидентів, скороченню часу реагування на кіберзагрози та загальному підвищенню рівня кіберстійкості університету.

Застосування механізму пріоритизації дозволило визначити послідовність розвитку функції інформаційної безпеки. Найвищий пріоритет отримали домени Protect, Detect та Identify, що відповідає специфіці університетського середовища та підтверджується даними провідних галузевих досліджень щодо економічної ефективності превентивних заходів захисту.

Розроблений підхід є універсальним та може бути використаний іншими закладами вищої освіти для самостійного оцінювання поточного стану кіберзахисту, визначення пріоритетних напрямів розвитку системи інформаційної безпеки та обґрунтованого розподілу наявних ресурсів.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ілляшенко А. М., Кучернюк П. В., Цурін О. П. Інформаційно-телекомунікаційні ресурси університету. КПІ ім. Ігоря Сікорського. 2007. URL: <https://kpi.ua/734-6> (дата звернення: 15.03.2026).
2. Riches A., Bhagat R., Bhagat S. Analysing Cyber Attacks and Cyber Security Vulnerabilities in the University Sector. Computers. 2025. Vol. 14, No. 2. Art. 49. URL: <https://doi.org/10.3390/computers14020049> (дата звернення: 22.04.2025).
3. State of IoT 2023: Number of Connected IoT Devices Growing 18% to 14.3 Billion Globally. IoT Analytics. 2023. URL: <https://iot-analytics.com/number-connected-iot-devices> (дата звернення: 25.04.2025).
4. 2024 Data Breach Investigations Report. Basking Ridge : Verizon Business, 2024. 102 p. URL: <https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf> (дата звернення: 28.04.2025).
5. Petcu A. G. 10 Common Network Vulnerabilities and How to Prevent Them. Heimdal Security Blog. 2024. URL: <https://heimdalsecurity.com/blog/common-network-vulnerabilities> (дата звернення: 05.04.2025).
6. COBIT 2019 Framework: Introduction and Methodology. Rolling Meadows : ISACA, 2018. 84 p.
7. The State of Ransomware in Education 2024. Oxford : Sophos, 2024. URL: <https://www.sophos.com/en-us/whitepaper/state-of-ransomware-education> (дата звернення: 01.05.2025).
8. Khalil M. Data Breaches in Education 2025: Why Schools Are the #1 Cyber Target. DeepStrike Blog. 2025. URL: <https://deepstrike.io/blog/data-breaches-education-2025> (дата звернення: 10.04.2025).
9. Education Under Attack: Cyberattack Trends Impacting Higher Education in 2024. Check Point Blog. 2024. URL:

<https://blog.checkpoint.com/education-cyberattacks-2024> (дата звернення: 03.05.2025).

10. Cyber Attacks Against Schools and Colleges. Arctic Wolf Blog. 2024. URL: <https://arcticwolf.com/resources/blog/cyber-attacks-against-schools-and-colleges> (дата звернення: 05.05.2025).

11. Stratton A., El-Hammamy N., Radukic E., Roberts J., Harding H., Shah J. N. Cyber Security Breaches Survey 2025: Education Institutions Findings. London : Department for Science, Innovation and Technology, 2025. URL: <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025-education-institutions-findings> (дата звернення: 25.05.2025).

12. AI vs. Human Deceit: Unravelling the New Age of Phishing Tactics. IBM X-Force. 2025. URL: <https://www.ibm.com/think/x-force/ai-vs-human-deceit-unravelling-new-age-phishing-tactics> (дата звернення: 10.05.2025).

13. Data Breaches in Education 2025: The Growing Cybersecurity Crisis. DeepStrike Blog. 2025. URL: <https://deepstrike.io/blog/data-breaches-education-2025> (дата звернення: 10.04.2025).

14. 2024 State of Ransomware in Education. ThreatDown Research. 2024. URL: <https://www.threatdown.com/blog/2024-state-of-ransomware-in-education-92-spike-in-k-12-attacks> (дата звернення: 07.05.2025).

15. Ransomware Attacks in Education Jump 23% Year Over Year. Higher Ed Dive. 2025. URL: <https://www.highereddive.com/news/ransomware-attacks-education-jump-23-percent-h1-2025/754011> (дата звернення: 10.05.2025).

16. Network Security Vulnerabilities: Types, Risks & Prevention. Heimdal Security Blog. 2024. URL: <https://heimdalsecurity.com/blog/network-security-vulnerabilities> (дата звернення: 05.04.2025).

