МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ПОЛІСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет інформаційних технологій,
обліку та фінансів
Кафедра комп'ютерних технологій
і моделювання систем

Кваліфікаційна робота
на правах рукопису

Дубовий Владислав Ігорович

УДК 004.056:004.42

КВАЛІФІКАЦІЙНА РОБОТА

ДОСЛІДЖЕННЯ ВЗАЄМОЗВ'ЯЗКУ МІЖ ЦИФРОВОЮ ГРАМОТНІСТЮ ТА КІБРЕБЕЗПЕКОЮ СУСПІЛЬСТВА

125 «Кібербезпека та захист інформації»

Подається на здобуття освітнього ступеня магістр

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

_____
(підпис, ініціали та прізвище здобувача вищої освіти)

Керівник роботи:
Євсеєв Сергій Петрович,
доктор технічних наук, професор

Житомир – 2024

Висновок кафедри_____

за результатами попереднього захисту:_____

Протокол засідання кафедри_____

№ ____ від «_____» _____ 20____ р.

Завідувач кафедри_____

_____ _____ _____

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

«_____» _____ 20____ р.

Результати захисту кваліфікаційної роботи

Здобувач вищої освіти _____ захистив (ла)

(прізвище ,ім'я, по батькові)

кваліфікаційну роботу з оцінкою:

сума балів за 100-бальною шкалою _____

за шкалою ECT8 _____

за національною шкалою _____

Секретар ЕК

_____ _____ _____

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

АНОТАЦІЯ

Дубовий В.І. Дослідження взаємозв’язку між цифровою грамотністю та кібербезпекою суспільства. – Кваліфікаційна робота на правах рукопису.

Кваліфікаційна робота на здобуття освітнього ступеня магістр за спеціальністю 125 – Кібербезпека та захист інформації. – Поліський національний університет, Житомир, 2024.

У роботі досліджено взаємозв’язок між цифровою грамотністю та кібербезпекою суспільства, визначено основні принципи цифрової грамотності. Проведено аналіз кіберзагроз та встановлено найбільш ціні типи інформації для зловмисників. Проаналізовано результати показників рівня кіберебезпеки, такі як DDLI та NCSI. Наведено приклади існуючих способів щодо підвищення та покращення рівня цифрової грамотності та кібербезпеки суспільства, сформовано рекомендації щодо покращення рівня кібербезпеки суспільства в Україні та підняття цифрової гармотності населення.

Отримані результати можуть бути використані для формування державних політик, спрямованих на підвищення кібербезпеки на національному рівні, а також для розробки конкретних програм та інструментів, що дозволяють зменшити вразливість до кіберзагроз.

Робота містить сторінок, 10 рисунків, 10 таблиць, 41 літературних джерел.

Ключові слова: кібербезпека, цифрова грамотність, кіберстійкість, цифровий розвиток.

SUMMARY

Dubovyi V.I. Research on the Relationship Between Digital Literacy and Society's Cybersecurity and Information Protection. – Qualification Thesis in Manuscript Form. Qualification thesis for the Master’s degree in specialty 125 – Cybersecurity. – Polissya National University, Zhytomyr, 2024.

The study explores the relationship between digital literacy and society's cybersecurity and identifies the key principles of digital literacy. An analysis of cyber threats is conducted, and the most valuable types of information for cybercriminals are determined. The study also examines cybersecurity performance indicators, such as DDLI and NCSI. Examples of existing methods for improving and enhancing the levels of digital literacy and cybersecurity in society are provided, along with recommendations for improving the state of cybersecurity in Ukraine and increasing the digital literacy of the population.

The obtained results can be used for developing national policies aimed at strengthening cybersecurity at the national level, as well as creating specific programs and tools to reduce vulnerability to cyber threats.

The thesis contains pages, 10 figures, 10 tables, and 41 references.

Keywords: cybersecurity, digital literacy, cyber resilience, digital development.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ДПП - державно-приватного партнерства

ЗМІ - засоби масової інформації

ІТ - інформаційна технологія

КБ - кібербезпека

ПЗ - програмне забезпечення

ПК - персональний комп’ютер

ШІ - штучний інтелект

ABI - Allied Business Intelligence

CISO - Chief Information Security Officer (Керівник із питань інформаційної безпеки)

CSA - Cyber Security Agency (Агентство кібербезпеки)

DBSCAN - Density-Based Spatial Clustering of Applications with Noise

DQ - коефіцієнта цифрового інтелекту

GCI - Global Cybersecurity Index (Глобальний індекс кібербезпеки)

GDPI - Global Data Protection Index (Глобальний індекс захисту даних)

ISO - International Organization for Standardization (Міжнародна організація зі стандартизації)

ITU - International Telecommunication Union (Міжнародний союз електрозв’язку)

ML - Machine learning (машинне навчання)

NCS - Національна стратегія кібербезпеки

NCSI - National Cybersecurity Index (Національний індекс кібербезпеки)

ВСТУП

Актуальність теми дослідження. Цифрова грамотність та кібербезпека є двома взаємопов’язаними аспектами, які безпосередньо впливають на здатність суспільства ефективно функціонувати в сучасному цифровому середовищі. Зі зростанням обсягів інформації та складності інформаційних систем, а також із постійними змінами у технологіях, країни та їх громадяни повинні мати необхідні знання та навички для захисту своїх особистих даних, а також для реагування на кіберзагрози.

Цифрова грамотність включає в себе здатність не лише використовувати технології, а й усвідомлено й відповідально взаємодіяти з ними, розуміти потенційні ризики та наслідки таких взаємодій. Натомість, високий рівень кібербезпеки передбачає, що користувачі, зокрема, здатні забезпечити захист своїх пристроїв і особистої інформації від зловмисних атак, а також розуміють основи конфіденційності та етики цифрового середовища.

Однією з основних проблем є недостатній рівень цифрової грамотності серед широких верств населення, що збільшує вразливість до кіберзагроз. Це включає в себе відсутність базових знань про захист персональних даних, вміння розпізнавати фішингові атаки, а також нерозуміння основних принципів безпеки в Інтернеті. Відсутність системної освіти в цій сфері може призвести до негативних наслідків, таких як витоки даних, фінансові збитки та інші форми кіберзлочинності.

Важливою складовою проблеми є також швидкий розвиток технологій, що вимагає постійної адаптації знань користувачів до нових умов. Зміни в алгоритмах, програмному забезпеченні, а також нові методи атак можуть створювати додаткові складнощі в забезпеченні кібербезпеки. Незважаючи на значний прогрес у розвитку технологій кібербезпеки, відсутність належної цифрової освіти серед широкого кола користувачів залишається одним з основних факторів, що ускладнює реалізацію ефективних механізмів захисту. Тому дослідження взаємозв’язку між цифровою грамотністю та кібербезпекою є надзвичайно актуальним, оскільки

підвищення рівня цифрових навичок населення є важливим кроком у зменшенні вразливості до кіберзагроз

Наукова новизна. Удосконалено модель взаємозв'язку між рівнем цифрової грамотності та кібербезпекою суспільства шляхом розробки нових підходів до оцінки її впливу в умовах сучасних глобальних і національних викликів.

Мета і завдання дослідження. Визначити взаємозв'язок між рівнем цифрової грамотності та кібербезпекою суспільства, а також розробити практичні рекомендації для підвищення рівня захищеності населення в умовах цифровізації. Зазначена мета досягається шляхом вирішення наступних завдань дослідження:

1. Дослідити сутність поняття цифрової грамотності, її компоненти та характеристики.
2. Провести аналіз тенденцій кіберзлочинності з урахуванням ролі цифрової грамотності.
3. Розробити практичні рекомендації щодо підвищення кібербезпеки в Україні через вдосконалення цифрової грамотності населення.
4. Дослідити взаємозв'язок між цифровою грамотністю та кібербезпекою суспільства

Об'єкт дослідження: процес взаємодії між цифровою грамостістю та кібербезпекою

Предмет дослідження: методи дослідження взаємозв'язоку між рівнем цифрової грамотності населення та станом кібербезпеки суспільства.

Структура роботи. Робота містить: вступ, 3 розділи, висновки, список використаних джерел літератури, додатки.

За темою кваліфікаційної роботи опубліковано наукові публікації, а саме:

- Дубовий В. І. . Критичне мислення та пам'ять : збірник праць учасників наукового журналу Advanced Top Technology, 2024. 90 с.

- Дубовий В. І. . Цифрова грамотність як ключ до кібербезпеки у сучасному просторі: збірник матеріалів Міжнародної науково-практичної конференції. Випуск XI / 2024. 1515 с.

- Дубовий В. І. . Взаємозв’язок цифрової грамотності та кібербезпеки як основа як основа безпечного розвитку суспільства: збірник матеріалів Міжнародної науково-практичної конференції. Випуск V / 2024. 974с.

РОЗДІЛ 1. ОГЛЯД ЛІТЕРАТУРИ

1.1 Цифрова грамотність: визначення сутності поняття, компоненти та характеристики

Активне проникнення цифрових технологій в усі сфери життєдіяльності суспільства призвело до необхідності законодавчого регулювання їх упровадження та використання. Так, у 2024 році з'явилася «Національна галузева програма проєкту, робіт з інформатизації України», концепція якої передбачає кардинальну модернізацію всіх видів виробництва, перехід до цифрових технологій, активне впровадження новітніх науково-технічних розробок [1]. Це означає, що вже зараз існує потреба у кваліфікованих кадрах на всіх рівнях господарської, виробничої, наукової діяльності, готових до життя в цифровому суспільстві, здатних гармонійно й успішно існувати в умовах нової реальності, створювати й трансформувати її.

Уряд України наголошує на необхідності впровадження цифрових технологій у практику освітньої діяльності, що відображено у Законі України «Про стимулювання розвитку цифрової економіки в Україні» [2] та Проєкті Концепції цифрової трансформації освіти і науки на період до 2026 року [3] на основі Стратегії цифрового розвитку 2030 [4]; Законі України «Про цифровий контент та цифрові послуги» [5]; Положенняі про електронні освітні ресурси [6]; Положенні про Національну освітню електронну платформу [7].

Уперше визначення поняття «цифрова грамотність» ми знаходимо в праці П. Ґілстера, опублікованій у 1997 р., у якій автор трактує це поняття як здатність розуміти та використовувати інформацію, надану в безлічі форматів із широкого спектра джерел за допомогою комп'ютерів [8].

Первісне визначення цифрової грамотності потребувало деякої актуалізації, що і було зроблено у 2015 році, в рамках проєкту «Індекс цифрової грамотності», який свідчив, що цифрова грамотність - це набір знань і вмінь, які необхідні для безпечного та ефективного використання цифрових технологій і ресурсів

Інтернету, що включає в себе цифрове споживання, цифрові компетенції, цифрову безпеку [9, с. 120-141].

Цифрову грамотність зазвичай розглядають через призму технічних аспектів, як комплекс знань та навичок, необхідних для ефективного використання цифрових технологій в особистих інтересах користувача. Однак важливо враховувати, що Інтернет виник як інструмент комунікації, і ця функція залишається однією з основних до сьогодні. Таким чином, цифрову грамотність слід аналізувати не лише з технічної, але й з комунікативної перспективи, як здатність ефективно взаємодіяти з іншими користувачами в цифровому середовищі [10].

Автори роботи [11, с. 55-59] характеризують цифрову грамотність як здатність використовувати ті можливості, що їх відкриває сучасне суспільство з усіма його технологіями, вміння комунікувати з людьми в новому соціальному форматі та бути етичними й уважними одне до одного. Тут на перший план виходять людські стосунки, етика спілкування в мережі, певні правила комунікації, частково оцифровані з реального життя або породжені процесом віртуального спілкування.

Загальновизнаним для світового співтовариства є також розуміння цифрової грамотності, запропоноване ЮНЕСКО, як набору базових навичок, що потрібні для роботи з цифровими медіа, з пошуком і обробкою інформації.

Деякі дослідники вважають, що цифрова грамотність - це нова форма грамотності, що має на увазі пошук, оцінювання та використання різноманітних джерел інформації з метою формування комплексного змістовного уявлення про конкретне питання, тему або ситуацію [12, с. 435-438]. Автори роботи [13] наголошують, що необхідність оцінювати достовірність інформації, інтегрувати дані з різноманітних джерел та використовувати гіпермедійні формати подання не створює принципово нових когнітивних процесів.

Як бачимо, наведені визначення свідчать про те, що розуміння будь-якого явища, зокрема цифрової грамотності, значною мірою зумовлене науковою сферою, у межах якої здійснює дослідження його автор. А отже, цифрова грамотність є яскравим прикладом взаємопроникнення технічних і гуманітарних

аспектів сучасної науки. Виходячи з цього, її можна визначити як базову компетенцію сучасної людини, що включає здатність отримувати, оцінювати, опрацьовувати та створювати інформацію за допомогою цифрових технологій. Це передбачає вибір оптимальних програмно-технічних засобів для досягнення поставлених цілей, забезпечення їх безпечного використання, а також ефективну взаємодію з іншими користувачами, вирішення комунікативних завдань у цифровому середовищі із дотриманням етичних норм та використанням усіх доступних сервісів.

Проаналізуємо наведене вище, створивши термінологічне визначення цифрової грамотності. У результаті аналізу наведених вище існуючих визначень цифрової грамотності було обрано кілька ключових аспектів цього поняття. Зокрема, цифрову грамотність визначають як набір знань та вмінь, необхідних для безпечного та ефективного використання цифрових технологій. Це включає як технічні навички (здатність опрацьовувати та використовувати цифрові інструменти), так і комунікативні вміння (ефективне взаємодіяння з іншими користувачами в цифровому середовищі). Крім того, важливими є етичні аспекти, такі як правильне використання інформації та дотримання безпеки в Інтернеті.

Таким чином, цифрова грамотність можемо визначити як здатність особи не лише користуватися технологіями, але й оцінювати та обробляти інформацію, створювати контент, взаємодіяти в цифрових середовищах, дотримуючись етичних норм та забезпечуючи безпеку у процесі використання цифрових ресурсів.

У нашій роботі ми опираємося на підхід, який визначає цифрову грамотність як сукупність п’яти ключових компонентів, оцінювання яких дозволяє об’єктивно визначити рівень її засвоєння (Додаток А).

Реалізуючись через технічні пристрої та цифрові технології, усі згадані базові компоненти цифрової грамотності слугують одній меті - забезпечити користувачеві максимально ефективну роботу в цифровому середовищі.

Однак наявність спільних елементів не свідчить про повну ідентичність усіх компонентів. Знання, уміння та навички, які є характерними для різних видів цифрової грамотності, можуть мати різні практичні застосування в залежності від

специфіки кожного з цих видів. Це особливо очевидно при аналізі методів реалізації цих компетенцій, що дозволяє зробити висновок, що наявність загальних характеристик не означає тотожності в застосуванні, адже кожен тип грамотності має свої унікальні аспекти, що визначають його функціональні межі та область використання. Ці відмінності наочно демонструються в таблиці Додатку А, котра ілюструє варіативність практичної реалізації окремих складових грамотності в контексті різних видів цифрових компетенцій [14-19].

1.3 Правовий контекст забезпечення кібербезпеки: законодавство, стандартизація

Кібербезпека є важливою для захисту інформаційної інфраструктури. Правова основа включає національні та міжнародні акти, що забезпечують захист інформаційних ресурсів. Закон «Про основні засади забезпечення кібербезпеки України» визначає принципи та механізми захисту критичної інфраструктури [20].

