МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ФАКУЛЬТЕТ СОЦІОЛОГІЇ ТА УПРАВЛІННЯ

КАФЕДРА СОЦІОЛОГІЇ

Кваліфікаційна робота
бакалавра

СОЦІОЛОГІЧНИЙ АНАЛІЗ КІБЕРЗЛОЧИННОСТІ В УМОВАХ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ

Виконала: студентка, IV курсу,
групи 6. 0540-смк
спеціальності 054 «Соціологія»
освітньої програми «Соціологія медіації і кримінології»
А.Р. Лобанова

Керівник: д.філос.н., професор,
професор кафедри соціології,
М.А. Лепський

Рецензент: к.філос.н., доцент,
доцент кафедри соціології,
І.О.Кудінов

Запоріжжя – 2024

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Соціології та управління
Кафедра Соціології
Рівень вищої освіти Бакалавр
Спеціальність 054 «Соціологія»
Освітня програма «Соціологія медіації і кримінології»

ЗАТВЕРДЖУЮ
Завідувач кафедри
В.О. Скворець _____
07 грудня 2023 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТЦІ

Лобановій Ангеліні Романівні

1. Тема роботи (проекту) Соціологічний аналіз кіберзлочинності в умовах російсько-української війни
Керівник роботи проф. к. соціології, проф., док. філос. н., Лепський М.А
Затверджені наказом ЗНУ від 18 січня 2024 року № 77-с
2. Строк подання студентом роботи 3 червня 2024 р.
3. Вихідні дані до роботи 1.Ларкін М. О., Артьомов Є. О. Кримінологія як окремий розділ соціології. *Часопис Академії адвокатури України*, 2015. Т. 8, № 3; 2.Бондаренко О.С., Рєпін Д.А. Кіберзлочинність в Україні: причини, ознаки та заходи протидії. *Електронне наукове видання «Порівняльно-аналітичне право»*, 2018. № 1. С. 246-248; 3.Павленко І.О. Світоглядні характеристики суб'єктів миру та війни. *Гуманітарний вісник ЗДІА*, 2015. № 60. С. 114; 4.Кононов І.Ф. Соціологія в умовах кризи і війни: проблема методологічної спроможності. *Вісник Луганського національного університету імені Тараса Шевченка: Соціологічні науки.* 2016. № 5 (302), травень. С. 5-54; 5. Гоблик В. В., Щербань Т. Прикладна соціологія: логістика і методи дослідження : навчальний посібник. Мукачево : РВВ МДУ, 2021. 108 с.
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):
1. Уточнити поняття «кіберзлочинність», «суспільство в умовах війни»; 2. Дослідити ґенезу соціологічного осмислення кіберзлочинності в умовах російсько-української війни; 3. Обґрутувати методологічні принципи та підходи дослідження кіберзлочинності в умовах російсько-української війни; 4. Проаналізувати інформаційний та кібернетичний вимір російсько-української війни; 5. Визначити зміст і форми кіберзлочинності в диджиталізованому суспільстві; 6. З'ясувати заходи безпеки кіберзлочинності в умовах російсько-української війни; 7. Обґрунтування соціологічного дослідження кіберзлочинності в умовах російсько-української війни; 8. Довести результати соціологічного дослідження кіберзлочинності в умовах російсько-української війни; 9. Визначити напрями вдосконалення боротьби з кіберзлочинністю в умовах російсько-української війни.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)
_____

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Розділ 1	професор кафедри соціології, професор, д.філос.н., Лепський М.А.	10.02.23	10.02.23
Розділ 2	професор кафедри соціології, професор, д.філос.н., Лепський М.А.	15.03.24	15.03.24
Розділ 3	професор кафедри соціології, професор, д.філос.н., Лепський М.А.	20.05.24	20.05.24

7. Дата видачі завдання 07 грудня 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Вибір та формулювання теми роботи	Листопад 2023	*виконано*
2.	Опрацювання наукових джерел	Грудень 2023	*виконано*
3.	Робота над вступом	Лютий 2024	*виконано*
4.	Робота над першим розділом	Лютий 2024	*виконано*
5.	Робота над другим розділом	Березень 2024	*виконано*
6.	Проведення соціологічного дослідження	Травень 2024	*виконано*
7.	Робота над третім розділом	Травень 2024	*виконано*
8.	Робота над висновками	Травень 2024	*виконано*

Студентка _____ А.Р. Лобанова

Керівник роботи (проекту) _____ М.А. Лепський

Нормоконтроль пройдено

Нормоконтролер _____ Т.О. Ратушна

РЕФЕРАТ

Дипломна робота: складається з 54 сторінок, 45 позицій у списку літератури, 2 додатків.

