МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Харківський національний університет імені В.Н. Каразіна

Факультет: **ННІ Каразінський банківський інститут**
Кафедра: **Інформаційних технологій та математичного моделювання**
Спеціальність: **125 Кібербезпека**
Освітня програма: **Кібербезпека у фінансових технологіях**

Група: АБ-41б **денна форма навчання**

КВАЛІФІКАЦІЙНА БАКАЛАВРСЬКА РОБОТА

на тему:

КІБЕРВІЙНА В ОЧАХ ГРОМАДСЬКОСТІ: ОЦІНКА ОБІЗНАНОСТІ, ДЕЗІНФОРМАЦІЇ ТА ДОВІРИ ЗА НАКАЗОМ № 4601-5/335 ВІД 07 ЛЮТОГО 2025 РОКУ

здобувача вищої освіти Самчук Дарини Сергіївни

Робота допущена до захисту в ЕК
протокол кафедри ІТММ № 13 від 31.05.2025р.

Завідувач кафедри ІТММ
к.п.н., доцент
_____ Н.І. Стяглик

Науковий керівник
к.п.н., доцент
_____ Н.І. Стяглик

м. Харків 2025 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Харківський національний університет імені В. Н. Каразіна

Факультет навчально-науковий інститут "Каразінський банківський інститут"
Кафедра інформаційних технологій та математичного моделювання
Рівень вищої освіти перший (бакалаврський)
Спеціальність 125 Кібербезпека
Освітня програма Кібербезпека у фінансових технологіях

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ **Н. І. Стяглик**
Підпис ініціали, прізвище

"08" лютого 2025 року

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ (ПРОЄКТ)

Самчук Дарини Сергіївни
(прізвище, ім'я, по батькові студента)

1. Тема роботи Кібервійна в очах громадськості: оцінка обізнаності, дезінформації та довіри

керівник роботи Стяглик Наталя Іванівна, к.п.н., доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від "08" лютого 2025 року № 4601-5/335

2. Строк подання студентом роботи 15 травня 2025 року

3. Перелік питань, які потрібно розробити:
У розділі 1: Розглянути поняття, сутність та ключові характеристики кібервійни як форми сучасного конфлікту. Ознайомитися з міжнародними стандартами, нормативно-правовою базою та законодавчим регулюванням кібербезпеки, зокрема в Україні. Навести методологічні підходи до вивчення рівня обізнаності громадськості щодо кіберзагроз.
У розділі 2: Ознайомитися з попередніми дослідженнями, присвяченими вивченню обізнаності населення про кібервійну. Обґрунтувати та описати методологію проведення соціологічного опитування. Здійснити аналіз отриманих результатів опитування та виявити основні тенденції і проблеми.
У розділі 3: Розробити практичні рекомендації для підвищення рівня обізнаності населення щодо кібервійни. Визначити ефективні стратегії протидії дезінформації в умовах кіберзагроз. Узагальнити результати дослідження та сформулювати підсумкові висновки.

4. План роботи

№ з/п	Назви етапів роботи
1	Вибір здобувачем теми кваліфікаційної бакалаврської роботи
2	Затвердження плану і завдання кваліфікаційної бакалаврської роботи
3	Здача кваліфікаційної бакалаврської роботи керівнику
4	Підпис кваліфікаційної бакалаврської роботи керівника
5	Підпис кваліфікаційної бакалаврської роботи у нормоконтролера
6	Допуск завідувачем кафедри до захисту кваліфікаційної бакалаврської роботи
7	Захист кваліфікаційної бакалаврської роботи

5. Дата видачі завдання 08 лютого 2025 року

Студент _____ Д.С. Самчук
підпис ініціали, прізвище

Керівник роботи _____ Н.І. Стяглик
підпис ініціали, прізвище

РЕФЕРАТ
НА КВАЛІФІКАЦІЙНУ БАКАЛАВРСЬКУ РОБОТУ
«КІБЕРВІЙНА В ОЧАХ ГРОМАДСЬКОСТІ: ОЦІНКА ОБІЗНАНОСТІ, ДЕЗІНФОРМАЦІЇ ТА ДОВІРИ»
Самчук Дарини Сергіївни

Кваліфікаційна бакалаврська робота містить 77 сторінок, 20 рисунків, список літератури з 50 найменувань, додатки 6 сторінок.

Об'єктом дослідження є громадська думка щодо кібервійни.

Предметом дослідження є рівень обізнаності населення про кібервійну, вплив дезінформації та рівень довіри до офіційних джерел інформації.

Мета кваліфікаційної бакалаврської роботи полягає у вивченні рівня обізнаності громадськості щодо кібервійни, аналізі впливу дезінформації на довіру до офіційних джерел та розробці рекомендацій для підвищення інформаційної стійкості населення.

Завданнями кваліфікаційної бакалаврської роботи є:

- дослідити рівень обізнаності громадськості щодо кібервійни;
- проаналізувати основні джерела дезінформації та їхній вплив на суспільство;
- визначити рівень довіри до офіційних джерел інформації;
- виявити ефективні методи підвищення обізнаності населення;
- сформулювати рекомендації щодо протидії дезінформації.

Актуальність дослідження:

Актуальність теми зумовлена необхідністю підвищення рівня обізнаності населення, зміцнення довіри до офіційних джерел інформації та розробки ефективних стратегій протидії дезінформації, яка активно використовується як інструмент кібервійни.

За результатами дослідження:

Було виявлено рівень обізнаності громадськості щодо кібервійни, проаналізовано вплив дезінформації на довіру до офіційних джерел, а також розроблено практичні рекомендації для підвищення інформаційної грамотності населення.

Практична новизна:

Робота пропонує комплексний підхід до оцінки обізнаності громадськості щодо кібервійни та вперше в межах дослідження поєднує соціологічне опитування з аналізом джерел дезінформації, що дозволяє сформувати цілісну картину інформаційної безпеки в суспільстві.

Одержані результати можуть бути використані державними органами, освітніми установами, громадськими організаціями та медіа для розробки інформаційних кампаній, освітніх програм та стратегій протидії дезінформації.

КЛЮЧОВІ СЛОВА:

кібервійна, кібербезпека, дезінформація, обізнаність громадськості, соціологічне опитування, інформаційна безпека, довіра до ЗМІ.

ABSTRACT

AT QUALIFICATION BACHELOR WORK

«CYBERWAR IN THE EYES OF THE PUBLIC: ASSESSMENT OF AWARENESS, DISINFORMATION, AND TRUST»

Daryna Samchuk

The bachelor's thesis contains 77 pages, 20 drawings, a list of references of 50 titles, applications 6 pages.

The object of the research is public opinion on cyberwar.

The subject of the research is the level of public awareness about cyberwar, the impact of disinformation, and the level of trust in official sources of information.

The purpose of the qualification bachelor's work is to study the level of public awareness of cyberwar, analyze the impact of disinformation on trust in official sources, and develop recommendations for increasing the information resilience of the population.

The tasks of a bachelor's degree are:

- to investigate the level of public awareness of cyberwar;
- to analyze the main sources of disinformation and their impact on society;
- to determine the level of trust in official sources of information;
- to identify effective methods of increasing public awareness;
- to formulate recommendations for countering disinformation.

The relevance of the topic is due to the need to increase the level of public awareness, strengthen trust in official sources of information, and develop effective strategies to counter disinformation, which is actively used as a tool of cyberwar.

According to the results of the research:
The level of public awareness of cyberwar was identified, the impact of disinformation on trust in official sources was analyzed, and practical recommendations for increasing the information literacy of the population were developed.

Main theoretical provisions on the topic of the practical relevance of the study concern the relationship between public awareness, the spread of disinformation, and trust in official sources during cyberwarfare. These provisions form the basis for developing strategies aimed at enhancing information resilience and countering the negative effects of information manipulation.

The results obtained can be used by government bodies, educational institutions, public organizations, and the media to develop information campaigns, educational programs, and strategies to counter disinformation.

KEYWORDS: cyberwar, cybersecurity, disinformation, public awareness, sociological survey, information security, trust in the media.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧОК, СИМВОЛІВ І ТЕРМІНІВ

ПЗ – програмне забезпечення

СУІБ – система управління інформаційною безпекою

NIST – National Institute of Standards and Technology (Національний інститут стандартів і технологій, США)

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

IEC – International Electrotechnical Commission (Міжнародна електротехнічна комісія)

DDoS – Distributed Denial of Service (Розподілена атака на відмову в обслуговуванні)

ISMS – Information Security Management System (Система управління інформаційною безпекою)

PIMS – Privacy Information Management System (Система управління конфіденційною інформацією)

ENISA – European Union Agency for Cybersecurity (Агентство Європейського Союзу з кібербезпеки)

ІКТ – інформаційно-комунікаційні технології

CCDCOE – Cooperative Cyber Defence Centre of Excellence (Центр передового досвіду з кібероборони НАТО)

ВСТУП

Актуальність роботи зумовлена тим, що з огляду на зростаючу кількість кібератак та їхню складність, зростає й важливість дослідження сприйняття цих загроз громадськістю, рівень її обізнаності, а також вплив дезінформації на довіру до офіційних джерел інформації. Окрім цього актуальність теми полягає в необхідності розробки ефективних стратегій для підвищення обізнаності населення та протидії дезінформації.

Кібервійна стала однією з найважливіших загроз сучасного світу, впливаючи на національну безпеку, економіку та суспільство. Кібератаки можуть мати різні форми, включаючи зломи, віруси, фішинг та інші методи, які можуть завдати значної шкоди як окремим особам, так і цілим організаціям. Вони можуть призводити до витоку конфіденційної інформації, фінансових втрат та навіть до порушення критичної інфраструктури. У зв'язку з цим, розуміння громадськістю сутності та наслідків кібервійни є надзвичайно важливим для забезпечення національної безпеки та стабільності.

Ступінь вивчення проблеми кібервійни визначається активним дослідженням в науковій літературі. В Україні значний вклад у вивчення цієї теми внесли дослідники з Національного інституту стратегічних досліджень, які аналізують кіберзагрози в контексті геополітичного суперництва [1]. Їхні дослідження висвітлюють різні аспекти кібервійни, включаючи технічні та соціальні рішення.

Інституційна підтримка кібервійни в Україні включає тиск на технологічних гігантів з метою посилення боротьби з фейками, пропагандою та шкідливим контентом [2]. Це підкреслює важливість співпраці між державними органами та приватним сектором у забезпеченні кібербезпеки.

Метою даного дослідження є оцінка рівня обізнаності громадськості щодо кібервійни, аналіз впливу дезінформації на довіру до офіційних джерел

інформації та розробка рекомендацій для підвищення обізнаності населення. Для досягнення цієї мети необхідно вирішити наступні задачі:

- вивчити рівень обізнаності громадськості щодо кібервійни;
- описати основні джерела дезінформації та їхній вплив на суспільство;
- встановити рівень довіри громадськості до офіційних джерел інформації;
- з’ясувати ефективні методи підвищення обізнаності населення;
- розробити рекомендації для протидії дезінформації.

Об’єктом дослідження є громадська думка щодо кібервійни.

Предметом дослідження є рівень обізнаності, вплив дезінформації та довіра до офіційних джерел інформації.

Методами дослідження є методи соціологічного опитування, контент-аналізу та статистичного аналізу даних. Інформаційна база дослідження включає наукові статті, звіти, дані соціологічних опитувань та офіційні документи. Соціологічні опитування дозволяють отримати дані про рівень обізнаності та ставлення громадськості до кібервійни, контент-аналіз допомагає виявити основні джерела дезінформації, а статистичний аналіз дозволяє оцінити взаємозв'язок між обізнаністю, дезінформацією та довірою до офіційних джерел.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ КІБЕРВІЙНИ

У XXI столітті кіберпростір перетворився на нову арену геополітичного протистояння, де кібервійна стала невід'ємною складовою сучасних конфліктів. Вона швидко перетворилася з поодиноких інцидентів хакерства в центральний компонент сучасної війни, що глибоко впливає на національну безпеку, економічну стабільність, соціальну згуртованість і соціальну стабільність у всьому світі. Оскільки технологічні інновації прискорюються, а суспільства стають все більш залежними від цифрових систем – від фінансових мереж і енергетичних мереж до комунікаційних платформ та інфраструктур охорони здоров’я – вразливість, притаманна цим взаємопов’язаним системам, зростає експоненціально. Особливо це стало очевидним після початку повномасштабної агресії російської федерації проти України у 2022 році, коли кібератаки стали систематичним інструментом ведення війни. Конфлікт продемонстрував, як кібероперації можуть доповнювати традиційні військові стратегії, посилюючи їхній вплив і ускладнюючи реагування країн-мішеней. У цьому контексті важливо розглянути визначення та сутність кібервійни, її основні характеристики, види, приклади, вплив на суспільство та заходи захисту.

Згідно з даними Державної служби спеціального зв'язку та захисту інформації України, у 2023 році кількість зареєстрованих кіберінцидентів зросла на 62,5% порівняно з попереднім роком, досягнувши 1105 випадків [3]. Це свідчить про зростаючу інтенсивність та масштабність кібератак, спрямованих на критичну інфраструктуру, державні установи та приватні компанії.

Фахівці CERT-UA також підтверджують цю тенденцію. Зокрема, у 2024 році кількість кібератак на Україну зросла на майже 70%, досягнувши 4315 інцидентів, що включали атаки на урядові сервіси, енергетичний сектор та оборонні об'єкти [4].

У Європейському Союзі ситуація також викликає занепокоєння. З липня 2023 по червень 2024 року публічні адміністрації в Європі стали мішенню майже 2000 кіберінцидентів, що робить їх найбільш атакованим сектором. Сектор транспорту посів друге місце з 1100 інцидентами, а фінансовий сектор – третє з приблизно 900 кіберінцидентами [5]. Також у 2023 році в Європі було зафіксовано 143 значущих випадки атак програм-вимагачів – зловмисних кампаній, спрямованих на шифрування даних і вимагання великих викупів. Це призвело до руйнування основних служб і викликало масові збої, що на 31% більше порівняно з попереднім роком [6]. Крім того, Європейська комісія повідомила, що у 2023 році понад 300 кіберінцидентів були зафіксовані в секторі охорони здоров'я, що робить його найбільш вразливим серед критичних секторів ЄС, оскільки ці порушення можуть призвести до значних фінансових втрат, поставити під загрозу конфіденційність пацієнтів, порушити медичні послуги, затримати лікування і навіть поставити під загрозу життя пацієнтів [7].

Ці дані підкреслюють необхідність глибокого теоретичного аналізу феномену кібервійни, її основних понять, класифікацій та особливостей ведення. Постає необхідність детального вивчення еволюції поняття «кібервійна», її відмінностей від традиційних форм збройного конфлікту, а також ключових аспектів, що визначають її специфіку у сучасному світі.

1.1. Визначення та сутність кібервійни

Кібервійна (англ. cyberwarfare) – це форма конфлікту, в якій держави або інші суб'єкти використовують цифрові інструменти та кіберактиви для атак на комп’ютерні системи, мережі та критичну інфраструктуру. Ці операції спрямовані на порушення, пошкодження або виведення з ладу життєво важливих цифрових і фізичних систем, часто спрямованих проти державних установ, військових об’єктів, економічних установ і соціальних мереж. Намір

полягає в тому, щоб послабити можливості супротивника, створити хаос або отримати стратегічні переваги. Такі атаки можуть призвести до серйозних наслідків, зокрема економічних втрат, порушення безпеки та суспільних розладів.

Згідно з визначенням, наданим TechTarget, кібервійна – це серія кібератак проти держави, які завдають їй значної шкоди, включаючи порушення роботи важливих комп'ютерних систем і навіть можливу втрату життя [8].

Характеристики

Кібервійна вирізняється своїми унікальними характеристиками, які відрізняють її від традиційних форм конфлікту. Наприклад, її асиметричність дозволяє слабшим акторам, таким як окремі хакери чи невеликі групи, впливати на набагато сильніших учасників конфлікту, таких як держави, вирівнюючи умови гри. Елемент анонімності ускладнює зусилля з виявлення та притягнення винних до відповідальності, що робить встановлення авторства серйозною проблемою. Швидкі темпи кібератак дозволяють зловмисникам наносити швидкі, вражаючі удари, які можуть порушити критичну інфраструктуру або викрасти конфіденційну інформацію за лічені миті. Крім того, глобальне охоплення кібервійни виходить за межі географічних кордонів, дозволяючи атакам з будь-якої точки світу націлюватися на жертв по всьому світу. Також її масштабованість дозволяє одночасно посилювати не тільки напади, але й шкоду та хаос. Ці риси в сукупності визначають кібервійну як складну, всепроникну загрозу сучасній безпеці цілих держав [9].

Види інструментів та атак

Кібервійна включає в себе широкий спектр зловмисних дій, що здійснюються за допомогою різноманітних цифрових засобів. Основні тактики її ведення включають кібератаки, призначені для знищення або пошкодження даних, виведення з ладу життєво важливої інфраструктури або викрадення конфіденційної інформації для отримання стратегічної переваги.

Кампанії з дезінформації також використовуються, щоб вплинути на громадську думку та посіяти розбрат, часто поширюючи неправдиві наративи на платформах соціальних мереж, або підкупляючи ЗМІ. Кібершпигунство передбачає таємне проникнення в системи для отримання конфіденційної урядової або корпоративної інформації, що ставить під загрозу національну безпеку та цілісність бізнесу. Саботаж може мати форму витоку інформації або внутрішніх погроз, коли довірені особи навмисно завдають шкоди зсередини. Атаки на критично важливу інфраструктуру, таку як електромережі та системи водопостачання, загрожують громадській безпеці та національній стабільності. Атаки розподіленої відмови в обслуговуванні (DDoS) перевантажують веб-сайти трафіком, роблячи їх недоступними. Програми-вимагачі шифрують файли та вимагають плату за їх розповсюдження, тоді як фішингові шахрайства змушують людей розкрити особисту або фінансову інформацію, що ще більше посилює кіберзагрози [8].

Історичні приклади

Одним із відомих випадків є атака Stuxnet, дуже складний комп’ютерний вірус, який, як вважають, є спільною операцією Сполучених Штатів та Ізраїлю. Це зловмисне програмне забезпечення було спеціально спрямоване на іранські ядерні об’єкти в Натанзі, щоб зірвати їхній процес збагачення урану. Проникнувши в промислові системи контролю, Stuxnet зміг непомітно пошкодити центрифуги, відкинувши ядерні амбіції Ірану та підкресливши зростаючу загрозу кіберзброї в геополітиці [9].