До міжнародних актів, що є релевантними для забезпечення КБ, належать не лише стандарти ISO/IEC, а й конвенції та нормативи, які визначають юридичну основу для боротьби з кіберзлочинністю та захисту інформації.

Будапештська конвенція про кіберзлочинність (2001) визначає правові механізми боротьби з кіберзлочинністю, зокрема злочини проти інформаційних систем і міжнародне співробітництво. Україна ратифікувала її у 2006 році, і вона криміналізує несанкціонований доступ, створення шкідливих програм та порушення авторських прав у цифровій сфері [21].

Ще одним важливим міжнародним актом є Резолюція Генеральної Асамблеї ООН № A/RES/68/167 (2013 рік), яка підкреслює необхідність захисту права на приватність в епоху цифрових технологій і встановлює основи для міжнародної співпраці у сфері забезпечення інформаційної безпеки [22].

Україна також враховує принципи Європейської конвенції з прав людини, особливо в контексті захисту права на приватність (стаття 8), що безпосередньо стосується забезпечення захисту персональних даних та інформаційної

конфіденційності. Це узгоджується із положеннями Закону України «Про захист персональних даних».

У контексті глобального підходу до безпеки інформаційної інфраструктури Україна орієнтується на рекомендації НАТО щодо кіберзахисту, оскільки є учасником програми співробітництва НАТО у сфері КБ. Важливими є також документи Європейського Союзу, зокрема Загальний регламент про захист даних (GDPR), який встановлює суворі вимоги до обробки персональних даних [23].

Україна активно імплементує міжнародні норми в національне законодавство для ефективного забезпечення КБ, зокрема через адаптацію ДСТУ до глобальних стандартів. Це підвищує рівень інформаційної безпеки та захищає бізнес і цифрові ресурси. Міжнародні стандарти ISO та IEC, розроблені для забезпечення безпеки в IT і кібербезпеці, визначають уніфіковані підходи до управління ризиками та захисту даних.

ISO охоплює широкий спектр стандартів, що стосуються КБ та складають підґрунтя для міжнародних зусиль щодо захисту інформації та забезпечення безпеки в цифровому просторі. Основні з них подано вище в таблиці (Додаток Б.2).

Для нашого дослідження, що зосереджене на впливі КБ на стабільність і розвиток суспільства в умовах цифрової трансформації, важливим є розгляд стандарту ISO/IEC 27032. Цей стандарт фокусується на взаємодії між державними структурами, бізнесом і користувачами, вирішуючи соціальні виклики кіберпростору, такі як захист персональних даних та запобігання фішингу. На відміну від ISO/IEC 27001, який стосується лише управління інформаційною безпекою в межах організацій, ISO/IEC 27032 охоплює ширший спектр соціальних і технічних аспектів.

Визначення КБ в стандарті ISO 27032 аналогічне класичному підходу до інформаційної безпеки, зокрема в аспекті захисту активів від загроз конфіденційності, цілісності та доступності, але в контексті кіберпростору — віртуального середовища, яке формується через дії людей, програм та сервісів в

Інтернеті. Кіберпростір охоплює віртуальні елементи, такі як гроші, аватари, хмари, посольства, злочини та розваги.

Основним пріоритетом забезпечення КБ є координація взаємодії між організаціями, що формують кіберпростір, оскільки окремі дії не здатні ефективно захистити від кіберзагроз. Тезаурус КБ інтегрує поняття інформаційної безпеки, безпеки застосунків, мережевої безпеки, безпеки Інтернету та безпеки критичної інфраструктури.

Ключову роль у забезпеченні КБ відіграють зацікавлені сторони, які захищають свої активи в кіберпросторі. Вони включають споживачів (фізичних осіб та організації) і провайдерів (наприклад, інтернет-доступу та інтернет-застосунків). Споживач може стати провайдером, створюючи віртуальні продукти чи послуги для інших. В стандарті наводяться приклади ролей зацікавлених сторін для впровадження управління доступом у системах КБ.

У безпеці активи включають все, що має цінність, як інформаційні, так і фізичні ресурси (наприклад, аватар і USB-ідентифікатор). Розрізняють персональні активи (наприклад, банківські дані) та активи організації (наприклад, URL-адреса). Таксономія кіберзагроз класифікує їх за різними ознаками, такими як види активів, внутрішні та зовнішні фактори, цілі та джерела.

Стандарт надає три основні керівництва для зацікавлених сторін щодо забезпечення КБ: оцінка та управління ризиками, дотримання вимог безпеки користувачами та забезпечення КБ для провайдерів. Рекомендації з оцінки ризиків ґрунтуються на ISO 27005 і підкреслюють необхідність додаткової відповідальності зацікавлених осіб у зв'язку з звітністю, поінформованістю, законодавчими аспектами та узгодженістю дій у разі інцидентів та заходів безпеки.

Конкретні заходи забезпечення КБ можуть бути визначені за результатами оцінювання ризиків і в рамках планування дій з підвищення безпеки активів. Стандарт представляє низку базових заходів, спрямованих на вирішення завдань, таких як забезпечення безпеки додатків, серверів, кінцевих користувачів, захисту від атак методами соціальної інженерії, підвищення готовності (Додаток Б.3).

Кіберстійкість (КС) є важливою частиною КБ, зосередженою на здатності організацій відновлювати свою функціональність після кібератак або інших загроз. Це включає як захист, так і реагування на інциденти, зменшення впливу атак і відновлення після порушень.

Щодо національних стандартів України, відповідні адаптовані ДСТУ ISO/IEC 27001 та ДСТУ ISO/IEC 27005 також регулюють аспекти КС. Вони дають рекомендації щодо створення систем управління безпекою інформації та аналізу ризиків, що є важливими для підтримки стабільності та стійкості інформаційних систем в умовах постійно змінюваних кіберзагроз.

У таблиці Б.5 наведено приклади національних стандартів, гармонізованих з ISO 27032. ISO 27032-2012 надає вказівки для підвищення КБ в Інтернеті, застосовуючи ризик-орієнтований підхід у інформаційній безпеці. Правовий контекст КБ в Україні базується на нормативно-правових актах, що визначають вимоги до захисту інформаційних систем та інфраструктури.

Водночас міжнародні стандарти ISO вносять суттєвий внесок у формування загальних вимог до захисту інформації, інтегруючи світовий досвід у національну практику. Ці стандарти охоплюють як технічні, так і організаційні аспекти кіберзахисту, формуючи правову основу для національної КБ, що відповідає міжнародним вимогам та забезпечує узгодженість із глобальними стандартами.

Висновок до розділу 1

Цифрова грамотність є необхідною умовою для ефективного функціонування особистості в сучасному інформаційному суспільстві. Вона визначається як здатність використовувати цифрові технології для доступу, оцінки, створення та комунікації інформації, що вимагає наявності низки ключових компонентів.

Цифрову грамотність є сукупністю п’яти ключових компонентів, оцінювання яких дозволяє об’єктивно визначити рівень її засвоєння: інформаційна грамотність, медійна грамотність, комп’ютерна грамотність, обчислювальна грамотність, комунікативна грамотність.

До основних складових цифрової грамотності належать вміння працювати з інформацією, її критичний аналіз, а також безпека в Інтернеті та здатність здійснювати етичну взаємодію в цифровому середовищі. Це дозволяє не лише оптимізувати використання технологій, а й гарантувати безпеку та відповідальність у процесах взаємодії з цифровими ресурсами.

Цифрова грамотність також передбачає володіння такими навичками, як програмування, обробка даних і використання цифрових інструментів для навчання та професійної діяльності.

Кібербезпека є фундаментальним аспектом у сучасному цифровому середовищі, що охоплює широкий спектр заходів, технологій, політик і практик, призначених для захисту інформаційних систем, мереж та ресурсів від несанкціонованого доступу, шкідливих дій та зловмисних атак.

Основними складовими КБ є захист даних, безпека мережевих комунікацій, обробка інформації, забезпечення конфіденційності, цілісності та доступності інформації. Критичні аспекти КБ включають оцінку ризиків, розробку політик і стандартів для забезпечення захисту, а також моніторинг і реагування на інциденти.

Роль КБ у захисті цифрових ресурсів, захисту персональної та корпоративної інформації є надзвичайно важливою, особливо в умовах постійно зростаючого використання Інтернету та інформаційно-комунікаційних технологій.

Правовий контекст забезпечення КБ охоплює нормативно-правову базу, що включає закони, стандарти та нормативи, які визначають вимоги до захисту інформаційних систем і даних. В Україні питання КБ регулюються рядом законодавчих актів, серед яких Закон України "Про основні засади забезпечення КБ України", який встановлює основні принципи, завдання і структуру КБ в країні.

Стандарти, такі як ISO 27032, пропонують міжнародні методики для захисту віртуальних середовищ, акцентуючи увагу на ризик-орієнтованому підході та координації між організаціями.

У правовому контексті важливою є також роль національних стандартів, зокрема ДСТУ, які адаптують міжнародні вимоги до специфіки українського законодавства і умов. Стандартизація в цій галузі сприяє не тільки формалізації процедур безпеки, але й забезпеченню відповідності міжнародним вимогам, що підвищує рівень кіберзахисту на національному та міжнародному рівнях.

РОЗДІЛ 2. ДОСЛІДЖЕННЯ ТЕНДЕНЦІЙ КІБЕРБЕЗПЕКИ З УРАХУВАННЯМ РОЛІ ЦИФРОВОЇ ГРАМОТНОСТІ

2.1 Методи оцінки рівня цифрової грамотності

З введенням понять «цифрова грамотність» і «цифрові компетенції» виникла потреба в універсальному інструменті для їх оцінювання. Спочатку рівень цифрової грамотності оцінювали за чотирма пунктами: медійна, комп'ютерна, візуальна та інформаційна грамотність. Згодом дослідники погоджувалися, що оцінювання повинно базуватися на навичках роботи з інформацією. Згодом акцент перемістився на технічні навички, зокрема комп'ютерну грамотність, при цьому інформаційна грамотність і критичне мислення не враховувалися.

Найбільшого визнання набув підхід, запропонований у 2017 р. у рамках Саміту G20 (м. Гамбург, Німеччина), новизна якого полягала в об'єднанні технічної та соціальної складової цифрової грамотності та оцінці її як сукупності інформаційної, медійної, комп'ютерної, комунікативної грамотності та ставлення до технологій. Кожен із компонентів пропонувалося оцінювати за трьома аспектами:

1) технічний - відображає розуміння принципів роботи різних пристроїв і технологій, навички пошуку інформації в різних її форматах;

2) когнітивний - включає в себе здатність до пошуку, сприйняття, аналізу, оцінки та створення інформації; сюди ж увійшли навички комунікації в цифровому середовищі;

3) етичний - являє собою розуміння особистої відповідальності та дотримання суспільних норм під час роботи з інформацією та спілкування в цифровому середовищі.

В Україні оцінка рівня цифрової грамотності проводиться через національний тест «Цифрограм», розроблений Міністерством цифрової трансформації за підтримки USAID. Тестування здійснюється через платформу

«Дія. Цифрова освіта», яка забезпечує доступ до ресурсів для розвитку цифрових навичок [23].

У таблиці В.1 представлено найбільш застосовувані індекси та показники цифрової грамотності, котрі використовуються для оцінки рівня цифрових навичок у різних сферах [25-26].

Індекс цифрової грамотності є важливим інструментом для оцінки рівня цифрових навичок, який здобув міжнародне визнання завдяки комплексній оцінці аспектів цифрової компетентності. Однак спроби стандартизувати цю оцінку на глобальному рівні і розробити універсальніші інструменти тривають. ISD (Index of Sustainable Development), що є аналогом Digital Development Level (DDL), також включає цифрову грамотність як одну з ключових складових. Цей індекс оцінює розвиток цифрової інфраструктури, доступність технологій, їх використання та підготовленість населення до цифрових змін, що підкреслює важливість цифрової грамотності для ефективного використання технологій у різних сферах життя.

ISD є комплексним інструментом, що оцінює ефективність державної політики в контексті сталого розвитку на національному рівні. Він враховує багато аспектів, таких як розвиток цифрових технологій, екологічна стійкість та соціальна інтеграція (табл. В.2).

Процес розрахунку індексу ISD включає використання різних кількісних і якісних індикаторів для оцінки цифрової політики країни в кількох сферах. Індекс ISD інтегрує ці компоненти, що дозволяє отримати загальну оцінку ефективності розвитку країни в умовах цифровізації та сталого розвитку. Він відображає, наскільки ефективно країна інтегрує цифрові інструменти у всі сфери суспільного життя.

Індекс ISD тісно пов'язаний з DDLI (Digital Development Level Index) та NCSI (National Cyber Security Index), який є глобальним рейтингом КБ. Цей зв'язок існує через важливість КБ для сталого цифрового розвитку, оскільки вона забезпечує надійність і безпеку цифрової інфраструктури. NCSI оцінює готовність країн до кіберзагроз і їх здатність забезпечувати безпечне функціонування цифрових технологій, що тісно переплітається з аспектами ISD і DDLI.

Оцінка цифрової грамотності повинна враховувати демографічні та економічні аспекти, адже вони впливають на здатність адаптуватися до цифрового середовища. Демографічні характеристики, такі як вік, освіта, соціальний статус та місце проживання, визначають доступ до технологій і рівень цифрових компетенцій. Молодші покоління, як правило, мають вищі цифрові навички через вплив цифровізації [26].

Економічний контекст також важливий для оцінки цифрової грамотності. У умовах глобалізації та розвитку цифрової економіки доступ до технологій стає необхідним для економічної активності. Рівень цифрових навичок впливає на участь у цифрових професіях і загальну економічну ефективність країни. Врахування економічних даних при оцінці цифрової грамотності дає змогу краще зрозуміти, як суспільство адаптується до нових економічних умов, спричинених розвитком інформаційних технологій [27].

Отже, оцінка рівня цифрової грамотності є важливим інструментом для вимірювання здатності індивідів адаптуватися до вимог цифрового середовища. Використання різноманітних методів, таких як тести, анкети та інтерв'ю, дозволяє точно визначити рівень технічних та когнітивних навичок. Розвиток таких інструментів, як індекс цифрової грамотності та коефіцієнт цифрового інтелекту, сприяє створенню єдиних стандартів оцінки і допомагає в ефективній підготовці громадян до життя в цифровій економіці.

2.2 Інституційні засади оцінки рівня кібербезпеки за рейтингами в GCI та NCSI

Поступальний розвиток цифрових технологій створив передумови для глибоких трансформацій суспільства, що охоплюють економічні, соціальні та культурні сфери. Ці процеси супроводжуються підвищенням залежності держав і громадян від цифрових інфраструктур. Водночас зростає масштаб кіберзлочинності, яка становить суттєву загрозу для стабільності цифрового простору. Сучасні кіберзагрози, такі як несанкціоновані втручання в інформаційні

системи, витоки даних і атаки на критичну інфраструктуру, вимагають від державних інституцій впровадження дієвих механізмів оцінювання й розвитку КБ.

