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

До захисту допущено
Завідувач кафедри

_____ **Дмитро ЛАНДЕ**
(підпис)

«_____»_____2024 р.

Дипломна робота

на здобуття ступеня бакалавра

за освітньо-професійною програмою «Системи, технології та математичні методи кібербезпеки»
спеціальності 125 «Кібербезпека»

на тему: Оцінка рівня кібербезпеки університету

Виконав (-ла): здобувач вищої освіти **IV** курсу, групи ФБ-05
(шифр групи)

Бобер Наталія Вікторівна
(прізвище, ім'я, по батькові) (підпис)

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

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

Рецензент: доцент кафедри математичного моделювання та аналізу даних

ННФТІ, к. т. н., доцент Хайдуров Владислав Володимирович
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище, ім'я, по батькові) (підпис)

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Здобувач вищої освіти _____
(підпис)

Київ – 2024 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»

До захисту допущено
Завідувач кафедри

_____ **Дмитро ЛАНДЕ**
(підпис)
«_____»_____2024 р.

ЗАВДАННЯ

на дипломну роботу здобувачу вищої освіти

Бобер Наталії Вікторівні
(прізвище, ім'я, по батькові)

1. Тема роботи Оцінка рівня кібербезпеки 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 31 травня 2024 р. № 2251-с

2. Термін подання здобувачем вищої освіти роботи 14 червня 2024 р.

3. Вихідні дані: статті та документація, що стосуються оцінки ризиків університету.

4. Зміст роботи: огляд термінів ризику та кіберризику, кіберризиків в організаціях та освітніх установах, огляд методів оцінки та аналізу безпеки освітньої організації, оцінка рівня кібербезпеки університету.

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо): презентація.

6. Дата видачі завдання 16 листопада 2023 р.

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів дипломної роботи	Примітка
1	Вибір теми роботи, формування завдання та мети	16.11.2023-22.12.2023	виконано
2	Опрацювання літературних джерел	22.12.2023-16.02.2024	виконано
3	Ознайомлення з поняттями ризику та кіберризику	16.02.2024-08.03.2024	виконано
4	Ознайомлення з кіберризиками організацій та освітніх установ	08.03.2024-29.04.2024	виконано
5	Ознайомлення з методами оцінки та аналізу безпеки освітньої організації	29.04.2024-15.04.2024	виконано
6	Проходження переддипломної практики	15.04.2024-19.05.2024	виконано
7	Аналіз та опрацювання отриманих результатів експертного оцінювання	19.05.2024-24.05.2024	виконано
8	Оцінка рівня кібербезпеки університету	24.05.2024-10.06.2024	виконано
9	Оформлення дипломної роботи	10.06.204-13.06.2024	виконано
10	Передзахист дипломної роботи	14.06.2024	виконано
11	Захист дипломної роботи	21.06.2024	виконано

Здобувач вищої освіти _____ Наталія БОБЕР
(підпис) (Власне ім’я, ПРІЗВИЩЕ)

Керівник роботи _____ Леонід ГАЛЬЧИНСЬКИЙ
(підпис) (Власне ім’я, ПРІЗВИЩЕ)

РЕФЕРАТ

Дипломна робота містить: 44 сторінок, 11 ілюстрацій, 13 таблиць, 17 джерел літератури.

Метою роботи є оцінка рівня кібербезпеки університету, що дозволяє оцінити рівень захищеності освітньої організації.

Об’єктом досліджень є інформаційна інфраструктура університету.

Предметом дослідження є метод для оцінки кіберризиків університету.

Методом дослідження є опрацювання літературних джерел за вибраною темою, дослідження існуючих методів оцінки кіберризиків освітніх організацій та розробка моделі оцінки рівня безпеки.

Робота містить опис процесу оцінки рівня кібербезпеки університету, а саме створення моделі оцінки безпеки, створення опитувальника для множини експертів, узгодження оцінок експертів та процеси підготовки даних до оцінки.

Ключові слова: ризик, кіберризик, електронне навчання, оцінка кіберризику, метод аналізу ієрархій.

ABSTRACT

The work includes 44 pages, 11 illustrations, 13 tables, 17 references.

The purpose of the work is to assess the level of cybersecurity of the university, which allows evaluating the level of security of the educational organization.

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

The subject of the study is a method for assessing university cyber risks.

The research method is to study the literature on the chosen topic, research existing methods for assessing cyber risks of educational organizations and develop a model for assessing the level of security.

The paper contains a description of the process of evaluating the level of cybersecurity of a university, namely the creation of a security assessment model, the creation of a questionnaire for a set of experts, the coordination of expert assessments and the processes of preparing data for assessment.

Keywords: risk, cyber risk, e-learning, cyber risk assessment, hierarchy analysis method.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ЗВО – заклад вищої освіти

МАІ – метод аналізу ієрархій

MCDM – багатокритеріальне прийняття рішень (англ. Multiple-Criteria Decision Making)

AHP – метод аналізу ієрархій (англ. The Analytic Hierarchy Process)

ВСТУП

Зростаюча популярність інформаційних технологій надає користувачам нові можливості, але водночас з’являються додаткові ризики для кібербезпеки.

У сучасних умовах агресії російської федерації проти України спостерігається тенденція до зростання кількості нападів на об’єкти критичної інфраструктури і стратегічні промислові об’єкти нашої держави. Це відображається у збільшенні кількості інцидентів, спрямованих на порушення інформаційної безпеки.

Водночас, ризики інформаційної безпеки входять до категорії найбільш ймовірних ризиків, поряд із природніми катаклізмами, екстремальними погодними умовами та іншими. Також вони містяться у шести найбільш критичних ризиків за можливою шкодою. Рівень захисту об’єктів інформаційної діяльності залежить від ризиків інформаційної безпеки, що зростають через збільшення кількості реалізованих нападів з урахуванням їх руйнівного потенціалу.

Управління ризиками інформаційної безпеки та підтримка їх на прийнятому рівні є важливою функцією кожної організації, установи чи підприємства.

Під час пандемії та повномасштабного вторгнення дистанційне навчання набуло своєї необхідності. Однією зі сфер, яка суттєво змінилася є освіта.

Навчальний процес трансформовано в електронне дистанційне навчання. Більшість шкіл та університетів змушені були використовувати засоби електронного навчання. Швидкий перехід на дистанційне навчання посилив цифровізацію освітньої системи та вплинув на збільшення кількості інцидентів безпеки, оскільки не було достатньо часу оцінити зміну рівня безпеки шляхом впровадження нових систем електронного навчання.

Актуальність роботи полягає в тому, що більшість освітніх організацій не мають достатньо ресурсів та знань, щоб оцінити ризики безпеки та керувати ними, фактична відсутність експертів з безпеки та їхньої належної уваги в освітніх організаціях призводить до потреби розробки оцінки рівня безпеки.

Метою роботи є оцінка рівня кібербезпеки університету, що дозволяє оцінити рівень захищеності освітньої організації.

Об’єктом дослідження є інформаційна інфраструктура університету.

Предметом дослідження є метод для оцінки кіберризиків університету.

Методом дослідження є опрацювання літературних джерел за вибраною темою, дослідження існуючих методів оцінки кіберризиків освітніх організацій та розробка моделі оцінки рівня безпеки.

Практичне завдання отриманих результатів полягає у можливості використання створеної моделі оцінки рівня безпеки для оцінки рівня кібербезпеки освітніх установ.

Результати дослідження були представлені на Міжнародній науково-практичній конференції «Інноваційний розвиток сучасної науки та освіти» (11.06.2024 р., м. Житомир, Україна).

1 ОСНОВИ КІБЕРРИЗИКІВ ТА ЇХ ВПЛИВ У РІЗНИХ СФЕРАХ

1.1 Загальні поняття ризику та кіберризику

Термін ризик має комплексний характер, оскільки його визначення вимагає враховувати багато факторів, які можуть впливати на ступінь критичності ситуації та аналіз усіх можливих наслідків до котрих такі ризики можуть призвести. Загалом ризик являє собою суму двох факторів, а саме небезпеки та уразливості.[1]

У сучасній літературі в тлумаченні поняття «ризик» акцентується на можливості втрат, небезпек, збитків та інших несприятливих наслідків. Таке розуміння сутності ризику суперечить його походженню – етимологічно ризик пов’язувався із поняттями «випадок», «шанс», «азарт». Враховуючи етимологічні дослідження сутності ризику, а також його мотиваційний аспект (надію на позитивний результат), найточніше сутність ризику можна сформулювати так: ризик – це рішення або інші дії, наслідком яких можуть бути позитивні, так і негативні результати під впливом непередбачуваних змін у внутрішньому і зовнішньому середовищі організації. [2].

Розглянемо ще кілька тлумачень цього терміну.

- Ризик[3] – прогнозована векторна величина збитку, що може виникати внаслідок ухвалення рішень в умовах невизначеності. Він є кількісною мірою безпеки, що дорівнює добутку ймовірності реалізації загрози на ймовірність величини (величину) можливого збитку від неї.
- Ризик – ймовірність заподіяння шкоди з урахуванням її тяжкості.
- Ризик інформаційної безпеки – потенціальна можливість використання вразливості актива або групи активів конкретної загрози для заподіяння шкоди організації. ISO 27005

Очевидно, що існує велика кількість різноманітних тлумачень поняття "ризик", оскільки вони виникають у різних сферах людської діяльності та взаємодії з оточуючим середовищем. Ця різноманітність пояснюється тим, що ризики проявляються по-різному в кожній сфері, і це призводить до багатьох різних визначень цього терміну.