Ще один важливий інцидент стався в 2015 році, коли Україна зазнала масштабної кібератаки, яка призвела до масових відключень електроенергії, залишивши понад 225 000 жителів без світла. Зловмисники використовували програмне забезпечення BlackEnergy, щоб проникнути в енергетичну інфраструктуру, порушуючи основні послуги та виявляючи вразливі місця в критично важливих системах країни [10]. Ця атака продемонструвала, як кібервійна може безпосередньо загрожувати безпеці та добробуту цивільного населення, підкресливши важливість надійної кібербезпеки.

Вплив на суспільство

Негативний вплив кібервійни виходить за межі безпосереднього фізичного та економічного збитку, глибоко впливаючи на суспільну стабільність. Це може спричинити значні економічні збитки, порушити життєво важливу інфраструктуру, як-от електроенергію, водопостачання та транспорт, і сприяти соціальному заворушенню через поширення пропаганди та дезінформації. Така тактика підриває довіру суспільства до офіційних джерел інформації, спонукаючи громадян звертатися до альтернативних, часто менш надійних джерел. Оскільки кіберзагрози продовжують розвиватися, країни повинні визначити пріоритетність заходів кібербезпеки, щоб захистити свою інфраструктуру та підтримувати згуртованість суспільства.

1.2. Міжнародні стандарти та законодавство у сфері кібербезпеки

Міжнародні стандарти кібербезпеки та законодавство є важливими для захисту інформаційних систем у всьому світі. Вони сприяють скоординованим зусиллям країн для ефективної боротьби з кіберзагрозами, що розвиваються. Встановлюючи чіткі нормативні рамки, ці стандарти сприяють узгодженим практикам безпеки, підвищують довіру та забезпечують єдиний підхід до захисту критичної цифрової інфраструктури в різних країнах і організаціях.

Міжнародні стандарти кібербезпеки

Міжнародна організація зі стандартизації (ISO) спільно з Міжнародною електротехнічною комісією (IEC) відіграє провідну роль у розробці та впровадженні глобальних стандартів у сфері кібербезпеки. Їхні стандарти забезпечують уніфіковану методологію для управління інформаційною безпекою в організаціях будь-якого розміру та галузі [11]. У стандартному стилі ISO та IEC спільно розробляють міжнародні стандарти кібербезпеки, причому серія ISO/IEC 27000 є основою. Ці стандарти надають організаціям у

всьому світі докладні вказівки щодо ефективного встановлення, впровадження, моніторингу та постійного вдосконалення їхніх систем управління інформаційною безпекою (ISMS) [12]. Дотримуючись цих комплексних інструкцій, організації можуть посилити свою позицію в галузі кібербезпеки, захистити конфіденційну інформацію та продемонструвати свою відданість підтримці безпечного та стійкого цифрового середовища.

ISO/IEC 27001, створений у 2005 році та востаннє переглянутий у 2022 році, є ключовим міжнародним стандартом кібербезпеки, який забезпечує комплексну основу для управління ризиками інформаційної безпеки. Він окреслює конкретні вимоги до розробки, впровадження, підтримки та постійного удосконалення ефективної системи управління інформаційною безпекою. Стандарт охоплює широкий спектр сфер, включаючи оцінку ризиків, контроль безпеки, розробку політики, навчання персоналу та реагування на інциденти. Організації, які приймають ISO/IEC 27001, демонструють свою занепокоєність захистом конфіденційних даних та забезпеченням конфіденційності, цілісності та доступності [13].

ISO/IEC 27002 служить комплексним кодексом практики, який доповнює ISO/IEC 27001, надаючи докладні рекомендації щодо встановлення та підтримки ефективних засобів контролю інформаційної безпеки. Він охоплює такі основні сфери, як управління ризиками, контроль доступу, криптографія та фізична безпека, спрямовуючи організації на застосування найкращих практик для захисту своїх активів [14].

ISO/IEC 27005 – це міжнародно визнаний стандарт, який містить вичерпні вказівки щодо управління ризиками інформаційної безпеки [15]. Будучі частиною серії ISO/IEC 27000, він пропонує структурований підхід до виявлення, аналізу, оцінювання, лікування та моніторингу ризиків, пов’язаних з інформаційною безпекою. Основна мета цього стандарту – допомогти організаціям ефективно захистити конфіденційність, цілісність і доступність своїх інформаційних активів. Дотримуючись стандарту ISO/IEC 27005, організації можуть систематично оцінювати потенційні загрози та вразливі

місця, визначати пріоритетність ризиків і впроваджувати відповідні запобіжні заходи [16]. Крім того, він заохочує постійний моніторинг і перегляд процесів управління ризиками, сприяючи розвитку культури постійного вдосконалення.

Наступний важливий стандарт це ISO/IEC 27017, який містить комплексні вказівки щодо безпеки, спеціально розроблені для постачальників хмарних послуг і користувачів [17]. Базуючись на основі стандарту ISO/IEC 27002, він пропонує детальні рекомендації щодо захисту віртуальних середовищ, ефективного управління обов'язками та посилення адміністративних процедур. Стандарт підкреслює важливість безперервного моніторингу активності для швидкого виявлення потенційних загроз і реагування на них. Крім того, він розглядає процедури відновлення активів для забезпечення цілісності даних і безперервності бізнесу. Дотримуючись стандарту ISO/IEC 27017, організації можуть підвищити підзвітність і підтримати довіру своїх клієнтів у середовище хмарних обчислень [18].

ISO/IEC 27018 розроблений для допомоги постачальникам хмарних послуг у захисті персональної інформації [19]. Цей стандарт підкреслює важливість впровадження надійних заходів безпеки для захисту ідентифікаційної інформації від несанкціонованого доступу та порушень. Він сприяє прозорості, заохочуючи чітке спілкування з клієнтами щодо практики обробки даних. Крім того, ISO/IEC 27018 виступає за суворі протоколи контролю доступу, ефективні процедури управління інцидентами та дотримання відповідних нормативних вимог. Базуючись на основоположних принципах ISO/IEC 27002 та інших пов'язаних стандартів, ISO/IEC 27018 забезпечує комплексну структуру для забезпечення конфіденційності та безпеки даних у хмарних середовищах.

ISO/IEC 27701 базується на ISO/IEC 27001 для конкретного вирішення питань управління конфіденційністю та забезпечення відповідності нормам GDPR [20]. Цей міжнародний стандарт містить вичерпні вимоги та вказівки для організацій щодо створення, впровадження, підтримки та постійного

вдосконалення системи управління конфіденційною інформацією (PIMS). Він наголошує на таких критичних аспектах, як захист особистих даних, керування контролем доступу та ефективне реагування на порушення конфіденційності. Інтегруючи ці практики, організації можуть продемонструвати свою прихильність до захисту прав особи на конфіденційність, зниженню ризиків, пов'язаних із порушенням даних, і досягненню відповідності нормативним вимогам [21].

NIST Cybersecurity Framework, спочатку опублікований у 2014 році та оновлений у 2024 році, пропонує повний набір інструкцій, розроблених для підвищення організаційної кібербезпеки [22]. Він структурований навколо п'яти основних функцій: ідентифікація, захист, виявлення, реагування та відновлення. Ці функції служать стратегічним підходом до управління ризиками кібербезпеки, допомагаючи організаціям зрозуміти свою безпеку, впроваджувати захисні заходи, виявляти потенційні загрози, ефективно реагувати на інциденти та швидко відновлюватися після будь-яких збоїв. Ця структура спрямована на посилення загальної стійкості кібербезпеки в різних галузях.

Міжнародні законодавчі акти

Будапештська конвенція, прийнята Радою Європи в 2001 році, є першим всеосяжним міжнародним договором, присвяченим боротьбі з кіберзлочинністю [23]. Він спрямований на встановлення єдиної правової бази шляхом криміналізації таких дій, як несанкціонований доступ до комп'ютерних систем, перехоплення даних і комп'ютерне шахрайство. Конвенція заохочує країни-члени оновлювати свої національні закони, щоб краще реагувати на мінливий ландшафт цифрових загроз, і сприяє міжнародній співпраці в розслідуванні та судовому переслідуванні, пов'язаному з кіберзлочинами. Станом на квітень 2023 року загалом 68 країн ратифікували Конвенцію, демонструючи широку міжнародну прихильність. Слід зазначити, що Україна приєдналася у 2005 році. Також відомо, що рф

виступає проти конвенції та відмовляється співпрацювати з правоохоронними органами у розслідуванні кіберзлочинів.

Прикладом зобов'язань Європейського Союзу щодо сприяння безпечному та стійкому цифровому середовищу є імплементація Директиви NIS у 2016 році [24]. Визнаючи критичну важливість кібербезпеки для забезпечення процвітання та безпеки своїх держав-членів, ЄС розробив цю Директиву як всеосяжну структуру для підвищення рівня колективного захисту від нових кіберзагроз. Директива NIS зобов'язує кожну країну-члена розробити та прийняти національні стратегії кібербезпеки, забезпечуючи скоординований і стратегічний підхід до боротьби з кіберризиками. Ці стратегії слугують для визначення ключових секторів, критично важливих для функціонування суспільства, таких як енергетика, транспорт, банківська справа, охорона здоров'я та цифрова інфраструктура, і встановлюють надійні заходи для захисту цих життєво важливих активів.

Центральним аспектом директиви є призначення операторів критичної інфраструктури, яким доручено впроваджувати спеціальні захисні заходи, адаптовані до їхніх мереж та інформаційних систем. Цей проактивний підхід спрямований на запобігання потенційним збоям і мінімізацію впливу кіберінцидентів. Крім того, Директива NIS наголошує на важливості сприяння культурі обміну інформацією між державами-членами та відповідними організаціями [24]. Сприяючи своєчасному обміну розвідувальними даними, індикаторами загроз і звітами про інциденти, директива прагне підвищити колективну обізнаність про ситуацію та забезпечити швидку, скоординовану відповідь на кіберзагрози.

Спираючись на цю основоположну структуру, ЄС запровадив Регламент (ЄС) 2019/881, широко відомий як Закон про кібербезпеку [25]. Цей регламент засновує Європейське агентство з кібербезпеки (ENISA), підвищуючи його роль для підтримки національних органів влади та інституцій ЄС у розробці ефективної політики та покращенні загальної стійкості до кіберзагроз. ENISA діє як центр експертних знань, досліджень і передового досвіду, сприяючи

міжнародній співпраці. Крім того, Закон про кібербезпеку запроваджує добровільні європейські схеми сертифікації кібербезпеки для продуктів, послуг і процесів ІКТ. Ці схеми створені для сприяння довірі та впевненості в цифрових рішеннях шляхом надання чітких стандартів і механізмів забезпечення.

Tallinn Manual є важливою віхою в поточному діалозі щодо застосування міжнародного права до кіберпростору [26]. Як всебічне наукове видання, яке не має обов'язкової сили, воно пропонує цінні вказівки та розуміння того, як усталені правові рамки, зокрема ті, що стосуються jus ad bellum (закону, що регулює застосування сили) і гуманітарного права, можна тлумачити та застосовувати в контексті кіберконфліктів і війни [27]. Заснування посібника було зумовлене колективним визнанням необхідності роз'яснити правові принципи в сфері, яка характеризується швидким технологічним прогресом і складними геополітичними міркуваннями. Цей впливовий проєкт був ініційований Спільним центром передового досвіду кіберзахисту НАТО (CCDCOE), розташованим у Таллінні, Естонія. Ініціатива об'єднала поважних експертів з міжнародного права та кібербезпеки під керівництвом професора Майкла Н. Шмітта з Військово-морського коледжу США. Їхні спільні зусилля були спрямовані на створення наукового ресурсу, який міг би слугувати орієнтиром для політиків, юристів-практиків і вчених, які прагнуть зрозуміти та орієнтуватися в правових проблемах, пов'язаних з кіберопераціями. Талліннський посібник складається з двох основних видань. Перший, Tallinn Manual 1.0, опублікований у 2013 році, зосереджується на серйозних кібероперація, які порушують заборону на застосування сили, порушують право на самозахист, або відбуваються в контексті збройного конфлікту. Він досліджує, як наявні міжнародні правові принципи можуть бути адаптовані до кіберінцидентів, наголошуючи на важливості ясності та передбачуваності у правових реакціях на такі події. Спираючись на цю основу, Талліннський посібник 2.0, випущений у 2017 році, розширює сферу застосування, щоб охопити всі дії в кібернетичному просторі, включно з тими, що проводяться в

мирний час [26] . Це розширене видання вводить детальні правові норми щодо державного суверенітету, юрисдикції та відповідальності в кіберпросторі, відображаючи визнання того, що кібердіяльність є невід'ємною частиною сучасної державності та міжнародних відносин.

Серед основних принципів, сформульованих у посібнику, є концепція суверенітету над кіберінфраструктурою. Цей принцип підтверджує, що держави мають виключну владу над своїми цифровими активами, і будь-які несанкціоновані проникнення або втручання вважаються порушенням міжнародного права. Юрисдикція, як обговорюється в посібнику, стосується юридичних повноважень держави над кібердіяльністю, яка відбувається на її території або зачіпає її, що ще більше підсилює важливість дотримання національних кордонів і правових кордонів у кіберпросторі. Загалом, Талліннський посібник є важливою науковою спробою подолати розрив між традиційними міжнародно-правовими принципами та унікальними проблемами, пов'язаними з сучасними кібероперaціями. Він сприяє поінформованому та детальному розумінню того, як міжнародне право може застосовуватися для забезпечення відповідальної поведінки в кіберпросторі, тим самим сприяючи стабільності та безпеці міжнародної спільноти [27].

Таким чином, міжнародні стандарти та законодавство у сфері кібербезпеки є невід'ємною частиною сучасної стратегії захисту інформаційних систем та мереж, забезпечуючи ефективну координацію зусиль різних країн у боротьбі з кіберзагрозами та підвищуючи загальний рівень кібербезпеки у світі.

1.3. Методи дослідження обізнаності громадськості

Вивчення обізнаності громадськості щодо кібервійни має першочергове значення у світі, який стає все більш цифровим. Розуміння того, як населення сприймає, розуміє та реагує на загрози та реалії кіберконфлікту, дає цінну

інформацію про поточні рівні знань, ставлення та поведінку. Таке розуміння має важливе значення для виявлення прогалин в обізнаності, які можуть перешкоджати ефективним механізмам захисту та реалізації політики. Крім того, оцінка впливу наявних інформаційних кампаній дає змогу політикам і зацікавленим сторонам удосконалити свої комунікаційні стратегії, забезпечуючи резонанс критичних повідомлень і охоплення різноманітних аудиторій.

Оскільки кібервійна є відносно новою сферою конфлікту, яка розгортається в основному в кіберпросторі, сприяння добре поінформованій громадськості є життєво важливим для отримання підтримки урядових ініціатив, спрямованих на посилення національної кібербезпеки. Громадське розуміння та підтримка можуть значно вплинути на успіх захисних заходів і стратегій стримування.

Дослідження суспільної обізнаності використовує різноманітні методологічні підходи. Кількісні опитування дозволяють збирати широкі, статистично значущі дані від великих груп населення, надаючи огляд загальних знань і ставлень. Крім того, якісні методи, такі як інтерв'ю та фокус-групи, глибше вивчають індивідуальні думки та сприйняття, виявляючи нюанси поглядів, які можуть бути пропущені під час більших опитувань. Разом різноманітні методи утворюють комплексну структуру, яка підтримує розробку обґрунтованих стратегічних ініціатив для підвищення обізнаності та стійкості населення щодо кібербезпеки.

Опитування громадської думки

Опитування громадської думки є важливим інструментом для розуміння суспільного сприйняття та ставлення до питань кібербезпеки. Застосування збалансованого поєднання кількісних і якісних методологій дозволяє дослідникам і політикам збирати вичерпну інформацію, сприяючи прийняттю обґрунтованих рішень і стратегічної комунікації [28].

Кількісні методи особливо цінуються за їх здатність отримувати вимірні та порівнювані дані. Серед них анкети виділяються своєю стандартністю та

простотою аналізу. Ці інструменти можна розповсюджувати через різні канали – особисто, поштою або найчастіше через онлайн-платформи – кожен із яких має певні переваги. Особисте розповсюдження дозволяє безпосередньо залучати, тоді як опитування поштою розширюють охоплення населення з обмеженим доступом до Інтернету. Онлайн-опитування, які набувають популярності завдяки своїй економічній ефективності та швидкому розгортанню, можуть включати різні формати запитань, такі як закриті запитання, відкриті відповіді та шкали оцінок. Ці методи особливо ефективні для оцінки рівня обізнаності громадськості щодо кіберзагроз, включаючи такі проблеми, як кібервійни, витоки даних і онлайн-шахрайство. Крім того, телефонні опитування є засобом для швидкого збору даних від великих, географічно розсіяних груп населення, хоча їхня ефективність може бути обмежена доступністю контактної інформації та потенційною втомою чи ігноруванням респондентів [28,29].

Доповнюючи ці кількісні підходи, якісні методи пропонують детальне розуміння громадського сприйняття та ставлення. Глибинні інтерв'ю сприяють детальним розмовам з окремими особами, розкриваючи особисті думки, мотивацію та досвід [30]. Такі взаємодії мають надзвичайну цінність для розуміння того, як люди сприймають кіберзагрози та реагують на них, а також для виявлення бар'єрів на шляху прийняття безпечної поведінки в Інтернеті. Фокус-групи, з іншого боку, передбачають керовані дискусії між кількома учасниками, що дозволяє дослідникам досліджувати низку думок та поглядів одночасно [31]. Цей підхід особливо корисний для оцінки ефективності кампаній з підвищення обізнаності з важливих питань, оскільки він забезпечує насичений контекстний зворотний зв'язок щодо стратегій обміну повідомленнями та сприйнятливості громадськості.

Загалом, інтеграція як кількісних, так і якісних методів дослідження пропонує комплексний підхід до вимірювання громадської думки.

Спостереження та аналіз

Контент-аналіз є дослідницькою методологією, яка полегшує всебічне вивчення обширних колекцій текстових і візуальних матеріалів, включаючи документи, відео, аудіозаписи та зображення [32]. Його головна мета – дати дослідникам змогу систематично оцінювати повідомлення, що передаються на різноманітних медіа-платформах, у соціальних мережах і блогах, забезпечуючи таким чином детальне розуміння комунікаційних моделей і тем. Цей підхід ефективно поєднує як кількісні методи, такі як підрахунок частоти конкретних слів або зображень, так і якісні дані, такі як інтерпретація основних значень і контекстуальних нюансів [33].