Глобальний індекс кібербезпеки (Global Cybersecurity Index, GCI), розроблений Міжнародним союзом електрозв'язку (ITU) у 2014 році, є одним з основних міжнародних інструментів, покликаних оцінювати та аналізувати рівень кіберзахисту на глобальному рівні [23]. GCI являє собою комплексну оцінку національних ініціатив у сфері КБ, орієнтуючись на законодавчі ініціативи, організаційні заходи, технічні стандарти та інфраструктуру, а також міжнародну співпрацю у цій сфері, що дозволяє створити зрозумілу картину готовності країни до протидії кіберзагрозам. Оцінка ґрунтується на 5 основних компонентах (рис. В.1), кожен з яких має свої особливості (табл. В.3).

Наведені в таблиці додатку В.1 компоненти охоплюють ключові аспекти національної КБ та взаємодії країн у цій сфері, що дозволяє отримати всебічну оцінку здатності держави протистояти кіберзагрозам та захищати свої цифрові інтереси на глобальному рівні.

Національний індекс КБ (NCSI), заснований у 2016 році Естонською академією електронного уряду, оцінює здатність країн реагувати на кіберзагрози та забезпечувати безпеку цифрового середовища. Він вимірює готовність до кіберінцидентів, здатність запобігати кіберзлочинам, а також розвиток інфраструктури та політик безпеки. Особливість NCSI — акцент на практичних аспектах КБ, таких як наявність органів, що відповідають за кібербезпеку, забезпечення цифрової інфраструктури і підготовка фахівців. Крім того, важливою є міжнародна співпраця в обміні інформацією про загрози [24].

NCSI враховує нормативно-правові механізми КБ, зокрема закони та політики, спрямовані на захист даних і приватності. Оцінюються також національні стандарти безпеки, захист критичної інфраструктури та заходи реагування на інциденти. Індекс акцентує на розвитку національної та міжнародної співпраці, особливо в обміні даними та моніторингу кіберзагроз. Це сприяє формуванню національних стратегій і адаптації до змін у кіберпросторі. Рейтинг NCSI є

важливим інструментом для урядів, міжнародних організацій та бізнесу для підвищення готовності до кіберзагроз [22].

Ці індекси оцінюють рівень КБ, порівнюють готовність країн і вдосконалюють стратегії, підкреслюючи важливість глобального співробітництва та зміцнення захисту в умовах цифровізації (табл. В.4).

Вивчивши Глобальний та Національний Індекс кібербезпеки, можна сказати, що фактори оцінювання є важливими для розроблення механізму КБ.

Отже, як бачимо з наведеного вище, GCI та NCSI оцінюють рівень КБ на глобальному та національному рівнях. GCI фокусується на готовності країн до кіберзагроз, враховуючи законодавчі, технічні та організаційні аспекти, а NCSI - на здатності реагувати на кіберінциденти та впроваджувати стратегії цифрової безпеки. Обидва індекси підкреслюють важливість інституційної підготовленості та міжнародної співпраці для забезпечення КБ.

2.3 Аналіз тенденцій кібербезлочинності відносно ролі цифрової грамотності

Цифрові технології відкривають нові можливості для розвитку суспільства, забезпечуючи сталий розвиток і соціальну інтеграцію через ефективне використання різних ресурсів. Водночас кіберзлочинці застосовують різноманітні методи атак, такі як фішинг, DDoS-атаки, мережеве сканування та поширення шкідливого ПО, що ставлять під загрозу безпеку громадян і критичні системи, зокрема в охороні здоров'я, транспорті та енергетиці, що підриває довіру до цифрових технологій [20].

З розширенням цифровізації кіберзагрози зростають через більшу кількість продуктів і послуг на основі ІТ та їхніх користувачів. Це створює нові виклики для безпеки, оскільки інтеграція цифрових рішень підвищує вразливість до кібератак, що може вплинути на добробут громадян і стабільність суспільства.

Аналізуючи дані таблиці В.5, можна зробити висновок, що персональні дані (19%) є лідерами серед цінних для зловмисників типів даних, зокрема ім’я, адреса та контакти. Це свідчить про зростання кіберзагроз, спрямованих на особисту

інформацію. Частка фішингу (24%) підтверджує використання маніпуляцій через фальшиві запити та веб-ресурси для крадіжки даних. Високий відсоток шкідливого ПЗ (18%) вказує на масові атаки на користувачів.

Дані про фінансову ситуацію (13%) також приваблюють зловмисників, оскільки відкривають можливості для викрадення коштів через кібератаки. Атаки на критичну інфраструктуру (15%) можуть призвести до серйозних порушень у роботі комунальних і транспортних мереж. Зростання атак зсередини (5%) свідчить про необхідність посилення внутрішньої безпеки.

Отже, для ефективного протистояння кіберзагрозам необхідно зміцнювати захист персональних, фінансових і урядових даних, а також підвищувати обізнаність громадян щодо небезпек у цифровому середовищі.

Для аналізу тенденцій кіберзлочинності важливими інструментами є показники DDLI та NCSI, оскільки вони відображають рівень цифрового розвитку та КБ в країні. DDLI оцінює рівень цифрової грамотності населення, що важливо для протидії кіберзагрозам, оскільки він визначає здатність суспільства реагувати на кіберзлочини. NCSI дає можливість оцінити ефективність національної кіберстратегії та готовність країни до кіберзагроз.

Поєднання цих індексів дозволяє сформувати уявлення про зв'язок між рівнем цифрової грамотності та кіберзлочинністю, що є критично важливим для розробки заходів КБ. DDLI тісно пов'язаний з NCSI, оскільки КБ забезпечує безпеку цифрової інфраструктури, а ефективність цієї безпеки прямо впливає на позицію країни в обох рейтингах. Інтеграція цих індексів дає змогу створити більш цілісну картину цифрової спроможності суспільства, орієнтуючи політики на безпеку та сталий розвиток [24].

Отже, розглянемо ці показники та їх динаміку детальніше. Станом на 2024 рік Останнє оновлення джерела - 24 серпня 2024 р,) Україна займає 13-те місце у рейтингу NCSI (рис. В.2).

У наданому рисунку показано порівняння двох індексів (NCSI та DDLI) для різних країн, а також різницю між цими значеннями. NCSI відображає готовність

країн до забезпечення КБ, в той час як DDLI оцінює рівень цифрового розвитку, що включає цифрову грамотність населення.

Чехія займає перше місце за рівнем КБ (98,33), але її рівень цифрового розвитку становить лише 72,04, що свідчить про значний розрив у 26,29 балів. Молдова та Азербайджан демонструють великі розбіжності між своїми показниками КБ та цифрового розвитку. У США, Нідерландах та Великобританії спостерігаються від'ємні показники різниці між рівнем цифрового розвитку та національним індексом КБ. У США мінімальна різниця (-0,04) відображає гармонійне поєднання цифрових технологій та рівня безпеки. Нідерланди мають більшу різницю (-3,27), що свідчить про недостатню підготовленість населення до нових технологій. У Великобританії різниця (-7,07) є найбільшою, що свідчить про проблеми в інтеграції КБ з цифровою грамотністю громадян при впровадженні нових технологій без належного навчання для їх безпечного використання.

Враховуючи вищезазначене, можна зробити висновок, що забезпечення КБ сприятиме покращенню цифрового розвитку в різних країнах. Цю гіпотезу доцільно перевірити шляхом проведення кореляційно-регресійного моделювання взаємозв'язку між DDLI та NCSI (рис. В.3)

За результатами логарифмічної регресії між рівнем цифрового розвитку (x) та національним індексом КБ (y) отримано таке рівняння:

$$y=-184.27+62.57\ln(x)$$

При цьому коефіцієнт детермінації $R^2 = 0.561$, що вказує на міцний зв'язок між цими двома змінними.

При $R^2 = 0{,}5148$, коефіцієнт кореляції буде $r = 0.749$.

Аналіз показав міцний лінійний зв'язок (за шкалою Чеддока) між рівнем цифрового розвитку та національним індексом КБ з коефіцієнтом кореляції $r = 0.749$. Також показник $P_{value} \leq 0{,}05$ підтверджує, що дана модель є досить достовірною.

Україна посідає 13 місце в рейтингу Національного індексу КБ, що свідчить про стабільний розвиток у сфері кіберзахисту. Це високий показник, що підтверджує наявність ефективних механізмів захисту інформації та стратегічних

ініціатив. Однак, різниця між рівнем цифрового розвитку (67,73) та індексом КБ (80,83) у 13,10 пунктів вказує на необхідність покращення цифрової грамотності. Важливими залишаються питання інформаційної безпеки, оскільки Україна стикається з кіберзагрозами, такими як фішинг та атаки на критичну інфраструктуру. Підвищення рівня обізнаності громадян щодо КБ дозволить знижувати ризики та покращити готовність країни до кіберзагроз.

Розглянемо більш детально показники рейтингу NCSI для України.

В першу чергу варто проаналізувати графік розробки NCSI - інструмент, що демонструє етапи вдосконалення та розвитку національних кіберзахисних стратегій в країні. Цей графік (рис. В.4) відображає, як змінювався рівень КБ в Україні з 2018 до 2024 рр. на основі визначених параметрів, таких як цифрова грамотність, інфраструктура безпеки, правові механізми та рівень розвитку технологій тощо.

Графік розвитку індексу NCSI для України з 2018 по 2024 роки (рис. В.5) демонструє поступове зростання національної готовності до кіберзахисту, з 58% у 2018 році до 81% у 2024 році. Це свідчить про активні зусилля щодо покращення цифрової інфраструктури та технологій. Основними причинами є впровадження державних політик, міжнародних ініціатив і посилене законодавче регулювання в сфері захисту даних. Військові дії з лютого 2022 року стали додатковим фактором для прискорення розвитку КБ, зокрема через значні кібератаки. Збільшення показників у 2022 (75%), 2023 (79%) і 2024 роках (81%) відображає покращення кіберзахисту, модернізацію інфраструктури та боротьбу з новітніми кіберзагрозами, що зміцнюють національну безпеку в умовах гібридної війни.

Наслідок таких заходів видно з хронології ранжування NCSI в Україні, частота якого значно зросла в 2024 році (рис. В.5).

Графік, що показує хронологію змін в NCSI, вказує на тенденцію поступового зростання індексу з 2020 по 2024 роки. Відмітка 2024 року (приблизно 1 на шкалі) свідчить про значне збільшення частоти ранжування індексу порівняно з попередніми роками (11). Це зростання відображає підвищення уваги та

пріоритету до КБ, обумовлене як внутрішніми чинниками розвитку країни, так і зовнішніми загрозами, зокрема військовим конфліктом.

Проаналізуємо ключові індикатори NCSI України щодо КБ, станом на 2024 рік, а саме:

1) стратегічні індикатори КБ;

2) превентивні індикатори КБ;

3) адаптивні індикатори КБ.

1. Стратегічні індикатори КБ NCSI включають політику КБ; глобальний внесок у КБ; освіту та професійний розвиток, дослідження та розробки в галузі КБ (рис. 1 додатку Г) [30]. Політика КБ впроваджена, що свідчить про високий рівень стратегічного планування та ефективну координацію заходів. Національна стратегія КБ сприяє підвищенню цифрової обізнаності громадян.

Глобальний внесок у кібербезпеку частково реалізований. Прогрес у кібердипломатії недостатній, що обмежує міжнародну інтеграцію країни.

У сфері освіти спостерігається неоднорідність: відсутність інтеграції основ КБ у початкову та середню освіту створює прогалини в цифровій грамотності. Розвиток професійних асоціацій недостатній.

Дослідження та розробки в галузі КБ є сильною стороною, що свідчить про розвинену інфраструктуру для наукових інновацій.

Отже, стратегічні індикатори демонструють високий рівень політики КБ та наукових розробок, проте потребують посилення в освітньому напрямку, включно із впровадженням цифрової грамотності, та активізації міжнародної діяльності.

2. Превентивні індикатори NCSI України щодо КБ включають КБ критичної інформаційної інфраструктури, КБ цифрових засобів, аналіз кіберзагроз та підвищення обізнаності, захист персональних даних. Розглянемо їх детальніше (рис. 2.7).

Як бачимо з рисунка 2 додатку Г [30], прогрес у забезпеченні КБ критичної інфраструктури полягає в ідентифікації ключових об’єктів та встановленні вимог для операторів, але відсутність нормативного регулювання для державного сектору

створює ризики. Цифрові компетентності співробітників є важливим фактором для зменшення цих ризиків та підвищення ефективності захисту.

Захист цифрових засобів демонструє високий рівень безпеки електронної ідентифікації та довірчих послуг. Однак недостатня увага до безпеки хмарних сервісів і ланцюгів постачання вказує на необхідність їх розвитку. Підвищення цифрової грамотності серед користувачів хмарних технологій допоможе знизити ризики вразливостей та зміцнити безпеку цифрових екосистем.

Система аналізу кіберзагроз забезпечує ефективний моніторинг завдяки публічним звітам і доступним ресурсам, але потребує покращення координації для підвищення обізнаності про культуру кіберзахисту серед широкої аудиторії. Інвестиції в цифрову грамотність, зокрема в навички виявлення кіберзагроз та реагування на інциденти, є важливими для популяризації КБ.

Захист персональних даних досягає високого рівня, що свідчить про надійну систему регулювання. Проте постійний розвиток цифрової грамотності користувачів, зокрема вміння захищати особисту інформацію та розуміння прав на конфіденційність, є критичними для підтримки безпеки в цифровому середовищі.

3. Адаптивні індикатори КБ NCSI України щодо КБ включають реагування на кіберінциденти, управління кіберкризовими ситуаціями , боротьбу з кіберзлочинністю, військовий кіберзахист (рис. 3 додатку Г) [30].

Аналіз адаптивних індикаторів КБ показує різний рівень готовності до реагування на кіберзагрози, управління кризовими ситуаціями та боротьби з кіберзлочинністю, підкреслюючи важливість цифрової грамотності для ефективного функціонування цих систем.

У сфері реагування на кіберінциденти досягнуто прогресу у національних можливостях та міжнародному співробітництві, але необхідно покращити механізми комунікації, зокрема централізовані інструменти для повідомлення.

Управління кіберкризовими ситуаціями має базовий рівень готовності через навчання, проте відсутність плану управління кризами вимагає вдосконалення цифрової компетентності та стратегічного планування.

Боротьба з кіберзлочинністю є найбільш успішною завдяки комплексному законодавчому підходу та високому рівню цифрової грамотності працівників у цій сфері.

Військовий кіберзахист демонструє високу готовність, проте важливо інтегрувати цифрову грамотність у підготовку особового складу для ефективного реагування на загрози.

Цифрова грамотність є основою для реалізації адаптивних індикаторів КБ та підвищення рівня національної безпеки.

Україна має потенціал для розвитку цифрової безпеки, але для досягнення високих результатів необхідна інтеграція DDLI та NCSI з освітою та підвищенням цифрової грамотності. Розрив між цими індексами вказує на необхідність посилення цифрової освіти, оскільки недостатня обізнаність може знизити ефективність технологічних заходів.

Висновок до розділу 2

Методи оцінки рівня цифрової грамотності є ключовим інструментом для вимірювання здатності індивідів і груп адаптуватися до вимог сучасного цифрового середовища. Сьогодні застосовуються різноманітні методи, серед яких найбільш поширеними є стандартизовані тести, інтерв’ю, анкети та спостереження.

Оцінка рівня цифрової грамотності, зокрема через індекси та коефіцієнти, таких як Digital Literacy Index або коефіцієнт цифрового інтелекту (DQ), дозволяє не лише виміряти технічні навички, але й оцінювати когнітивні, метакогнітивні та емоційні компетенції, що забезпечують повну картину здатності індивіда до ефективного використання цифрових технологій.