При вивченні різноманітних ризиків можна виявити спільні ознаки серед них. Зрозуміло, що результати такого дослідження будуть залежати від обсягу і складу ризикових груп, які були представлені для аналізу. Однак є загальна характеристика, що властива всій множині ризиків: це наявність невизначеності, яка в суті породжує сам ризик.

Кіберризик – це ризик, пов'язаний з використанням комп'ютерного обладнання та програмного забезпечення як у локальних мережах, так і в глобальній Інтернет-мережі; в розрахунково-платіжних системах, системах інтернет-торгівлі, промислових системах управління, а також ризик пов'язаний із накопиченням, зберіганням і використанням особистих персональних даних даних.[4]

Кіберризик – це будь-який ризик, пов'язаний із фінансовими втратами, перебоями в роботі або шкодою репутації організації через негативну подію, що вплинула на інформацію організації та/або інформаційні системи. [5]

Кіберризик можна розуміти як потенційну можливість (ймовірність) наражати інформаційні та комунікаційні системи підприємства на небезпечні суб'єкти, елементи чи обставини, здатні спричинити збитки чи збитки. Ризик передбачає певну ймовірність або ймовірність того, що відбудеться подія. [6]

Кіберризик базується на ймовірності поганої події, що станеться з інформаційними системами вашого бізнесу, що призведе до втрати конфіденційності, цілісності та доступності інформації.

Кіберризики можуть виникати де завгодно: ззовні через віруси чи сторонніх постачальників із слабкою системою безпеки або внутрішньо через саботаж нечесних співробітників чи невиконання слабких методів безпеки, як-от нерегулярне оновлення програмного забезпечення.

У науковій статті [7] автори згрупували кіберризики за такими ознаками як: 1) втрата або крадіжка носіїв інформації та мобільних пристроїв; 2) доступ сторонніх осіб до конфіденційної інформації за допомогою вразливих хмарних сховищ; 3) ненавмисне розголошення співробітниками конфіденційної інформації; 4) навмисні дії співробітників (інсайдерів); 5) неконтрольоване копіювання даних

співробітниками. На основі цих ознак було складено таку класифікацію кіберризиків:

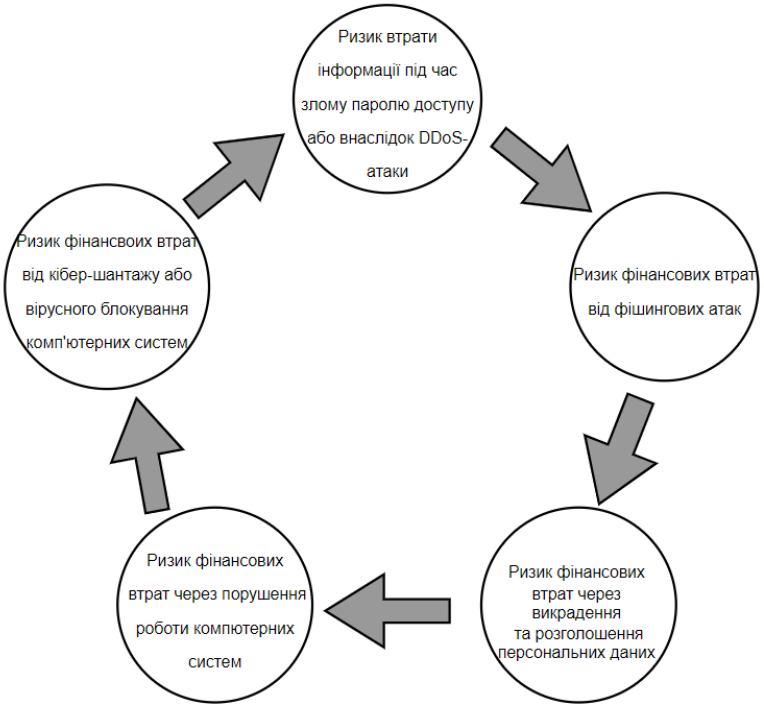

Рисунок 1.1 - Класифікація кіберризиків

1.2 Кіберризики в організаціях

Останнім часом кількість кіберзагроз стрімко зростає, кіберзлочинність лише посилюється і сама нікуди не зникне. Тому організації та компанії вимушені вживати заходів у сфері кібербезпеки, яка нині є пріоритетом.

Організації стають усе більш залежними від інформаційних систем, що робить їх уразливими для кіберризиків: витоку даних внаслідок кібератак і комп’ютерних вірусів, втрати даних через людський фактор або збоїв у роботі носіїв інформації.

Кіберризики можуть призводити до прямих та непрямих грошових втрат в організаціях. В першому випадку можна легко виміряти збитки в грошовому еквіваленті, в другому випадку необхідно залучати експерта або фахівця для якісної оцінки величини збитків в організації.

На міжнародному економічному форумі в 2015 році кіберризики названі одними з ключових комерційних ризиків, оскільки наслідки втрати даних можуть бути катастрофічними.

З огляду на стрімкий розвиток інформації, інформаційних та комп'ютерних технологій, можна вважати, що найбільшою проблемою є кіберризики. Тому питання класифікації та управління кіберризиками набуває особливої актуальності.[7]

Кіберризики є найбільш недооціненими ризиками в довгостроковій перспективі.

Яскравим прикладом цього є те, що у 2017 році під час кібератаки вірусу Petya постраждали понад 1500 організацій, 125 тисяч комп'ютерів було заражено, а розмір збитків склав $466,3 млн.

Також варто згадати кібератаку, яка відбулася нещодавно, це атака на найбільшого в Україні оператора зв'язку «Київстар». По всій країні у 24 мільйонів абонентів «Київстар» зник мобільний зв'язок та інтернет. Збої виникли у всього обладнання, яке використовувало цей зв'язок, що призвело до серйозних інфраструктурних проблем по всій країні.

1.3 Кібер-ризики в освітніх організаціях

Згідно зі звітом компанії Cybersecurity Ventures про ризики кібербезпеки пишеться, що згідно прогнозів до 2025 року глобальний збиток від кіберзлочинності достигне $10,5 трильйонів у рік, порівняно з $3 трильйонами у 2015 році. До 2031 року світ буде стикатися з атаками кожні 2 секунди.[8]

Це пов'язано зі спалахом пандемії COVID-19 та повномасштабним вторгненням ворогів на територію України, багато організацій змушені були швидко відправити своїх співробітників на віддалену роботу для забезпечення безпеки. Це порушило архітектуру мережі організацій, зробило її більш відкритою, чим створило нові вразливі місця для використання зловмисниками. Переважно

кібератаки спрямовані на дані й активи урядів, корпорацій різних компаній та підприємств. Проте у цьому переліку не стали винятком університети та освітні установи. Ризик атак на освітні мережі зростає, оскільки вони стають дедалі більш залежними від відкритого середовища і використання мобільних технологій.

У закладах вищої освіти циркулюють великі обсяги персональних даних і фінансової інформації про студентів, викладачів та співробітників, а також конфіденційна інформація про наукові дослідження, що робить їх привабливою мішенню для кіберзлочинців.

Саме тому кожен освітній заклад має оцінити свій профіль кіберризиків, враховуючи те, які його активи і процеси піддаються впливу вразливості. Відповідно тому, необхідно обирати таке програмне забезпечення, інструменти та методології безпеки, які найкраще та найефективніше контролюватимуть доступ до цих даних та захищатимуть їх.

Згідно з даними Microsoft[9], сектор освіти став найбільшою жертвою корпоративних кібератак і посідає перше місце 80,8% від загальної кількості виявлених випадків зловмисного програмного забезпечення, порівняно з іншими галузями, такими як торгівля 9,19%, медицина 4,9% , телекомунікації 2,2% , фінанси 1,74% та енергетика 1,17%.

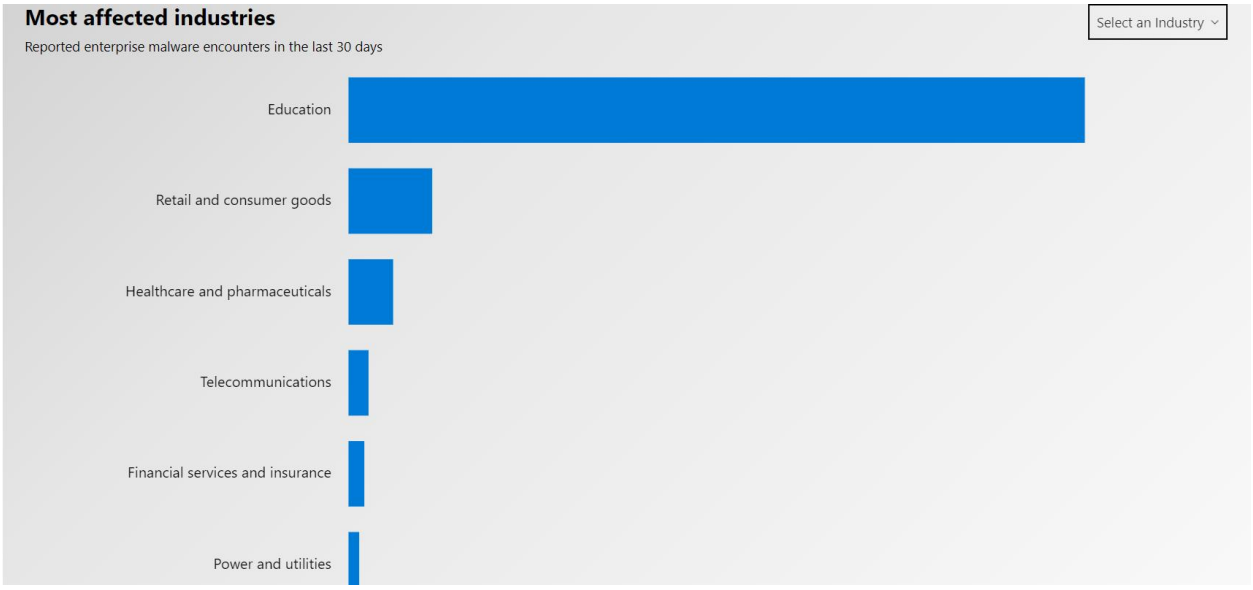

Рисунок 1.2 – Найбільш постраждалі галузі від кібератак згідно Microsoft

За даними дослідження Check Point Software Technologies [10] , у 2022 -2023 роках головними цілями кібератак були освіта та наукові дослідження: у середньому на організацію було зареєстровано 1158 атак на тиждень. Причому явно спостерігається тенденція до зростання.