КІБЕРЗЛОЧИННІСТЬ, ВІЙНА, СУСПІЛЬСТВО

Мета наукового дослідження: визначення напрямів вдосконалення боротьби кіберзлочинності в російсько-української війни у соціологічному вимірі.

Об'єкт наукового дослідження: кібернетична організація суспільства в умовах російсько-української війни, кіберзлочинність, а також вплив війни на збільшення або зміну обсягу та характеру кіберзлочинності.

Предмет наукового дослідження: є напрями запобігання кіберзлочинності в диджиталізованому суспільстві в умовах російсько-української війни.

Методи наукового дослідження: контент-аналіз медіа ресурсів.

Гіпотеза дослідження: в умовах війни кіберзлочинність зростає, змінюя типи та мотивації, стає зброєю на тлі протистояння.

Висновки: 1. Дослідження підкреслює значне зростання кількості кіберзлочинів під час російсько-української війни, особливо кібератак, фінансових шахрайств, кібершпигунства та дезінформації, що вказує на використання кіберпростору як стратегічного інструменту у військовому конфлікті.

2. Контент-аналіз медійних джерел виявив зміну мотивацій кіберзлочинців, які під час війни частіше спрямовані на дестабілізацію суспільства, політичний вплив і військову стратегію, порівняно з довоєнним періодом, коли домінували фінансові мотиви.

3. Ефективна боротьба з кіберзлочинністю у військовому контексті потребує комплексного підходу, включаючи підвищення обізнаності громадськості, мобілізацію громадянського суспільства, міжнародну співпрацю та інтеграцію соціологічних підходів для розуміння соціокультурних аспектів проблеми.

SUMMARY

Diploma thesis consists of 54 pages, 45 literature sources,2 annex.

CYBERCRIME, WAR, SOCIETY

Research purpose is is the definition of directions for improving the fight against cybercrime in the Russian-Ukrainian war in the sociological dimension.

Research object is a cybernetic organization of society in the context of the Russian-Ukrainian war, cybercrime, as well as the impact of war on increasing or changing the volume and nature of cybercrime.

Research subject are the directions of preventing cybercrime in a digitalized society in the context of the Russian-Ukrainian war.

Research methods content analysis of media resources

Research hypothesis is in the conditions of war that cybercrime is growing, changing types and motivations, becoming a weapon against the background of confrontation.

Conclusions: 1. The study highlights a significant increase in the number of cybercrimes during the Russian-Ukrainian war, especially cyberattacks, financial fraud, cyberespionage and disinformation, which indicates the use of cyberspace as a strategic tool in military conflict.

2. Content analysis of media sources revealed a change in the motivations of cybercriminals, which during the war are more often aimed at destabilizing society, political influence and military strategy, compared to the pre-war period, when financial motives dominated.

3. An effective fight against cybercrime in a military context requires an integrated approach, including raising public awareness, mobilizing civil society, international cooperation and integrating sociological approaches to understand the socio-cultural aspects of the problem.

ЗМІСТ

ВСТУП

Актуальність дослідження. Останні роки характеризуються стрімким розвитком цифрових технологій, що призвело до збільшення загрози кіберзлочинності на всіх рівнях — від особистих до державних та корпоративних систем. Цей розвиток створює нові можливості для злочинців у кіберпросторі та потребує постійного оновлення захисних методів. Війна в Україні додатково підсилює цю загрозу, викликаючи не лише зростання кібератак, але й збільшення їх складності та обсягу. В умовах війни обидві сторони використовують кіберзброю для спроб маніпулювати інформацією, дестабілізувати противника та завдати шкоди його інфраструктурі. Тому ефективна кібербезпека стає надзвичайно важливою як для держави, так і для приватних суб'єктів, і вимагає постійного вдосконалення та удосконалення заходів захисту.

Аналіз кіберзлочинності дозволяє розкрити складні механізми її функціонування, виявити основні зразки та методи, що використовуються злочинцями. Це дозволяє розробляти більш ефективні заходи безпеки та протидії кіберзагрозам.