Для точності результатів важливим є врахування контексту - різні методи оцінки можуть включати або виключати окремі аспекти, такі як кібербезпека, цифрові права, або управління інформацією. Враховуючи динамічний розвиток цифрових технологій, зростає потреба в адаптації методів оцінки, що дозволяє краще відображати актуальні виклики та можливості цифрової трансформації.

Використання методів тестування та анкетування на платформі, як-от «Дія. Цифрова освіта», надає можливість проводити оцінку на національному рівні, що робить ці методи особливо корисними для моніторингу і покращення цифрової грамотності громадян на широкому рівні.

Інституційні засади оцінки рівня КБ через індекси GCI та NCSI демонструють важливість комплексного підходу до управління кіберзагрозами.

Глобальний індекс КБ (GCI) відображає готовність країн до реагування на кіберзагрози, оцінюючи законодавчі, технічні та організаційні аспекти, а також міжнародну співпрацю.

У свою чергу, Національний індекс КБ (NCSI), заснований на практичних аспектах, зосереджується на можливості держав оперативно реагувати на інциденти, захищати критичну інфраструктуру та впроваджувати стратегії КБ.

Обидва індекси підкреслюють значення інституційної підготовленості та міжурядової співпраці для підвищення загального рівня кіберзахисту, що сприяє розробці більш ефективних стратегій і політик у глобальному контексті КБ.

Персональні дані (19%) і фішинг (24%) є основними цілями кіберзагроз. Шкідливе програмне забезпечення (18%) вказує на масові атаки, а фінансові дані (13%) — на загрозу викрадення коштів. Атаки на критичну інфраструктуру (15%) та внутрішні загрози (5%) підкреслюють важливість посилення безпеки на всіх рівнях. Для ефективного протистояння сучасним кіберзагрозам суспільству необхідно зміцнювати захист персональних, фінансових і урядових даних, а також підвищувати обізнаність громадян щодо можливих небезпек в цифровому середовищі.

За результатами лінійної регресії між DDLI та NCSI – сильний логарифмічний зв’язок з коефіцієнтом кореляції $r = 0.749$. Це означає, що підвищення рівня КБ не завжди є достатнім для забезпечення розвитку цифрової грамотності.

Розрив між двома індексами DDLI та NCSI свідчить про те, що цифрова грамотність, хоча й є важливою складовою цифрового розвитку країни, не завжди узгоджується з її стратегіями в сфері КБ

Країни з великими розривами між індексами можуть потребувати додаткових зусиль для покращення цифрової грамотності своїх громадян, оскільки навіть із сильними технологічними заходами відсутність свідомості та навичок у населення може зробити ці заходи менш ефективними.

РОЗДІЛ 3. ШЛЯХИ ПІДВИЩЕННЯ РІВНЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ

3.1 Міжнародний досвід у сфері забезпечення кібербезпеки

У рамках дослідження розглядався досвід низки успішних країн згідно з міжнародним рейтингом у сфері КБ та цифровізації. Згідно з NCSI Велика Британія, США, Сінгапур, Естонія та Литва, є країнами-лідерами у сфері КБ.

На національному рівні КБ є спільною відповідальністю, яка вимагає скоординованих дій щодо запобігання, підготовки, реагування та відновлення після кіберінцидентів. Для забезпечення безперебійної роботи та забезпечення безпечної, надійної та відмово-стійкої цифрової сфери необхідна всеосяжна стратегія, яка має розроблятися та впроваджуватися за участю зацікавлених сторін. Ця стратегія часто згадується як Національна стратегія кібербезпеки (NCS) і є критично важливим документом для соціально-економічної безпеки будь-якої країни [33].

Досвід Великобританії. Уряд Великобританії щорічно аналізує порушення КБ. Цифрова економіка відіграє важливу роль, стимулюючи економіку на 145 мільярдів фунтів стерлінгів щороку (цифрова стратегія 2022–2025). Fujitsu зазначає, що Великобританія має найбільшу інтернет-економіку серед G20.

У 2023 році зафіксовано 200 масштабних інцидентів, пов’язаних із кібербезпекою, що в 100 разів перевищує показник 2022 року. Репрезентативне опитування 1 008 підприємств і 30 глибинних інтерв’ю вказали на поширеність проблеми КБ. Малі підприємства отримали доступ до державної підтримки, включно з рекомендаціями та безкоштовним онлайн-навчання.

Уряд Великобританії підтримує малий бізнес, пропонуючи посібники та безкоштовні онлайн-курси для захисту від кіберзагроз. Короткі 30-хвилинні курси забезпечують швидкий доступ до знань і навичок для протидії кіберзлочинності.

Для фахівців із закупівель створено безкоштовний онлайн-курс у співпраці з Chartered Institute of Procurement & Supply, який навчає ефективній протидії кіберзагрозам. Цей досвід варто врахувати в Україні для посилення КБ у сфері державних закупівель, що сприятиме прозорості та запобіганню корупції.

На порталі Великобританії доступний інструмент «Exercise in a Box» від Національного центру кібербезпеки (NCSC), що дозволяє організаціям відпрацьовувати реакції на кібератаки, а також посібник із захисту в кіберпросторі. Посібник містить низку технічних порад, таких як: режим управління ризиками; дім і мобільна робота (робота у віддаленій мережі); управління подіями; запобігання шкідливим програмам; управління користувацькими привілеями; мережева безпека; знімні засоби управління мультимедіа; навчання користувачів та обізнаність.

NCSC також розроблено вебсторінку «Cyber Essentials - Кібер основи». Цей проєкт також підтримується урядом та допомагає організаціям захистити себе від поширених онлайн-загроз. Даний сайт містить кілька секцій, розроблених для: індивідуумів і сім'ї; самозайнятих та індивідуальних підприємців; малих і середніх організації, де кількість співробітників до 250 осіб; великих організації (більш ніж 250 співробітників); державних секторів; експертів у сфері КБ.

Досвід США. Уряд США на 2024 фінансовий рік виділив 15 мільярдів доларів на діяльність, пов'язану з КБ. Це на 4 % більше, ніж у 2023 році. Найбільше фінансування отримує Міністерство оборони, бюджет якого становить майже 8,5 мільярда доларів, потім національна безпека - близько 1,7 мільярда доларів США [33].

Оновлена стратегія КБ США 2023 року спрямована на зміцнення лідерства та захист інтересів країни в онлайн-просторі. Пріоритетом є багатостороння модель управління Інтернетом, а висококваліфікований персонал у сфері КБ визнано стратегічним активом, що стимулює урядові програми пошуку талантів у світі. Американські військові розробили програму «Cyber Command» для захисту інтернет-інфраструктури, координації кібероперацій і підвищення стійкості до загроз національній безпеці

Американський проєкт «Savvy Cyber Kids», заснований у 2007 році, навчає дітей комп'ютерній грамотності, кібербезпеці та етиці. Освітні ресурси орієнтовані на балансування технологій, захист даних, етику в Інтернеті та безпеку в іграх. Сім'ї можуть використовувати безкоштовні книжки для дітей 3-7 років, що

пояснюють основи Інтернет-безпеки та управління екранним часом. Для педагогів доступні матеріали для кіберуроків, які підвищують обізнаність молоді щодо загроз і етичних норм у цифровому середовищі [40].

Цей досвід може бути корисним для України у впровадженні програм цифрової грамотності для дітей і підлітків.

Цей досвід є корисним для України, оскільки співпраця між державним та приватним секторами може покращити національний рівень КБ. Адаптація практик Великої Британії та США стане важливим кроком для України в сфері кіберзахисту.

Досвід Сінгапуру. Агентство кібербезпеки Сінгапуру (CSA) відповідає за нагляд та реалізацію Національної стратегії кібербезпеки, зокрема для запобігання та реагування на кіберзагрози. Закон про кібербезпеку, ухвалений у 2018 році, регулює діяльність власників критичної інфраструктури та постачальників кіберпослуг, а також сприяє інтеграції з міжнародними стандартами та ініціативами.

Основна діяльність CSA включає взаємодію з місцевими та міжнародними партнерами, проведення інформаційних кампаній та підвищення обізнаності про кібербезпеку. Агентство працює над формуванням надійної екосистеми КБ та реагує на кіберзагрози, захищаючи критично важливі сектори економіки, зокрема енергетику, водопостачання та банківську систему. Місією CSA є забезпечення КБ для підтримки цифрової економіки та захисту національної безпеки і благополуччя громадян (рис.Г.4).

3.2 Розробка рекомендацій щодо забезпечення кібербезпеки в Україні

У сучасну епоху цифровізації всі сфери життя переживають зміни, що призводять до зростання складності кіберзагроз. Україна, активно інтегруючись у світовий цифровий простір, стикається з викликами у сфері КБ, які вимагають системного підходу. Низький рівень цифрової грамотності та недостатня обізнаність про кібергігієну створюють умови для зловмисників, які застосовують

соціальну інженерію та фішинг. Тому підвищення цифрової грамотності є ключовим фактором для розвитку технологій кіберзахисту та підвищення національної безпеки, що вимагає впровадження рекомендацій для поліпшення інфраструктури безпеки та культури безпечного цифрового середовища.

На основі дослідження цифрової грамотності та КБ в Україні, сформовано рекомендації для підвищення обізнаності населення, покращення нормативно-правової бази, зміцнення кіберінфраструктури та розвитку міжнародного співробітництва. Рекомендації включають інтеграцію цифрової освіти та створення умов для розвитку технологій кіберзахисту, що забезпечує стійкість до кіберзагроз і формує культуру безпечної поведінки. Графічна ієрархія демонструє взаємозв'язок основних напрямів для ефективної КБ в Україні (рис. 3.2).

Ці рекомендації спрямовані на створення стійкої системи КБ, що базується на підвищенні обізнаності населення, формуванні культури цифрової безпеки та інституційному розвитку. Розглянемо їх більш детально.

1. *Підвищення цифрової грамотності* є важливим елементом стратегії КБ в Україні. Для цього необхідно впроваджувати національні програми цифрової освіти для всіх вікових груп, зокрема для дітей, підлітків, дорослих та літніх людей, з акцентом на основи КБ, захист особистої інформації та уникання кіберзагроз. Важливо організовувати масові заходи, вебінари та інформаційні кампанії, щоб забезпечити доступ до знань про цифрову безпеку для широкої аудиторії.

2. *Зміцнення нормативно-правової бази у сфері КБ* є ключовим для захисту від кіберзагроз. Необхідно розробити нормативні акти, які визначатимуть стандарти цифрової грамотності як частину стратегії КБ. Це включає вимоги щодо навчання населення основам цифрової безпеки, інтеграцію стандартів у систему освіти та бізнес, а також механізми контролю виконання норм.

Зміцнення нормативно-правової бази створить основи для розвитку комплексної системи КБ, що є необхідним для забезпечення стійкості держави до сучасних цифрових загроз.

3. *Розвиток національної інфраструктури КБ* включає створення інтегрованої платформи для моніторингу та попередження загроз. Платформа

повинна збирати і аналізувати дані для оперативного виявлення загроз на різних рівнях, враховуючи цифрову підготовку користувачів. Важливо, щоб вона адаптувалася до рівня грамотності, пропонуючи індивідуалізовані рекомендації та прості інтерфейси для користувачів з мінімальними знаннями.

Розвиток інфраструктури КБ включає адаптивний захист критичної інфраструктури, зокрема енергетичних систем, транспорту та фінансових установ, через використання інноваційних методів, таких як аналіз поведінкових моделей.

4. *Освіта в сфері КБ* є важливою для забезпечення цифрової безпеки на національному рівні. Включення курсів з цифрової грамотності та КБ у навчальні плани шкіл, університетів і професійних закладів формує компетентне та обізнане населення, здатне захищати свої дані від кіберзагроз.

Важливим аспектом є підготовка кваліфікованих фахівців, здатних не лише захищати інформаційні системи, а й навчати інших основам КБ. Це включає підготовку викладачів, тренерів і консультантів, які проводитимуть навчання для різних категорій громадян щодо принципів КБ, методів захисту та реагування на кіберінциденти. Формування таких фахівців сприятиме розвитку національної КБ та підвищенню рівня цифрової грамотності населення, створюючи більш стійке і безпечне цифрове середовище в Україні.

5. *Інформування громадськості про кіберзагрози* є важливим для підвищення обізнаності щодо цифрової безпеки. Національні кампанії повинні акцентувати зв'язок між цифровою грамотністю та КБ, підвищуючи знання про захист даних, паролі та безпечне спілкування в Інтернеті. Це допоможе зменшити ризики, пов'язані з низьким рівнем обізнаності про кіберзагрози.

6. *Посилення міжнародного співробітництва в кібербезпеці* необхідне для створення глобальної системи захисту від кіберзагроз. Участь у міжнародних ініціативах, що поєднують розвиток цифрової грамотності та кіберзахисту, дозволяє країнам забезпечити не лише власну безпеку, а й внести вклад у глобальну. Обмін досвідом із країнами з високим рівнем цифрової грамотності допомагає Україні адаптувати передові практики. Інтернаціональне співробітництво зміцнює міжнародні відносини та сприяє створенню безпечного

цифрового простору. Україна має можливість активно долучатися до цих ініціатив для підвищення кіберстійкості та зменшення глобальних кіберзагроз.

7. *Розробка технологічних інновацій для навчання та забезпечення КБ* є важливим кроком у боротьбі з кіберзагрозами та підвищенні цифрової грамотності. Використання штучного інтелекту (ШІ) для створення інтерактивних платформ з кібергігієни дозволяє персоналізувати навчання, адаптуючи матеріали під рівень знань користувача.

8. *Фінансування освітніх і інфраструктурних проєктів у кібербезпеці* є необхідним для створення ефективної системи захисту. Державне фінансування має підтримувати навчальні програми та розвиток інфраструктури для підвищення знань у КБ. Приватний сектор також повинен інвестувати у освітні проєкти, співпрацюючи з навчальними закладами та фінансуючи програми для працівників. Це дозволить створити основу для підвищення цифрової грамотності та протидії кіберзагрозам в Україні.

9. *Розробка національної стратегії цифрової грамотності та КБ* є ключовою для забезпечення стійкості держави до кіберзагроз. Це включає створення національних стандартів цифрової грамотності, платформ для навчання та підвищення обізнаності, а також освітніх програм з основ цифрової безпеки. Інтеграція цифрової грамотності у стратегію кіберзахисту вимагає співпраці держави, освітніх установ, приватного сектору та громадськості, а також розвитку нормативно-правових актів і системи моніторингу кіберзагроз.

Як бачимо з наведеного у цьому параграфі, розробка національної стратегії цифрової грамотності та КБ є важливим елементом у забезпеченні безпеки України в умовах глобальних цифрових трансформацій. Це дозволить створити цілісну та скоординовану систему, яка не лише забезпечить захист від кіберзагроз, а й сприятиме формуванню цифрової культури серед населення, підвищуючи його здатність ефективно реагувати на нові виклики у цифровому середовищі.

Висновок до розділу 3

У рамках дослідження розглянуто досвід низки успішних країн згідно з міжнародним рейтингом у сфері КБ та цифровізації. Згідно з NCSI Велика Британія, США, Сінгапур, Естонія та Литва, є країнами-лідерами у сфері кібербезпеки.