17. Pearson's Correlation Coefficient: A Comprehensive Overview. Statistics Solutions. URL: <https://www.statisticssolutions.com/free-resources/directory-of-statistical-analyses/pearsons-correlation-coefficient> (дата звернення: 20.04.2025).

18. Cyber Signals Issue 8: Education Under Siege. Redmond : Microsoft Security, 2024. URL: <https://www.microsoft.com/uk-ua/security/security-insider/intelligence-reports/cyber-signals-issue-8-education-under-siege> (дата звернення: 15.04.2025).

19. Наріжна В. Масштабна кібератака на дев'ять тисяч навчальних закладів: що відомо про злам Canvas. *Дзеркало тижня*. 2026. 9 трав. URL: <https://zn.ua/ukr/TECHNOLOGIES/masshtabna-kiberataka-na-devyat-tisjach-navchalnikh-zakladiv-shcho-vidomo-pro-zlam-canvas.html> (дата звернення: 05.06.2026)

20. Torregosa J. T., Orong M. Y., Ricalde G. T., Amin W. D., Lonzon H. A., Alcontin R. B. Assessing the Conformity Level of Information Security Management System of the Higher Education Institutions: Basis for the Development of Policies and Guidelines. *Mediterranean Journal of Basic and Applied Sciences*. 2021. Vol. 5, Issue 1. P. 57–71. DOI: <https://doi.org/10.46382/MJBAS.2021.5105>.

21. ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements. Geneva : ISO, 2022. 36 p.

22. NIST Cybersecurity Framework (CSF) 2.0. Gaithersburg : National Institute of Standards and Technology, 2024. URL: <https://doi.org/10.6028/NIST.CSWP.29> (дата звернення: 12.04.2025).

23. The NIST Cybersecurity Framework (CSF) 2.0 : NIST Special Publication CSWP 29. Gaithersburg : National Institute of Standards and Technology, 2024. 32 p. URL: <https://doi.org/10.6028/NIST.CSWP.29> (дата звернення: 12.04.2025).

24. Da Costa B. et al. Cybersecurity Strategy for Higher Education Institutions: A Thematic Analysis on Standards and Frameworks. *Journal of Information Systems Engineering and Management*. 2024. Vol. 9, No. 2. URL: <https://doi.org/10.55267/iadt.07.14388> (дата звернення: 18.04.2025).

25. Cost of a Data Breach Report 2024 / IBM Security ; Ponemon Institute. Armonk : IBM Corporation, 2024. 87 p. URL: <https://www.ibm.com/reports/data-breach> (дата звернення: 15.05.2025).
26. State of Cybersecurity 2026: Prevention ROI and Breach Cost Analysis. Stack Cyber Security. 2026. URL: <https://stackcybersecurity.com/posts/dont-delay-cybersecurity-investment> (дата звернення: 20.05.2025).
27. CIS Controls Version 8. East Greenbush : Center for Internet Security, 2021. 189 p.
28. Гальчинський Л. Ю., Стурчак М. В. Захист даних в інформаційній моделі модуля "кафедра" автоматизованої інформаційної системи університету. Інформаційні технології і засоби навчання. 2024. Вип. 99, № 1. С. 95–117. DOI: <https://doi.org/10.33407/itlt.v99i1.5537>.
29. Singh U. K., Joshi C. Information Security Risk Management Framework for University Computing Environment. International Journal of Network Security. 2017. Vol. 19. P. 742–751.
30. Ramanauskaitė S., Urbonaitė N., Grigaliūnas Š. et al. Educational Organization's Security Level Estimation Model. Applied Sciences. 2021. Vol. 11, No. 17. Art. 8061. DOI: <https://doi.org/10.3390/app11178061>.
31. Тарасенко А. В., Гальчинський Л. Ю. Підхід для оцінювання рівня кібербезпеки університету. Science and Education: Synergy of Innovation : матеріали X Міжнар. наук.-практ. конф., Берлін, Німеччина, 18–20 трав. 2026 р. Berlin : MDPC Publishing, 2026. С. 148–152. URL: <https://sci-conf.com.ua/x-mizhnarodna-naukovo-praktichna-konferentsiya-science-and-education-synergy-of-innovation-18-20-05-2026-berlin-nimechchina-arhiv> (дата звернення: 25.05.2026).
32. Cyber Resilience: The Future for Higher Education. EDUCAUSE Review. 2023. URL: <https://er.educause.edu/articles/sponsored/2023/3/cyber-resilience-the-future-for-higher-education> (дата звернення: 22.04.2025).