Актуальність соціологічного аналізу війни через кіберзлочинність полягає в тому, що кібератаки стають не тільки загрозою для безпеки державних і корпоративних систем, але і впливають на соціальну сферу, включаючи поведінку громадян, їхню довіру до влади, а також сприйняття конфлікту та взаємин між державами. Соціологічний аналіз дозволяє розкрити вплив кіберзлочинності на соціальні процеси, ідентифікувати фактори, що сприяють її поширенню, та розробляти стратегії протидії, які враховують специфіку сучасного конфлікту із застосуванням кіберзасобів.

Практичне значення соціологічного аналізу кіберзлочинності в контексті російсько-української війни полягає в тому, що він допомагає розуміти не лише технічні аспекти кібератак, але й їхні соціальні наслідки. Аналіз виявляє, як кіберзлочинність впливає на менталітет суспільства,

сприйняття війни та влади, а також на довіру громадян до технологій та мережі. Теоретичне значення полягає в розширенні розуміння сучасного конфлікту через призму кіберзасобів, що важливо для подальших досліджень у сфері політики, соціології та кібербезпеки. Розуміння динаміки кіберзлочинності у військовому контексті дозволяє розробляти ефективні стратегії протидії та захисту як на національному, так і на міжнародному рівні.

У сучасних умовах, коли технології стають необхідним інструментом ведення війни, кіберзлочинність набуває нових форм і методів впливу. Вона може включати в себе дезінформацію через соціальні мережі, кібершпигунство, кібератаки на критичну інфраструктуру та інші прояви.

Сьогодні кіберзлочинність для нашої держави є більш небезпечною, ніж колись. Під час війни кіберзлочинність набуває особливого значення і актуальності через свою здатність до ефективного впливу на військові, стратегічні та громадські процеси. Кібертероризм, або використання кіберзасобів для терористичних дій та загроз національній безпеці, стає серйозним засобом атаки. Це може включати кібератаки, масове поширення дезінформації та маніпуляцію громадською думкою з метою створення паніки та хаосу за чим ми щодня можемо спостірігати на просторах соціальних мереж.

Кібератаки, в свою чергу, можуть бути спрямовані на знищення або паралізацію військових систем, комунікаційних мереж, критично важливих об'єктів та інфраструктури. Це може значно ускладнити ведення військових операцій та завдати серйозної шкоди обороноздатності країни. Найвідомішою за останій час є атака на мережу зв’язку Київстар, через яку зник з’язок та інтернет цієї мережи яка у свою чергу налічує 24 мільйони абонентів. Це викликало збої у всьому обладнанні яке використовувало цю мережу.

Кібершпигунство, як збирання конфіденційної інформації та розвідувальні дії через кіберзасоби, також має велике значення під час війни. Це може включати отримання розвідувальної інформації про військові плани,

стратегії та дії противника, що дозволяє здійснювати оборонні дії та приймати ефективні рішення на полі бою.

Всі ці елементи кіберзлочинності невід'ємно поєднанні в контексті цього конфлікту, а зокрема російсько-української кібервійни. З початком повномасштабного вторгнення актуальність цього феномену лише зростає, в контексті війни, кіберзлочинність може бути інструментом гібридної війни, що стає особливо актуальним у сучасних конфліктах, де інформаційна та технологічна складові стають ключовими аспектами боротьби.

Проблемна ситуація. Соціологічне дослідження кіберзлочинності в умовах війни розкриває динаміку цього явища та його соціальні наслідки для різних соціальних груп. Воно також спрямоване на пошук ефективних методів контролю та запобігання кіберзагрозам. Це дослідження допомагає підвищити увагу до кібербезпеки як ключового компонента національної безпеки та міжнародних відносин. Соціологічний аналіз кіберзлочинності дозволяє розуміти соціокультурні та психологічні аспекти цього явища, виявляти мотивації та умови, що сприяють виникненню кіберзлочинних вчинків в умовах війни. А отже, дослідження кіберзлочинності з соціологічної перспективи в контексті російсько-української війни є важливим для розуміння сучасних викликів безпеки та вироблення стратегій захисту суспільства від кіберагресій.

Після початку повномасштабного вторгнення Росії в Україну спостерігається значне збільшення кількості злочинів у кіберпросторі, зокрема таких, що спрямовані на руйнування критичної інфраструктури та дестабілізацію суспільства. Це зростання пов'язане з еволюцією мотивацій кіберзлочинців, які, поряд із традиційними цілями фінансової вигоди, дедалі частіше використовують кіберпростір як засіб для досягнення політичних та військових цілей, спрямованих на підрив стабільності та безпеки держави.