Аналіз досвіду інших країн у сфері кібербезпеки вказує на важливі аспекти для України. Зокрема, досвід Сінгапуру, де Агентство кібербезпеки координує національну стратегію і реагує на кіберзагрози, може бути корисним для створення або зміцнення відповідного органу в Україні. Сінгапур також виділяє значні кошти на дослідження кібербезпеки, що є важливим для України.

Велика Британія активно підтримує малий бізнес, надаючи ресурси для покращення кібербезпеки, що є важливим для України. Водночас США активно працюють над кіберосвітою, і Україні слід розвивати подібні ініціативи серед молоді.

Литва активно співпрацює на міжнародному рівні, що допомагає в підвищенні кваліфікації кадрів, і Україні варто посилити свою участь у міжнародних ініціативах. Естонія продемонструвала важливість правового регулювання кібербезпеки, і Україні необхідно ухвалити подібні закони для захисту цифрового простору.

Традиційні методи захисту систем виявляються недостатніми в умовах швидко змінюваних тактик кіберзлочинців, що вимагає впровадження динамічних стратегій безпеки. Враховуючи ці виклики, машинне навчання як частина штучного інтелекту представляє ефективний інструмент для покращення процесів виявлення загроз, оперативного реагування на інциденти та адаптації механізмів захисту в умовах постійно змінюваного кіберпростору.

Машинне навчання охоплює широкий спектр завдань, починаючи від класифікації та регресії до кластеризації та навчання з підкріпленням. Вибір підходу залежить від конкретного завдання і характеру даних. Ці підходи

охоплюють: навчання з учителем, навчання без учителя, навчання з підкріпленням, обробка природної мови (NLP), комп'ютерний зір, аналіз часових рядів, ансамблеві методи, виявлення аномалій та кластеризація, графове навчання.

Кожне завдання машинного навчання вимагає різного підходу і алгоритму, і вибір підходу залежить від факторів, таких як характер даних, бажаний результат і кількість доступних розмічених даних. Вибір методології критичний для визначення успіху проєкту з машинного навчання.

Розроблені нами рекомендації щодо комплексної стратегії забезпечення кібербезпеки в Україні, котрі включають в себе підвищення цифрової грамотності, зміцнення нормативно-правової бази, розвиток національної інфраструктури, освіту фахівців, інформування громадськості, міжнародне співробітництво, технологічні інновації, фінансування та розробку національної стратегії, є необхідним кроком для забезпечення стійкості держави до кіберзагроз.

Залучення усіх секторів суспільства, від державних структур до приватного сектору, дозволить створити надійну систему захисту в цифровому середовищі. Ці підходи сприяють формуванню свідомого та підготовленого населення, здатного ефективно реагувати на кіберзагрози, що забезпечить національну безпеку та стійкий розвиток цифрових технологій в Україні.

ВИСНОВКИ

Цифрова грамотність є ключовою умовою ефективного функціонування в інформаційному суспільстві, охоплюючи п’ять основних компонентів: інформаційну, медійну, комп’ютерну, обчислювальну та комунікативну грамотність. Вона включає вміння працювати з інформацією, здійснювати її критичний аналіз, забезпечувати безпеку в Інтернеті та етичну взаємодію в цифровому середовищі, що сприяє оптимальному використанню технологій і гарантує відповідальність у цифрових взаємодіях.

КБ є ключовим елементом у сучасному цифровому середовищі, що включає заходи, технології та політики для захисту інформаційних систем і мереж від несанкціонованого доступу та шкідливих атак. Основні складові включають захист даних, безпеку мережевих комунікацій, забезпечення конфіденційності, цілісності та доступності інформації. Важливими аспектами є оцінка ризиків, розробка політик і стандартів, а також моніторинг і реагування на інциденти. КБ грає критичну роль у захисті цифрових ресурсів та персональної інформації в умовах зростаючого використання Інтернету та ІКТ.

Правовий контекст КБ включає нормативно-правову базу, яка визначає вимоги до захисту інформаційних систем і даних. В Україні питання КБ регулюються рядом законів, зокрема Законом України «Про основні засади забезпечення КБ України», який окреслює принципи та структуру КБ. Міжнародні стандарти, такі як ISO 27032, надають методики для захисту віртуальних середовищ, зосереджуючи увагу на ризик-орієнтованому підході та координації між організаціями. Важливими є також національні стандарти, зокрема ДСТУ, що адаптують міжнародні вимоги до українських умов, сприяючи підвищенню рівня кіберзахисту.

Методи оцінки цифрової грамотності, такі як тести, інтерв’ю та анкети, дозволяють виміряти технічні, когнітивні та емоційні навички. Індекси, як Digital Literacy Index та DQ, оцінюють здатність ефективно використовувати цифрові

технології. Для точних результатів важливо враховувати контекст і адаптувати методи відповідно до нових викликів цифрової трансформації.

Використання методів тестування та анкетування на платформі, як-от «Дія. Цифрова освіта», надає можливість проводити оцінку на національному рівні, що робить ці методи особливо корисними для моніторингу і покращення цифрової грамотності громадян на широкому рівні.

Інституційні засади оцінки КБ через індекси GCI та NCSI підкреслюють важливість комплексного підходу до управління кіберзагрозами. GCI оцінює готовність країн до реагування на кіберзагрози, включаючи законодавчі, технічні та організаційні аспекти, а NCSI зосереджується на здатності держав реагувати на інциденти та захищати критичну інфраструктуру. Обидва індекси наголошують на значенні інституційної підготовленості та міжнародної співпраці для підвищення рівня КБ.

Персональні дані (19%) і фішинг (24%) є основними цілями кіберзагроз. Шкідливе програмне забезпечення (18%) вказує на масові атаки, а фінансові дані (13%) — на загрозу викрадення коштів. Атаки на критичну інфраструктуру (15%) та внутрішні загрози (5%) підкреслюють важливість посилення безпеки на всіх рівнях. Для ефективного протистояння сучасним кіберзагрозам суспільству необхідно зміцнювати захист персональних, фінансових і урядових даних, а також підвищувати обізнаність громадян щодо можливих небезпек в цифровому середовищі.

За результатами логарифмічної регресії між DDLI та NCSI - сильний зв’язок з коефіцієнтом кореляції $r = 0.749$. Це означає, що підвищення рівня КБ не завжди є достатнім для забезпечення розвитку цифрової грамотності.

Розрив між двома індексами DDLI та NCSI свідчить про те, що цифрова грамотність, хоча й є важливою складовою цифрового розвитку країни, не завжди узгоджується з її стратегіями в сфері КБ. Країни з великими розривами між індексами можуть потребувати додаткових зусиль для покращення цифрової грамотності своїх громадян, оскільки навіть із сильними технологічними заходами

відсутність свідомості та навичок у населення може зробити ці заходи менш ефективними.

У рамках дослідження розглянуто досвід низки успішних країн згідно з міжнародним рейтингом у сфері КБ та цифровізації. Згідно з NCSI Велика Британія, США, Сінгапур є країнами-лідерами у сфері КБ. Аналіз досвіду інших країн у КБ вказує на важливі аспекти для України. Зокрема, досвід Сінгапуру, де Агентство кібербезпеки координує національну стратегію і реагує на кіберзагрози, може бути корисним для створення або зміцнення відповідного органу в Україні. Сінгапур також виділяє значні кошти на дослідження КБ, що є важливим для України.

Традиційні методи захисту систем не відповідають вимогам швидко змінюваних кіберзагроз, що робить необхідним впровадження динамічних стратегій безпеки. Машинне навчання, як складова штучного інтелекту, є ефективним інструментом для виявлення загроз, реагування на інциденти та адаптації захисних механізмів у змінному кіберпросторі. Воно включає різні підходи, такі як навчання з учителем, без учителя, навчання з підкріпленням, аналіз природної мови, комп'ютерний зір, а також методи виявлення аномалій та кластеризації, що дозволяють вибирати оптимальні стратегії для конкретних завдань.

Розроблені нами рекомендації щодо стратегії кібербезпеки в Україні включають підвищення цифрової грамотності, зміцнення правової бази, розвиток інфраструктури, освіту фахівців, інформування громадськості, міжнародну співпрацю, технологічні інновації, фінансування та створення національної стратегії. Ці заходи є важливим кроком до забезпечення стійкості країни до кіберзагроз. Залучення всіх секторів суспільства дозволить сформувати надійну систему захисту в цифровому середовищі, сприяючи національній безпеці та розвитку цифрових технологій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Типовий проект галузевої програми, проекту, робіт з інформатизації. Наказ Міністерства цифрової трансформації України «Про затвердження Типового проекту галузевої програми, проекту, робіт з інформатизації» від 15 липня 2024 року № 108. URL: https://ips.ligazakon.net/document/FN083418

2. Закон України «Про стимулювання розвитку цифрової економіки в Україні» (Відомості Верховної Ради України (ВВР), 2023, №№ 6-7, ст.18). URL: https://zakon.rada.gov.ua/laws/show/1667-20#Text

3. Проєкт Концепції цифрової трансформації освіти і науки на період до 2026 року. Затверджено постановою Кабінету Міністрів України від 30 січня 2019 р. № 56. URL: https://mon.gov.ua/ua/news/koncepciya-cifrovoyi-transformaciyi-osviti-i-nauki-mon-zaproshuye-do-gromadskogo-obgovorennya

4. Digital strategy 2030. Міністерство цифрової трансформації: Стратегія цифрового розвитку 2030. URL: https://www.kmu.gov.ua/news/mintsyfry-prezentuvala-stratehiiu-rozvytku-elektronnykh-komunikatsii-do-2030-doluchaitesia-do-obhovorennia

5. Закон України «Про цифровий контент та цифрові послуги» від 10.08.2023 р. No 3321-IX. URL: https://cutt.ly/ReQkTIl6

6. Положення про електронні освітні ресурси: Наказ президента України від 19.07.2019 No z1696-12. URL: https://zakon.rada.gov.ua/laws/show/z1695-12#Text

7. Про затвердження «Положення про Національну освітню електронну платформу»: Наказ Міністерства освіти і науки України від 19.04.2019 No 521. URL: https://zakon.rada.gov.ua/laws/show/z0702-18#Text

8. Digital Education Action Plan (2021-2027). URL: https://education.ec.europa.eu/focus-topics/digital-education/action-plan

9. Gilster P. Digital Literacy. New York: Wiley. 8-th ed. 2019. 279 p.

10. Davydov S. G., Logunova O. S. Project “Digital Literacy Index”: methodical experiments. *Sociology: methodology, methods, mathematical modeling* (4M). 2015. № 41. Pp. 120−141.

11. Давиденко Г. Цифрова інклюзія та доступність: соціальна діджиталізація: монографія. Вінниця: ТВОРИ. 2023. 240 с. URL: https://cutt.ly/meEwKWe4

12. Chetty K., Wenwei L., Josie J., Shenglin B. Bridging The Digital Divide: Measuring Digital Literacy. The G20 Insights Platform offers policy proposals 2023. URL: https://www.g20-insights.org/wp-content/uploads/2023/04/-Digital-Bridgingthe-Digital-Divide-Measuring-Digital-Literacy.pdf

13. Уманець Н. Цифрова грамотність як інструмент включення людей похилого віку у сучасне суспільство. *Духовність особистості: методологія, теорія і практика.* 2024. Випуск 1. DOI: https://doi.org/10.33216/2220-6310/2023-107-3-203-211.

14. Bushati E., Bregu Z. The Process of Digitalization of Audiovisual Media in Albania. *Balkan Social Science Review.* 2023. Volume 21, Issue 21. P. 255–277. DOI: https://doi.org/10.46763/BSSR2321255b

15. Borian L.O. Computer literacy is the basis of the information culture of a modern person. *Modern computer technologies in economics and education: materials of the Black Sea regional scientific and practical conference of the professorial and teaching staff, Mykolaiv: MDAU*. 2022. Pp 126-128.

16. Комплементарність інформаційно-цифрових і соціально-економічних перетворень як умова стабільного розвитку суспільства : монографія. За ред. чл.-кор. НАН України А.А. Гриценка; НАН України, ДУ «Ін-т екон. та прогнозув. НАН України». К.: 2021. 400 с.

17. Сокальська Н.Л., Дмитрієва Н.Б., Крикляс В.Г., Крикляс К.В., Третьякова Т.М. Актуалізація комунікаційної компетентності педагога у цифровому форматі діяльності. *Інноваційна педагогіка. Теорія та методика навчання (з галузей знань)*. 2024. Випуск 71. Том 2. С. 23-29. DOI: https://doi.org/10.32782/2663-6085/2024/71.2.4

18. Панасюк В. М. Інформатизація та цифровізація: тенденції та напрями розвитку в Україні. *Інтелект XXI.* 2020. № 1. С. 160-165. DOI: https://doi.org/10.32782/2415-8801/2020-1.29

19. Cybersecurity and Digital Business Risk Management. URL: https://www.gartner.com/en/information-technology/insights/cybersecurity

20. Корченко О.Г., Бурячок В.Л., Гнатюк С.О. Кібернетична безпека держави: характерні ознаки та проблемні аспекти. *Безпека інформації.* 2020. Т. 1. № 19. С. 40-44.

21. Пановик У. П., Ткачук Р. Л.Кібербезпека через призму системного аналізу. *Computer technologies of printing*. 2023. № 1(49). С. 197-208.

22. Мінцифри презентувало нову версію національного тесту на цифрову грамотність «Цифрограм 2.0». URL: https://itc.ua/news/minczifri-prezentuvalo-novu-versiyu-naczionalnogo-testu-na-czifrovu-gramotnist-czifrogram-2-0/

23. Цифрограм «Дія. Цифрова освіта». Тестування для оцінки рівня цифрової грамотності за європейськими стандартами DigComp 2.1. URL: https://osvita.diia.gov.ua/digigram

24. Національний тест на цифрову грамотність втілений за підтримки Агентства США з міжнародного розвитку (USAID). URL: https://thedigital.gov.ua/news/pershi-50000-ukraintsiv-pochali-skladati-natsionalniy-test-na-tsifrovu-gramotnist-tsifrogram

25. Давидов С. Г., Логунова О. С. Проєкт «Індекс цифрової грамотності»: методичні експерименти. *Соціологія: методологія, методи, математичне моделювання.* 2023. № 41. С. 120-141.

26. Ребко О. В. Інформаційна грамотність: визначення, компоненти та стандарти. *Студентська наука і XXI століття. 2020*. Т. 17. № 2 (20). С. 257-259.

27. Global Cybersecurity Index. GCI: 5th edition. 2024. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI/GCI-Media.aspx

28. National Cyber Security Index, NCSI framework. URL: NCSI :: Methodology

29. National Cyber Security Index, NCSI. Description of indicators. URL: NCSI :: Description of indicators

30. NCSI, eGA's National Cyber Security Index. URL: Cybersecurity - e-Governance Academy

31. Ranking of the National cybersecurity Index. URL: https://ncsi.ega.ee/ncsiindex/.

32. Shafqat N., Masood A. Comparative analysis of various national cyber security strategies. *International Journal of Computer Science and Information Security*. 2024. Vol. 14. №. 1. Pp. 129-137.

33. NCSI. Archived data. URL: NCSI :: Ranking

34. NCSI. Ranking data. Ukraine. URL: NCSI :: Ukraine

35. ITU Committed to connecting the world. Legislation. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/legislation.aspx.

36. Issabayeva S., Yesseniyazova B., Grega M. Electronic Public Procurement: Process and Cybersecurity Issues. NISPAcee *Journal of Public Administration and Policy*. 2024. Т. 12. №. 2. С. 61-79.