Процес аналізу вмісту зазвичай складається з кількох ретельно структурованих етапів. По-перше, дослідники визначають об’єкт дослідження, вибираючи релевантні джерела – це можуть бути новинні статті, дописи в соціальних мережах або контент трансляцій. Далі вони займаються кодуванням, яке передбачає ідентифікацію та класифікацію ключових тем, зображень, тверджень або символів у даних. Цей крок є вирішальним для організації інформації та підготовки її до аналізу. Згодом дослідники аналізують закодовані дані за допомогою статистичних методів, щоб визначити поширеність і контекстуальну значущість виявлених тем, надаючи розуміння закономірностей і тенденцій. Наприклад, аналіз статей новин за певний період може виявити, які теми найчастіше обговорюються та як різниться висвітлення в різних ЗМІ. Крім того, моніторинг коментарів, відгуків і взаємодії користувачів допомагає оцінити суспільні настрої та думку. Загалом, контент-аналіз є універсальним і точним інструментом, що дозволяє вченим і практикам робити значущі висновки щодо комунікаційних процесів і суспільної динаміки [33].

Експериментальні методи

Експерименти являють собою фундаментальний дослідницький підхід, який дозволяє систематично оцінювати реакцію громадськості на різноманітні типи інформації в ретельно контрольованому середовищі [34]. Процес починається з формулювання точної гіпотези, яка керує подальшим

плануванням експерименту. Це передбачає вибір відповідних змінних, встановлення методів вимірювання та забезпечення надійності та неупередженості методології. Збір даних потім здійснюється між різними групами респондентів, щоб отримати повне розуміння відповідей. Зібрані дані згодом аналізуються за допомогою відповідних статистичних методів для отримання значущої інформації. Наприклад, можна використовувати експерименти для порівняння ефективності різних інформаційних кампаній – наприклад, позитивних і негативних повідомлень – щоб оцінити їхній вплив на громадське ставлення та поведінку [35]. Загалом, цей метод надає цінні докази, які можуть стати основою для стратегічних комунікаційних зусиль, покращити розробку політики та сприяти глибшому розумінню суспільної динаміки, сприянню прийняттю обґрунтованих рішень та більш ефективній взаємодії з громадськістю.

Аналіз великих даних

Аналіз великих даних служить використовує величезну та різноманітну інформацію, отриману через соціальні медіа, пошукові системи та різні онлайн-платформи [36]. Процес починається з систематичного збору даних із авторитетних джерел, таких як Facebook, Twitter, блоги та інші цифрові джерела, що забезпечує повне розуміння публічного дискурсу. Після збору даних виконується ретельна обробка даних, щоб очистити, упорядкувати та структурувати інформацію, тим самим підвищуючи її надійність і зручність використання для аналізу. Передові аналітичні методи, включаючи статистичні методи та алгоритми машинного навчання, потім використовуються для виявлення значущих закономірностей, нових тенденцій і тонких змін у ландшафті даних. Щоб полегшити інтерпретацію та передачу цих ідей, використовуються інструменти візуалізації даних, такі як Tableau, які перетворюють складні набори даних у доступні та інтуїтивно зрозумілі візуальні формати. Цей інтегрований підхід дає змогу зацікавленим сторонам розкривати переважаючі теми, оцінювати емоційні реакції та відстежувати зміну громадської думки з часом. Зрештою, Big Data Analytics пропонує

стратегічну перевагу в інформуванні процесів прийняття рішень, сприянні оперативній політиці та культивуванні глибшого розуміння суспільної динаміки [36].

Таким чином, методи дослідження обізнаності громадськості є ключовими для розуміння рівня знань, ставлення та поведінки населення щодо певної теми. Використання кількісних та якісних опитувань дозволяє отримати репрезентативні дані та глибокі інсайти про думки громадськості. Спостереження та аналіз, включаючи контент-аналіз та моніторинг коментарів, допомагають виявити, як тема представлена в медіа та які аспекти найбільше обговорюються. Експериментальні методи дозволяють оцінити реакцію громадськості на різні види інформації, а аналіз великих даних надає можливість вивчати тенденції та патерни у поведінці населення. Комплексне використання цих методів забезпечує всебічне розуміння обізнаності громадськості та сприяє розробці ефективних стратегій для підвищення рівня знань та безпеки.

РОЗДІЛ 2. АНАЛІЗ ОБІЗНАНОСТІ ГРОМАДСЬКОСТІ ЩОДО КІБЕРВІЙНИ

2.1. Огляд попередніх досліджень та їх результати

Analysing the Awareness of Cyber Crime and Designing a Relevant Framework with Respect to Cyber Warfare: An Empirical Study

Перше дослідження для розгляду – це «Аналіз обізнаності про кіберзлочини та розробка відповідної структури щодо кібервійни: емпіричне дослідження», проведене незалежною дослідницькою групою, не пов’язаною з державними структурами, що забезпечує об’єктивність отриманих результатів. Дослідження було опубліковане в журналі International Journal of Mechanical Engineering and Technology (IJMET) у 2018 році [37]. Воно аналізує обізнаність користувачів інтернету щодо кіберзлочинів та кібервійни. Воно включає опитування 325 користувачів для оцінки їхнього розуміння кіберзагроз та використання захисного програмного забезпечення.

Анкета складалася з двох основних частин: вступного блоку з описом мети дослідження та основного блоку запитань. Респондентам пропонувалося оцінити низку факторів, що впливають на обізнаність про кіберзлочинність і кібервійну, за допомогою п’ятибальної шкали Лайкерта (від 1 – «немає впливу» до 5 – «дуже серйозний вплив»). Питання були сформульовані простою мовою, щоб забезпечити легкість сприйняття та точність відповідей. Вони охоплювали як загальні уявлення про кіберзагрози, так і практичні аспекти – використання захисного програмного забезпечення, досвід взаємодії з фішингом, ставлення до державної політики у сфері кібербезпеки. Для аналізу результатів було використано статистичні методи, зокрема критерій хі-квадрат та точний критерій Фішера, що дозволило виявити статистично значущі зв’язки між рівнем обізнаності та окремими характеристиками

респондентів. Отримані дані були оброблені за допомогою програмного забезпечення SPSS.

Учасники продемонстрували знайомство насамперед із загальними термінами, такими як віруси та хакери, але обмежене розуміння основних механізмів цих загроз або ефективних стратегій їх подолання. Це підкреслює критичний розрив між уявною та фактичною компетентністю в кібербезпеці, що потенційно може наражати користувачів на підвищені ризики.

Дослідження також показує, що хоча респонденти зберігають широке використання антивірусного програмного забезпечення, такі практики, як регулярне оновлення інструментів безпеки або застосування додаткових заходів захисту, таких як брандмауери або двофакторна автентифікація, застосовуються менш послідовно. Ця невідповідність підкреслює вразливість у поточній практиці кібербезпеки та свідчить про те, що просте встановлення захисного програмного забезпечення не означає надійний захист.

Крім того, інтригуючим аспектом, виявленим під час дослідження, є схильність учасників переоцінювати свої навички кібербезпеки, що призводить до хибного відчуття безпеки, яке може перешкоджати проактивній захисній поведінці. Використовуючи кількісні методи, насамперед за допомогою структурованих опитувальників, дослідження успішно фіксує репрезентативний знімок рівнів обізнаності в різних соціальних групах. Дані підкреслюють повсюдний дефіцит знань у фундаментальних аспектах кібербезпеки, підкреслюючи нагальну потребу в цільових громадських освітніх ініціативах. Ці знання є цінними для організації майбутніх інформаційних кампаній, втілення освітніх програм та розробки політики, спрямованої на формування більш поінформованого та стійкого цифрового населення.

Методологія, продемонстрована в цьому дослідженні, виявляється універсальною та адаптованою, пропонуючи надійну основу для оцінки кіберобізнаності серед різних демографічних і професійних груп. Щоб поглибити розуміння розбіжностей в обізнаності, майбутні дослідження

можуть включати детальніший аналіз того, як такі фактори, як вік, професія чи освіта, впливають на сприйняття кібербезпеки та поведінку. Таке уточнене розуміння дозволить адаптувати освітні заходи до конкретної аудиторії, тим самим підвищуючи їхню ефективність.

Підсумовуючи, це дослідження не лише висвітлює критичні прогалини в розумінні громадськістю кіберзагроз, але й надає фундаментальну модель для поточних досліджень та освітніх зусиль. Оскільки кіберзагрози продовжують ускладнюватися та вдосконалюватися, формування добре поінформованої бази користувачів залишається важливим компонентом національних і глобальних стратегій кібербезпеки.

Cyberattacks, cyber threats, and attitudes toward cybersecurity policies

Дослідження під назвою «Кібератаки, кіберзагрози та ставлення до політики кібербезпеки», опубліковане в журналі Journal of Cybersecurity у 2021 році, було проведене зовнішньою академічною групою дослідників – Keren Snider, Ryan Shandler, Shay Zandani та Daphna Canetti – і мало на меті з’ясувати, як впливає експозиція до кібератак на підтримку громадськістю державної політики у сфері кібербезпеки пропонує цінну інформацію про складний взаємозв’язок між досвідом людей з кіберзагрозами та їх подальшою підтримкою правил кібербезпеки [38].

Використовуючи суворий експериментальний план, у дослідженні взяли участь 1022 ізраїльських учасники, які були ретельно та випадковим чином розподілені на три різні групи. Перша група була піддана перегляду імітованих новинних повідомлень, які зображували смертоносні кібератаки на критично важливу національну інфраструктуру, що представляє найсерйознішу форму кіберзагрози. Друга група розглядала звіти про нелетальні кібератаки, які, тим не менш, викликали серйозні занепокоєння, але не призвели до негайної шкоди. Третя група була контрольною, не отримувала впливу сценаріїв кібератак. Цей методологічний підхід дозволив дослідникам систематично оцінювати, як різні ступені сприйняття загрози впливають на ставлення до політики кібербезпеки.

Висновки цього розслідування показують, що вплив кіберзагроз загалом підвищує підтримку суворіших заходів кібербезпеки. Учасники, які зіткнулися зі смертельними сценаріями кібератак, продемонстрували чітку підтримку політики, яка виступає за підвищення прозорості уряду та обміну інформацією, визнаючи необхідність всебічної обізнаності та готовності. Подібним чином ті, хто зазнав несмертельних атак, також продемонстрували значну схильність до політики, яка сприяє прозорості та інформативним ініціативам, підкреслюючи, що навіть менш серйозні загрози можуть формувати суспільне ставлення.

Ключовий внесок дослідження полягає у з'ясуванні основного механізму сприйняття загрози. Підвищена обізнаність про кіберризики, здається, сприяє більшій готовності громадськості підтримувати обмежувальні політики, навіть якщо вони можуть потенційно порушувати громадянські свободи та права на конфіденційність. Ця динаміка підкреслює тонкий баланс, який повинні досягти політики між посиленням безпеки та повагою до особистих свобод.

Крім того, дослідження покращує наше розуміння того, як громадську думку формує мінливий ландшафт кіберзагроз. Він підкреслює важливість освітніх ініціатив і комунікаційних стратегій, які ефективно інформують громадян про виклики кібербезпеки та обґрунтування певних політичних заходів. Рандомізований експериментальний підхід, використаний у цьому дослідженні, не тільки зміцнює довіру до його висновків, але й забезпечує цінну методологічну основу для майбутніх досліджень у цій галузі. Такі підходи можуть бути корисними для інформування політиків і зацікавлених сторін, коли вони розробляють стратегії для вирішення багатогранних викликів, створених кіберзагрозами у все більш цифровому світі.

The Impact of Cyberwarfare on the National Security

Стаття під назвою «Вплив кібервійни на національну безпеку» була опублікована у 2023 році в журналі Future Human Image (випуск 19) [39]. Автором дослідження є Темур Дігмелашвілі – дослідник з Кавказького

міжнародного університету (Тбілісі, Грузія), який розглядає кібервійну як один із ключових викликів національній безпеці в умовах сучасних конфліктів.

Дослідження має аналітично-оглядовий характер і не базується на кількісному опитуванні, однак воно є цінним з точки зору систематизації загроз, пов'язаних із кібератаками, та аналізу їхніх наслідків для державних інституцій, критичної інфраструктури, військових систем і демократичних процесів. Автор підкреслює, що кібервійна здатна не лише порушити функціонування державних служб, а й спричинити втрату довіри до уряду, дестабілізувати політичну ситуацію та навіть вплинути на результати виборів.

Важливий аспект дослідження підкреслює значні фінансові втрати, завдані кіберзагрозами. Крадіжка конфіденційних даних, злом фінансових систем і збій банківських операцій призводять до мільярдних збитків щорічно. Такі порушення підривають довіру суспільства до урядових і фінансових установ, ще більше послаблюючи соціальну структуру. Крім того, кібершпигунство стає постійною загрозою, коли зловмисники викрадають конфіденційну військову та стратегічну інформацію, тим самим ставлячи під загрозу спроможність національної оборони. Хоча дослідження не містить емпіричних даних, воно пропонує концептуальну рамку для розуміння кібервійни як багатовимірного явища, що вимагає міждисциплінарного підходу – поєднання технічних, правових, політичних та освітніх заходів.

Окрім проблем економіки та безпеки, дослідження підкреслює політичну вразливість, спричинену кібервійною. Маніпуляції виборчими процесами та поширення дезінформації можуть вплинути на громадську думку та підірвати демократичні інститути. Ця тактика загрожує дестабілізувати уряди та сприяти політичним заворушенням.

Враховуючи ці зростаючі загрози, дослідження виступає за розробку та впровадження надійних стратегій кібербезпеки. У ньому наголошується на важливості міжнародного співробітництва, передових технологічних засобів

захисту та всебічної політики для пом’якшення ризиків, пов’язаних з кібервійною.

Загалом, усі ці дослідження надають комплексне уявлення про обізнаність громадськості щодо кіберзагроз та кібервійни, виявляють ключові проблеми та пропонують напрямки для подальшого дослідження та розробки ефективних стратегій кібербезпеки. Вони також підкреслюють необхідність постійного моніторингу та адаптації освітніх програм та політик для забезпечення високого рівня обізнаності та захисту населення.

2.2. Методологія проведення опитування

Мета та завдання опитування

Опитування розроблено для комплексної оцінки обізнаності громадськості про кібервійну, щоб зрозуміти, наскільки добре люди усвідомлюють загрози та виклики, пов’язані з цифровими конфліктами. Воно намагається визначити основні джерела, з яких люди збирають інформацію про проблеми кібербезпеки, а також оцінити рівень довіри до цих джерел. Крім того, опитування має на меті виявити поширеність дезінформації, пов’язаної з кіберзагрозами.

Спираючись на результати попередніх досліджень, зокрема роботи, проведеної в Індії, яка виявила розрив між суб’єктивною впевненістю респондентів у своїх знаннях і фактичним рівнем цифрової грамотності, а також експериментального дослідження в Ізраїлі, що показало вплив емоційного контексту кібератак на підтримку державної політики, постало питання: чи спостерігаються подібні тенденції в українському суспільстві? Зокрема, чи існує розрив між уявленнями громадян про власну обізнаність і реальними знаннями? Чи впливає вік, джерело інформації або досвід взаємодії з кіберзагрозами на рівень довіри до державних ініціатив у сфері кібербезпеки?

Таким чином, опитування має на меті не лише зібрати емпіричні дані про рівень обізнаності, а й перевірити гіпотезу про наявність вікових, поведінкових та інформаційних відмінностей у сприйнятті кіберзагроз. Це дозволяє провести паралелі з міжнародними дослідженнями та адаптувати їхні висновки до українського контексту, що є особливо актуальним в умовах гібридної війни та зростання ролі інформаційної безпеки.

Завдання опитування:

1. Виявлення прогалин у знаннях:
    . Визначити, які аспекти кібервійни є найменш зрозумілими для громадськості.
    . Виявити, які терміни та концепції потребують додаткового пояснення.
2. Оцінка впливу дезінформації:
    . Визначити, як часто громадяни стикаються з неправдивою або маніпулятивною інформацією про кіберзагрози.
    . Оцінити, наскільки дезінформація впливає на сприйняття реальних кіберзагроз.
2. Визначення рівня довіри до різних джерел інформації:
    . Оцінити, які джерела інформації (соцмережі, новинні сайти, телебачення, офіційні державні сайти тощо) користуються найбільшою довірою серед громадськості.
    . Визначити, які джерела інформації вважаються найбільш надійними для отримання новин про кіберзагрози.
2. Аналіз кібергігієни:
    . Визначити, які інструменти та методи кібербезпеки використовуються громадянами для захисту своїх даних.
    . Оцінити рівень обізнаності про кібергігієну та готовність громадян до навчання у цій сфері.
2. Рекомендації для підвищення обізнаності:

. Розробити рекомендації щодо підвищення рівня обізнаності громадськості про кіберзагрози.

. Запропонувати ефективні заходи для боротьби з дезінформацією та підвищення довіри до надійних джерел інформації.

Вибірка респондентів

Цільовою аудиторією опитування були громадяни віком від 18 до 65 років, різної статі, професійної діяльності та рівня освіти. Загалом долучилося 164 людини. Для опитування було виокремлено три соціальні групи залежно від їх віку і розподілені наступним чином:

1. 18-29 років: 62 респонденти
2. 30-49 років: 52 респонденти
3. 50+ років: 50 респондентів

Це допомагає зрозуміти, як люди різного віку знають про такі речі, як кібератаки, і звідки вони отримують інформацію. Стать респондентів включала жінок, чоловіків та тих, хто не бажав вказувати свою стать, у кількості 103, 51 та 10 відповідно.

Інструменти збору даних

У стандартному стилі опитування була розроблена анкета з 17 питань, щоб зібрати вичерпні дані від учасників. Анкета складалася з 15 основних запитань, спрямованих на вивчення думок, поведінки та ставлення учасників, а також 2 демографічних елементів для збору важливої довідкової інформації, такої як вік та стать. Запитання використовували різноманітні формати для максимального залучення та ясності. Закриті запитання з варіантами відповідей надавали прості дані, які піддавалися кількісному вимірюванню, тоді як можливість надати відкриту відповідь дозволяло респондентам висловлювати свої думки та досвід власними словами. Крім того, рейтингові шкали просили учасників оцінити свій рівень довіри до різних джерел за шкалою від 1 до 5, полегшуючи вимірювання інтенсивності довіри. Цей різноманітний підхід забезпечив збалансований збір як кількісних, так і

якісних даних, підвищивши загальну надійність і глибину результатів дослідження.

Опитування проводилося онлайн за допомогою Google Forms, щоб забезпечити зручність, ефективність і доступність. Ця платформа дозволила респондентам заповнювати анкету у зручний для них час, враховуючи їхній індивідуальний графік і збільшуючи рівень участі. Цифровий формат сприяв швидкому збору даних і автоматичному збереженню відповідей, спрощуючи процес аналізу. Запрошення взяти участь в опитуванні поширювалися через соціальні мережі (Facebook, Instagram) та різноманітні дискусійні чати (у WhatsApp, Telegram, Messenger) протягом тижня. Цей стратегічний підхід допоміг максимізувати охоплення опитування, забезпечивши різноманітну та достатню вибірку. Загалом онлайн-методологія виявилася ефективною для збору своєчасних і вичерпних даних для дослідження. Також опитування проводилось двома мовами – українською та англійською – для більшого охоплення людей із різним досвідом та для розширення вибірки.