Стан наукової розробленості проблеми. За даними аналізу фахової літератури, наразі існує значна кількість досліджень, які досліджують різні аспекти кіберзлочинності у різних галузях науки. Ця тема актуальна як для

українських дослідників так й для зарубіжних. Але в свою чергу серед соціологів ця тема є новою та на етапі вивчення. Соціологами що вивчають конкретні соціологічні аспекти кіберзлочинності є М. Єнін , Г. Коржов [1]., О. Данильян, О.Дзьобань [2]., М. Ларкін[3]. та інші.

Об'єктом дослідження є кібернетична організація суспільства в умовах російсько-української війни, кіберзлочинність, а також вплив війни на збільшення або зміну обсягу та характеру кіберзлочинності. Розглядаються мотивації та стратегії кіберзлочинців, їхній вплив на суспільство та можливі наслідки для кібербезпеки та міждержавних відносин. Дослідження також охоплює реакцію суспільства, урядів та міжнародних організацій на кіберзлочинність в умовах воєнного конфлікту, спрямовану на забезпечення стабільності та безпеки в кіберпросторі.

Предметом дослідження є напрями запобігання кіберзлочинності в диджиталізованому суспільстві в умовах російсько-української війни.

Метою даного дослідження є визначення напрямів вдосконалення боротьби кіберзлочинності в російсько-української війни у соціологічному вимірі.

Наукові завдання цього дослідження для досягнення мети роботи полягають у такому:

- уточнити поняття «кіберзлочинність», «суспільство в умовах війни»;

- дослідити ґенезу соціологічного осмислення кіберзлочинності в умовах російсько-української війни;

- обґрунтувати методологічні принципи та підходи дослідження кіберзлочинності в умовах російсько-української війни.

- проаналізувати інформаційний та кібернетичний вимір російсько-української війни;

- визначити зміст і форми кіберзлочинності в диджиталізованому суспільстві;

- з’ясувати заходи безпеки кіберзлочинності в умовах російсько-української війни;

- обґрунтувати соціологічного дослідження кіберзлочинності в умовах російсько-української війни;

- довести результати соціологічного дослідження кіберзлочинності в умовах російсько-української війни;

- визначити напрями вдосконалення боротьби з кіберзлочинністю в умовах російсько-української війни.

Основною гіпотезою роботи є припущення про те, умови віни змінюють природу кіберзлочинності, а самеобсяг та характер.

Основна гіпотеза роботи уточнюється у двох *допоміжних гіпотезах:*

1. Природа кіберзлочинності демонструє зміщення об’єкта злочину з фінансового та спрямованого на окремі організації та особистості на цілісність держави та основних інституцій.
2. Кіберзлочинність в умовах війни набуває характеру частину комплексу гібрідної війни.

Методи дослідження. Під час написання дипломної роботи я використовувала принципи об’єктивності, розвитку, ціннісного підходу, загального зв’язку, системний, структурно-функціональний та комунікативний підходи в соціології середнього рівня соціології комунікацій, у прикладному дослідженні застосовано контент-аналіз. Зокрема, я використовувала цей метод для аналізу змісту статей, документів, або інших наукових джерел інформації, що стосуються теми. Це дозволило мені систематично оцінити та класифікувати інформацію з певних аспектів, що було важливим для розуміння тенденцій та виявлення ключових патернів у цій сфері.

Структура роботи. Робота складається з вступу, трьох розділів, висновків, списку використаних джерел, а також додатків.

РОЗДІЛ 1
МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ КІБЕРЗЛОЧИННОСТІ В УМОВАХ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ

1.1. Уточнення основних понять «кіберзлочинність», «війна»

Закон України визначає кіберзлочин (комп'ютерний злочин) як діяння, яке відбувається у кіберпросторі або з його використанням і є суспільно небезпечним та винним. Відповідальність за такі дії передбачена законодавством України про кримінальну відповідальність або визнана злочином за міжнародними договорами України. Таким чином, кіберзлочинність представляє собою сукупність різних кіберзлочинів.

Термін «кіберзлочин» виник у результаті поєднання двох понять: «кіберпростір» і «злочин». «Кіберпростір» визначається як інформаційний простір, що створюється за допомогою комп'ютера, де діють програми та обробляються дані. У світовій науковій літературі часто використовується термін «віртуальний простір» або «віртуальний світ». Автор використовує термін «кіберзлочин» не як юридичну категорію, а як ознаку соціального та технічного проявів відносин людей за посередництвом комп’ютерної техніки.