37. Cyber security: advice for small businesses, Official UK Government Website. URL: https://www.gov.uk/government/publications/cyber-security-what-smallbusinesses-need-to-know.

38. Large organisations, National Cyber Security Center of the UK. URL: https://www.ncsc.gov.uk/section/information-for/large-organisations.

39. National Cyber Security Center of the UK. URL: https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security.

40. Cyber Essentials powered by National Cyber Security Center of the UK. URL: https://www.cyberessentials.ncsc.gov.uk

41. Кібербезпека в інформаційному суспільстві : інформаційно-аналітичний дайджест / відп. ред. О. Довгань ; упоряд. О. Довгань, Л. Литвинова, С. Дорогих. Державна наукова установа «Інститут інформації, безпеки і права НАПрН України» ; Національна бібліотека України ім. В.І. Вернадського. Київ, 2023. № 10. 320 с.

ДОДАТКИ

Додаток А

Таблиця А - Практична реалізація основних знань, умінь та навичок за компонентами цифрової грамотності

Характерні знання, вміння та навички	Види цифрової грамотності				
	Інформаційна грамотність	Медійна грамотність	Комп'ютерна грамотність	Обчислювальна грамотність	Комунікативна грамотність
1	2	3	4	5	6
Розуміння структури цифрових медіа	Користувач розуміє, як влаштовані ЗМІ (в т.ч. цифрові)	Користувач знайомий з технічною стороною функціонування цифрових ЗМІ	Користувач розуміє, яким чином налаштовуються розсилки, інформаційна стрічка та яке програмне забезпечення використовується з цією метою	Має значення в частині програмування та технічного розміщення інформації в цифровому середовищі (вебдизайн, анімації тощо)	Користувач розуміє та вміє ефективно застосовувати механізми роботи цифрових медіа для вирішення своїх комунікативних завдань
Розуміння та вміння ефективно використовувати різні формати представлення даних	Користувач розуміє, що інформація може бути представлена в різних форматах, і вміє шукати необхідні дані, виходячи з цього знання	Користувач розбирається у форматах представлення даних, програмних засобах роботи з ними	Має слабкий вираз, відноситься лише до розуміння того, яка програма здатна відкрити файл з тим чи іншим розширенням	Має значення лише в тій мірі, як це стосується програмування та технічної сторони розміщення інформації в цифровому середовищі	Користувач знає та вміє застосовувати різні формати подання даних для найбільш ефективного досягнення своїх комунікативних цілей у цифровому середовищі
Пошук та управління інформацією	Користувач усвідомлює цінність інформації, наслідки її поширення для своєї та чужої репутації, застосовує ці знання для досягнення своїх цілей	Користувач обізнаний, який вплив має аудивізуальне та текстове подання інформації	Має слабке вираження, відноситься лише до вміння користуватися програмами для пошуку файлів та папок	Має значення лише тією мірою, як це стосується програмування і технічної боку розміщення інформації у цифровій середовищі. Наприклад, просування веб-сайтів, виведення в топ пошукових систем	Користувач вміє ефективно керувати своїм цифровим слідом, знає, яким чином створюється цифрова ідентичність, має навички вибудовування ефективної цифрової комунікації в особистих, ділових та суспільних цілях
Вирішення комунікативних завдань найвідповідніщими цифровими засобами	Користувач вміє скласти пошуковий запит так, щоб знайдена інформація відповідала його цілям та завданням	Користувач вміє подати необхідну інформацію в різних форматах, що найбільш підходять до його цілей та завдань	Користувач вміє працювати з комп'ютерними програмами для обміну повідомленнями	Має значення лише тією мірою, як це стосується програмування і технічної боку розміщення й обміну інформацією цифровому середовищі. Наприклад, створення різних чатів та месенджерів	Користувач знає, в якому форматі його інформація буде представлена найбільш наочно та ефективно досягне поставленої мети, та вміє вибирати формати та способи подання даних залежно від ситуації спілкування та комунікативних цілей
Критичне мислення	Користувач обізнаний про вплив «фейкової» інформації, про технології та причини її появи, відрізняє рекламну, недостовірну інформацію від достовірної	Користувач обізнаний з технологіями створення «фейкових» фото-, відео- та аудіоматеріалів, а також про способи їх перевірки на справжність	Користувач обізнаний про вплив шкідливих програм, вміє їх відрізнити та боротися з ними, а також знає та застосовує способи захисту від них	Має значення тією мірою, як це стосується оцінки якості та необхідності створення програмного продукту	Користувач вміє аналізувати інформацію, що надходить, і реагує на неї найбільш відповідним для конкретної ситуації чином

Навички роботи з ПК	Має значення в частині вміння шукати інформацію будь-якими способами (онлайн та офлайн)	Користувач впевнено оперує програмним забезпеченням для створення мультимедійних продуктів	Користувач має достатнє знання базових комп'ютерних програм і вміє з їх допомогою вирішувати свої робочі, навчальні та особисті завдання	Користувач може сам створювати найпростіші програмні продукти	Користувач вміє вирішувати свої комунікативні завдання в цифровому середовищі, застосовуючи для цього найбільш відповідні програмно-технічні засоби
Розуміння інформаційної мети та складання пошукових запитів на її основі	Користувач усвідомлює свою інформаційну мету, розуміє, якими засобами може її досягти та з яких джерел може отримати необхідну інформацію	Користувач вміє шукати з урахуванням різних форматів представлення даних	Користувач обізнаний про те, як влаштовані та за якими принципами працюють пошукові системи	Користувач знає та вміє налаштовувати систему пошуку в своїх програмних продуктах	Користувач вміє знаходити та використовувати інформацію, що сприяє досягненню його комунікативної мети
Створення власної інформації	Користувач створює інформацію залежно від поставленої мети та вибирає найефективніші засоби для її поширення	Користувач створює власні мультимедійні продукти для візуалізації необхідної інформації	Користувач знайомий з технічними та програмними засобами виробництва, обробки, зберігання, захисту та поширення інформації, вміє ефективно їх застосовувати	Користувач знайомий з принципами роботи програмних засобів для створення, зберігання, обробки, захисту та поширення інформації, вміє налаштувати їх роботу найефективнішим чином	Користувач володіє технологіями створення, зберігання, захисту, поширення інформації та ефективно застосовує їх для досягнення своїх комунікативних цілей
Знання принципів роботи програмного та апаратного забезпечення	Користувач розуміє принцип роботи засобів пошуку, створення, розповсюдження та перевірки інформації	Користувач розуміємо, як працюють засоби створення аудіовізуального та мультимедійного контенту	Користувач знайомий з пристроєм, принципами створення та функціонування програмно-апаратного комплексу	Користувач знайомий з пристроєм, принципами створення та функціонування програмно-апаратного комплексу	Користувач обізнаний з принципами роботи засобів створення та розповсюдження інформації, вміє ефективно використовувати відповідне ПЗ для досягнення комунікативних цілей

Рисунок А - П'ять компонентів цифрової грамотності

Додаток Б

Таблиця Б.1 - Хронологія розвитку кібератак від початку їх появи до сьогодення

Рік	Кібератака \ Кіберзагроза	Опис	Наслідки
1988	Черв'як Морріса	Перший відомий випадок використання комп'ютерного черв'яка, який поширювався через Інтернет	Уражено 10% комп'ютерів у мережі ARPANET
1995	Макровіруси	З'явилися віруси, які вбудовувалися у файли Microsoft Word, поширюючись через електронну пошту	Масове зараження офісних документів
1999	Вірус Melissa	Вірус, що поширювався через електронну пошту, використовуючи інфіковані вкладення	Збої в роботі систем та поширення вірусу через мільйони листів
2000	DDoS-атаки на Yahoo та Amazon	Масові атаки на популярні вебсайти, які перевантажували сервери запитами	Значні перебої в роботі популярних інтернет-ресурсів
2007	Кібератака на Естонію	Масштабна кібератака, яка заблокувала урядові та банківські системи країни	Збої в роботі інфраструктури країни, підвищення уваги до кібербезпеки
2010	Стакснет (Stuxnet)	Вірус, розроблений для ураження ядерних об'єктів Ірану, який впливав на фізичне обладнання	Пошкоджено центрифуги для збагачення урану в Ірані
2013	Злам Yahoo	Викрадення даних 3 мільярдів облікових записів користувачів	Масове розголошення особистих даних
2017	WannaCry	Вірус-вимагач, який шифрував дані та вимагав викуп у криптовалюті за їх розшифровку	Постраждало понад 200 тисяч систем у 150 країнах
2020	Злам SolarWinds	Хакерська атака через заражене програмне забезпечення для моніторингу	Викрадено дані урядових і приватних компаній США
2021	Ransomware-атаки на Colonial Pipeline	Вірус-вимагач, що паралізував роботу трубопроводу в США	Збої в постачанні палива та виплата викупу в криптовалюті
2022	Кібератаки на Україну	Масштабні кібератаки під час військової агресії, спрямовані на урядові та критичні інфраструктури	Пошкодження баз даних, дестабілізація інфраструктури
2024	Штучний інтелект (ШІ, AI) у кібератаках	Використання AI для створення складніших фішингових схем, автоматизації DDoS-атак та вдосконалення зловмисного ПЗ	Посилення складності виявлення атак, підвищення витрат на кіберзахист

Таблиця Б.2 - Міжнародний та вітчизняний огляд терміна «кібербезпека»

Автор / Ресурс	Визначення
Ю. І.Когут	Кібербезпека – це стан захищеності інформації в електронній формі та середовища її обробки, зберігання, передавання (електронних інформаційних ресурсів, інформаційних систем та інформаційно-комунікаційної інфраструктури) від зовнішніх і внутрішніх загроз, тобто інформаційна безпека у сфері інформатизації [42]
Ю. П. Лісовська	Кібербезпека – це постійне застосування передових практик, спрямованих на забезпечення та збереження конфіденційності, цілісності й доступності цифрової інформації, а також безпеки людей та навколишнього середовища» [43]
Lexico (Оксфордський словник)	Кібербезпека – це стан захищеності від злочинного чи несанкціонованого використання електронних даних або заходи, прийняті для досягнення цієї мети [44]
Кембриджський словник	Кібербезпека – це дії, які робляться для захисту особи, організації чи країни та їхньої комп'ютерної інформації від злочинів або атак, здійснених через Інтернет [45]
Компанія Cisco	Кібербезпека – це реалізація заходів для захисту систем, мереж і програмних додатків від цифрових атак [46]

IT Gartner	Кібербезпека – це сукупність людей, політик, процесів і технологій, які використовує підприємство для захисту своїх кібер-активів [47]
Національний інститут стандартів і технологій (NIST)	Кібербезпека – це процес захисту інформації шляхом запобігання, виявлення та реагування на атаки [48]

Таблиця Б.3 - Стандарти ISO/IEC щодо забезпечення КБ

№ стандарту	Назва стандарту	Опис стандарту	Рік публікації
ISO/IEC 27001	Система управління інформаційною безпекою (ISMS)	Визначає вимоги для створення, впровадження та вдосконалення системи управління інформаційною безпекою	2005
	Управління конфіденційністю (PIMS)	Розширення до ISO/IEC 27001 для управління конфіденційністю даних	2019
	Оновлення системи управління інформаційною безпекою (ISMS)	Оновлені вимоги до управління інформаційною безпекою, включаючи аспекти контексту організації та оцінки ризиків	2022
ISO/IEC 27002	Практики інформаційної безпеки	Рекомендації щодо впровадження заходів безпеки в організації	2005
	Оновлення практик інформаційної безпеки	Оновлені рекомендації для організацій щодо впровадження заходів безпеки, з новими контрольними заходами	2022
ISO/IEC 27005	Управління ризиками інформаційної безпеки	Стандарт для аналізу та управління ризиками інформаційної безпеки	2011
ISO/IEC 27017	Захист персональних даних у хмарі	Стандарт, що фокусується на захисті персональних даних у хмарних середовищах	2015
ISO/IEC 27018	Захист персональних даних у хмарі	Стандарт, що фокусується на захисті персональних даних у хмарних середовищах	2014
ISO/IEC 27032	Безпека в кіберпросторі	Зосереджується на захисті у кіберпросторі та взаємодії між різними секторами	2012 (останнє оновлення 2023)
ISO/IEC 27035	Управління інцидентами інформаційної безпеки	Охоплює процеси управління інцидентами та реагування на кіберзагрози	2011
ISO/IEC 22301	Управління безперервністю бізнесу	Охоплює аспекти КБ у разі кризових ситуацій та відновлення після інцидентів	2012
ISO/IEC 15408	Common Criteria	Стандарт для оцінки безпеки інформаційних технологій, використовується для сертифікації	1999 (останнє оновлення 2017)

Таблиця Б.4 - Базові заходи КБ

Категорія безпеки	Захід безпеки
Безпека застосунків	Повідомлення користувачів про політику безпеки
	Захист сесій веб-додатків
	Контроль коректності введених даних (захист від SQL-інжекцій)
	Забезпечення безпеки скриптів (захист від атак міжсайтового скриптингу)
	Аудит коду та незалежне тестування програмного коду
	Підтвердження автентичності провайдера для споживачів
Безпека серверів	Безпечне конфігурування серверів
	Встановлення системи оновлень безпеки
	Контроль системних журналів
	Захист від шкідливих програм
	Регулярне сканування контенту на наявність шкідливих програм
	Регулярне сканування вразливостей сайту і додатків
	Виявлення спроб злому
Безпека кінцевих користувачів	Використання рекомендованих версій операційних систем
	Використання рекомендованих версій програмних додатків
	Використання антивірусних засобів
	Налаштування веб-браузерів у безпечному режимі
	Блокування або безпечне виконання скриптів
	Використання фільтрів фішингу

	Використання додаткових механізмів безпеки веб-браузерів
	Використання персональних міжмережевих екранів і систем виявлення вторгнень
	Використання автоматичних оновлень довірених програм
Захист від атак методами соціальної інженерії	Розроблення та впровадження політик безпеки
	Категорування та класифікація інформації
	Навчання та підвищення обізнаності користувачів
	Тестування співробітників
	Мотивація і стимулювання співробітників
	Використання технічних механізмів контролю
Підвищення готовності	Використання пасток у "порожній" мережі
	Перенаправлення шкідливого трафіку
	Зворотне трасування