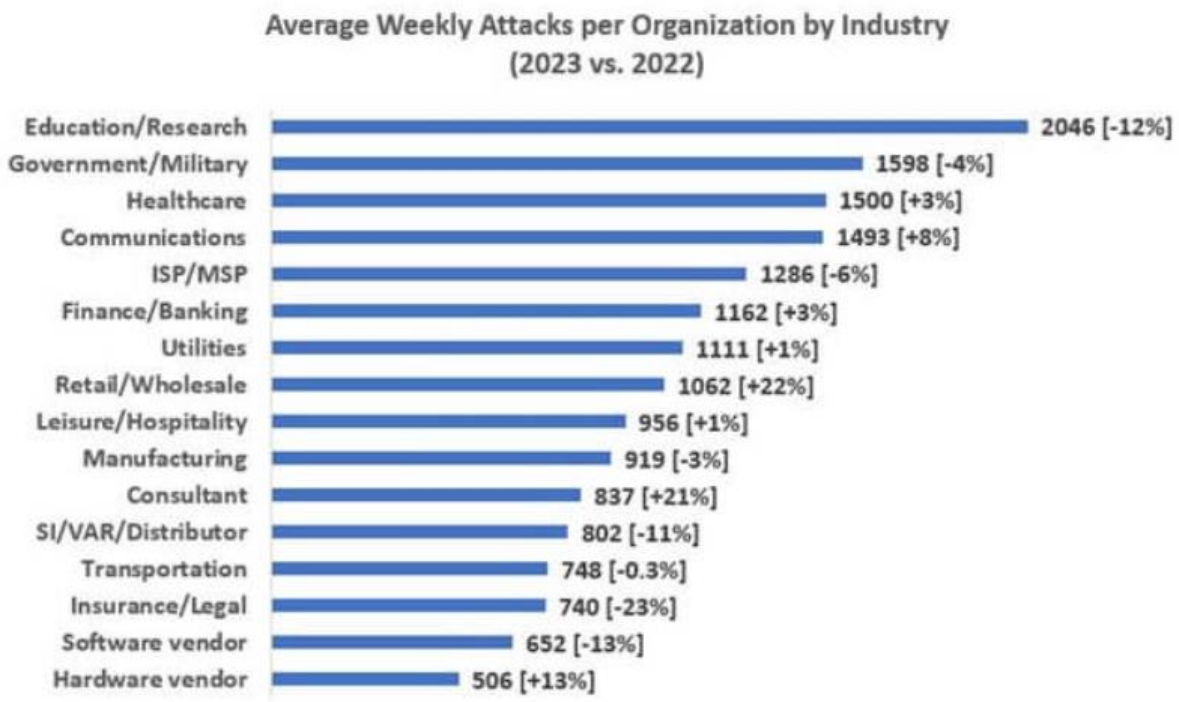

Рисунок 1.3 – Головні цілі кібератак згідно Check Point Software Technologies

Інтерес кіберзлочинності до освітнього сектора зумовлений наявністю значної кількості персональних даних як студентів, так і штату працівників.

Багато університетів мають інформацію про передові наукові дослідження, технологічні інновації та інтелектуальну власність, що робить її цільовою мішенню для хакерів. При цьому традиційно освітні установи вищої школи дотримуються академічної відкритості та сприяють вільному обміну інформацією з іншими дослідниками як всередині, так і поза межами університету, що робить їх мішенню і ставить під підвищений ризик кібератак.

Такі взаємозв’язки в ЗВО продовжують зростати, а відтак пропорційно зростає поле доступу для кібератак. Усе це становить виклики для кібербезпеки, які не спостерігаються в інших галузях. Парадокс полягає в тому, що численні науковці вишів досліджують сучасні проблеми кібербезпеки і публікують свої

дослідницькі статті щодо її забезпечення, тоді як сам сектор вищої освіти часто має проблеми з кіберзахистом і потребує спеціалізованого захисту. Проте через обмежені бюджетні можливості не всі університети можуть дозволити собі належний рівень кіберзахисту.[11]

Сектор вищої освіти стикається з широким спектром кіберзагроз, включаючи крадіжку особистих даних і комерційних секретів, атаки програм-вимагачів, несегментовані мережі віддалених працівників і студентів, а також взаємодію між різними підрозділами, філіалами та комерційними партнерами.

Наявність багатьох комп'ютерних лабораторій у різних структурних підрозділах університетів, де студенти та викладачі з різним рівнем технічних знань мають доступ до комп'ютерів і системних пристроїв, також ускладнює забезпечення інформаційної безпеки. Це призводить до того, що заходи з кібербезпеки часто нехтуються на користь зручності та функціональності. Крім того, постійний потік нових студентів і співробітників також робить освітні заклади вразливими перед кіберзагрозами.

Також слід зазначити, що освітні установи часто піддаються атакам через недостатню підготовленість персоналу, студентів та співробітників у питаннях кібербезпеки. Низький рівень обізнаності користувачів щодо основних принципів захисту інформації створюють додаткові вразливості.

Використання різноманітного програмного забезпечення для навчання і досліджень, яке може мати власні вразливості, ще більше ускладнює забезпечення комплексного захисту інформаційної інфраструктури. Крім того, багато університетів активно співпрацюють з зовнішніми організаціями та використовують сторонні сервіси для обробки та зберігання даних, що може призводити до витоку інформації через недостатній контроль з боку університету.

Інциденти, пов'язані з кібератаками, можуть негативно вплинути на репутацію університетів, знижуючи довіру до їх здатності захищати особисті дані

та конфіденційну інформацію. Це може мати серйозні наслідки для залучення нових студентів і фінансування з боку держави та приватних інвесторів.

Таким чином, питання кібербезпеки в освітньому секторі є надзвичайно актуальним і вимагає комплексного підходу для оцінки рівня захисту.

Висновки до розділу 1

Кількість кібератак стрімко зростає, що робить питання кібербезпеки пріоритетним для організацій та компаній. Залежність інформаційних систем підвищує уразливість до кіберризиків, які можуть призводити до значних фінансових втрат. Приклади кібератак, такі як атака вірусу Petya в 2017 році та недавня атака на «Київстар» демонструють катастрофічні наслідки таких інцидентів підкреслюючи важливість управління та оцінки кіберризиків.

У даному розділі було розглянуто проблему захисту освітніх організацій. Сектор вищої освіти став особливою мішенню для кіберзлочинців через значну кількість персональних даних, конфіденційну інформацію про дослідження та відкритий обмін інформацією. Очевидно, що існує проблема захисту цих організацій, вона актуальна та має певні особливості, такі як відсутність експертів з безпеки та обмежені фінансові ресурси для впровадження належних захисних заходів. Ця проблема викликає необхідність її вирішення. І першим кроком на цьому шляху має бути оцінка рівня вразливості. До недавнього часу ця проблема не вважалась важливою. Проте наразі ситуація змінюється.

Існує готове рішення для проведення оцінки рівня вразливості. Для того щоб зробити висновки, потрібно побудувати модель оцінки рівня безпеки та на основі цієї моделі провести оцінку.

2 МЕТОД ОЦІНКИ ТА АНАЛІЗУ БЕЗПЕКИ ОСВІТНЬОЇ УСТАНОВИ

2.1 Метод кількісної оцінки рівня безпеки

Для спрощення оцінки рівня безпеки освітньої організації кількісна модель дозволить моделювати різні ситуації та порівнювати їх, аналізувати вплив деяких факторів, що впливають на безпеку. У той же час модельний додаток буде більш доступним у разі автоматизованого або, принаймні, відсутності спеціальних знань у сфері безпеки, які вимагають збору даних про організацію. Враховуючи, що повністю автоматизовані рішення не можуть надати дані про політики та процеси безпеки організації, вибрано ручне подання даних про організацію. Прийнявши модель використання дискретних вхідних значень, оцінка яких не потребує спеціальних знань у сфері безпеки, навіть невеликі організації, в яких немає фахівців безпеки, зможуть моделювати ситуації з рівнем безпеки організації.

Для моделі оцінки рівня безпеки використовується багатокритеріальний підхід до прийняття рішень, щоб гарантувати, що всі особливості будуть прийняті до уваги. Базовий принцип використання MCDM в моделі представлений на Рисунку 2.1. Для цієї моделі оцінюють набір критеріїв, що визначають рівень безпеки організації освіти та піддаються дискретній оцінці. Критерії вибираються так, щоб відобразити як безпеку, так і безпеку організації, тобто ризики, пов'язані з третіми особами, а також вплив окремих працівників на організацію. Для того, щоб оцінити важливість кожного критерію виконується попарне порівняння критеріїв. Таке порівняння дозволяє оцінити ступінь узгодженості думок експертів. Тому для оцінки важливості критеріїв використовуються лише дані експертів з безпеки, які мають єдину думку.