Далі, термін «кіберзлочини» використовується як синонім до «транснаціональних комп'ютерних злочинів» чи «злочинів, вчинених через мережу Інтернет». Під «кіберзлочинами» розуміється мотивована атака з використанням мережі Інтернет на інформацію у комп'ютерних системах, програмах чи даних, що здійснюється окремою особою або групою. Це явище має суспільну небезпеку для стабільності України, її політичної та економічної систем, прав і свобод громадян [4].

Кіберзлочинність, як розглядається М. Кравцовим та Г. Чернишовим, є соціально-правовим явищем, що охоплює заборонену законом кримінальну діяльність частини населення. Ця діяльність включає в себе використання електронно-обчислювальних машин, телекомунікаційних систем, комп’ютерних мереж і мереж електрозв'язку. Конкретно, це означає систему

злочинів, які вчиняються в кіберпросторі з використанням або проти комп'ютерних даних, мереж або систем, а також інших телекомунікаційних мереж, включаючи Інтернет та технології мобільного зв'язку [5, с.17].

Кіберзлочинність, за М. Кравцовою та іншими авторами, має ряд ознак, які визначають її характер. Перш за все, кіберзлочини визначаються як ті кримінальні правопорушення, які законодавець об'єднав у Розділі XVI Особливої частини Кримінального кодексу. Це відокремлює їх від інших видів злочинів і визначає їхню приналежність до кіберзлочинності. Друга ознака полягає в тому, що кіберзлочини вчиняються з використанням електронно-обчислювальних машин, телекомунікаційних систем, комп'ютерних мереж і мереж електрозв'язку. Це є ключовою характеристикою, яка відокремлює ці злочини від інших видів правопорушень. Крім того, кіберзлочини можуть мати комп'ютерну інформацію як предметом або знаряддям вчинення. Це означає, що комп'ютер може бути або об'єктом злочину, або знаряддям, або способом його вчинення. Кіберпростір виступає як середовище, предмет і спосіб вчинення кіберзлочинів, що підкреслює їхню специфіку та унікальність серед інших видів правопорушень [5, с. 19-20].

Визначення кіберзлочинності визначається метою використання цього терміну. Основною характеристикою кіберзлочинності є обмежене число дій, спрямованих на порушення конфіденційності, цілісності та доступності комп'ютерних даних або систем. Ці дії мають на меті отримання особистого або фінансового прибутку, завдання особистої або фінансової шкоди. Крім того, кіберзлочинність може включати злочинні дії, що пов'язані з використанням персональних даних [6].

К. Тарасюк визначає «кіберзлочини» як суспільно-небезпечні діяння, пов'язані з кіберпростором і комп'ютерною інформацією, що обробляється комп'ютерами. Ці діяння характеризуються високою прихованістю, складністю виявлення та розслідування, а також складністю доказування їх у суді. Вони часто мають транснаціональний характер і в основному

відбуваються через інформаційну мережу Інтернет. Навіть одиничні кримінальні правопорушення можуть призводити до великих збитків [7].

На сьогоднішній день широко використовується класифікація кіберзлочинів на дві категорії: агресивні та неагресивні. До першої групи відносяться такі види кіберзлочинів: кібертероризм, загрози фізичної розправи, кіберпереслідування, кібersталкінг (включаючи протиправне сексуальне домагання через Інтернет), а також діяльність з дитячою порнографією (створення, розповсюдження та отримання доступу до порнографічних матеріалів з участю дітей). Друга група включає в себе: кіберкрадіжку, кібервандалізм, кібершахрайство, кібершпигунство, розсилання спаму та вірусних програм [8, с.332].

При розгляді кіберзлочинності в умовах війни необхідно розглянути такі ключові поняття як кібертероризм, кібершпигунство, кібератаки та кібервійна.

Згідно законодавства, кібертероризм – це терористична діяльність, що здійснюється у кіберпросторі або з його використанням.

Сергій Гнатюк в своїй роботі: «Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи». приводить 25 визначень кібертероризму, з яких виводить твердження про те що це «різновид тероризму, що полягає у свідомому та цілеспрямованому застосуванні ресурсів інформаційних систем для реалізації терористичних дій у кіберпросторі, а також для досягнення інших суміжних цілей в інтересах терористичних угруповань.» Також він відокремлює невід’ємне за структурою кібертероризму поняття – кібератака. «реалізація у КбП (кіберпросторі) загроз безпеці його компонентів (а саме загроз порушення конфіденційності, цілісності та доступності) з урахуванням їх уразливостей.» [9].