Процедура проведення опитування

Початковий етап передбачав розробку комплексного опитування з 17 запитань, що включає різні формати запитань, такі як закриті та рейтингові шкали, а також демографічні запити. Потім опитування було ретельно переглянуто та протестовано на невеликій групі людей (5 осіб), щоб перевірити його точність, узгодженість та ефективність у зборі потрібної інформації, заклавши міцну основу для подальшого збору та аналізу даних. Розгляд результатів тестового опитування не передбачено у дослідженні, а лише використано для виявлення можливих проблем та недоліків, тобто покращення його якості. Тестування допомогло переконатися, що питання зрозумілі та не викликають труднощів у відповідях. На основі отриманих відгуків були внесені необхідні корективи.

Респонденти отримали коротке пояснення щодо мети опитування, його анонімності, та можливості отримати вигоду у вигляді роздумів на таку важливу тему та перевірки власних знань. Уся інформація була надана через

супроводжувальний текст у Google Forms та при поширенні форми у соціальних мережах.

Дані були збережені у форматі Excel, що дозволяє легко проводити статистичний аналіз та створювати діаграми. Для кожного питання були створені зведені таблиці та відповідні графіки (гістограми, кругові діаграми, стовпчасті діаграми) для візуалізації результатів.

Обмеження дослідження

Основні обмеження дослідження зосереджені навколо питання репрезентативності вибірки. Хоча стратифікована вибірка була застосована для забезпечення різноманітності між різними підгрупами, залишається ймовірність того, що вона не повністю відображає ширшу сукупність. Деякі соціальні чи професійні групи можуть бути недостатньо представленими, що може вплинути на можливість узагальнення результатів. Крім того, упередження відповідей може викликати занепокоєння; учасники могли дати неточні або необ'єктивні відповіді через різні причини, такі як недостатнє розуміння питань, бажання надати соціально бажані відповіді або просто випадкові помилки. Ці обмеження підкреслюють необхідність обережної інтерпретації результатів і припускають, що майбутні дослідження повинні розглянути додаткові методи для підвищення точності та інклюзивності.

У стандартному дослідницькому підході інструменти збору даних, такі як онлайн-опитування, широко використовуються завдяки їх зручності та ефективності. Однак ці інструменти мають властиві обмеження, які можуть вплинути на точність і надійність зібраних даних. Наприклад, респонденти можуть надавати нечесні відповіді або поспішно відповідати на запитання, в результаті чого відповіді не точно відображають їхні справжні думки чи досвід. Чималу роль відіграють і зовнішні фактори; технічні перепони, такі як проблеми з підключенням до Інтернету або системні збої, можуть призвести до неповних даних або навіть до повної втрати відповідей. Крім того, середовище, в якому учасники заповнюють опитування – вдома, на робочому місці чи в громадських місцях – може вплинути на рівень комфорту та

чесності, потенційно спотворюючи результати. Хоча дослідники часто запевняють учасників в анонімності, щоб стимулювати відкритість, деякі люди все одно можуть відчувати дискомфорт або недовіру, особливо якщо вони стурбовані конфіденційністю або наслідками. Ці фактори підкреслюють важливість ретельного планування та адміністрування онлайн-опитувань, щоб пом’якшити такі обмеження та підвищити достовірність даних. Враховуючи такі фактори, форма опитування була поширена переважно у час, коли респонденти теоретично перебувають у комфортних умовах вдома (або за спокійних обставин), а також у робочі та вихідні дні, для урізноманітнення вибірки.

2.3. Аналіз результатів опитування

Для ефективного представлення результатів опитування буде використано різноманітні візуалізації, такі як кругові діаграми та гістограми. Ці діаграми проілюструють розподіл відповідей, дозволяючи чітко визначити закономірності та тенденції. Гістограми відображатимуть розподіл відповідей між різними категоріями, тоді як кругові діаграми забезпечуватимуть пропорційне уявлення про різні сегменти даних. Гістограми полегшать порівняння між окремими групами, підкреслюючи помітні відмінності та подібності. Для поглиблення аналізу дані будуть організовані за віковими групами, що дозволить порівняти рівні обізнаності та довіри до різних джерел інформації серед різних демографічних груп. Цей підхід допоможе визначити, які вікові групи більш поінформовані або більше довіряють певним джерелам. Крім того, аналіз включатиме деякі гендерні порівняння, щоб дослідити, як сприйняття кібервійни та ставлення до джерел інформації відрізняються між чоловіками та жінками, пропонуючи повне розуміння цих точок зору.

Повний зміст опитування розміщено у Додатку А.

Анкета була продумано організована в кілька тематичних блоків, кожен з яких призначений для охоплення окремих аспектів сприйняття респондентами кібербезпеки. Цей структурований підхід має на меті сприяти комплексному та чіткому аналізу різних факторів, які впливають на розуміння та ставлення людей до кіберзагроз і заходів безпеки.

Перший блок під назвою «Обізнаність про кібервійну» має на меті оцінити рівень знань респондентів щодо кібератак і ширшого поняття кібервійни. У ньому розглядається, як учасники визначають кібервійну, ключові елементи, які вони з нею асоціюють, і їхнє сприйняття її серйозності та наслідків для національної безпеки. Другий блок, «Джерела інформації та довіра», розповідає про те, звідки люди в основному отримують інформацію про кібербезпеку та наскільки вони довіряють цим джерелам. Відповіді на питання з цього блоку висвітлять сфери, де дезінформація може підірвати точне розуміння. Далі в блоці «Дезінформація» досліджується поширеність і вплив неправдивих або оманливих даних, з якими стикаються респонденти. Він досліджує, як часто люди стикаються з дезінформацією, ступінь, до якого вона впливає на їхні думки щодо питань кібербезпеки тощо. Блок «Кібергігієна» присвячений особистим практикам, пов’язаним з кібербезпекою. Він охоплює такі дії, як використання антивірусного програмного забезпечення, стратегії керування паролями тощо. Нарешті, у сегменті «Сприйняття та політика» оцінюється ставлення до урядових ініціатив у сфері кібербезпеки, сприйняття ефективності політики та переважаючі проблеми безпеки. У сукупності ці тематичні блоки утворюють комплексну структуру для розуміння багатогранного ландшафту сприйняття кібербезпеки.

Обізнаність про кібервійну

У цьому блоці питань розглядається, як респонденти сприймають кібервійну, вивчається їхній рівень технічних знань і розуміння цифрових загроз. Він також оцінює їхнє усвідомлення пов’язаних ризиків та їх ставлення до потенційного впливу на національну безпеку. Досліджуючи ці перспективи,

ми отримуємо розуміння громадського сприйняття та важливості викликів кібербезпеки, з якими сьогодні стикається нація.

Перше питання – «Що, на вашу думку, є кібератакою?». Найпоширеніша відповідь – «Замах на комп'ютерні або інформаційні системи з метою завдати шкоди, викрасти дані або порушити роботу» – була обрана 141 респондентом. Це свідчить про те, що приблизно 86% учасників опитування ототожнюють кібератаку з її класичним, технічно точним визначенням (рис. 2.1).

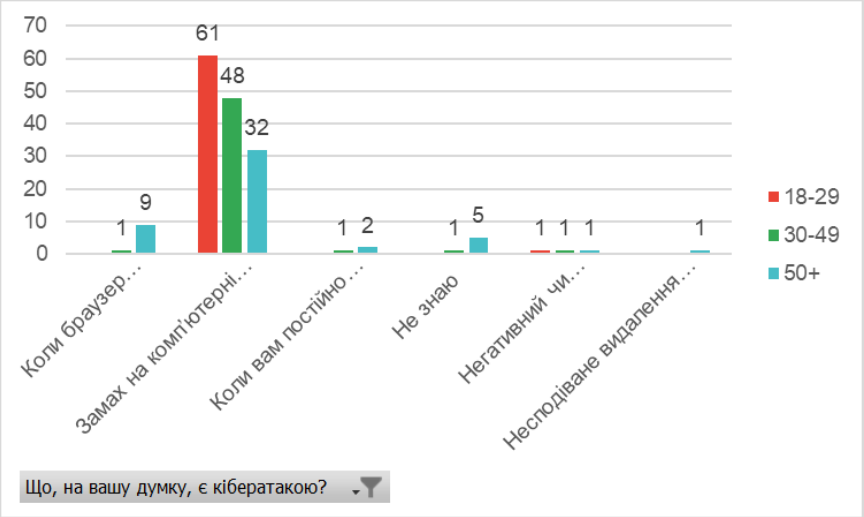

Рис. 2.1 Що, на вашу думку, є кібератакою?

Віковий розподіл відповідей: 18–29 років – 61 із 62 (≈98%); 30–49 років – 48 із 52 (≈92%); 50+ років – 32 із 50 (≈64%). Така динаміка вказує на те, що молодші респонденти краще орієнтуються в традиційному розумінні кібератак, тоді як серед старших учасників рівень обізнаності дещо нижчий.

Окрім основного технічного визначення, частина респондентів надала відповіді, які свідчать про ширше або менш точне розуміння поняття «кібератака». Одним із таких варіантів була відповідь «Коли браузер автоматично відкриває нові вкладки з рекламою», яку обрали 10 осіб.

Розподіл за віком: 18–29 років – 0 респондентів; 30–49 років – 1 респондентів; 50+ років – 9 респондентів. Цей варіант виявився популярнішим серед

старших вікових груп, що може свідчити про те, що старші учасники частіше сприймають рекламні спливаючі вікна як ознаку кібератаки або загрозливого програмного впливу.

Інші альтернативні варіанти включали:

- «Коли вам постійно телефонують із рекламними пропозиціями»
- «Несподіване видалення фото або файлів із телефону»
- «Негативний чи образливий коментар у соцмережах»
- «Не знаю»

Як висновок, більшість респондентів ототожнюють кібератаку з навмисним втручанням у комп'ютерні або інформаційні системи з метою завдання шкоди, викрадення даних або порушення їхньої роботи. Це свідчить про загальне розуміння терміну відповідно до його класичного технічного визначення. Молодші респонденти віком, як правило, сприймають кібератаки переважно як традиційні загрози, такі як віруси, зловмисне ПЗ або спроби злому, ймовірно, через те, що вони більше знайомі та комфортні з цифровими технологіями. На відміну від цього, літні люди у трактують цей термін інакше, охоплюючи ширший спектр питань, включаючи крадіжку особистих даних, онлайн-шахрайство, витік даних і тактику соціальної інженерії. Ця різниця в розумінні підкреслює різний рівень цифрової грамотності та обізнаності вікових груп щодо загроз кібербезпеці.

Питання «Чи чули ви термін «кібервійна»?» служить показником того, наскільки добре різні вікові групи розуміють термінологію та концепції кібербезпеки. Відповіді респондентів – «Так», «Ні» або «Важко відповісти» – допомагають виявити конкретні прогалини в розумінні (рис. 2.2). Ця інформація має значення для спрямування цілеспрямованих освітніх зусиль, дозволяючи викладачам і політикам розробляти індивідуальні програми, які покращують рівень кібербезпеки. Зрештою, підвищення обізнаності про такі терміни, як «кібервійна», підвищує загальну готовність проти цифрових загроз і сприяє формуванню більш поінформованого суспільства.

Із загальної кількості опитаних 117 із 164 респондентів (приблизно 71%) зазначили, що вже стикалися з терміном «кібервійна». Це свідчить про достатній рівень поширення поняття в інформаційному середовищі.

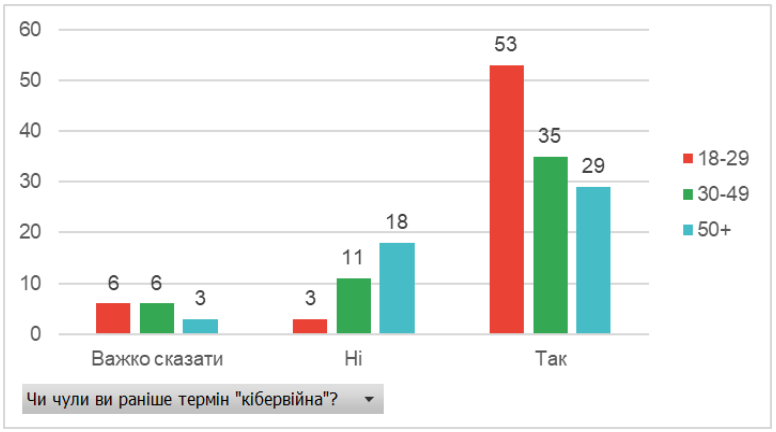

Рис. 2.2. Чи чули ви термін «кібервійна»?

Молодь продемонструвала найвищий рівень обізнаності – майже 85% учасників відповіли ствердно. У групі 30–49 років рівень обізнаності дещо нижчий – близько 67% респондентів відповіли «так». Серед найстарших респондентів лише 58% виявили знайомство з терміном. Водночас 36% представників цієї групи відповіли «ні», що може свідчити про інформаційний розрив та потребу в цільових освітніх ініціативах, спрямованих на підвищення рівня кіберграмотності серед старшого населення.

Питання «Чи вважаєте ви кібервійну реальною загрозою національній безпеці?» спрямоване на визначення ставлення респондентів до актуальної проблеми кіберзагроз, зокрема – чи сприймають вони кібервійну як явну небезпеку для державного суверенітету та стабільності країни. Отримані результати допомагають зрозуміти, яку частину аудиторії спонукає до пошуку інформації та підвищення особистої кібербезпеки, а також вказують на необхідність адаптації державної політики для різних демографічних сегментів (рис. 2.3).

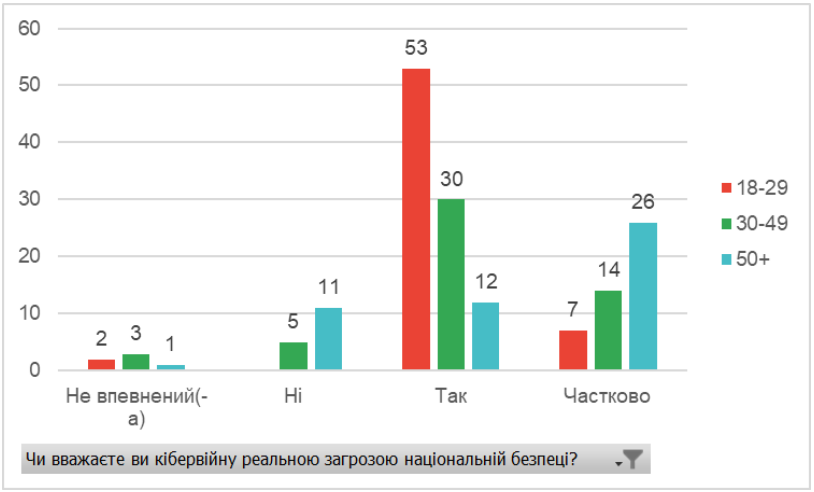

Рис. 2.3. Чи вважаєте ви кібервійну реальною загрозою національній безпеці?

Більшість респондентів висловили стурбованість з цього питання:

−95 осіб (≈57,9%) дали ствердну відповідь, чітко визнаючи кібервійну реальною загрозою.

−47 респондентів (≈28,7%) обрали варіант «Частково», що свідчить про певну невизначеність або обережність у сприйнятті загрози.

−16 осіб (≈9,8%) заперечили наявність загрози, що може бути пов’язано з недовірою до джерел інформації або альтернативним баченням кібербезпеки.

−6 респондентів (≈3,7%) не змогли визначитися з відповіддю.

Вікові відмінності:

- 18–29 років: у цій групі переважна більшість (≈85,5%) вважає кібервійну реальною загрозою. Ще 11,3% відповіли «Частково», і лише 3,2% залишилися невпевненими. Відповідей «Ні» не зафіксовано. Це свідчить про високий рівень усвідомлення ризиків серед молоді.
- 30–49 років: тут ≈57,7% респондентів дали ствердну відповідь, а ≈26,9% – часткову. Водночас ≈9,6% заперечили загрозу, а ≈5,8% не змогли визначитися. Такий розподіл демонструє більш збалансоване, але все ще переважно стурбоване ставлення.
- 50+ років: лише 24% респондентів цієї групи вважають кібервійну реальною загрозою. 52% обрали варіант «Частково», 22% – «Ні», і лише 2%

залишилися невпевненими. Це свідчить про найнижчий рівень категоричного сприйняття загрози серед усіх вікових категорій.

Загалом, понад 86% опитаних визнають кібервійну загрозою – повністю або частково. Водночас рівень впевненості у цьому значно варіюється залежно від віку. Молодші респонденти демонструють вищу обізнаність і рішучість, що, ймовірно, пов’язано з їхньою активною присутністю у цифровому середовищі. У старших вікових групах спостерігається більша обережність або скепсис, що може бути наслідком меншої поінформованості або обмеженого досвіду у сфері кібербезпеки.

Запитання «Що з наведеного ви вважаєте проявами кібервійни?» мало на меті з’ясувати, які саме дії або явища респонденти пов’язують із поняттям кібервійни. Оскільки питання було багатовибірковим, учасники могли обрати декілька варіантів, що дозволило отримати широку картину сприйняття кіберзагроз. Аналіз відповідей дозволяє встановити, які саме прояви кібервійни є найбільш впізнаваними та актуальними для громадськості, що, у свою чергу, відображає загальний рівень обізнаності та інформаційного впливу (рис. 2.4).

Рис. 2.4. Що з наведеного ви вважаєте проявами кібервійни?»

Аналіз відповідей щодо проявів кібервійни демонструє широке та нюансоване розуміння серед учасників. Найбільш часто згадуваним занепокоєнням був злом урядових веб-сайтів, із 133 згадками, що підкреслює

поширений страх перед атаками, спрямованими на важливі державні установи та національну безпеку. Крім того, багато учасників наголошували на загрозі дезінформаційних кампаній (123 згадки, що відображають усвідомлення інформаційної війни, спрямованої на вплив на громадську думку та дестабілізацію суспільства). Саботаж критичної інфраструктури також викликав серйозне занепокоєння, на що звернувся 121 респондент, що вказує на визнання технічної вразливості, яка може загрожувати комунальним службам, транспорту та комунікаційним мережам. Витоки даних, обрані 88 разів, вказували на занепокоєння з приводу порушень конфіденційності та зловживання особистою інформацією, підкреслюючи важливість кібербезпеки для захисту прав особи. Примітно, що лише двоє учасників висловили невпевненість щодо природи чи проявів кібервійни, що свідчить про те, що загалом серед респондентів існує сильне та добре поінформоване розуміння.