Таблиця Б.5 - Національні стандарти в галузі КБ

Позначення ДСТУ	Найменування
Системи управління інформаційною безпекою	
ДСТУ ISO/IEC 27001:2015	ІТ. Система управління інформаційною безпекою. Вимоги
ДСТУ ISO/IEC 27701:2021	ІТ. Розширення до ISO/IEC 27001 та ISO/IEC 27002 для управління конфіденційністю (PIMS)
ДСТУ ISO/IEC 27002:2015	ІТ. Методи захисту. Звід практик щодо заходів інформаційної безпеки
ДСТУ ISO/IEC 27003:2020	ІТ. Настанови щодо впровадження системи управління інформаційною безпекою
Управління ризиками	
ДСТУ ISO/IEC 27005:2015	ІТ. Управління ризиками інформаційної безпеки
ДСТУ ISO 31000:2020	ІТ. Менеджмент ризиків. Принципи та настанови
Оцінка безпеки	
ДСТУ ISO/IEC 15408-1:2020	ІТ. Методи захисту. Критерії оцінки безпеки інформаційних технологій. Частина 1
ДСТУ ISO/IEC 15408-2:2021	ІТ. Методи захисту. Критерії оцінки безпеки інформаційних технологій. Частина 2
ДСТУ ISO/IEC 15408-3:2021	ІТ. Методи захисту. Критерії оцінки безпеки інформаційних технологій. Частина 3
Гарантії безпеки	
ДСТУ ISO/IEC 15026-1:2015	ІТ. Системи та програмне забезпечення. Гарантії безпеки. Принципи та концепції
Безпека мереж	
ДСТУ ISO/IEC 27033-1:2021	ІТ. Методи захисту. Безпека мереж. Огляд і концепції
Захист хмарних сервісів	
ДСТУ ISO/IEC 27017:2021	ІТ. Методи захисту. Кодекс практики для хмарних сервісів
ДСТУ ISO/IEC 27018:2021	ІТ. Методи захисту. Захист персональних даних у хмарних обчисленнях
Забезпечення безперервності бізнесу	
ДСТУ ISO 22301:2014	ІТ. Системи управління безперервністю бізнесу. Вимоги
ДСТУ ISO/IEC 27031:2016	ІТ. Настанови щодо забезпечення готовності ІКТ до підтримання безперервності бізнесу
ДСТУ ISO/IEC 27035:2021	ІТ. Управління інцидентами інформаційної безпеки
Проєктування систем безпеки	
ДСТУ ISO/IEC 21827:2019	ІТ. Інженерія безпеки систем. Модель зрілості процесу

Додаток В

Таблиця В.1 - Ключові індекси та показники цифрової грамотності

Категорія	Назва показника/індексу	Опис	Приклади застосування
Індекси цифрової грамотності	Індекс цифрової грамотності (Digital Literacy Index)	Узагальнений показник базових та спеціалізованих цифрових навичок: інформаційна, технологічна, комунікативна грамотність	Оцінювання рівня цифрових навичок громадян для освітніх та економічних досліджень
	Індекс готовності до цифрової економіки (DESI)	Комплексний індекс, що охоплює цифрові навички в контексті економіки та суспільного розвитку.	Визначення рівня готовності країн до цифрової трансформації
	ISD (Index of Sustainable Development) або DDLI (Digital Development Level Index)	Інтегрує оцінку доступності цифрової інфраструктури, цифрової грамотності та адаптації технологій до потреб сталого розвитку	Аналіз впливу цифрових технологій на соціально-економічний розвиток
Показники цифрової грамотності	Показник інформаційної грамотності	Оцінка здатності ефективно шукати, аналізувати та використовувати інформацію в цифровому середовищі	Визначення ефективності роботи з інформацією (наприклад, час пошуку даних, точність їх обробки)
	Показник технічних навичок	Кількісна оцінка виконаних технічних завдань (робота з текстами, таблицями, програмами тощо)	Аналіз ефективності використання програмного забезпечення у робочих процесах
	Показник комунікації в цифровому середовищі	Визначає здатність взаємодіяти через онлайн-сервіси, брати участь у відеоконференціях, соцмережах	Вимірювання ефективності дистанційної роботи або навчання
	Показник кіберзахисту	Оцінює дотримання правил безпеки в інтернеті (захист даних, уникнення кіберзагроз)	Аналіз навичок користувачів щодо уникнення фішингових атак, створення надійних паролів
Національні системи оцінки	Національний індекс цифрової грамотності України	Інструмент для визначення середнього рівня цифрових навичок громадян України	Результати тестування на платформах, таких як «Дія.Цифрова освіта»
Комплексні рейтинги	Global Connectivity Index (GCI)	Оцінка розвитку цифрової інфраструктури та рівня грамотності в різних країнах	Порівняння країн за рівнем доступності цифрових технологій
	Digital Inclusion Index	Показує доступність цифрових технологій, освітній рівень та готовність населення до використання ІТ	Використовується для визначення рівня включеності у цифрове суспільство

Таблиця В.2 - Ключові напрями оцінки цифрового сталого розвитку за ISD

Сфера застосування	Характеристика
Цифрова інфраструктура та доступність технологій	Оцінюється рівень доступу до цифрових технологій, швидкість Інтернету та доступність широкосмугового зв’язку
Рівень цифрових навичок	Важливим компонентом є оцінка рівня цифрової грамотності громадян, доступність програм навчання та підтримка розвитку навичок
Кібербезпека та захист даних	Оцінка безпеки цифрових технологій, захисту персональних даних та рівня готовності країни до кіберзагроз
Інновації та НДДКР	Вимірюється рівень інвестицій в інновації та розвиток технологій, що сприяють сталому економічному розвитку

Соціальна інтеграція та інклюзивність	Цей аспект відображає рівень соціальної інтеграції, включаючи доступ до цифрових послуг для соціально незахищених груп населення, підтримку рівних можливостей і мінімізацію цифрового розриву серед різних соціальних верств, сприяє забезпеченню рівного доступу до технологій, а також включенню у цифрове суспільство всіх громадян, незалежно від їх соціального чи економічного статусу

Рис. В.1 - П’ять компонентів оцінки рівня КБ за GCI

Таблиця В.3 - П’ять компонентів оцінки рівня КБ за GCI

Компонент оцінки	Опис
Юридичний	Оцінка наявності та ефективності законодавчих і нормативних актів, що забезпечують КБ на національному рівні. Це включає закони щодо захисту даних, боротьби з кіберзлочинністю та кіберзлочинністю, захисту прав і приватності в Інтернеті. Включає також національні стратегії КБ та зобов’язання щодо міжнародного співробітництва
Технічний	Оцінка технологічної інфраструктури і здатності країни захищати свої критичні інформаційні системи від кіберзагроз. Це включає розгортання систем моніторингу, реагування на кіберінциденти, забезпечення стійкості і безпеки інфраструктури критичних секторів економіки, таких як енергетика, транспорт, фінанси
Організаційний	Оцінка створення інститутів і організацій на державному та недержавному рівнях для управління, стратегії й координації національних ініціатив у сфері КБ. Це включає наявність органів, відповідальних за політику КБ, розробку планів дій у разі інцидентів, а також співпрацю з іншими державами
Підготовка кадрів	Оцінка наявності національних програм освіти та тренінгів, спрямованих на розвиток кваліфікації фахівців з КБ. Це включає також вивчення рівня кваліфікації персоналу в установах і підприємствах, готовність працювати з кіберзагрозами та організацію сертифікацій для фахівців
Співпраця	Оцінка рівня міжнародної співпраці країни в сфері КБ, включаючи участь у міжнародних організаціях, обмін інформацією та координацію дій з іншими державами. Важливим аспектом є наявність двосторонніх і багатосторонніх угод про співпрацю з питань КБ та спільне реагування на кіберінциденти

Таблиця В.4 - Порівняльний аналіз методів оцінювання GCI та NCSI

Найменування	Глобальний індекс КБ	Національний індекс КБ
Мета дослідження	GCI вимірює прихильність країн до КБ на глобальному рівні - для підвищення обізнаності про важливість і різні аспекти цієї проблеми	NCSI вимірює готовність країн до запобігання кіберзагрозам та управління кіберінцидентами. Ресурси бази даних можуть використовуватися для нарощування потенціалу національної КБ

Основний метод	Онлайн-опитування* з аналізом підтверджувальних документів (сайти)	Збір даних (факти, НПА, офіційні документи та сайти)
Основні показники / параметри	- розвиток потенціалу; - правові заходи; - технічні; - показники; - організаційні заходи; - співпраця	- чинне законодавство; - створені підрозділи (організації); - формати співпраці
Кількість індикаторів	25: щодо них сформульовано 157 запитань	46 (3 категорії та 12 характеристик)

*Примітка: * - якщо країна не відповідає на онлайн-опитування, то дослідження проводиться незалежно Центром на підставі відкритих онлайн-ресурсів країни*

Таблиця В.5- Найцінніші дані для зловмисників та ключові кіберзагрози для суспільства в 2023 році

Найбільш цінні дані для зловмисників	%	Кіберзагрози для суспільства	%
Персональні дані громадян (ім'я, адреса, контакти)	19	Фішинг	24
Медичні записи	14	Шкідливе ПЗ	18
Фінансові дані (банківські рахунки, кредити)	13	Атаки на критичну інфраструктуру	15
Дані урядових організацій	10	Кібератаки для викрадення коштів	14
Логіни та паролі для особистих акантів	10	Шахрайство	12
Конфіденційна інформація освітніх закладів	8	Викрадення інтелектуальної власності	8
Дані з соціальних мереж	7	Спам	6
Інформація про майно чи активи громадян	5	Атаки "зсередини"	5
Запити на соцдопомогу чи благодійність	4	Кібератаки для знищення даних	4
Стратегічні документи місцевих адміністрацій	3	Шпіонаж	2

Рангу	Країна	Національний індекс кібербезпеки	Рівень цифрового розвитку	Різниця
1.	Чеська Республіка	98.33	72.04	26.29
2.	Польща	92.50	72.29	20.21
3.	Бельгія	92.50	74.86	17.64
4.	Італія	88.33	72.98	15.35
5.	Канада	87.50	78.55	8.95
6.	Австралія	87.50	82.21	5.29
7.	Естонія	85.83	80.02	5.81
8.	Литва	85.00	73.93	11.07
9.	Австрія	85.00	78.57	6.43
10.	США	84.17	84.21	-0.04
11.	Молдова (Республіка)	81.67	60.10	21.57
12.	Нідерланди	81.67	84.94	-3.27
13.	Україна	80.83	67.73	13.10
14.	Словакія	80.83	68.58	12.25
15.	Латвія	79.17	71.88	7.29
16.	Ірландія	77.50	76.59	0.91
17.	Кіпр	76.67	72.52	4.15
18.	Великобританія	75.00	82.07	-7.07
19.	Азербайджан	73.33	57.47	15.86
20.	Сербія	72.50	67.03	5.47

Рисунок В.2 - Порівняння NCSI та DDLI в різних країнах (ТОП-20 рейтингу)

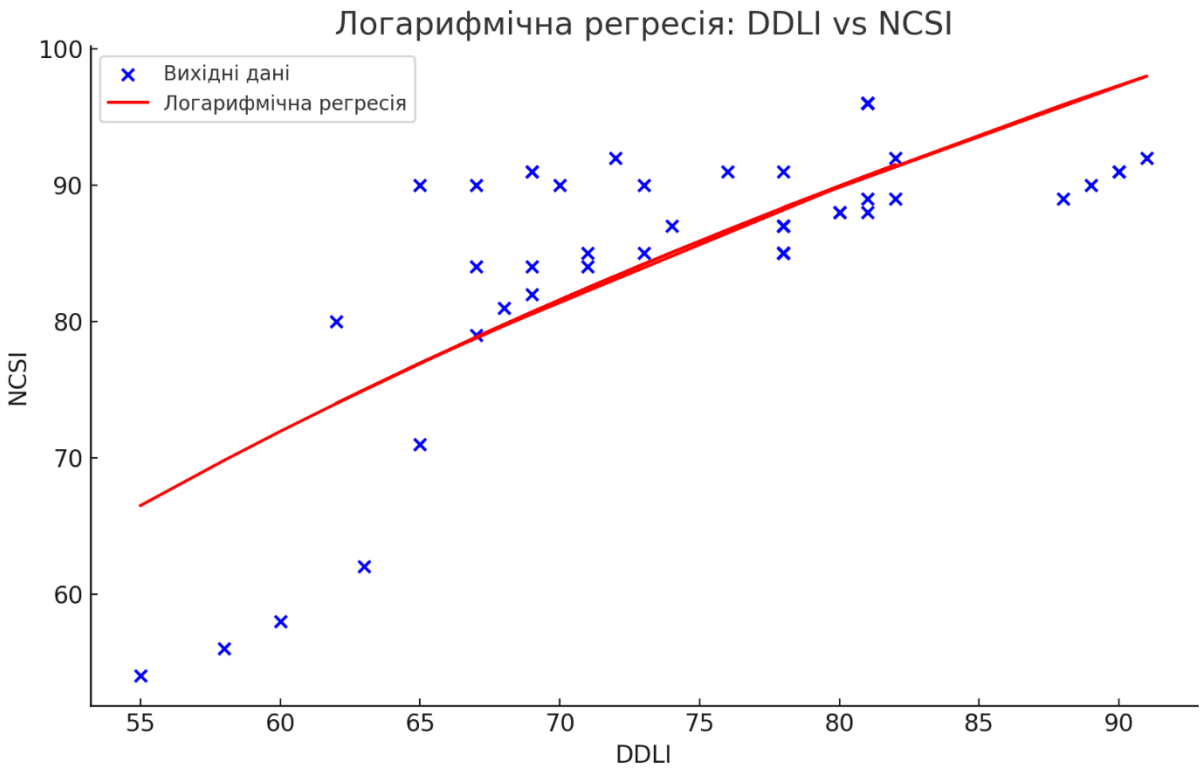

Рисунок В.3 – Логарифмічна регресія між DDLI та NCSI країн

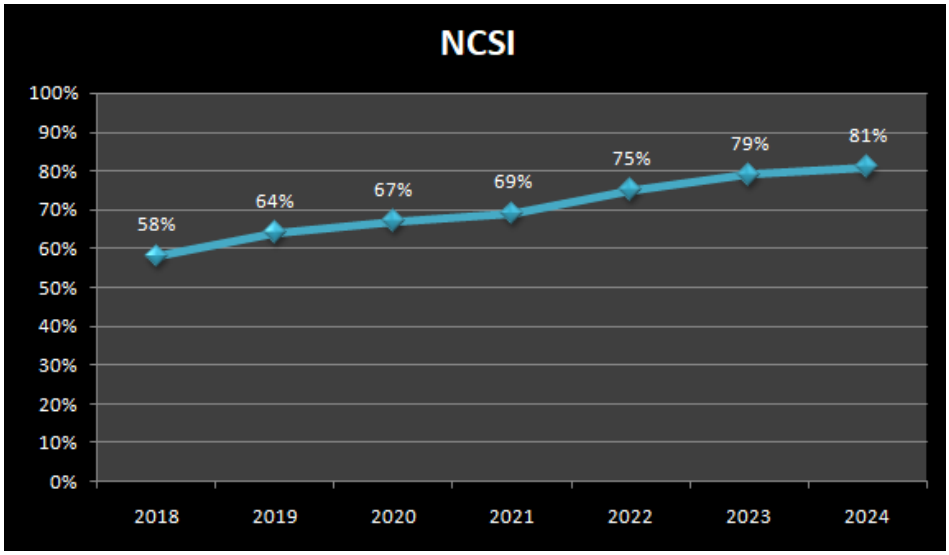

Рисунок В.4 - Графік розробки NCSI для України з 2018 до 2024 рр.