В свою чергу відповідно до закону про основні принципи забезпечення кібербезпеки України, кібератака – це навмисні дії в інтернеті, що робляться за допомогою різних електронних засобів (як комп'ютерні програми, інші технології) з метою порушення безпеки, отримання несанкціонованого доступу до інформації або завдає шкоди електронним системам та ресурсам.

Що до «кібершпигунства», згідно з Кримінальним кодексом України, воно полягає в передачі або збиранні з метою передачі іноземній державі, іноземній організації або їх представникам інформації, яка є державною таємницею, якщо це робить іноземець або особа без громадянства. Основним об'єктом шпигунства, включаючи кібершпигунство, є зовнішня безпека України, її суверенітет, територіальна цілісність, обороноздатність, а також державна, економічна та інформаційна безпека [10].

Усе це використовується як невід'ємна зброя під час ведення кібервійни, зокрема Росії проти України. Відповідно до своїх попередників термін «кібервійна» складається з двох ключових понять «кіберпростір» та «війна», як й в попередніх випадках конкретного та чіткого визначення цих термінів немає. Термін «кібервійна» є дискусійним і метафоричним. Використання терміну «кібервійна» вказує на нові форми протистояння між впливовими учасниками міжнародних відносин за допомогою інформаційних технологій [11]. Й відповідно до цього визначаємо що кібервійна – це війна, яка ведеться у кіберпросторі. Багато людей вже чули про такі терміни, як гібридна війна, сіткоцентрична війна та інформаційна війна. У даному випадку кібервійна входить у кожен з цих видів війни [11].

Разом з тим, метафорічність «кібервійни» зникає під час реальної російсько-української війни, у якій кіберскладова – кібервійна є важливою частиною бойових дій та уражень. У цьому контексті кіберпростір перетворюється на ще одне поле бою, де відбуваються стратегічні атаки, спрямовані на порушення критичної інфраструктури, розвідку та дезінформацію. Кібероперації доповнюють традиційні воєнні дії, створюючи нові виклики для захисників та змушуючи переглядати концепції безпеки та оборони.

Дослідники С. Матвієнків та Н. Головчинський виявили, що різні джерела надають різні, але цікаві визначення поняття «війна», які в основному мають подібний та схожий зміст. Наприклад, тлумачний словник української мови розглядає війну як організовану збройну боротьбу між державами,

народами або збройними угрупованнями всередині країни. У політологічному енциклопедичному словнику війна тлумачиться як збройна боротьба між державами або соціальними, етнічними та іншими спільнотами, а також як засіб боротьби за світову гегемонію та захист національних інтересів. Оксфордський політичний словник розглядає війну як збройний конфлікт між двома або більшою кількістю сторін, який зазвичай відбувається для досягнення політичних цілей. У політологічному довіднику війну визначають як соціальне явище, одну з форм розв'язання суспільно-політичних, економічних, ідеологічних, національних, релігійних, територіальних та інших протиріч за допомогою насильницьких засобів. Війна розглядається як найгостріша форма розв'язання протиріч на різних рівнях. Воєнно-теоретичне розуміння визнає війну як продовження політики за допомогою засобів збройного насильства для досягнення різних цілей [12].

Розглядаючи російсько-українську кібервійну не можна оминути термін «гібридна війна», через який вона у переважній більшості досліджень і розглядається.

Гібридна війна, за визначеннями експертів, є складною ситуацією, що об'єднує різні форми ведення бойових дій і включає такі аспекти, як традиційна бойова діяльність, неконвенційні методи, тероризм та підривні дії. Основними характеристиками гібридної війни є використання різних видів збройних формувань, зокрема недержавних акторів, для проведення бойових операцій, що можуть бути незаконними або поза рамками міжнародних конвенцій.

У контексті гібридної війни, важливою є також інформаційна складова, яка включає в себе боротьбу за розум і душі людей через різні засоби масової комунікації, такі як ЗМІ, телебачення, Інтернет та інші канали. Ця боротьба за інформаційний простір має великий вплив на розвиток подій під час конфлікту, адже вона спрямована на формування громадської думки і підтримки певної сторони конфлікту [13].