Джерела інформації та довіра

Цей блок опитування спрямований на з’ясування того, через які джерела респонденти найчастіше отримують інформацію про кібератаки, а також наскільки вони довіряють цим каналам. Сукупний аналіз відповідей дозволяє краще зрозуміти, як інформаційне середовище впливає на сприйняття кібербезпеки в суспільстві та які канали комунікації є найбільш ефективними для поширення знань у цій сфері.

Запитання «Де ви зазвичай дізнаєтесь про кібератаки?» було спрямоване на виявлення основних джерел інформації, які використовують респонденти для отримання відомостей про кіберзагрози. Аналіз відповідей дозволяє з’ясувати, які канали – як традиційні медіа, так і цифрові платформи – відіграють провідну роль у формуванні уявлень про кібербезпеку (рис.2.5).

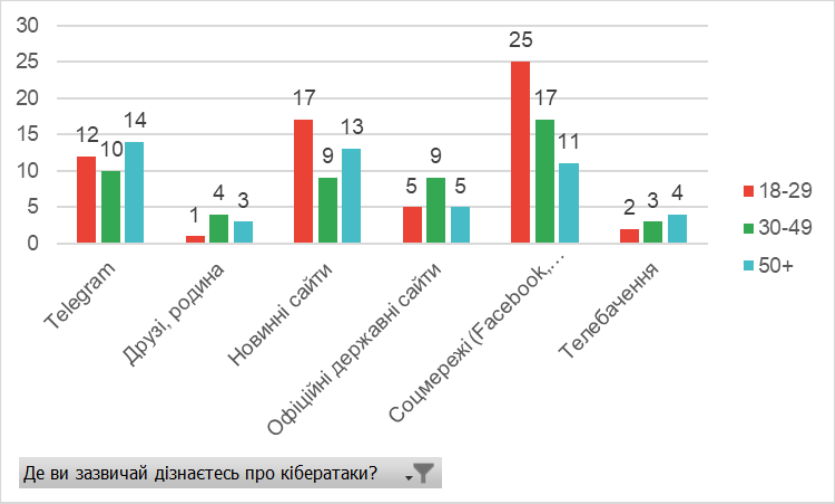

Рис. 2.5. Де ви зазвичай дізнаєтесь про кібератаки?

Найбільшу кількість згадок отримали соціальні мережі, зокрема Facebook та Instagram – 53 респонденти вказали ці канали як основне джерело. Це свідчить про значний вплив соціальних медіа на формування уявлень про кіберзагрози, особливо серед молоді. У віковій групі 18–29 років соціальні мережі були згадані 25 разів, що становить майже половину всіх відповідей у цій категорії. У групах 30–49 років та 50+ кількість згадок зменшується до 17 і 11 відповідно, що вказує на поступове зниження активності в соціальних мережах із віком.

Цікавою є динаміка використання Telegram. Хоча цей месенджер часто асоціюється з молоддю, найбільшу кількість згадок він отримав саме серед респондентів віком 50+ – 14 відповідей. У групах 18–29 та 30–49 років Telegram згадували 12 і 10 респондентів відповідно. Такий результат може свідчити про зростаючу популярність цього каналу серед старших користувачів, можливо, через доступ до спеціалізованих інформаційних каналів або груп, орієнтованих на певні інтереси. Новинні сайти залишаються стабільно популярними серед усіх вікових груп. Найбільше їх згадували респонденти віком 18–29 років (17 відповідей), що узгоджується з тенденцією до споживання новин в онлайн-форматі. У групах 30–49 та 50+ кількість згадок становила 9 і 13 відповідей відповідно, що свідчить про збереження довіри до цього типу джерел серед ширшої аудиторії. Офіційні державні сайти

були згадані 19 разів загалом, причому найбільше – у групі 30–49 років (9 відповідей). Це може свідчити про прагнення представників середнього віку отримувати інформацію з перевірених, авторитетних джерел. Молодь (18–29 років) та старші респонденти (50+) згадували цей канал рідше – по 5 разів у кожній групі. Традиційні джерела інформації, такі як телебачення та особисте спілкування з друзями чи родиною, мають найнижчі показники. Телебачення згадали лише 9 респондентів загалом, з них 4 – у групі 50+, 3 – у групі 30–49, і лише 2 – серед молоді. Інформацію від близького кола (друзі, родина) зазначили 8 респондентів, з яких лише 1 – у віковій категорії 18–29 років. Це свідчить про поступове зниження ролі традиційних каналів у поширенні інформації про кіберзагрози, особливо серед молодшого покоління.

Узагальнюючи, можна стверджувати, що молодь (18–29 років) орієнтується переважно на цифрові джерела – соціальні мережі та новинні сайти. Середній вік (30–49 років) демонструє більш збалансовану модель інформаційного споживання, поєднуючи як цифрові, так і офіційні джерела. Старше покоління (50+), попри очікування, активно використовує Telegram, а також частіше звертається до телебачення та новинних сайтів. Такий розподіл інформаційних уподобань є важливим для розробки ефективних комунікаційних стратегій, які мають враховувати вікові особливості аудиторії з метою підвищення рівня обізнаності про кіберзагрози та формування стійкої культури кібербезпеки.

Запитання «Наскільки ви довіряєте цим джерелам кіберновин?» було розроблено, щоб оцінити, як респонденти сприймають надійність різних інформаційних каналів кібербезпеки. Учасників попросили оцінити свою довіру за п’ятибальною шкалою від низького до високого. При цьому варіанти відповідей не були позначені як обов’язкові до оцінки, враховуючи, що респонденти можуть не користуватись даним каналом інформації. Як наслідок, деякі опції мають трохи менше 164 відповідей. Основна мета полягала в тому, щоб зрозуміти сприйману довіру до різних джерел, таких як онлайн-видання новин, платформи соціальних мереж, урядові установи тощо.

Аналізуючи ці відповіді, можна виявити відмінності в рівнях довіри між віковими групами, виявивши потенційні прогалини в поширенні інформації. Ці відомості мають вирішальне значення для підвищення кіберграмотності серед населення, оскільки вони допомагають визначити, яким каналам найбільше довіряють і де може поширюватися дезінформація.

Перший варіант відповіді – «Державні джерела». Результати опитування свідчать про наявність чітких вікових відмінностей у рівні довіри до державних джерел інформації про кібербезпеку (рис. 2.6). Респонденти оцінювали довіру за шкалою від 1 до 5, де 1 означає повну недовіру, а 5 – найвищий рівень довіри.

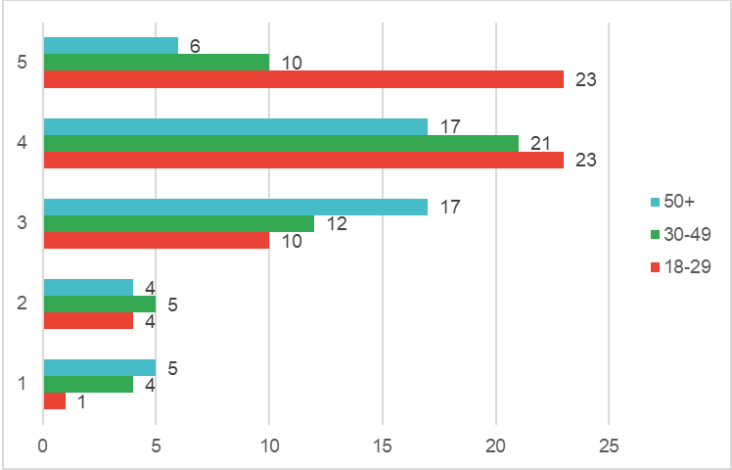

Рис. 2.6. Довіра до державних джерел

Аналіз відповідей респондентів за віковими групами показав чіткі поколіннєві відмінності у сприйнятті державних джерел кіберновин. Молодь демонструє найвищий рівень довіри: близько 75% респондентів цієї групи оцінили довіру на рівні 4 або 5. Група 30–49 років виявила більш помірковане ставлення – переважають оцінки 3 і 4, а максимальні оцінки трапляються рідше. Старші респонденти (50+) частіше обирали середні або низькі оцінки (1–3), що свідчить про нижчий рівень довіри до державних джерел у цій категорії. Ці результати вказують на необхідність віково орієнтованих інформаційних стратегій.

Аналіз відповідей щодо довіри до місцевих ЗМІ показав помірно позитивне ставлення у всіх вікових групах, із деякими відмінностями (рис. 2.7).

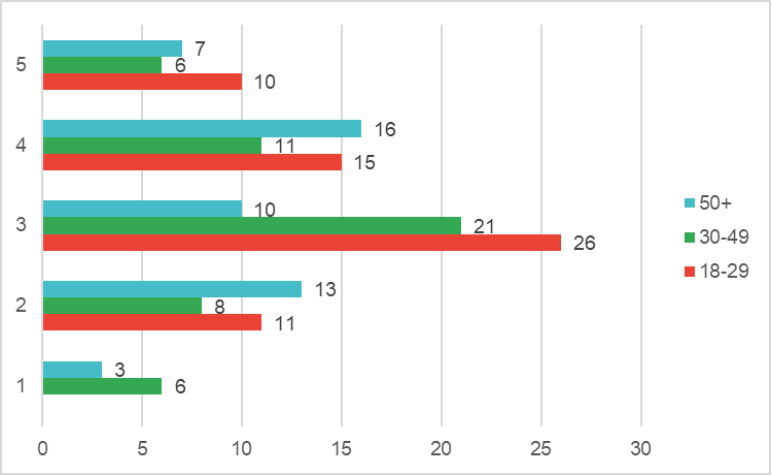

Рис. 2.7. Довіра до місцевих ЗМІ

Молодь (18–29 років) продемонструвала найвищий середній бал довіри – 3.39. Найбільше відповідей припало на оцінку 3, але значна частка респондентів також обрала високі оцінки (4 і 5), що свідчить про загалом позитивне сприйняття місцевих ЗМІ. Група 30–49 років виявила найнижчий середній бал – 3.06, що вказує на більш стримане ставлення. Розподіл відповідей зосереджений навколо середніх значень, а кількість максимальних оцінок є меншою. Старші респонденти (50+ років) мали середній бал 3.22, що свідчить про помірну довіру. Отже місцеві ЗМІ сприймаються як відносно надійне джерело інформації про кіберзагрози, особливо серед молоді. Ці результати можуть бути корисними для подальшого аналізу ролі локальних медіа у формуванні обізнаності про кібербезпеку та для розробки інформаційних кампаній на місцевому рівні.

Аналіз відповідей щодо довіри до міжнародних ЗМІ виявив виразні вікові відмінності у сприйнятті таких джерел (рис. 2.8). Молодь демонструє найвищий рівень довіри: понад 64% респондентів цієї групи оцінили довіру на

рівні 4 або 5 (відповідно 43.5% і 21%). Це свідчить про загальне позитивне ставлення до міжнародних ЗМІ серед молодших користувачів.

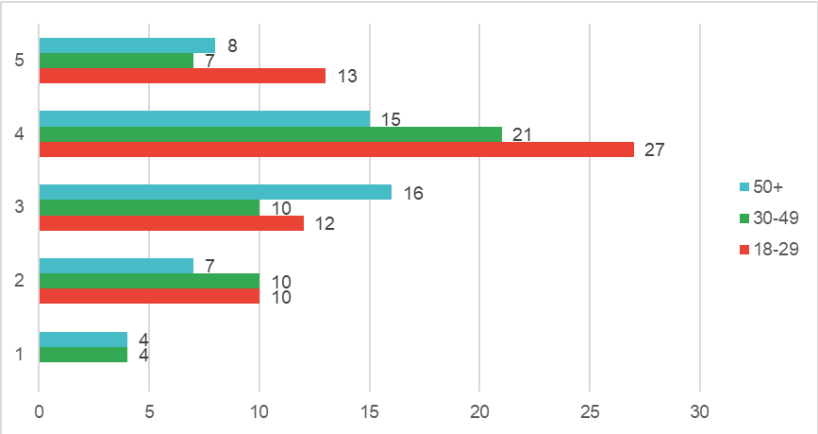

Рис. 2.8. Довіра до міжнародних ЗМІ

У віковій групі 30–49 років також переважають позитивні оцінки: понад 53% респондентів обрали рівні 4 або 5. Водночас близько 19% респондентів цієї групи поставили оцінку 3, що свідчить про помірковану довіру. Старші респонденти (50+) виявили найбільшу обережність: лише 46% обрали рівні 4 або 5, тоді як 32% поставили оцінку 3, а ще 22% – низькі оцінки 1 або 2. Це вказує на нижчий рівень довіри до міжнародних ЗМІ серед старшого населення. Отримані результати підкреслюють потребу в адаптації міжнародного контенту до очікувань різних вікових груп, зокрема – у підвищенні довіри серед старших респондентів шляхом прозорості, локалізації та зрозумілості подачі інформації.

Аналіз довіри до блогерів як джерела кіберновин виявив загалом низький рівень довіри у всіх вікових групах, із деякими відмінностями (рис. 2.9).

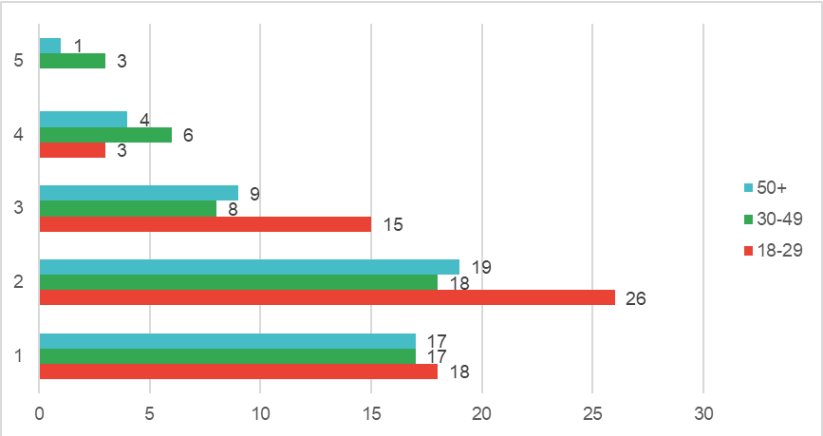

Рис. 2.9. Довіра до блогерів

Молодь найчастіше обирала оцінки 1 (29%) та 2 (42%), що свідчить про переважно критичне ставлення до блогерів як джерела інформації. Лише близько 5% респондентів цієї групи поставили оцінку 4, жоден не обрав найвищу оцінку 5. У віковій групі 30–49 років ситуація подібна: понад 67% респондентів поставили оцінки 1 або 2, а лише близько 17% – оцінки 4 або 5. Це вказує на обмежену довіру до блогерів серед представників середнього віку. Старші респонденти також демонструють низький рівень довіри: 72% обрали оцінки 1 або 2, а лише 10% – оцінки 4 або 5. Найвищу оцінку 5 поставив лише 1 респондент. Блогери сприймаються як менш надійне джерело кіберновин у всіх вікових категоріях. Це може бути пов’язано з відсутністю перевірки фактів, суб’єктивністю подачі інформації або недостатнім рівнем експертності. Отримані результати підкреслюють важливість критичного мислення при споживанні контенту від блогерів, особливо в контексті кібербезпеки.

Рівень довіри до соціальних мереж показав загалом низький рівень довіри у всіх вікових групах, із чіткою тенденцією до зниження довіри з віком (рис. 2.10).

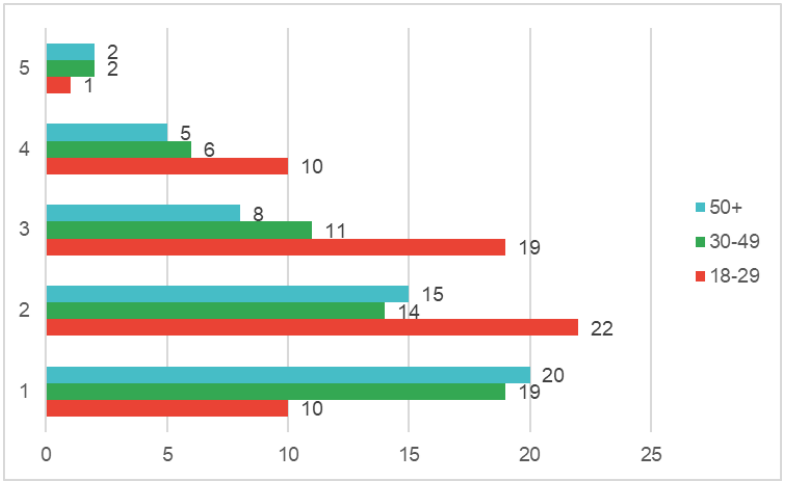

Рис. 2.10. Довіра до соціальних мереж

Представники молодшої вікової категорії виявили найбільш збалансоване ставлення: понад 47% респондентів обрали оцінки 3 або 4, що свідчить про помірну довіру. Водночас понад 51% поставили оцінки 1 або 2, а лише 1.6% – найвищу оцінку 5. У віковій групі 30–49 років майже 64% респондентів обрали оцінки 1 або 2, що вказує на переважно критичне ставлення до соцмереж як джерела кіберновин. Лише 15% поставили оцінки 4 або 5. Старші респонденти виявили найнижчий рівень довіри: 70% обрали оцінки 1 або 2, а лише 14% – оцінки 4 або 5. Це свідчить про значну недовіру до соціальних мереж серед старшого населення. Загалом, соціальні мережі сприймаються як менш надійне джерело кіберновин, особливо серед старших вікових груп. Це може бути пов’язано з поширенням дезінформації, відсутністю модерації та низьким рівнем перевірки фактів у таких каналах.

Останнє джерело – Telegram канали. Виявлено помірну довіру серед молодших вікових груп і значну недовіру серед старших (рис. 2.11).