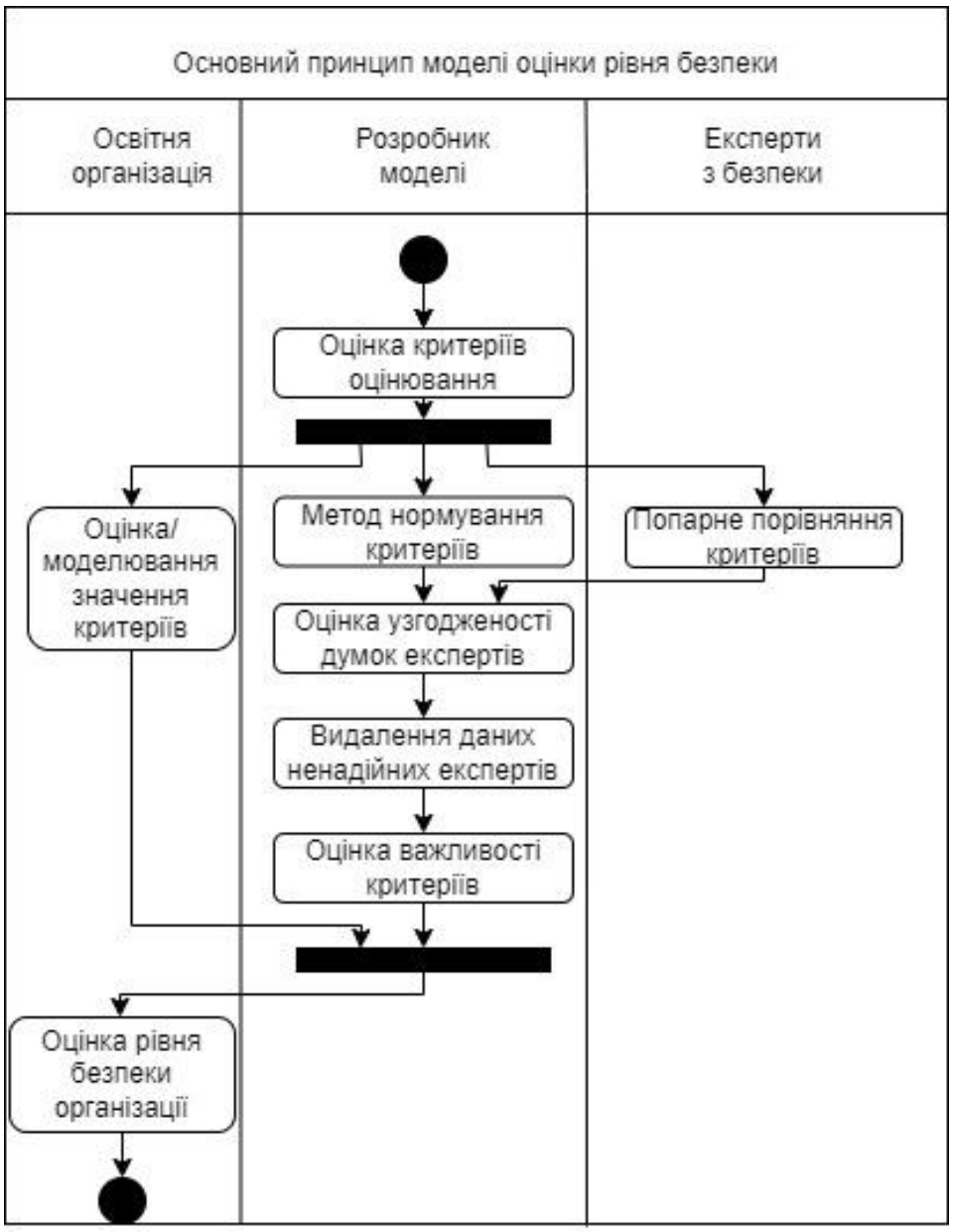

Рисунок 2.1 – Модель оцінки рівня безпеки освітньої організації

Експерти з безпеки не аналізують дані організації, а тільки визначають важливість кожного критерія. Отже, освітня організація може представити значення критеріїв, описуючи поточну або змодельовану ситуацію в організації, без залучення експертів з безпеки, оскільки значення критеріїв є дискретними і не потребують інтерпретації рівня безпеки. З використанням коефіцієнтів важливості (оцінюваних за думкою експертів безпеки), даних освітньої організації (представлених організацією) і методом нормалізації критеріїв (визначених розробником моделі) розраховується рівень безпеки організації.

2.2 Розробка набору критеріїв оцінки рівня безпеки освітньої організації

Чотири «Р» безпеки визначають policies, processes, people та products як базові елементи для побудови комплексної безпекової стратегії. Ті ж чотири елементи необхідні освітнім організаціям для забезпечення рівня своєї безпеки.

Policies - сукупність керівних принципів, правил, процедур і практичних прийомів в галузі безпеки, які регулюють управління, захист і розподіл цінної інформації. У загальному випадку такий набір правил являє собою певну функціональність програмного продукту, який необхідний для його використання в конкретній організації. [12]

Processes - комплекс заходів, процедур і практик, спрямованих на захист інформаційних систем, даних та інфраструктури від різних загроз і атак. Це включає в себе захист даних, виявлення загроз, запобігання загрозам, відповідь на інциденти.

People – в контексті безпеки означає людський аспект кібербезпеки, який включає в себе заходи пов’язані з підготовкою, навчанням і поведінкою людей для забезпечення безпеки інформаційний систем. Цей аспект є критично важливим, оскільки найкращі технічні засоби захисту можуть виявитися марними, якщо люди не розуміють або не дотримуються правил безпеки.

Products – апаратні та програмні засоби, які призначені для захисту інформаційних систем, даних та мереж від різних загроз і атак. Вони включають в себе включають різноманітні інструменти та технології, які допомагають виявляти, запобігати та реагувати на кіберзагрози.

Таким чином, (1) політики безпеки, (2) процеси безпеки, (3) поінформованість людей про безпеку та (4) оброблювані дані та/або системи, що використовуються, є чотирма основними критеріями оцінки рівня безпеки. [13]

Ці чотири критерії є складовими, і було б складно оцінити їх окремі значення без залучення експертів з безпеки чи автоматизованих інструментів. Тому чотири критерії діляться на дрібніші, що призводить до використання MAI. На основі MAI кожен критерій має бути поділений на дрібніші, при цьому критерії надалі будуть оцінними або неподільними.

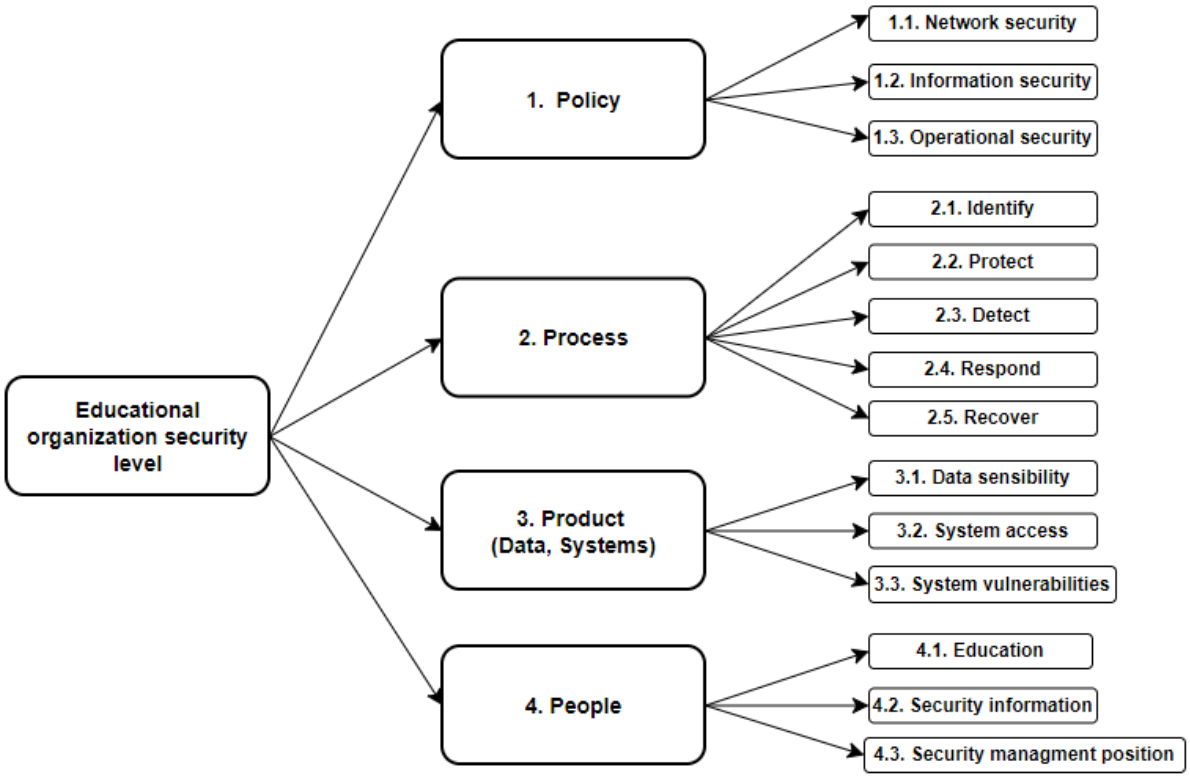

Рисунок 2.2 – Побудована деревоподібна структура критеріїв

Кібербезпека складається з кількох категорій: мережна безпека, безпека додатків, інформаційна безпека, операційна безпека, аварійне відновлення, навчання кінцевих користувачів. На основі цих категорій ми визначаємо безпекову політику як комбінацію політик кожної з цих категорій: (1.1) політика мережної безпеки, (1.2) політика безпеки додатків, (1.3) політика інформаційної безпеки. Освітня організація повинна мати всі ці політики і важливо досягти максимально можливого рівня зрілості. Встановлення політик безпеки не дає бажаного ефекту, якщо вони не повторюються, чітко не визначаються, не керуються та не оптимізуються для конкретної організації.