Зауважемо, що війна, яка сьогодні часто описується як гібридна та кібернетична, також приймає форму інформаційної. Я. Малик зазначає, що концепцію «інформаційна війна» вперше ввів у науковий обіг американський дослідник М. Маклюен, який стверджував, що справжня тотальна війна полягає у протистоянні за допомогою інформації. Він вбачав, що наша епоха характеризується зростанням значення обміну знаннями над обміном товарами, а засоби масової комунікації виступають як нові «природні ресурси», які збагачують суспільство. Отже, боротьба за капітал і простори для збуту поступається місцем боротьби за доступ до інформаційних ресурсів і знань. Це призводить до того, що війни переважно відбуваються у сфері інформаційного простору та з використанням інформаційних видів озброєнь [14].

У противагу «киберзлочинності» виступає «кібербезпека» – це захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [15]. Тобто основа для протидії кіберзлочинності та створення теоретичних засад для її запобігання.

Одже, у подальшому ми будемо використовувати основні поняття роботи «кіберзлочин» та «війна» у таких визначеннях:

«кіберзлочин» – це поняття, що позначає протиправну діяльність, здійснювану в цифровому середовищі з використанням комп'ютерних систем, мереж та інтернету,

«війна» – це поняття, яке відображає складний і багатогранний феномен, що включає в себе організовану збройну боротьбу, соціальні, політичні, економічні, ідеологічні, національні, релігійні та територіальні протиріччя, вирішувані насильницькими методами.

1.2. Генеза соціологічного осмислення кіберзлочинності в умовах російсько-української війни.

У цьому параграфі ми розглядаємо зародження та подальший процес соціологічного осмислення кіберзлочинності в умовах російсько-української війни.

Звернемося до соціологічного осмислення, розвитку та вивчення соціологами кіберзлочинності в контексті війни, зокрема, в рамках подій, пов'язаних із російсько-українською війною. Такий підхід дозволить глибше розібратися у взаємозв'язку між кіберзлочинністю та воєнною діяльністю, з'ясувати, як ці явища впливають одне на одного та які соціальні наслідки можуть виникнути внаслідок таких процесів. Дослідження цієї теми допоможе розкрити основні тенденції у сучасному світі, де кіберзлочинність та війна нерозривно пов'язані із загальними соціальними процесами та викликами.

Явище війни є відомим з найдавніших часів і досі. Воєнні конфлікти, які виникали з різних причин - від територіальних чи релігійних до економічних та політичних, завжди привертали увагу для вивчення різними галузями науки. Історики досліджували воєнні події, спрямовуючи увагу на причини та наслідки війни, роль військових стратегій та технологій у воєнних діях. Політологи аналізували воєнно-політичні відносини між державами та їхніми союзниками, вивчали міжнародні правові аспекти воєнних конфліктів. Соціологи зосереджувались на соціальних наслідках війни для суспільства, вивчаючи її вплив на соціальні структури, цінності та поведінку людей.

У стародавні часи соціологічним вивченням війни займалися вчені та філософи, такі як Демокріт, Геродот, Платон та Арістотель. У своїх філософських працях «Держава», «Закони», «Федон», та «Тімей» Платон (427-347 рр. е.) приділяв значну увагу темі війни. Філософ розглядав війну як постійну складову життя людського суспільства, вважаючи, що «протягом життя йде безперервна війна з усіма державами». Для нього мир був лише пустим словом, але насправді не існуючим. Платон вважав, що причини війни

знаходяться в людській природі, її тілесних пристрастях, жадобі до багатства та задоволення.

Погляд соціолога на війну зазвичай розглядається через призму соціальних динамік, структур та процесів. Соціологи досліджують, як війна впливає на соціальні групи, інституції, культурні практики та сприйняття. Вони також аналізують роль масових медіа, політичних лідерів та ідеологій у формуванні підтримки або опозиції до війни в суспільстві.

Одним з перших, хто розкривав війну з соціологічної перспективи, був Е. Дюркгейм. У своїх роботах, таких як «Самогубства» (1897) та «Правила соціологічного методу» (1895), він досліджував соціальні фактори, що впливають на війни та конфлікти у суспільстві. Е. Дюркгейм вважав, що соціальні нерівності, релігійні та моральні питання, а також відчуття групової ідентичності можуть бути основою для виникнення конфліктів та війн. Його роботи стали важливим внеском у розвиток соціології конфліктів та війни.