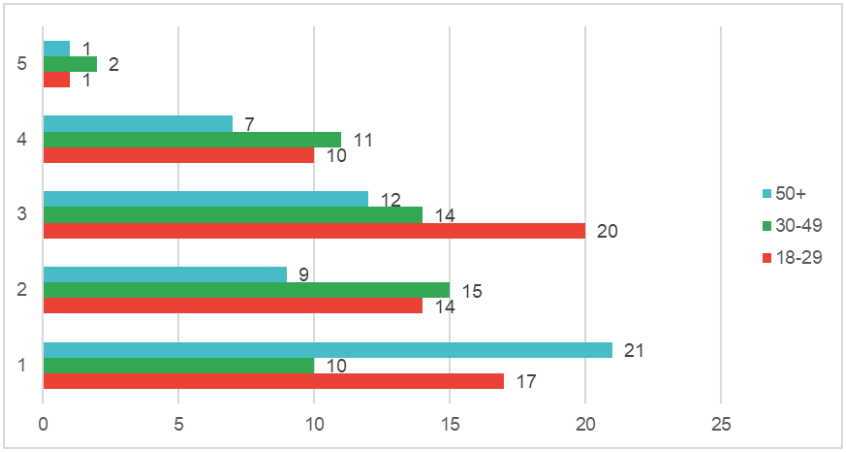

Рис. 2.11. Довіра до Telegram каналів

Молодь демонструє найбільш збалансоване ставлення: понад 48% респондентів обрали оцінки 3 або 4, що свідчить про помірну довіру. Водночас понад 27% поставили оцінку 1, а лише 1.6% – найвищу оцінку 5. У віковій групі 30–49 років також переважають середні оцінки: майже 49% респондентів обрали рівні 3 або 4, а 28.9% – оцінку 2. Частка найвищої оцінки 5 становить лише 3.9%. Старші респонденти виявили найнижчий рівень довіри: 42% обрали оцінку 1, а ще 18% – оцінку 2. Лише 16% респондентів цієї групи поставили оцінки 4 або 5, що свідчить про значну недовіру до телеграм-каналів серед старшого населення. Загалом, телеграм-канали сприймаються як відносно надійне джерело кіберновин серед молоді, тоді як старші вікові групи ставляться до них з обережністю. Це може бути пов’язано з різницею у цифровій грамотності, досвіді користування месенджерами та рівнем критичного мислення щодо контенту в таких каналах.

Аналіз відповідей респондентів щодо довіри до різних джерел кіберновин виявив чіткі вікові відмінності у сприйнятті інформації. Молодь загалом проявляє вищий рівень довіри до цифрових джерел, зокрема до телеграм-каналів, міжнародних ЗМІ та місцевих медіа. Водночас вона критично ставиться до блогерів і соціальних мереж, хоча й активно ними користується. Громадяни середнього віку виявляють більш стримане ставлення до всіх джерел, демонструючи помірну довіру до офіційних каналів і обережність щодо неформальних платформ. Їхній інформаційний вибір є

найбільш збалансованим, що може свідчити про прагнення до перевірених і різноманітних джерел. Старша вікова група загалом демонструє найнижчий рівень довіри до цифрових джерел, особливо до блогерів, соціальних мереж і телеграм-каналів. Водночас вона частіше звертається до традиційних або офіційних джерел, таких як державні та міжнародні ЗМІ.

Дезінформація

Цей блок дослідження спрямований на вивчення того, як часто респонденти стикаються з фейковими повідомленнями про кібератаки, чи траплялося їм самостійно поширювати таку інформацію, а також які країни, на їхню думку, є основними джерелами кібердезінформації.

Перше питання – «Як часто ви зустрічаєте неправдиву або маніпулятивну інформацію про кібератаки?». Аналіз відповідей засвідчив, що більшість респондентів усвідомлюють наявність кібердезінформації в інформаційному просторі (рис. 2.12).

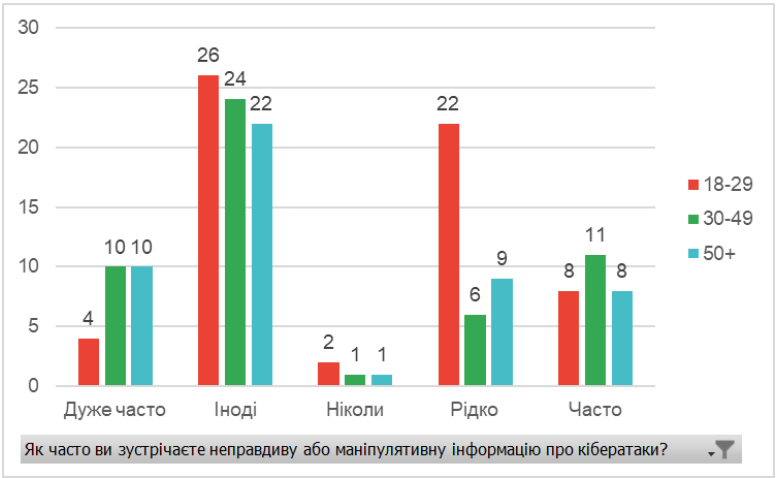

Рис. 2.12. Як часто ви зустрічаєте неправдиву або маніпулятивну інформацію про кібератаки?

Найпоширенішою відповіддю серед усіх вікових груп стало «іноді» – її обрали близько 42% молоді (18–29 років), 46% респондентів віком 30–49 років і 44% осіб віком 50+. Водночас старші респонденти частіше зазначали, що стикаються з фейками «дуже часто» (приблизно 19% у групах 30–49 і 50+),

тоді як серед молоді цей показник становить лише 6,5%. Варіант «ніколи» обрали лише 2–3% опитаних, що свідчить про загальне визнання проблеми дезінформації. Молодь частіше вказувала, що стикається з фейками «рідко», тоді як середній і старший вік схильні оцінювати частоту таких випадків як «часто». Це може свідчити як про різницю у сприйнятті інформації, так і про відмінності в рівні критичного мислення та медіаграмотності.

Наступне питання – «Чи траплялось вам випадково поширити фейкову інформацію про кібератаку?». Аналіз виявив помітні вікові відмінності (рис. 2.13).

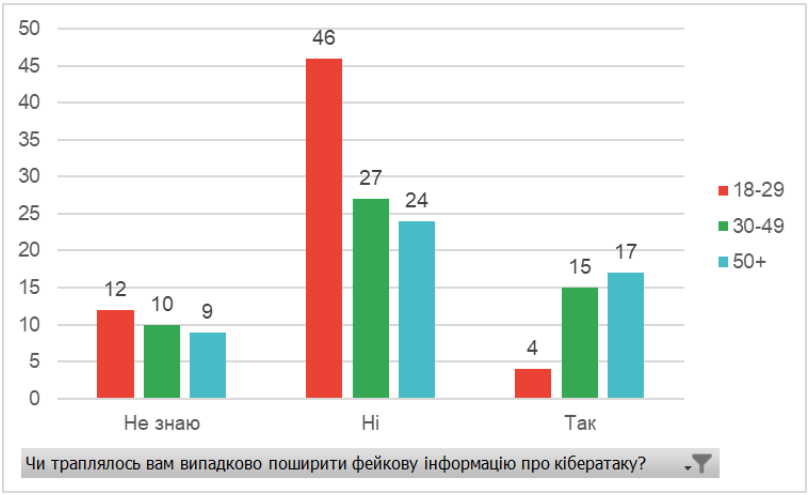

Рис. 2.13 Чи траплялось вам випадково поширити фейкову інформацію про кібератаку?

Найменше таких випадків зафіксовано серед молоді: лише 6,5% респондентів цієї групи відповіли «так», тоді як 74% зазначили, що ніколи не поширювали фейкову інформацію. У віковій групі 30–49 років частка тих, хто визнає випадкове поширення фейків, зросла до 29%, а серед старших респондентів – до 34%. Водночас близько 18–19% респондентів у всіх вікових групах обрали варіант «не знаю», що може свідчити про недостатню впевненість у достовірності поширюваної інформації або про низький рівень критичного аналізу контенту. Отримані результати підкреслюють важливість

підвищення медіаграмотності, особливо серед старших вікових груп, для запобігання ненавмисному поширенню кібердезінформації.

Останнє питання в блоці – «На вашу думку, яка країна найбільше поширює кібердезінформацію?» – виявило значну поляризацію поглядів (рис. 2.14).

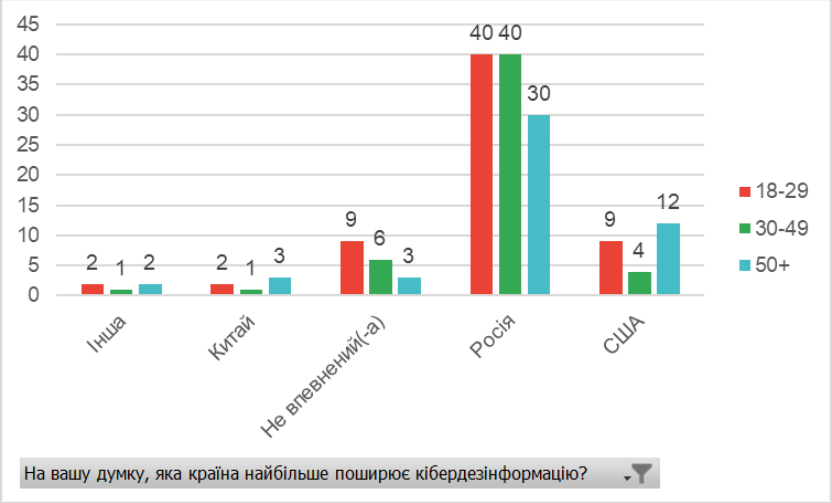

Рис. 2.14. На вашу думку, яка країна найбільше поширює кібердезінформацію?

Найбільше респондентів у всіх вікових групах вказали на росію: по 36% серед молоді і респондентів віком 30–49 років, а також 27% серед старших. Водночас США були обрані як джерело дезінформації 36% молоді та 48% респондентів віком 50+, що свідчить про неоднозначне сприйняття ролі західних країн у кіберпросторі. 50% відповідей «не впевнений(-а)» обрала молодь, що може свідчити про недостатню поінформованість або обережність у формуванні суджень. Відповідь «Китай» частіше обирали старші респонденти (троє осіб з 6 загалом). Загалом, результати демонструють широкий спектр уявлень про джерела кібердезінформації, що, ймовірно, відображає як вплив медіа, так і геополітичні настрої в суспільстві.

Аналіз цього блоку питань показав, що більшість респондентів регулярно стикаються з кібердезінформацією, найчастіше – у формі маніпулятивних повідомлень про кібератаки. Старші вікові групи частіше

вказують на високу частоту таких випадків, тоді як молодь – на рідкісні або поодинокі. Щодо джерел дезінформації, більшість респондентів назвали росію, але також згадували США та Китай.

Кібергігієна

Цей блок дослідження спрямований на вивчення рівня обізнаності та практик респондентів у сфері особистої кібербезпеки. Зокрема, аналізується, чи користуються вони захисними інструментами (наприклад, антивірусами, двофакторною автентифікацією тощо), чи проходили навчання з цифрової безпеки, а також чи знають, куди звертатися у разі кібератаки або фішингової атаки. Отримані результати дозволяють оцінити не лише рівень технічної підготовленості населення, а й потенціал для впровадження освітніх ініціатив у сфері кібербезпеки.

Перше питання в блоці – «Чи користуєтесь ви такими інструментами для особистої кібербезпеки?» (рис. 2.15).

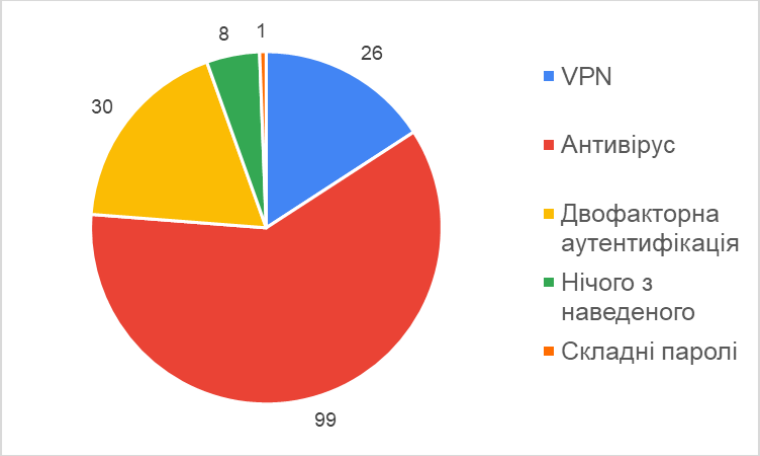

Рис. 2.15 Чи користуєтесь ви такими інструментами для особистої кібербезпеки?

Найпоширенішим засобом захисту є антивірусне програмне забезпечення, яким користуються понад 60% опитаних. Двофакторну аутентифікацію застосовують близько 18% респондентів, а VPN – майже 16%. Водночас майже 5% учасників опитування не використовують жодного з наведених інструментів, що свідчить про потенційні ризики для їхньої

цифрової безпеки. Лише 0,6% респондентів зазначили, що користуються складними паролями як основним засобом захисту, що може вказувати на недооцінку цього базового елементу кібергігієни. Отримані результати підкреслюють потребу в інформуванні населення про важливість комплексного підходу до особистої кібербезпеки.

Наступне питання стосується досвіду проходження навчання з кібербезпеки чи цифрової гігієни. Аналіз відповідей респондентів щодо проходження навчання з кібербезпеки або цифрової гігієни показав, що рівень обізнаності в цій сфері є нерівномірним серед різних вікових груп (рис. 2.16).

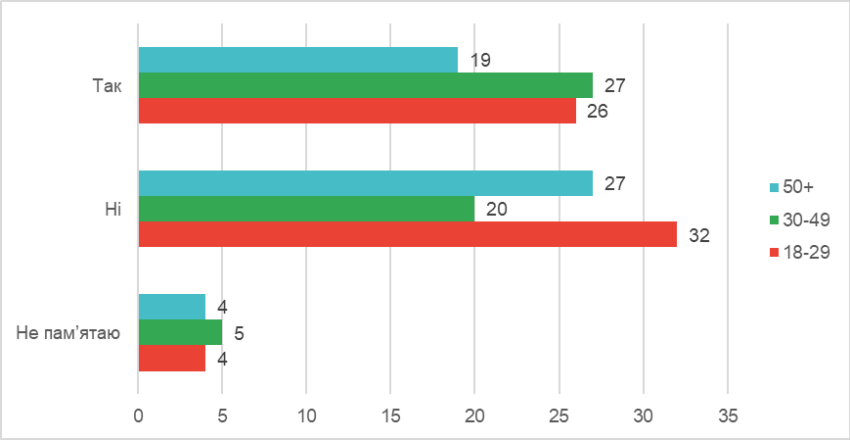

Рис. 2.16 Чи проходили ви навчання або курс з кібербезпеки чи цифрової гігієни?

Найвищу частку тих, хто проходив відповідне навчання, зафіксовано у віковій групі 30–49 років – понад 51%. Серед молоді таких респондентів 42%, а серед старших – 38%. Водночас понад половина респондентів старшої групи зазначили, що не проходили жодного навчання, що є найвищим показником серед усіх категорій. Варіант «не пам’ятаю» обрали 6–9% респондентів у кожній групі. Ці результати свідчать про потребу в розширенні доступу до освітніх програм з кібергігієни, особливо для старшого населення.

Останнє питання має на меті виявити обізнаність стосовно того, куди повідомити про кібератаку або фішинг у своїй країні. Результати свідчать про

значні відмінності у рівні поінформованості щодо механізмів реагування на кіберінциденти (рис. 2.17).

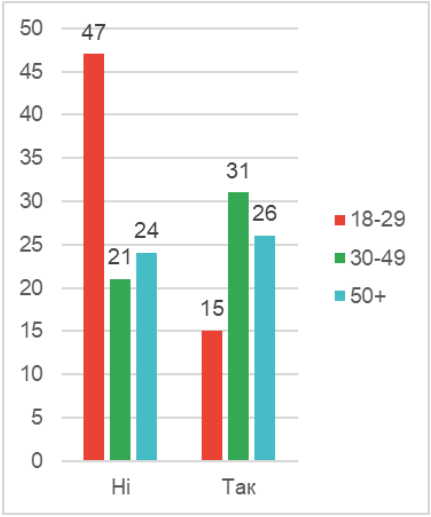

Рис. 2.17. Чи знаєте ви, куди повідомити про кібератаку або фішинг у своїй країні?

Лише 24% молоді знають, куди звертатися у разі кібератаки або фішингу, тоді як понад 75% не мають такої інформації. У віковій групі 30–49 років ситуація протилежна: майже 60% респондентів знають, куди повідомити про інцидент. Серед старших респондентів рівень обізнаності також є відносно високим – 52% відповіли ствердно. Ці результати вказують на потребу в цілеспрямованих інформаційних кампаніях, особливо орієнтованих на молодь, яка, попри активне користування цифровими технологіями, часто не знає, як діяти у разі кіберзагроз.

Результати аналізу питань цього блоку свідчать про недостатній рівень практик кібергігієни серед респондентів, особливо молоді. Хоча більшість користуються антивірусами, інші інструменти захисту застосовуються рідко. Навчання з кібербезпеки проходила лише частина опитаних, а знання про те, куди звертатися у разі кібератаки, мають переважно респонденти середнього та старшого віку. Це підкреслює потребу в посиленні просвітницьких заходів, зокрема для молоді.

Сприйняття та політика

Цей блок дослідження спрямований на вивчення громадської думки щодо ролі держави у сфері кібербезпеки: чи повинні уряди більше інвестувати в кібероборону та освіту, наскільки ефективною вважається державна реакція на кіберзагрози, а також чи визнають респонденти вплив кібервійни на політичні процеси, зокрема вибори.

Перше питання у блоці – «Чи повинні уряди більше інвестувати в кібероборону та освіту у сфері кібербезпеки?». Більшість респондентів підтримують ідею посилення державних інвестицій у кібероборону та освіту з кібербезпеки, однак рівень підтримки суттєво відрізняється між віковими групами (рис. 2.18).

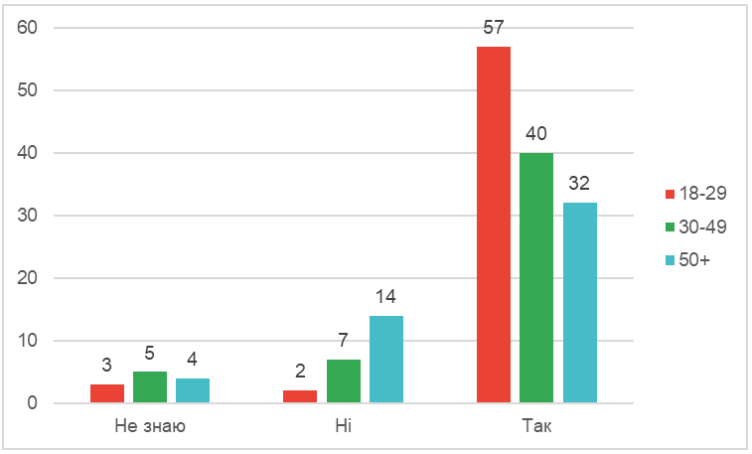

Рис. 2.18. Чи повинні уряди більше інвестувати в кібероборону та освіту у сфері кібербезпеки?

Найвищу частку позитивних відповідей зафіксовано серед вікової категорії 18–29 років – понад 44%. Серед осіб віком 30–49 років таку позицію підтримали 31%, а серед старших – 25%. Водночас понад 60% респондентів старшої вікової групи висловилися проти збільшення інвестицій, що є найвищим показником серед усіх категорій. Варіант «не знаю» обрали 25–42% респондентів, що може свідчити про недостатню поінформованість або невизначеність у ставленні до державної кіберполітики.