Та сама ідея рівня зрілості стосується процесів безпеки — важливо оптимізувати процеси безпеки, щоб підвищити рівень безпеки. Однак процеси безпеки можуть представляти різні етапи управління безпекою; тому критеріальні процеси безпеки поділяються на більш конкретні. Підкритерії визначаються на основі п’яти функцій безпеки, представлених NIST: (2.1) ідентифікація, (2.2) захист, (2.3) виявлення, (2.4) відповідь, (2.5) відновлення.

Останні тенденції підтверджують, що найслабшою ланкою безпеки підприємства є люди. Через цю тенденцію недостатньо мати політику навчання безпеки зацікавлених сторін; отже, модель повинна включати дані про те, наскільки зацікавлені сторони кваліфіковані у сфері безпеки. Таким чином, критерій обізнаності людей у сфері безпеки поділяється на чотири підкритерії: (3.1) наявність посад, відповідальних за безпеку в організації, (3.2) наявність системного навчання безпеки, (3.3) наявність обміну інформацією, пов’язаною з безпекою.

Критерії 3.1 не поділяються на більш дрібні, а решта два критерії поділені на підкатегорії, що представляють дві різні групи зацікавлених сторін: співробітників і студентів. Ці групи мають ще глибші категорії, де працівники поділяються на адміністрацію та викладацький склад. Тоді як студенти розподілені з урахуванням чутливих груп. Тому ми маємо дві підкатегорії для студентів: студенти та особи, пов’язані зі студентами (батьки, піклувальники тощо).

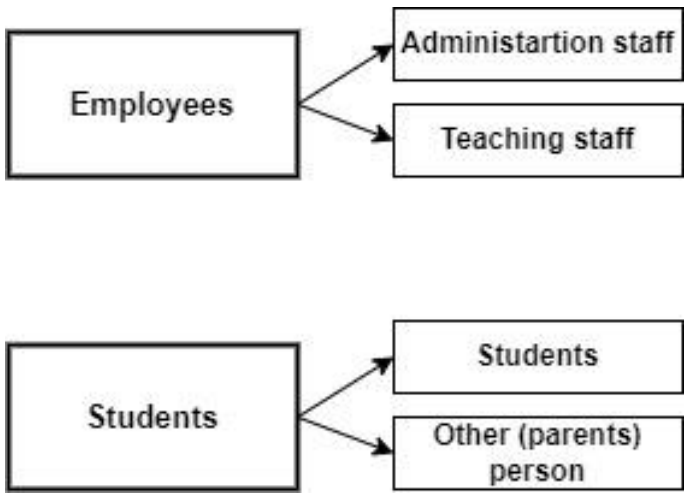

Рисунок 2.3 – Групи користувачі поділені на два абстрактних класи

Оброблені дані та/або використані системи є найбільш технічними критеріями верхнього рівня. Для відображення безпеки даних і системи використовуються чотири підкритерії: чутливість даних, доступ до системи, уразливості системи, відповідальність за управління інформаційними технологіями.

2.3 Коефіцієнт кореляції Пірсона

Коефіцієнт кореляції Пірсона є мірою сили лінійного зв'язку між двома змінними. Він вважається найбільш ефективним методом оцінки асоціацій, оскільки він ґрунтується на коваріації. Цей коефіцієнт показує не тільки величину кореляції, а й її напрям. [14]

Коефіцієнт кореляції Карла Пірсона найчастіше використовують, для того щоб отримати кількісну оцінку сили зв’язку. Він слугує оцінкою ступеня лінійності зв’язку між випадковими величинами.

Обчислюється коефіцієнт шляхом нормування коваріації змінних на добуток їх середньоквадратичних відхилень:

$$r = \frac{\sum(x-\overline{x})(y-\overline{y})}{\sqrt{\sum(x-\overline{x})^2 \sum(y-\overline{y})^2}} \qquad (2.1)$$

Де r – коефіцієнт кореляції;

x,y – оцінки пари експертів.

Коефіцієнт кореляції варіюється від +1 до -1, де 1 або -1 означає наявність сильного зв’язку, а 0 означає слабкий зв’язок або взагалі його відсутність.

Якщо коефіцієнт кореляції від’ємний, це означає наявність протилежного зв’язку, чим вище значення однієї змінної, тим нижче значення іншої, тобто зі збільшенням однієї величини друга величина має тенденцію до зменшення.

Якщо коефіцієнт кореляції близький до нуля, значить між величинами немає лінійного зв’язку, але не виключена наявність нелінійного.

Таблиця 2.1 - Значення сили кореляції

Сила кореляції	Коефіцієнт, r
Мала	від 0,1 до 0,3
Середня	від 0,3 до 0,5
Велика	від 0,5 до 1,0

2.4 Метод нормалізації значень критеріїв

При багатокритеріальному прийнятті рішень всі значення критеріїв повинні бути нормалізовані. Тому повинні бути представлені методи перетворення кожного значення критерію в числове значення в діапазоні [0, 1].

Для всіх підкритеріїв політики та процесу як значення використовується рівень зрілості. Рівень зрілості дозволяє оцінити, наскільки оптимізовані політика та процеси. Особливо це важливо, коли йдеться про модернізацію, розвиток, коли в організації має бути розроблений чіткий план управління змінами та суспільство ризику. Рівень зрілості дозволяє не вдаватися в дуже конкретні деталі організації; однак забезпечує основний рівень або політику та якість процесу в організації. Він може мати одне з шести значень (п’ять рівнів і одне значення, яке вказує на відсутність політики для цієї області).

Нормовані числові значення для кожного можливого значення представлені в Таблиці 1.1. Там кожному значенню присвоєно числове значення пропорційно від 0 до 1.

Таблиця 2.2 - Асоціація значення критерію з нормалізованим значенням для підкритеріїв критеріїв верхнього рівня політики та процесу.

Критерій/Значення	**Опис**	**Нормалізоване значення**
Ніякої політики/процесу не існує	В організації немає такої політики/процесу	0.0
Рівень зрілості: початковий	Хаотичний, погано контрольований, реактивний	0.2
Рівень зрілості: керований	Планується, виконується, вимірюється та контролюється, але все ще реактивний	0.4
Рівень зрілості: визначений	Добре охарактеризовані та зрозумілі, описані в стандартах процедури, інструменти та методи є активними	0.6
Рівень зрілості: кількісно керований	Встановлюються кількісні цілі щодо якості та ефективності, які використовуються як критерії.	0.8
Рівень зрілості: оптимізація	Цілі кількісного вдосконалення встановлюються, постійно переглядаються, щоб відобразити мінливі цілі, і використовуються як критерії управління покращенням.	1.0

Найширша різноманітність методів нормалізації необхідна для критеріїв «оброблені дані та/або використані системи». У більшості випадків значення класифікуються і повинні бути перетворені в числові значення. Таблиці для переведення значення критерію в нормоване значення наведено в Таблиці 2.3, Таблиці 2.4, Таблиці 2.5. Кожен з них генерується за допомогою того самого методу — усі значення перераховуються, а пропорційні значення від 0 до 1 призначаються кожному з можливих значень критерію.

Таблиця 2.3 - Асоціація значення критерію з нормалізованим значенням для чутливості даних підкритерію.

Критерій/Значення	Опис	Нормалізоване значення
Дані не зберігаються	Жодні дані не зберігаються та не використовуються в проаналізованій категорії.	1.0
Збережені дані є нечутливими	Жодна секретна чи особиста інформація не зберігається та не використовується, оскільки зберігаються та використовуються лише неконфіденційні дані (конфіденційні дані анонімні та не піддаються відстеженню).	0.5
Зберігаються конфіденційні особисті дані	Зберігаються або використовуються дані, пов’язані з особистими даними осіб, медичними записами, даними приватних організацій або іншими конфіденційними даними.	0.0

Таблиця 2.4 - Асоціація значення критерію з нормалізованим значенням для підкритерію доступу до системи.

Критерій/Значення	Опис	Нормалізоване значення
Глобально загальнодоступний	Система доступна в Інтернеті та індексується пошуковими системами.	0.00
Таємно у відкритому доступі	Система доступна в Інтернеті, але є недоступна для індексування, використовує IP-адресу, а не доменне ім’я.	0.25
Доступно тільки локально	Система доступна тільки в локальній мережі.	0.50

Кінець таблиці 2.4

Доступно локально через VPN	Система доступна лише за допомогою віртуальної приватної мережі.	0.75
Недоступний	Система вимкнена або до неї немає доступу в мережі.	1.00

Таблиця 2.5 - Асоціація значення критерію з нормалізованим значенням для підкритерію відповідальності за управління інформаційними технологіями

Критерій/Значення	Опис	Нормалізоване значення
Власник	Організація володіє інфраструктурою/системою та несе за неї повну відповідальність.	0.00
Контролер	Організація має всі права управління інфраструктурою/системою, але не володіє нею.	0.33
Процесор	Організація має обмежені права використання, не маючи можливості повністю ним керувати.	0.66
Не використовується	Інфраструктура/система не використовується в організації	1.00

2.5 Оцінка важливості критеріїв

Хоча всі можливі значення критеріїв оцінюються і нормалізуються на основі деякої теоретичної основи, оцінка важливості критеріїв має емпіричну основу. Для оцінки важливості критеріїв було залучено 5 експертів по управлінню безпекою (A, B, C, D, E). Всі п’ять спеціалістів мають рівень не нижче магістра кібербезпеки і за своєю професійною діяльністю на даний час тісно пов’язані з IT.