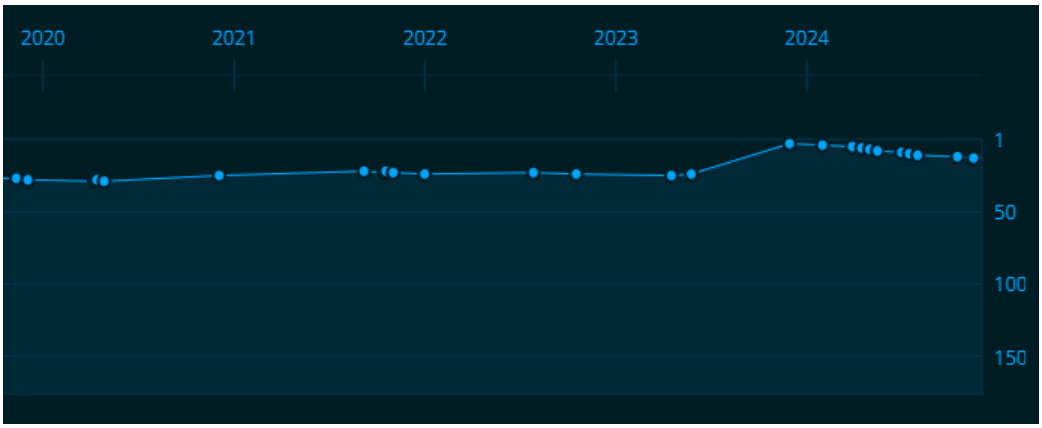

Рисунок В.5 - Хронологія ранжування NCSI в Україні за 2019-2024 рр.

Додаток Г

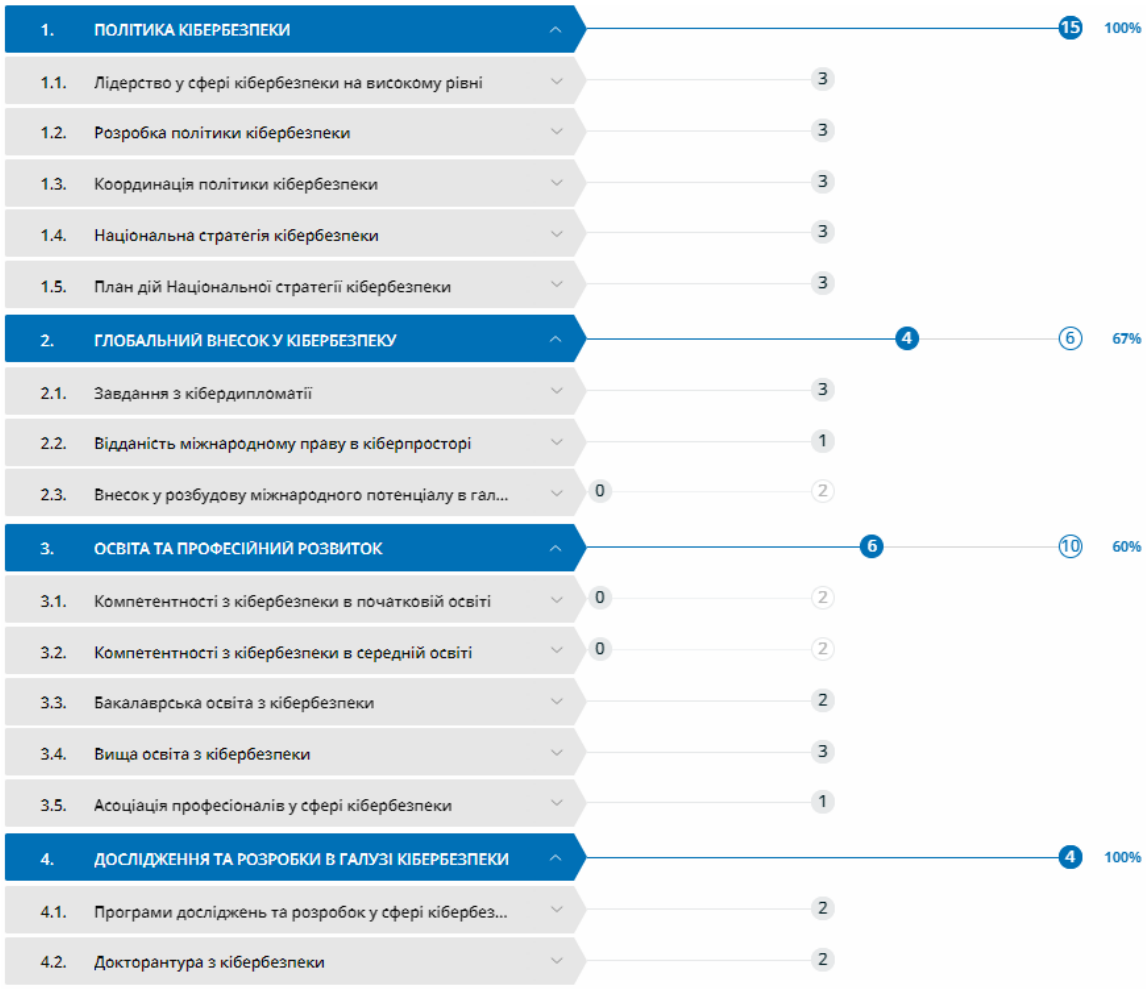

Рисунок Г.1 - Стратегічні індикатори КБ NCSI України в 2024 році

Додаток Г - продовження

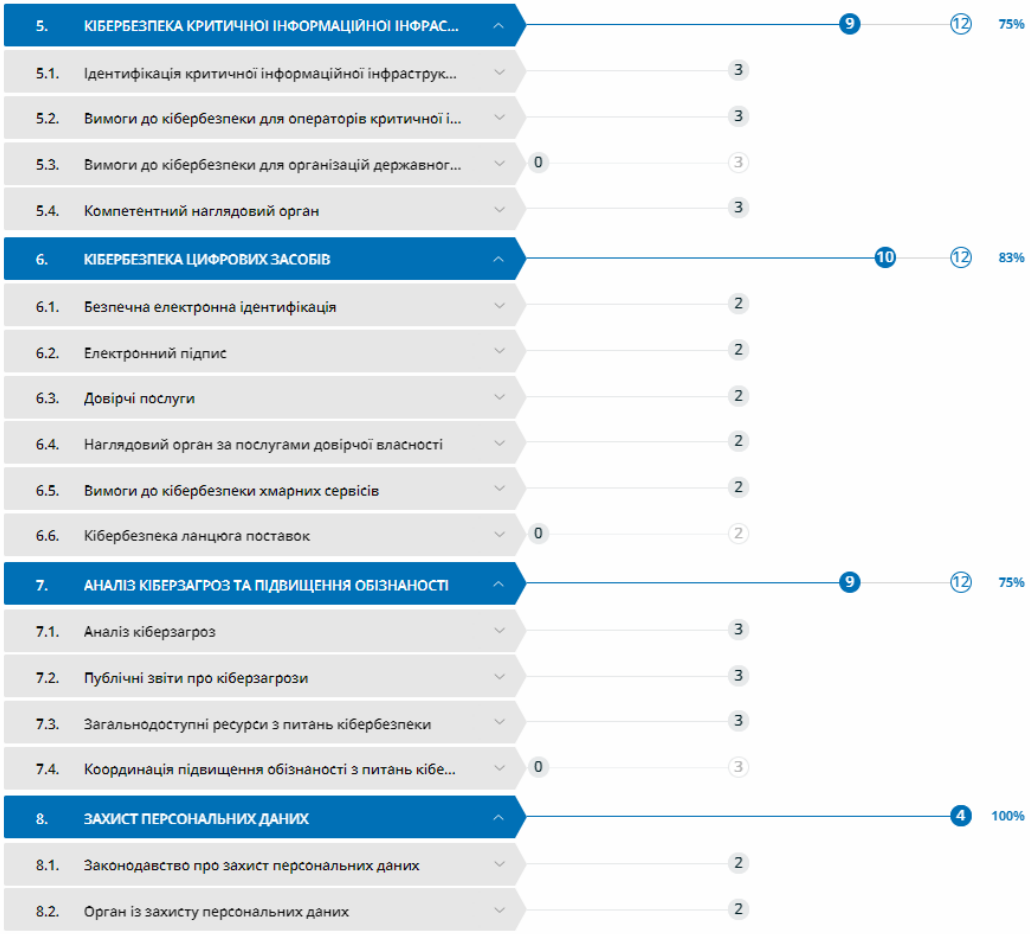

Рисунок Г.2 - Превентивні індикатори NCSI України в 2024 році

Додаток Г - продовження

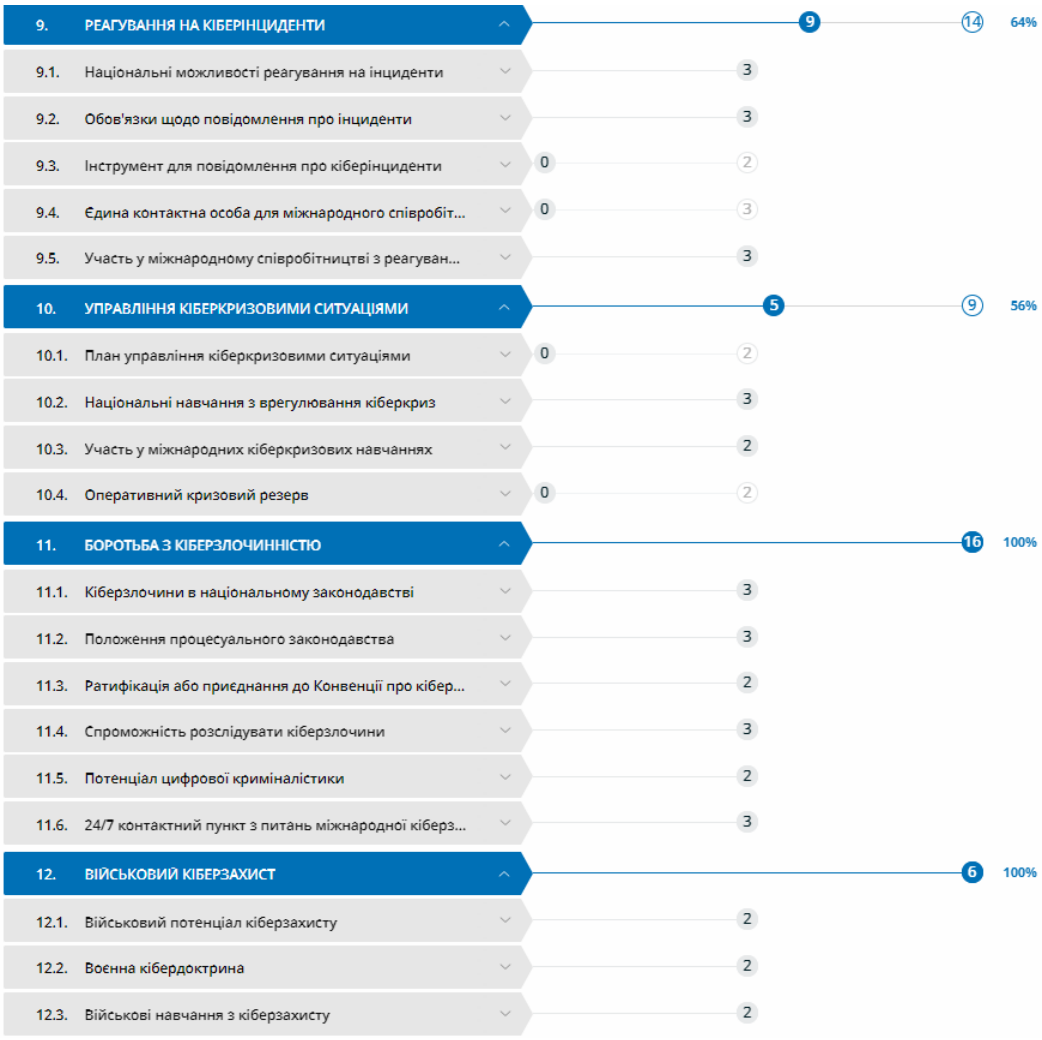

Рисунок Г.3 - Адаптивні індикатори КБ NCSI України у 2024 році

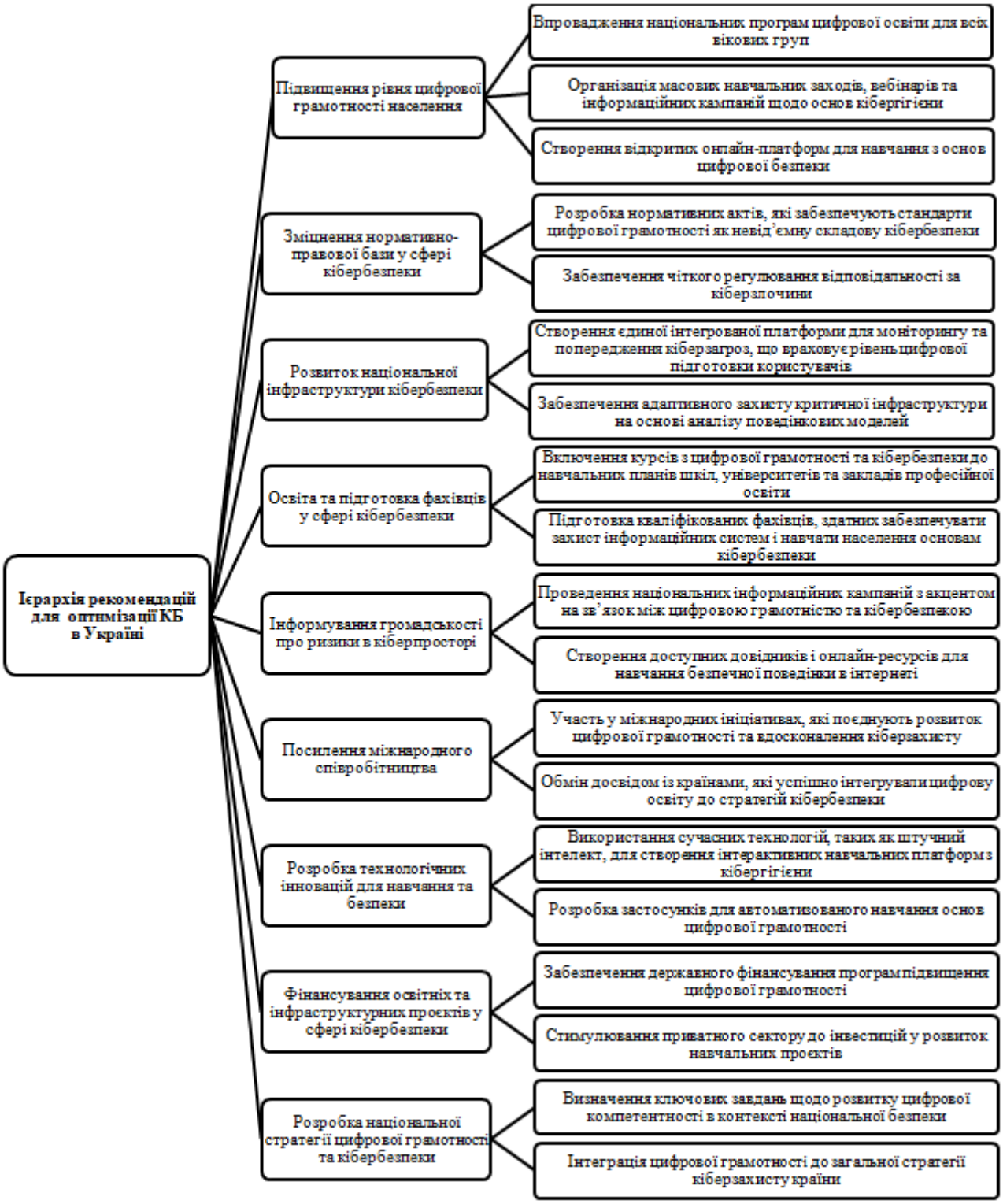

Рисунок Г.4 - Структура рекомендацій щодо забезпечення КБ в Україні