Оцінка ефективності державної реакції на кіберзагрози виявила переважно стримане ставлення серед респондентів усіх вікових груп (рис. 2.19).

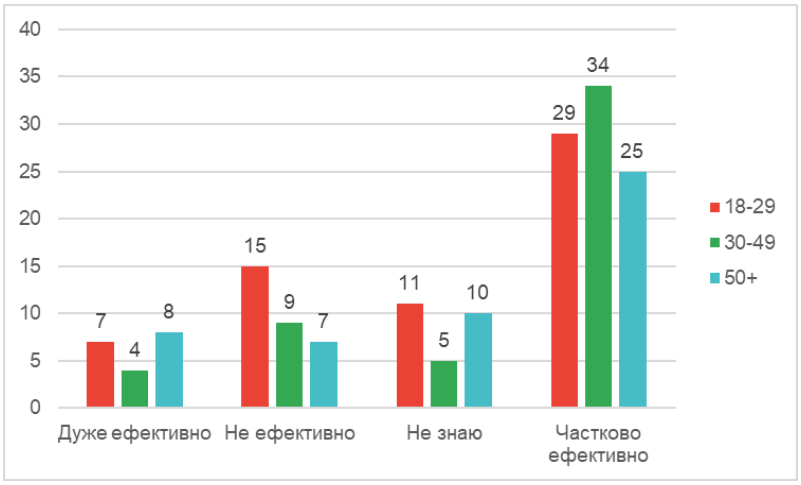

Рис. 2.19. Наскільки ефективно, на вашу думку, ваша країна реагує на кіберзагрози?

Найпоширенішою відповіддю стала «частково ефективно», яку обрали 47% молоді, 65% респондентів віком 30–49 років та 50% старших респондентів. Водночас лише 7–16% вважають реакцію держави «дуже ефективною», а 14–24% – «не ефективною». Відповідь «не знаю» обрали 10–18% респондентів, що може свідчити про недостатню поінформованість або складність оцінки державної кіберполітики. Загалом, результати вказують на помірну довіру до дій держави у сфері кібербезпеки, з переважанням критично-обережного погляду.

Останнє питання у блоці – «Чи вірите ви, що кібервійна може впливати на політичну думку та вибори?». Більшість респондентів погоджуються з тим, що кібервійна здатна впливати на політичну думку та виборчі процеси (рис. 2.20).

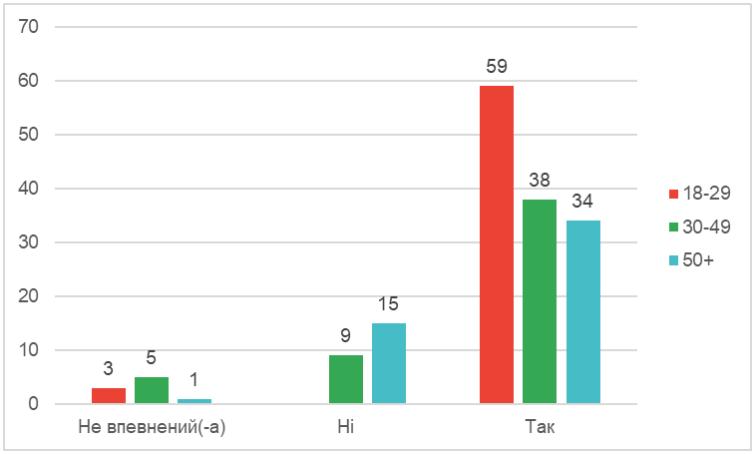

Рис. 2.20. Чи вірите ви, що кібервійна може впливати на політичну думку та вибори?

Найвищий рівень згоди зафіксовано серед молоді – понад 95% відповіли ствердно. У віковій групі 30–49 років цю думку поділяють 73% респондентів, а серед старших – 68%. Водночас 30% респондентів старшої групи не вірять у такий вплив, що є найвищим показником серед усіх категорій. Варіант «не впевнений(-а)» обрали лише 2–10% респондентів. Ці результати свідчать про загальне усвідомлення потенційної загрози кібервтручання у політичні процеси, особливо серед молоді.

Результати аналізу відповідей на питання цього блоку свідчать про загальне усвідомлення важливості кібербезпеки як на індивідуальному, так і на державному рівні. Більшість респондентів підтримують ідею посилення інвестицій у кібероборону та освіту, хоча рівень підтримки знижується з віком. Державну реакцію на кіберзагрози респонденти оцінюють переважно як частково ефективну, з помірним рівнем довіри. Водночас переважна більшість опитаних, особливо молодь, визнають, що кібервійна може впливати на політичну думку та вибори. Це підкреслює важливість прозорої та активної кіберполітики, а також необхідність залучення громадськості до формування культури цифрової безпеки.

Висновки до розділу 2

Комплексне дослідження забезпечило поглиблену оцінку обізнаності, ставлення та поведінки респондентів щодо питань кібербезпеки. У ньому систематично розглядаються різні аспекти, починаючи від фундаментальної термінології до практичних практик кібергігієни, сприйняття дезінформації та поглядів на державну політику, пов’язану з цифровою безпекою. Висновки показують суміш позитивних зрушень і сфер, які потребують подальшої уваги як з боку навчальних закладів, державних установ, так і громадських організацій.

Значна частина респондентів правильно визначає термін «кібератака» як навмисну дію, спрямовану на порушення цифрових систем або викрадення конфіденційних даних. Обізнаність щодо поняття «кібервійна» є особливо високою серед учасників, понад 70% загалом знайомі з цим терміном. Більшість учасників сприймають кібервійну як справжню загрозу з потенціалом значного впливу на національну політику та соціальну стабільність. Досліджуючи дезінформацію, респонденти чітко усвідомлюють її поширеність, головним чином виходячи з таких джерел, як платформи соціальних мереж, блогери та канали Telegram. Молодші люди повідомляють, що частіше стикаються з фейковими новинами, що узгоджується з їхньою більшою активністю в соціальних мережах. Однак цікаво те, що вони з меншою ймовірністю визнають, що активно поширюють неправдиву інформацію, що свідчить про певну обережність або усвідомлення наслідків.

Загалом дослідження підкреслює як прогрес, досягнутий у цифровій грамотності, так і постійні проблеми, які залишаються. Хоча багато користувачів знають про ключові кіберзагрози та тактики дезінформації, прогалини в розумінні та відповідальній поведінці підкреслюють нагальну потребу в цілеспрямованих освітніх ініціативах. Крім того, висновки вимагають посилення державної політики та громадських зусиль для сприяння безпечнішому онлайн-середовищу та сприянню критичному залученню до цифрового контенту. Надана інформація закладає міцну основу для розробки

стратегій, спрямованих на підвищення обізнаності про кібербезпеку серед усіх демографічних груп, забезпечуючи більш стійке цифрове суспільство.

РОЗДІЛ 3. РЕКОМЕНДАЦІЇ ТА ВИСНОВКИ

3.1. Рекомендації для підвищення обізнаності населення

В епоху, яка характеризується швидким технологічним прогресом і взаємопов'язаними суспільствами, підвищення обізнаності громадян щодо кібербезпеки стало важливою складовою сучасної державної політики. Оскільки цифрові платформи стають невід'ємною частиною повсякденного життя, сприяючи комунікації, комерції та розповсюдженню інформації, загрози, які ховаються в кіберпросторі, стають дедалі складнішими та поширеними. Кібервійни, витоки даних, фішингові схеми та кампанії дезінформації зараз становлять значні ризики для національної безпеки, економічної стабільності та конфіденційності особи. Отже, уряди в усьому світі визнають, що поінформоване та пильне населення є важливою лінією захисту від цих цифрових загроз.

Молодші люди, яких часто називають «цифровими вихідцями», як правило, краще знайомі з онлайн-середовищем і кіберзагрозами. Їх часте спілкування з соціальними медіа, ігровими платформами та мобільними додатками сприяло відносно вищому рівню цифрової грамотності. Проте людям похилого віку, які, як правило, не росли в цифрових технологіях, часто важко розпізнавати кіберзагрози та ефективно реагувати на них. Ця невідповідність підкреслює нагальну потребу в індивідуальних освітніх ініціативах, орієнтованих на вік, спрямованих на подолання розриву в знаннях і сприяння безпечним онлайн-практикам серед усіх демографічних груп.

Інтерактивні формати, такі як онлайн-курси, мобільні додатки та гейміфіковані навчальні платформи, є дуже ефективними. Ці методи не лише залучають молодих користувачів, але й надають практичні вказівки в реальному часі щодо виявлення загроз, створення надійних паролів і уникнення шахрайства. Наприклад, гейміфіковані модулі можуть імітувати

сценарії кібератак, допомагаючи користувачам розвивати навички критичного мислення в безпечному середовищі. І навпаки, літні люди отримують переваги від автономних, більш персоналізованих підходів. Особисті тренінги та громадські семінари, що проводяться в бібліотеках або громадських центрах, можуть відповідати їхнім навчальним уподобанням і рівням цифрової грамотності. Ці налаштування сприяють прямій взаємодії, дозволяючи інструкторам вирішувати конкретні проблеми та роз'яснювати помилкові уявлення про кібербезпеку.

Окрім цільової освіти, широкомасштабні інформаційні кампанії з використанням сучасних каналів зв'язку є незамінними. Платформи соціальних мереж, телебачення, радіо та впливові особи можуть поширювати життєво важливі повідомлення про кібергігієну та безпечну поведінку в Інтернеті серед широкої аудиторії. Прикладом успішної практики є кампанія Національного банку України «#ШахрайГудбай», яка через креативні відео та інтерактивні матеріали підвищує обізнаність громадян про фінансову кібербезпеку [40]. Поєднуючи креативний контент з інтерактивними матеріалами, кампанія успішно залучила громадян, підвищуючи обізнаність про загрози кібербезпеці та просуваючи методи захисту. Такі ініціативи демонструють силу мультимедійного охоплення у вихованні культури кіберпильності.

Активна участь громадян в освітніх ініціативах відіграє вирішальну роль у посиленні кібербезпеки. Створюючи мережі спеціалізованих кіберволонтерів, спільноти можуть підвищувати обізнаність і забезпечувати рівному рівному навчання, надаючи людям можливість розпізнавати цифрові загрози та ефективно реагувати на них. Підтримка місцевих проектів, які зосереджуються на освіті з кібербезпеки, допомагає культивувати культуру відповідальності та пильності серед громадян. Наприклад, Естонія є взірцевою моделлю, успішно інтегрувавши комплексну цифрову освіту у свою національну політику, що значно підвищило її кіберстійкість [41]. Крім цього, у Фінляндії понад 82% населення мають принаймні базові цифрові навички, а

відкриті навчальні курси з кібербезпеки є частиною національної цифрової стратегії [42]. Також країна активно підтримує цифрову трансформацію малого та середнього бізнесу, що також сприяє загальному підвищенню цифрової культури. У шкільній освіті Фінляндії цифрова грамотність інтегрована в навчальні програми, що дозволяє формувати критичне мислення та навички безпечного користування інформаційними технологіями з раннього віку. Для створення безпечного цифрового середовища важлива цілісна стратегія, яка передбачає співпрацю між державними установами, організаціями громадянського суспільства та звичайними громадянами. Завдяки спільним зусиллям, обізнаності та постійному навчанню суспільства можуть краще захищатися від кіберзагроз, що розвиваються, і створювати стійке, поінформоване населення, здатне безпечно рухатися в епоху цифрових технологій.

Підсумовуючи, побудова стійкого цифрового суспільства потребує комплексного підходу, який поєднує освіту відповідно до віку та широкі інформаційні кампанії. Спеціальні стратегії гарантують, що всі громадяни – від технічно підкованої молоді до людей похилого віку, які розуміються на цифрових технологій – отримають знання та навички, необхідні для безпечної навігації у складному ландшафті кіберпростору. Оскільки кіберзагрози продовжують розвиватися, проактивні та інклюзивні освітні зусилля є незамінними для захисту національної безпеки та прав особистості в епоху цифрових технологій.

З огляду на визначені аспекти, сформуємо список відповідних рекомендацій:

1. Розробка вікових освітніх програм з кібербезпеки для різних демографічних груп.
2. Використання інтерактивних та гейміфікованих платформ для залучення молоді.
3. Проведення персоналізованих тренінгів для людей похилого віку в громадських центрах.

4. Запуск масштабних інформаційних кампаній через соціальні мережі, ЗМІ та інфлюенсерів.
5. Створення мереж кіберволонтерів для підтримки локальних ініціатив.
6. Інтеграція цифрової грамотності в шкільну освіту.
7. Забезпечення міжсекторальної співпраці між державою, громадськими організаціями та громадянами.

3.2. Стратегії протидії дезінформації

Дезінформація стала не лише інструментом маніпуляції, а й складовою гібридної війни, що має на меті підрив довіри до державних інституцій, деморалізацію населення та дестабілізацію суспільства. Результати проведеного опитування свідчать про високу обізнаність респондентів щодо наявності фейкової інформації у цифровому середовищі, однак також виявлено значні відмінності у здатності розпізнавати та критично оцінювати такі повідомлення. Особливо вразливими до дезінформації виявилися старші вікові групи, що потребує цілеспрямованих заходів з підвищення медіаграмотності.

Одним із ключових напрямів протидії дезінформації є розвиток критичного мислення та медіаграмотності серед населення. Це передбачає впровадження навчальних програм, тренінгів та онлайн-курсів, які навчають громадян розпізнавати маніпулятивні техніки, перевіряти джерела інформації та аналізувати контент. В Україні такі ініціативи реалізуються, зокрема, Центром стратегічних комунікацій та інформаційної безпеки при Міністерстві культури та інформаційної політики [43]. Центр проводить інформаційні кампанії, створює пояснювальні матеріали, організовує пресконференції та співпрацює з медіа для підвищення стійкості суспільства до інформаційних атак.

Важливу роль у протидії дезінформації відіграють громадські організації. Наприклад, ГО «Вокс Україна» у співпраці з Центром протидії дезінформації РНБО розробила методичні рекомендації для регіональних медіа та органів місцевого самоврядування [44]. Ці матеріали містять практичні поради щодо виявлення фейків, аналізу інформаційного середовища та організації локальних інформаційних кампаній. Такий підхід дозволяє не лише централізовано реагувати на загрози, а й формувати мережу локальних лідерів думок, здатних оперативно реагувати на виклики у своїх громадах.

Окремим напрямом є використання технологічних рішень для виявлення та блокування дезінформації. Алгоритми штучного інтелекту, системи фактчекінгу, автоматизовані платформи моніторингу соціальних мереж – усе це дозволяє оперативно виявляти поширення фейкових наративів. Водночас важливо забезпечити баланс між безпекою та свободою слова, що потребує чітких етичних та правових рамок.

В Україні активно функціонують низка платформ, які допомагають громадянам перевіряти достовірність інформації. Наприклад, проєкт StopFake спеціалізується на спростуванні російської пропаганди, тоді як ВоксЧек від ГО «Вокс Україна» перевіряє заяви політиків і публікації на предмет маніпуляцій [45,46]. Ініціатива «По той бік новин» публікує розбори фейків і пояснює механізми їх поширення, а платформа «Без Брехні» зосереджується на перевірці регіональних новин і підвищенні медіаграмотності [47,48]. Крім того, ініціатива EU vs Disinfo, підтримана Європейським Союзом, документує приклади дезінформації, зокрема з боку росії, і поширює аналітичні матеріали для підвищення обізнаності [49].

Міжнародний досвід також свідчить про ефективність міжсекторальної співпраці. У рамках ініціативи Nations Against Disinformation, підтриманої Європейським Союзом, створено платформу для обміну знаннями, ресурсами та методиками боротьби з дезінформацією між країнами [50]. Така координація дозволяє швидше реагувати на транснаціональні інформаційні загрози та адаптувати найкращі практики до національного контексту.

Таким чином, ефективна протидія дезінформації потребує поєднання освітніх, технологічних та комунікаційних стратегій. Важливо не лише інформувати громадян про загрози, а й надавати їм інструменти для самостійного аналізу інформації, формуючи культуру критичного мислення як основу інформаційної безпеки демократичного суспільства.

Висновки до розділу 3

У третьому розділі наголошується на важливості впровадження практичних заходів для підвищення цифрової обізнаності та ефективної боротьби з дезінформацією. Щоб досягти цього, він рекомендує ряд цільових стратегій. По-перше, слід розробити освітні програми для кожного віку, щоб гарантувати, що люди будь-якого віку розуміють ризики, пов’язані з дезінформацією, і як визначити надійні джерела. Широкомасштабні інформаційні кампанії також необхідні для охоплення широкої аудиторії та сприяння відповідальній цифровій поведінці.

Крім того, виховання навичок критичного мислення за допомогою навчальних програм може надати людям можливість ретельніше аналізувати інформацію та відрізняти правду від брехні. Підтримка місцевих ініціатив може допомогти адаптувати рішення до конкретних проблем громади, заохочуючи залучення низового рівня.

Технологічні інструменти, такі як алгоритми та системи штучного інтелекту, слід використовувати для швидкого виявлення та позначення фейкових повідомлень. Успіх цих заходів залежить від міжгалузевої співпраці, як це продемонстрували Естонія та Фінляндія, де співпраця між урядовими установами, освітніми закладами, громадськими організаціями та громадянами підкреслює важливість об’єднаних зусиль у захисті цифрового простору.

ВИСНОВКИ

У процесі написання дипломної роботи було здійснено комплексне дослідження громадського сприйняття кібервійни, рівня обізнаності населення щодо кіберзагроз, поширення дезінформації та довіри до державної політики у сфері кібербезпеки. Робота поєднала теоретичний аналіз, емпіричне опитування та розробку практичних рекомендацій, що дозволило отримати цілісне уявлення про сучасний стан цифрової обізнаності в українському суспільстві.

На теоретичному рівні було визначено, що кібервійна є не лише технічним явищем, пов’язаним із атаками на цифрову інфраструктуру, а й потужним інструментом інформаційного впливу, який використовується для маніпуляції громадською думкою, дестабілізації політичної ситуації та підриву довіри до державних інституцій. У роботі підкреслено важливість міжнародного співробітництва, створення правових механізмів регулювання кіберпростору та формування глобальної культури цифрової відповідальності. Особливу увагу приділено ролі громадськості як активного учасника процесу забезпечення кібербезпеки.

Емпіричне дослідження, проведене у формі соціологічного опитування, дозволило виявити ключові тенденції у сприйнятті кіберзагроз. Було встановлено, що більшість респондентів мають загальне уявлення про поняття «кібератака» та «кібервійна», однак рівень обізнаності значною мірою залежить від віку. Молодь демонструє вищу цифрову грамотність, краще орієнтується в технічних аспектах загроз, тоді як старші респонденти частіше стикаються з труднощами у розпізнаванні фейкової інформації та реагуванні на кіберінциденти. Водночас, попри високу обізнаність про наявність дезінформації, значна частина опитаних не має чітких уявлень про механізми перевірки достовірності інформації або про дії у разі кіберінциденту. Це свідчить про наявність прогалин у сфері медіаграмотності та потребу в системному підході до цифрової освіти.