За думкою Т.Л. Сааті [15], при використанні метода MAI достатньо одного судді-експерта. Однак, щоб оцінити подібність думок експертів з думкою більш ширшого кругу експертів з ризиків безпеки, в цей процес були включені всі дані

експерти. Через брак часу і вимог до компетентності експертів було обрано тільки п’ять експертів. Вимога полягала в тому, щоб мати рівень не нижче магістра з кібербезпеки і в теперішній час працювати у сфері пов’язаною з управління безпекою.

Всі експерти заповнили представлену форму опитувальника, в якому вони оцінили кожен критерій.

Вагові коефіцієнти для вирахування впливу кожного з експертів вираховуються за формулою:

$$w_i = \frac{k_i}{\sum k_i} \tag{2.2}$$

Де w_i – ваговий коефіцієнт;

k_i – коефіцієнт кореляції і – го експерта.

2.6 Метод аналізу ієрархій

Analytic Hierarchy Process (AHP) - метод аналізу ієрархій (MAI) є широко вживаним методом для вирішення багатокритеріальних задач. MAI являє собою математичний інструмент системного підходу до складних проблем прийняття рішень, розроблений американським математиком Томасом Сааті.

MAI — це математичний метод, який можна використовувати для визначення ваги критерію шляхом попарного порівняння відносної важливості двох критеріїв. [16]

Процес прийняття рішень у MAI поєднує психологічні аспекти та математичні методи. Альтернативи оцінюються експертами на основі їхнього розуміння проблеми, після чого отримана інформація структурується та аналізується за допомогою математичного апарату.

Метод аналітичної ієрархії базується на принципах декомпозиції та синтезу, що дозволяє зменшити кількість можливих помилок при отриманні інформації від експерта. Цей метод дає змогу перевірити узгодженість висловлювань експерта. Використовуючи MAI, створюється ієрархічна структура, яка замінює складні порівняння попарними порівняннями, завдяки використанню матриць попарного порівняння.

Процес аналітичної ієрархії (AHP): огляд із п’яти кроків [17]:

1. Структуризація ієрархії

   Перший крок AHP - організувати основні компоненти вашої проблеми прийняття рішень в ієрархію, що складається щонайменше з трьох рівнів.
2. Попарне порівняння критеріїв

   Другий крок AHP – оцінити відносну важливість ваших критеріїв та підкритеріїв. Ця оцінка проводиться у вигляді серії парних порівнянь критеріїв.
3. Розрахунок ваги критеріїв

   Ваги критеріїв, що відображають їхню відносну важливість, виводяться з коефіцієнтів переваг, отриманих на попередньому етапі за допомогою обчислень.
4. Оцінка альтернатив

   Визначивши ваги критеріїв, четвертий крок AHP — оцінити альтернативи, які розглядаються за цими критеріями.
5. Об'єднання ваги і балів, щоб ранжувати альтернативи.

   Останній крок AHP включає об'єднання ваг критеріїв з кроку 3 з оцінками альтернатив з кроку 5 шляхом їх множення і підсумовування для отримання загального балу для кожної альтернативи, за яким їх можна ранжувати.

   Таким чином, як і більшість методів багатокритеріального аналізу рішень (MCDA), AHP базується на моделях виваженої суми, також відомих в

академічній літературі як адитивні «багатокритеріальні моделі значень» або «багатоатрибутні моделі значень».

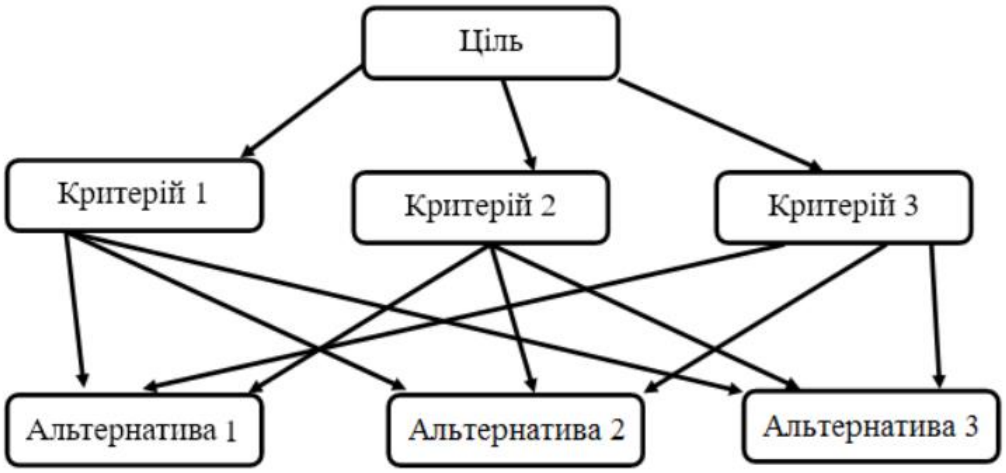

Рисунок 2.4 – Структура методу аналізу ієрархій

Теоретично доказано, що метод аналізу ієрархій дозволяє спростити процес прийняття складних рішень на основі різноманітної та неструктурованої інформації. Визначено, що велике значення має правильна постановка задачі у процесі застосування MAI, завдання початкових, граничних умов, підбір експертів та вибір критеріїв.

Висновки до розділу 2

В даному розділі було описано метод кількісної оцінки рівня безпеки та проведено огляд моделі оцінки рівня захисту. Розглянуто метод MCDA, а саме метод аналізу ієрархій. Також було розглянуто метод узгодженості, а точніше коефіцієнт кореляції Пірсона, метод нормалізації значень критеріїв та оцінку важливості критеріїв.

Було розроблено набір критеріїв для оцінки рівня безпеки освітньої організації та описані всі методи для подальшої роботи над оцінкою.

3 ОЦІНКА РІВНЯ КІБЕРБЕЗПЕКИ УНІВЕРСИТЕТУ

3.1 Створення опитувальника

Першим кроком підготовки до оцінки рівня кібербезпеки університету було створено опитувальник для множини експертів. Він складається з питань розбитих на чотири розділи, що відповідають чотирьом критеріям P(Policies, Processes, People, Products).

Таблиця 3.1 – Опитувальник

1. Політика безпеки	
Підкритерій	Оцінка
1.1 Оцініть за вказаною шкалою рівень безпеки мережі університету.	
1.2 Оцініть за вказаною шкалою рівень інформаційної безпеки університету.	
1.3 Оцініть за вказаною шкалою рівень операційної безпеки університету.	
2. Безпека процесів	
2.1 Оцініть за вказаною шкалою рівень надійності ідентифікації користувачів.	
2.2 Оцініть за вказаною шкалою рівень захисту даних.	
2.3 Оцініть за вказаною шкалою рівень виявлення вразливостей.	
2.4 Оцініть за вказаною шкалою рівень відповіді на вразливість.	
2.5 Оцініть за вказаною шкалою час відновлення системи після вразливості.	
3. Захист даних	
3.1 Оцініть за вказаною шкалою наявність посад, відповідальних за безпеку.	
3.2 Оцініть за вказаною шкалою наявність системного навчання безпеки.	
3.3 Оцініть за вказаною шкалою існування обміну інформацією, пов’язаною з безпекою.	
3.4 Оцініть за вказаною шкалою існування проведення навчання з безпеки студентам раз у рік.	

Кінець таблиці 3.1

3.5 Оцініть за вказаною шкалою існування проведення навчання безпеки батькам раз у рік.	
3.6 Оцініть за вказаною шкалою існування проведення навчання безпеки викладачам раз у рік.	
3.7 Оцініть за вказаною шкалою наявність отримання інформації, пов'язаної з безпекою, викладачами, студентами та їх батьками.	
3.8 Оцініть за вказаною шкалою чи можуть викладачі, студенти та їх батьки повідомити про проблеми пов'язані з безпекою.	
4. Компетентність людей	
4.1 Оцініть за вказаною шкалою рівень чутливості даних.	
4.2 Оцініть за вказаною шкалою рівень доступу до систем університету.	
4.3 Оцініть за вказаною шкалою рівень відповідальності за управління інформаційними технологіями.	

Кожному експерту пропонувалось на засадах анонімності виставити свою оцінку за певною шкалою, а саме за шкалою Сааті від 1 до 10.

Наступним етапом відбувався підбір експертів та їхнє анкетування. Провести анкетування погодилось 5 експертів, причому було усвідомлення, що рівень їх компетентності різний, хоча всі вони були рівня не нижче магістра кібербезпеки і за своєю професійною діяльністю пов'язані з ІТ.