Окремим аспектом дослідження стало вивчення рівня довіри до державної політики у сфері кібербезпеки. Респонденти загалом підтримують ідею посилення інвестицій у кібероборону та освіту, однак оцінка ефективності державних заходів залишається помірною. Це вказує на необхідність прозорої комунікації, адаптації інформаційних кампаній до потреб різних соціальних груп та активного залучення громадян до формування політики у сфері кібербезпеки.

У третьому розділі було сформульовано низку практичних рекомендацій, спрямованих на підвищення цифрової обізнаності населення та протидію дезінформації. Зокрема, запропоновано впровадження віково орієнтованих освітніх програм, реалізацію масштабних інформаційних кампаній, розвиток критичного мислення, підтримку локальних ініціатив, а також використання технологічних рішень для виявлення фейкових повідомлень. У роботі також проаналізовано міжнародний досвід, зокрема приклади Естонії та Фінляндії, які демонструють ефективність міжсекторального підходу до формування цифрової стійкості. Ці країни активно інтегрують цифрову грамотність у систему освіти, підтримують громадські ініціативи та забезпечують доступ до відкритих навчальних ресурсів.

Усі поставлені в роботі завдання були успішно реалізовані. Було досягнуто мети дослідження – оцінити рівень обізнаності громадськості щодо кібервійни, виявити основні джерела дезінформації та визначити рівень довіри до державної політики у сфері кібербезпеки. Робота надала цілісне уявлення про сучасний стан цифрової культури в Україні та окреслила шляхи її подальшого розвитку.

Перспективи подальших досліджень полягають у глибшому аналізі впливу конкретних інформаційних кампаній на зміну поведінкових моделей громадян, вивченні ефективності освітніх програм з медіаграмотності в різних регіонах України, а також у дослідженні ролі штучного інтелекту у виявленні та нейтралізації дезінформації. Також доцільним є порівняльний аналіз

державних стратегій кібербезпеки в Україні та країнах ЄС з метою адаптації найкращих практик до національного контексту. Усе це сприятиме формуванню більш стійкого, обізнаного та захищеного цифрового суспільства.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Шимченко Л. А. Кіберзагрози в Україні як проблема в умовах геополітичного суперництва [Електронний ресурс] / Л. А. Шимченко // Економічний вісник університету. – 2019. – Режим доступу: https://cyberleninka.ru/article/n/kiberzagrozi-v-ukrayini-yak-problema-v-umovah-geopolitichnogo-supernitstva

2. Баловсяк Н. Як ведуться сучасні кібервійни. Попередній аналіз [Електронний ресурс] / Н. Баловсяк // Український тиждень. – 2022. – 14 липня. – Режим доступу: https://tyzhden.ua/iak-vedutsia-suchasni-kibervijny-poperednij-analiz/

3. Як росія використовує кібератаки проти України [Електронний ресурс] // Державний центр кіберзахисту. – 2024. – Режим доступу: https://scpc.gov.ua/uk/articles/334

4. CERT-UA минулого року опрацювала 4315 кіберінцидентів [Електронний ресурс] // Державна служба спеціального зв'язку та захисту інформації України. – 2025. – 8 січня. – Режим доступу: https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv

5. Number of cyber incidents in Europe in 2022, by sector [Електронний ресурс] // Statista. – 2023. – Режим доступу: https://www.statista.com/statistics/1310994/number-of-cyber-incidents-in-europe-by-sector/

6. Major ransomware attacks in Europe in 2022 and 2023 [Електронний ресурс] // Statista. – 2024. – Режим доступу: https://www.statista.com/statistics/1398137/europe-major-cases-ransomware-attacks/

7. WHO/Europe launches guide to strengthen cybersecurity in digital health [Електронний ресурс] // World Health Organization. – 2025. – 26 березня.

– Режим доступу: https://www.who.int/europe/news/item/26-03-2025-who-europe-launches-guide-to-strengthen-cybersecurity-in-digital-health

8. Cyberwarfare – definition and meaning [Електронний ресурс] // TechTarget. – Режим доступу: https://www.techtarget.com/searchsecurity/definition/cyberwarfare

9. Що таке кібервійна: визначення, види та приклади [Електронний ресурс] // FutureNow. – 2023. – 9 липня. – Режим доступу: https://futurenow.com.ua/shho-take-kibervijna-vyznachennya-vydy-ta-pryklady/

10. Таран В. Кіберперемир'я не буде: як росія продовжуватиме війну в цифровому просторі [Електронний ресурс] / Віктор Таран // Укрінформ. – 2025. – 13 березня. – Режим доступу: https://www.ukrinform.ua/rubric-ato/3970241-kiberperemira-ne-bude-ak-rosia-prodovzuvatime-vijnu-v-cifrovomu-prostori.html

11. EN, ISO, IEC standards – What is what? [Електронний ресурс] // Estonian Centre for Standardisation and Accreditation (EVS). – 2023. – 31 жовтня. – Режим доступу: https://www.evs.ee/en/standard-what-is-what

12. ISO/IEC 27000 family [Електронний ресурс] // Wikipedia. – Режим доступу: https://en.wikipedia.org/wiki/ISO/IEC_27000_family

13. ISO/IEC 27001 – Information Security Management [Електронний ресурс] // IT Governance UK. – Режим доступу: https://www.itgovernance.co.uk/iso27001

14. ISO/IEC 27002 [Електронний ресурс] // Wikipedia. – Режим доступу: https://en.wikipedia.org/wiki/ISO/IEC_27002

15. ISO/IEC 27005:2022 – Information security, cybersecurity and privacy protection – Information security management systems – Requirements [Електронний ресурс] // International Organization for Standardization (ISO). – Режим доступу: https://www.iso.org/standard/80585.html

16. ISO/IEC 27005 [Електронний ресурс] // Wikipedia. – Режим доступу: https://en.wikipedia.org/wiki/ISO/IEC_27005

17. ISO/IEC 27005:2022 – Information security, cybersecurity and privacy protection – Guidance on managing information security risks [Електронний ресурс] // International Organization for Standardization (ISO). – Режим доступу: https://www.iso.org/standard/43757.html

18. ISO/IEC 27017 [Електронний ресурс] // Wikipedia. – Режим доступу: https://en.wikipedia.org/wiki/ISO/IEC_27017

19. ISO/IEC 27018 [Електронний ресурс] // Wikipedia. – Режим доступу: https://en.wikipedia.org/wiki/ISO/IEC_27018

20. ISO/IEC 27701 [Електронний ресурс] // Wikipedia. – Режим доступу: https://en.wikipedia.org/wiki/ISO/IEC_27701

21. ISO/IEC 27701:2019 – Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines [Електронний ресурс] // International Organization for Standardization (ISO). – Режим доступу: https://www.iso.org/standard/71670.html

22. NIST CSWP 29 – The NIST Cybersecurity Framework (CSF) 2.0 [Електронний ресурс] // National Institute of Standards and Technology (NIST). – Режим доступу: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

23. Будапештська конвенція про кіберзлочинність [Електронний ресурс] // Чернівецький національний університет імені Юрія Федьковича. – Режим доступу: https://law.chnu.edu.ua/budapeshtska-konventsiia-pro-kiberzlochynnist/

24. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [Електронний ресурс] // EUR-Lex. – Режим доступу: https://eur-lex.europa.eu/eli/dir/2016/1148/oj/eng

25. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

[Електронний ресурс] // EUR-Lex. – Режим доступу: https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng

26. Tallinn Manual [Електронний ресурс] // NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). – Режим доступу: https://ccdcoe.org/research/tallinn-manual/

27. Tallinn Manual on the International Law Applicable to Cyber Warfare [Електронний ресурс] // Center for Ethics and the Rule of Law (CERL). – Режим доступу: https://www.penncerl.org/wp-content/uploads/2021/12/6481-tallinn-manual-on-the-international-law-applicable.pdf

28. Основні види опитування [Електронний ресурс] // Stud.com.ua. – Режим доступу: https://stud.com.ua/115517/marketing/osnovni_vidi_opituvannya

29. Методи опитувань [Електронний ресурс] // Stud.com.ua. – Режим доступу: https://stud.com.ua/19460/marketing/metodi_opituvan

30. Методи опитувань [Електронний ресурс] // Київський міжнародний інститут соціології (КМІС). – Режим доступу: https://kiis.com.ua/?lang=ukr__cat=methods__method=40

31. Групове інтерв'ю (фокус-групи) [Електронний ресурс] // Stud.com.ua. – Режим доступу: https://stud.com.ua/19465/marketing/grupove_intervyu_fokus_grupi

32. Лекція 11. Застосування методу контент-аналізу [Електронний ресурс] // Alexus.com.ua. – Режим доступу: https://alexus.com.ua/lekciya-11-zastosuvannya-metodu-kontent-analizu/

33. Контент-аналіз [Електронний ресурс] // Київський міжнародний інститут соціології (КМІС). – Режим доступу: https://kiis.com.ua/?lang=ukr&cat=content_analysis

34. Методи експериментальних досліджень [Електронний ресурс] : [навчальний матеріал] / Івано-Франківський нац. техн. ун-т нафти і газу. — Режим доступу: https://studfile.net/preview/10554145/

35. Сиротюк П. Що таке експериментальна психологія [Електронний ресурс] / Павло Сиротюк. — Режим доступу: https://psihologonline.pro/shcho-take-eksperymentalna-psykholohiya/

36. Скляр А. Використання Big Data у веб-аналітиці: як працювати з великими обсягами даних [Електронний ресурс] / Ангеліна Скляр. — 01.08.2024. — Режим доступу: https://blog.dropplatforma.com.ua/veb-analitika/vykorystannya-big-data-u-veb-analityczi-yak-praczyuvaty-z-velykymy-obsyagamy-danyh/

37. Mali P. Analysing the awareness of cyber crime and designing a relevant framework with respect to cyber warfare: an empirical study [Електронний ресурс] / Prashant Mali // *International Journal of Mechanical Engineering and Technology (IJMET)*. — 2018. — Vol. 9, No. 2. — С. 110–124. — Режим доступу: https://www.academia.edu/36080825

38. Snider K. L. G., Shandler R., Zandani S., Canetti D. Cyberattacks, cyber threats, and attitudes toward cybersecurity policies [Електронний ресурс] // *Journal of Cybersecurity*. — 2021. — Vol. 7, No. 1. — Article ID: tyab019. — Режим
доступу: https://academic.oup.com/cybersecurity/article/7/1/tyab019/6382745

39. Digmelashvili T. The Impact of Cyberwarfare on the National Security [Електронний ресурс] / Temur Digmelashvili // *Future Human Image*. — 2023. — Vol. 19. — Режим доступу: https://www.fhijournal.org/journals/2023/19/FHI19_Digmelashvili.pdf

40. #ШахрайГудбай: інформаційна кампанія з протидії фінансовому шахрайству [Електронний ресурс] / Національний банк України. — Режим доступу: https://promo.bank.gov.ua/stopfraud/

41. Ілвес Л. «Ми хочемо, щоб Естонія була не просто цифровою, а розумною державою» : інтерв'ю / Лукас Ілвес ; розмову вів Ярослав Жахалов // *DOU.ua* [Електронний ресурс]. — 2023. — Режим доступу: https://dou.ua/lenta/interviews/luukas-ilves-mriik/

42. Finland 2024 Digital Decade Country Report [Електронний ресурс] // *Shaping Europe's Digital Future*. — 2024. — Режим доступу: https://digital-strategy.ec.europa.eu/en/factpages/finland-2024-digital-decade-country-report

43. Centre for Strategic Communication and Information Security [Електронний ресурс] // *Wikipedia*. — Режим доступу: https://en.wikipedia.org/wiki/Centre_for_Strategic_Communication_and_Information_Security

44. Методичні рекомендації для регіональних медіа та місцевих органів влади [Електронний ресурс] / ГО «Вокс Україна», Центр протидії дезінформації при РНБО України. — 2024. — Режим доступу: https://voxukraine.org/wp-content/uploads/2024/08/Metodychni-rekomendatsii-dlya-regionalnyh-media-ta-mistsevyh-organiv-vlady-ICAP.pdf

45. About Us / StopFake.org [Електронний ресурс]. — Режим доступу: https://www.stopfake.org/en/about-us/

46. VoxCheck 2: боротьба з дезінформацією в Україні [Електронний ресурс] / VoxUkraine. — Режим доступу: https://voxukraine.org/ru/voks-chek-2

47. По той бік новин: незалежна інформаційна кампанія з медіаграмотності, фактчекінгу та розвитку критичного мислення [Електронний ресурс]. — Режим доступу: https://behindthenews.ua/

48. Історія створення та діяльність проєкту «Без Брехні» [Електронний ресурс]. — Режим доступу: https://without-lie.info/istoriia-stvorennia-ta-diial-nist-proe/

49. About EUvsDisinfo [Електронний ресурс] / EUvsDisinfo. — Режим доступу: https://euvsdisinfo.eu/about/

50. Nations Against Disinformation: міжнародна ініціатива протидії дезінформації [Електронний ресурс]. — Режим доступу: https://ua.nationsagainstdisinformation.org/

ДОДАТКИ

Додаток А

Опитування на тему «Кібервійна в очах громадськості: оцінка обізнаності, дезінформації та довіри»

1. Що, на вашу думку, є кібератакою? What do you think a cyberattack is?
   a) An attempt on computer or information systems aimed at causing harm, stealing data, or disrupting operations / Замах на комп'ютерні або інформаційні системи з метою завдати шкоди, викрасти дані або порушити роботу
   b) Receiving persistent promotional phone calls / Коли вам постійно телефонують із рекламними пропозиціями
   c) When your browser opens new tabs with ads automatically / Коли браузер автоматично відкриває нові вкладки з рекламою
   d) A rude or offensive comment on social media / Негативний чи образливий коментар у соцмережах
   e) Unexpected deletion of photos or files from your phone / Несподіване видалення фото або файлів із телефону
   f) When your computer starts making loud fan noises / Коли комп'ютер починає гудіти або шуміти голосніше зазвичай
   g) I don't know / Не знаю
2. Have you heard the term "cyberwarfare" before?/ Чи чули ви раніше термін "кібервійна"?
   a) Yes / Так
   b) No / Ні
   c) Not sure / Важко сказати
3. Do you consider cyberwarfare a real threat to national security? / Чи вважаєте ви кібервійну реальною загрозою національній безпеці?
   a) Yes / Так
   b) Partially / Частково
   c) No / Ні

d) Not sure / Не впевнений(-а)

4. Which of the following do you associate with cyberwarfare? / Що з наведеного ви вважаєте проявами кібервійни? (Choose all that apply / Оберіть усі, що підходять)
   a) Hacking government websites / Злам державних сайтів
   b) Spreading disinformation / Поширення дезінформації
   c) Infrastructure sabotage (e.g., electricity) / Саботаж інфраструктури (електроенергія тощо)
   d) Leaking personal data / Витік персональних даних
   e) I don't know / Не знаю
5. Where do you usually get information about cyberattacks? / Де ви зазвичай дізнаєтесь про кібератаки?
   a) Social media (Facebook, Instagram) / Соцмережі (Facebook, Instagram)
   b) Telegram / Telegram
   c) News websites / Новинні сайти
   d) Television / Телебачення
   e) Official government websites / Офіційні державні сайти
   f) Friends/family / Друзі, родина
6. How much do you trust these sources when it comes to cyber-related news? Наскільки ви довіряєте цим джерелам щодо кіберновин? (Rate from 1 – Not at all to 5 – Fully / Оцініть від 1 – зовсім не довіряю до 5 – повністю довіряю)
   a) Government sources / Державні джерела
   b) Local media / Місцеві ЗМІ
   c) International media / Міжнародні ЗМІ
   d) Telegram channels / Телеграм-канали
   e) Bloggers / Блогери
   f) Social media / Соцмережі
   g) Disinformation / Дезінформація

7. How often do you come across false or misleading information about cyberattacks? / Як часто ви зустрічаєте неправдиву або маніпулятивну інформацію про кібератаки?
   a) Very often / Дуже часто
   b) Often / Часто
   c) Sometimes / Іноді
   d) Rarely / Рідко
   e) Never / Ніколи
8. Have you ever accidentally shared false information about a cyberattack? / Чи траплялось вам випадково поширити фейкову інформацію про кібератаку?
   a) Yes / Так
   b) No / Ні
   c) I don't know / Не знаю
9. In your opinion, which country is the most active in spreading cyber disinformation? / На вашу думку, яка країна найбільше поширює кібердезінформацію?
   a) Russia / Росія
   b) China / Китай
   c) USA / США
   d) Other / Інша
   e) Not sure / Не впевнений(-а)
10. Do you use any of the following tools for personal cybersecurity? / Чи користуєтесь ви такими інструментами для особистої кібербезпеки? (Select all that apply / Оберіть усі, що підходять)
    a) Antivirus / Антивірус
    b) VPN
    c) Two-factor authentication / Двофакторна аутентифікація
    d) Strong passwords / Складні паролі
    e) None of the above / Нічого з наведеного

11. Have you ever received training or taken a course on cybersecurity or digital hygiene? / Чи проходили ви навчання або курс з кібербезпеки чи цифрової гігієни?
    a) Yes / Так
    b) No / Ні
    c) I don't remember / Не пам’ятаю
12. Do you know where to report a cyberattack or phishing attempt in your country? / Чи знаєте ви, куди повідомити про кібератаку або фішинг у своїй країні?
    a) Yes / Так
    b) No / Ні
13. Should governments invest more in cyber defense and cybersecurity education? / Чи повинні уряди більше інвестувати в кібероборону та освіту у сфері кібербезпеки?
    a) Yes / Так
    b) No / Ні
    c) Not sure / Не знаю
14. How effective is your country in responding to cyber threats? / Наскільки ефективно, на вашу думку, ваша країна реагує на кіберзагрози?
    a) Very effective / Дуже ефективно
    b) Somewhat effective / Частково ефективно
    c) Not effective / Не ефективно
    d) I don’t know / Не знаю
15. Do you believe cyberwarfare can influence political opinion and elections? / Чи вірите ви, що кібервійна може впливати на політичну думку та вибори?
    a) Yes / Так
    b) No / Ні
    c) Not sure / Не впевнений(-а)
16. Age / Вік

a) 18–29
b) 30–49
c) 50+

17. Gender / Стать:
    a) Male / Чоловіча
    b) Female / Жіноча
    c) Prefer not to say / Не хочу вказувати