Нижче наведено оцінки, які надав кожен експерт:

Таблиця 3.2 – Оцінки експертів

Підкритерій	**Експерт**				
	A	**B**	**C**	**D**	**E**
1.1	7	7	4	7	7
1.2	6	7	8	8	6
1.3	6	7	4	8	7
2.1	8	8	2	6	6
2.2	6	6	4	7	6
2.3	8	6	4	8	5
2.4	7	5	5	7	6
2.5	5	5	4	7	6
3.1	9	5	4	9	4
3.2	6	6	3	9	4
3.3	5	6	3	7	5

Кінець таблиці 3.2

3.4	0	5	3	9	4
3.5	0	3	3	3	3
3.6	0	4	4	9	5
3.7	2	4	4	9	5
3.8	10	5	3	7	5
4.1	7	8	3	8	7
4.2	9	7	6	8	6
4.3	9	7	5	7	6

3.2 Узгодженість експертних даних

Оскільки рівень компетентності експертів різний виникла потреба в оцінці узгодженості і перевірки рівня довіри до оцінок.

В основу оцінки узгодженості була покладена гіпотеза про опорного експерта, тобто того, чия оцінка викликає найбільшу довіру. А далі були проведені оцінки попарного порівняння оцінок опорного експерта з кожним іншим з чотирьох, що залишились. Це порівняння робилося шляхом розрахунку коефіцієнта кореляції Пірсона.

Було визначено, що якщо значення коефіцієнта кореляції не перевищує 0,3, то дані такого експерта не узгоджуються та не враховуються у подальшому аналізі. У Таблиці 3.3 та на Рисунку 3.1, Рисунку 3.2, Рисунку 3.3, Рисунку 3.4 показані результати даних відповідних розрахунків.

Таблиця 3.3 – Узгодженість експертних даних

Експерт- експерт	Коефіцієнт кореляції
A-B	0,627706
A-C	0,184899
A-D	0,050603
A-E	0,450472

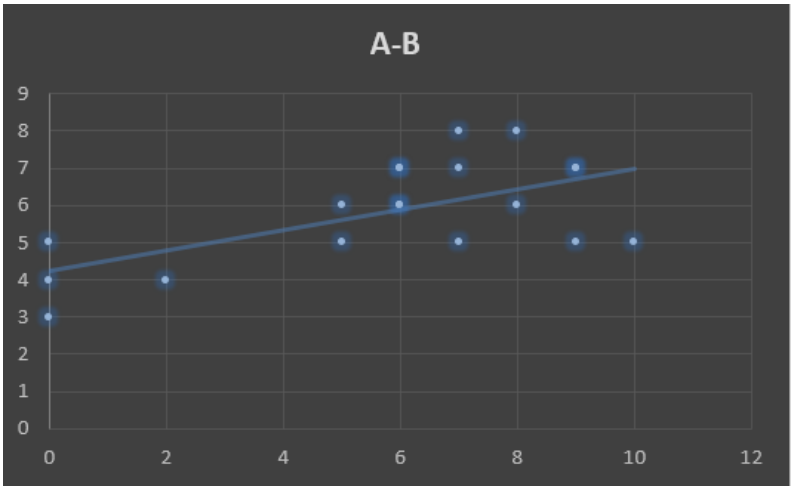

Рисунок 3.1 – Коефіцієнт кореляції експертів A-B

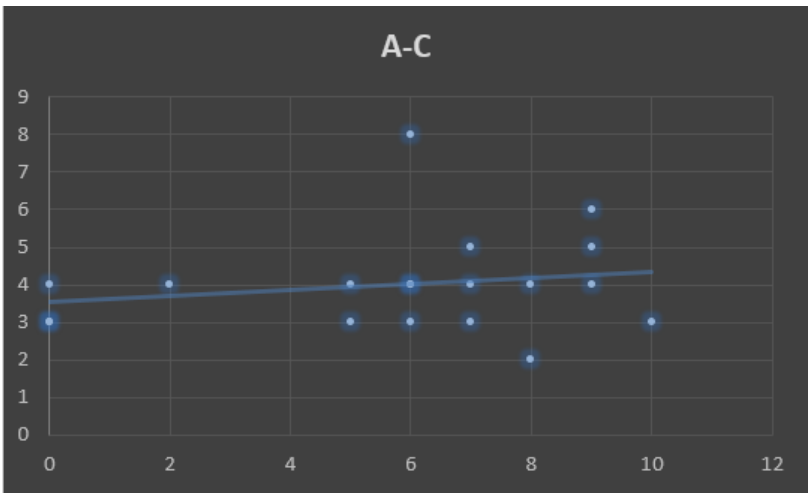

Рисунок 3.2 – Коефіцієнт кореляції експертів A-C

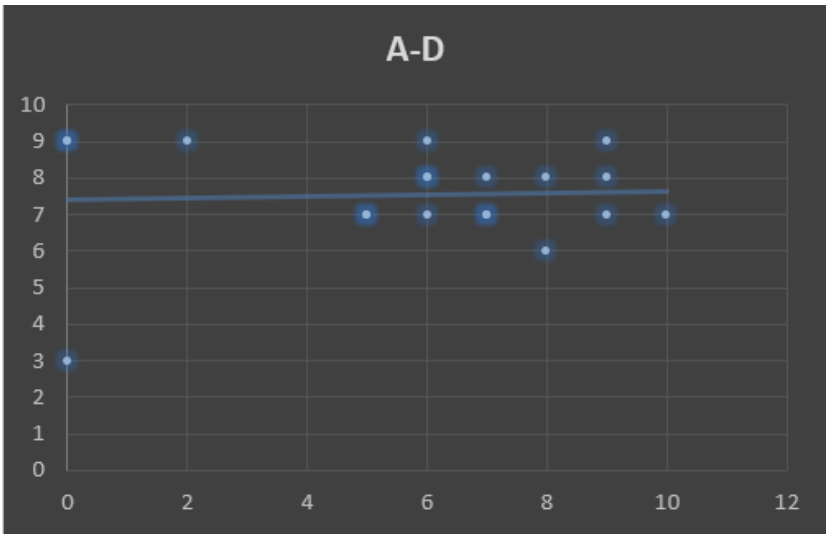

Рисунок 3.3 – Коефіцієнт кореляції експертів A-D

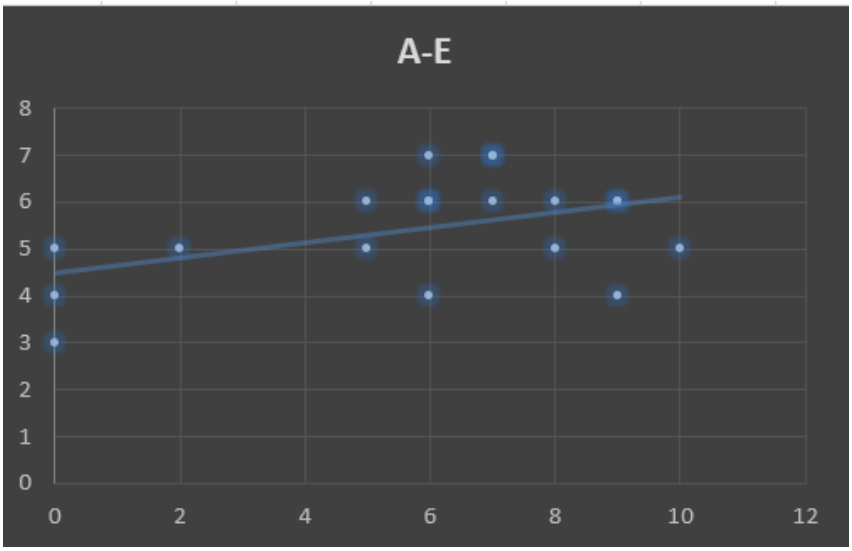

Рисунок 3.4 – Коефіцієнт кореляції експертів A-E

Як видно з таблиці та рисунків дані експертів C та D не узгоджені, тобто не перевищують значення 0,3 , і у подальшій оцінці не враховуються.

3.3 Нормалізація значень критеріїв

Мета нормалізації даних полягає в тому, щоб перевести величини з різними розмірами в ту саму безрозмірну форму. Метод багатокритеріального прийняття рішень (MCDM), вимагає визначення ваги для кожного критерію, тому нормалізація даних повинна бути виконана.

Оскільки експерти C та D не узгоджені, нормалізація відбуватиметься між експертами A, B, E.

Щоб нормалізувати значення набору даних між 0 і 1, буде використана формула:

$$z_i = \frac{(x_i - \min(x))}{\max(x) - \min(x)} \qquad (3.1)$$

Таблиця 3.4 – Оцінки експертів A,B,E

	A	B	E
Policy	7	7	7
	6	7	6
	6	7	7
Process	8	8	6
	6	6	6
	8	6	5
	7	5	6
	5	5	6
Products	9	5	4
	6	6	4
	5	6	5
	0	5	4
	0	3	3
	0	4	5
	2	4	5
	10	5	5
People	7	8	7
	9	7	6
	9	7	6

Таблиця 3.5 – Нормалізовані оцінки експертів A,B,E

	A	B	E
Policy	0	0	0
	0	1	0
	0	1	1
Process	1	1	0
	0	0	0
	1	0,33	0
	1	0	0,5
	0	0	1

Кінець таблиці 3.5

Products	1	0,2	0
	1	1	0
	0	1	0
	0	1	0,8
	0	1	1
	0	0,8	1
	0	0,67	1
	1	0	0
People	0	1	0
	1	0,33	0
	1	0,33	0

3.4 Оцінка рівня кібербезпеки університету

1. Для початку потрібно зважити експертів. Оскільки вагові коефіцієнти в сумі мають давати 1, тоді експерт А буде мати коефіцієнт важливості 0,5 , оскільки він є опорним, експерт В буде мати коефіцієнт важливості 0,3 і експерт Е – 0,2.

2. Тепер потрібно отримати середньозваженого експерта. Для кожного з чотирьох Р, для кожного його показника, кожного підкритерія потрібно порахувати середньозважений показник за формулою:

$$C_{ij} = \sum_{i=1}^{N} w_i \cdot C_{ij} \qquad (3.3)$$

Де w_i – ваговий коефіцієнт;

і – й критерій, j – підкритерій в і-му критерії.

$$C_{ij} = 0{,}5 \cdot A_i + 0.3 \cdot B_i + 0.2 \cdot E_i \qquad (3.4)$$

Таблиця 3.6 – Середньозважений показник P

	Середньозважений показник P
Policy	0
	0,3
	0,5
Process	0,8
	0
	0,60
	0,6
	0,2
Products	0,56
	0,8
	0,3
	0,46
	0,5
	0,44
	0,40
	0,5
People	0,3
	0,60
	0,60

3. Далі необхідно зважити важливість чотирьох P. Найважливішим з цих чотирьох P є People, тому цей критерій матиме коефіцієнт 0,35 , Process – 0,25 , Products – 0,2 і Policy – 0,2. Щоб порахувати важливість кожного критерія необхідно додати оцінку всіх експертів кожного з підкритеріїв кожного критерію і помножити на вагу критерію.

Таблиця 3.7 – Важливість кожного P

	A	B	E	Sum P	Ваги P	Важливість критерію P
Policy	0	0	0	3	0,2	0,6
	0	1	0			
	0	1	1			
Process	1	1	0	5,83	0,25	1,46
	0	0	0			
	1	0,33	0			
	1	0	0,5			
	0	0	1			

Кінець таблиці 3.7

Products	1	0,2	0	12,47	0,2	2,49
	1	1	0			
	0	1	0			
	0	1	0,8			
	0	1	1			
	0	0,8	1			
	0	0,67	1			
	1	0	0			
People	0	1	0	3,66	0,35	1,28
	1	0,33	0			
	1	0,33	0			

4. Отримано одного середньозваженого експерта і зважені критерії. На основі цих даних можна рахувати оцінку. Найпростіше це отримати суму всіх без винятку балів і поділити на суму максимальних оцінок. Але це занадто груба оцінка.

   Тому, для обрахунку оцінки рівня кібербезпеки, потрібно порахувати суму середньозваженого експерта по кожному критерію помножити на його ваговий коефіцієнт, всіх їх додати та поділити на максимальний бал.

Таблиця 3.8 – Сума середньозваженого експерта по кожному P помножена на вагу кожного P

	A	B	E	Середньозважений показник/експерт	Sum середньозваженого експерта по кожному P	S - Sum середньозваженого експерта по кожному P помножена на вагу P
Policy	0	0	0	0	0,8	0,16
	0	1	0	0,3		
	0	1	1	0,5		
Process	1	1	0	0,8	2,20	0,55
	0	0	0	0		
	1	0,33	0	0,60		
	1	0	0,5	0,6		
	0	0	1	0,2		

Кінець таблиці 3.8

Products	1	0,2	0	0,56	3,96	0,79
	1	1	0	0,8		
	0	1	0	0,3		
	0	1	0,8	0,46		
	0	1	1	0,5		
	0	0,8	1	0,44		
	0	0,67	1	0,40		
	1	0	0	0,5		
People	0	1	0	0,3	1,50	0,52
	1	0,33	0	0,60		
	1	0,33	0	0,60		
						2,03

Отже, отримано суму середньозваженого експерта по кожному P і помножена на вагу кожного P, тоді середньозважену оцінку рівня кібербезпеки закладу вищої освіти можна отримати з виразу:

$$ES = \sum_{i=1}^{4} \sum_{l=1}^{M} v_i \cdot C_{il} \quad (3.5)$$

Де ES – оцінка рівня кібербезпеки закладу вищої освіти;

$$ES = 0.20 \quad (3.6)$$

Висновки до розділу 3

У цьому розділі було проведено оцінку рівня кібербезпеки університету.

Було створено опитувальник для множини експертів. На основі якого відбувалась подальша робота з оцінками експертів. Збір даних експертів про важливість критеріїв освітньої організації показав, що за необхідності застосування великої кількості критеріїв може виникнути деяка неузгодженість. Люди – експерти не завжди здатні врахувати всі фактори і послідовно представити їх відносну значимість. Тому для отримання більш точного заключення експертів було проведено узгодженість експертів.

За допомогою коефіцієнту кореляції Пірсона було узгоджено експертів на основі опорного експерта та відсіяно експертів, які не відповідають цій узгодженості. Було нормалізовано значення оцінок. Як результат, на основі різних перетворень було отримано оцінку рівня кібербезпеки університету.

ВИСНОВКИ

Дипломну роботу було виконано з метою створення моделі оцінки рівня кібербезпеки освітньої організації та проведення оцінки рівня кібербезпеки.

Проведений аналіз літератури показав, що кожне направлення має свою специфіку оцінки рівня безпеки. Таким чином, спільні моделі оцінки ризиків потребують знань в області безпеки. Між цим, існуючи моделі оцінки рівня безпеки освітніх організацій орієнтовані на технічні аспекти і не приділяють уваги управлінню безпекою. Таким чином, в цілому модель безпеки освітньої організації була б корисна для спрощення моделювання безпеки.

В ході роботи написання дипломної роботи було проведено аналіз літератури, ознайомлено з такими поняттями як ризик та кіберризик, оглянуто проблеми кіберризиків в організація та освітніх установах, побудовано модель оцінки рівня безпеки та розроблено набір критеріїв оцінки рівня безпеки освітньої організації, створено опитувальник та проведено опитування експертів з безпеки, на основі цих даних було проведено оцінку рівня кібербезпеки університету.

Можна прийти до такого висновку, що отримана оцінка рівня захисту університету досить низька. Це потребує додаткових досліджень з використанням більш сучасних та вартісних застосунків.

Дана модель оцінки рівня безпеки являється універсальною і має перевагу в тому, що може бути використана освітніми організаціями для розрахунку власного рівня безпеки.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Аналіз ризиків та вразливостей населення України до надзвичайних ситуацій [Електронний ресурс] - Режим доступу до ресурсу: https://ekmair.ukma.edu.ua/server/api/core/bitstreams/5c4890d0-9b75-4b02-95ac-2b4cdbb64b15/content
2. Управління ризиками [Електронний ресурс] - Режим доступу до ресурсу: https://ep3.nuwm.edu.ua/12301/1/Управління%20ризиками_навчальний%20посібник.pdf
3. Архипов О.Є ВСТУП ДО ТЕОРІЇ РИЗИКІВ:НФОРМАЦІЙНІ РИЗИКИ [Електронний ресурс] - Режим доступу до ресурсу: https://drive.google.com/file/d/1YyY2JE6SmFPpEEdWBB9MZZR4sPFqXNgn/view
4. Страхування кіберризиків підприємств в умовах інтернету речей [Електронний ресурс] - Режим доступу до ресурсу: https://kon-insurance.mnau.edu.ua/files/work_2019/20.pdf
5. What is Cyber Risk? [Електронний ресурс] - Режим доступу до ресурсу: https://cyber-risk.com.au/
6. What is Cyber Risk? [Електронний ресурс] - Режим доступу до ресурсу: https://hyperproof.io/resource/what-is-cyber-risk/
7. КІБЕР-РИЗИКИ ЯК ОДИН ІЗ ВИДІВ СУЧАСНИХ РИЗИКІВ У ДІЯЛЬНОСТІ МАЛОГО ТА СЕРЕДНЬОГО БІЗНЕСУ ТА УПРАВЛІННЯ НИМИ [Електронний ресурс] - Режим доступу до ресурсу: http://www.easterneurope ebm.in.ua/journal/16_2018/21.pdf
8. Top 10 Cybersecurity Predictions And Statistics For 2024 [Електронний ресурс] - Режим доступу до ресурсу: https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2021-to-2025/
9. Global threat activity [Електронний ресурс] - Режим доступу до ресурсу: https://www.microsoft.com/en-us/wdsi/threats

10. Check Point Software Technologies [Електронний ресурс] - Режим доступу до ресурсу: https://www.infosec.com.tr/en/check-point-research/
11. КІБЕРРИЗИКИ В ОСВІТНЬОМУ СЕКТОРІ [Електронний ресурс] - Режим доступу до ресурсу: https://dspace.onua.edu.ua/server/api/core/bitstreams/cefb6943-2f0c-484b-a1a5-451b0c139046/content
12. Політика безпеки [Електронний ресурс] - Режим доступу до ресурсу: https://wiki.tntu.edu.ua/Політика_безпеки
13. Educational Organization's Security Level Estimation Model [Електронний ресурс] - Режим доступу до ресурсу: https://www.mdpi.com/2076-3417/11/17/8061
14. Pearson's Correlation Coefficient: A Comprehensive Overview [Електронний ресурс] - Режим доступу до ресурсу: https://www.statisticssolutions.com/free-resources/directory-of-statistical-analyses/pearsons-correlation-coefficient/
15. How Many Judges Should There Be in a Group ? [Електронний ресурс] - Режим доступу до ресурсу: https://www.researchgate.net/publication/270891405_How_Many_Judges_Should_There_Be_in_a_Group
16. Analytical Hierarchy Process [Електронний ресурс] - Режим доступу до ресурсу: https://www.sciencedirect.com/topics/social-sciences/analytical-hierarchy-process
17. Analytic-hierarchy-process-ahp-a-five-step-overview [Електронний ресурс] - Режим доступу до ресурсу: https://www.1000minds.com/decision-making/analytic-hierarchy-process-ahp#analytic-hierarchy-process-ahp-a-five-step-overview