Ще одним, визначним соціологом що зробив значний внесок у соціологічне вивчення війни є П. Сорокін, вперше визначивши методологію її дослідження. Це дало можливість об'єктивно оцінювати місце війни у суспільних відносинах і проводити порівняльний аналіз воєн. Він розглядав феномен війни поза рамками ідеологічних тлумачень і історичних контекстів кожного конфлікту окремо.П. Сорокін вводив критерії, які мали загальне значення для будь-якого суспільства, незалежно від політичних режимів, ідеологій чи міждержавних відносин. Серед таких критеріїв він вказував на абсолютні та відносні параметри, такі як розміри армій та їхнє співвідношення з населенням держав, кількість жертв війн та кількість збройних конфліктів, що мали місце протягом століть. У своєму великому дослідженні «Соціальна та культурна динаміка», П. Сорокін досліджував велику кількість війн і внутрішніх конфліктів, вивчаючи закономірності їхньої динаміки та вплив на суспільство. Він спрямовувався на вирішення питань про закономірності розвитку воєн, їхній вплив на суспільство з плином часу, агресивність держав та їхні взаємовідносини, співвідношення війни і миру в історії країн, а також

періодизацію західної культури. Для цього він розробив систему об'єктивних індикаторів, які дозволили провести аналіз на основі фактів і даних, уникнувши суб'єктивних оцінок, характерних для багатьох історичних і соціологічних досліджень [16].

Сьогодні вивченням війни, зокрема російсько-української, займаються більшість соціологів країни та світу: М. Требін [16]., І. Павленко[17]., М. Лепський [18]., І. Кононов[19]., Я. Пилипенко[20]. та інш.

Узагальнюючи історичні аспекти появи комп'ютерних злочинів, можна виділити такі події:

1. Кінець 70-х років – пограбування «Секьюріті пасифік банк» на суму 10,2 млн доларів.
2. 1979 р. – викрадення коштів у Вільнюсі на суму 78584 крб.
3. 1984 р. – поява першого комп'ютерного вірусу в світі.
4. 1985 р. – взлом електронної системи голосування в конгресі США за допомогою вірусу.
5. 1986 - 1988 р. – СРСР з'явився перший комп'ютерний вірус.
6. 1989 р. – американський студент заблокував 6000 комп'ютерів Пентагону.
7. 1990 р. – міжнародний з'їзд комп'ютерних «піратів» у Голландії з демонстрацією здатності необмеженого втручання в системи комп'ютерів.
8. 1991 р. – розкраданням коштів у Зовнішекономбанку на суму 125,5 тис. доларів [21, с. 133].

Один із прикладів кіберзлочинності в Україні – це кібератака на енергетичну інфраструктуру. Наприклад, у грудні 2015 року сталася серія кібератак, що спрямовувалися на електроенергетичні підприємства в Західній Україні, що призвело до відключення електропостачання для тисяч споживачів. Ця атака, відома як «BlackEnergy», була спрямована на порушення роботи систем керування та управління енергосистемами. Вона стала однією з перші кібератаки на критичну інфраструктуру та підкреслював загрозу кібербезпеці у сучасному світі.

Кіберзлочинність – це дуже молоде поняття порівняно з війною, і серед соціологів воно тільки починає вивчатися, завдяки чому зберігає свою актуальність. На мою думку, в контексті соціології кіберзлочинність розглядає аспекти взаємодії суспільства з цифровим простором, вплив кіберзлочинності на соціальні структури та взаємовідносини між людьми, а також її вплив на формування нових норм та цінностей в сучасному світі.

Ми важаємо, що досліджуючи феномену кіберзлочинності, ми повинні звертати увагу на кілька важливих аспектів. По-перше, вивчити соціальні та культурні контексти, які сприяють виникненню кіберзлочинності, включаючи фактори, що стимулюють індивідів або групи до вчинення кібератак тощо. Далі, важливо проаналізувати соціальні наслідки кіберзлочинності, такі як порушення довіри у суспільстві, втрата конфіденційності та загроза кібербезпеці. Також важливо розглянути роль соціальних мереж та медіа в поширенні інформації про кібератаки та їх вплив на громадську думку та поведінку. Нарешті, соціолог мусить дослідити соціальні наслідки заходів по боротьбі з кіберзлочинністю, включаючи законодавчі і технічні заходи, і їх вплив на суспільство та індивідуальні права та свободи.

Українська соціологія, на відмінну від загального вивчення кіберзлочинності, більш активно зосереджується на феномені кібервійни, що представляє собою унікальне поєднання кіберзлочинності та війни, або навіть може бути розглянута як новий етапом еволюції ведення війни. Зокрема, у зв'язку з війною Росії проти України, виникає необхідність аналізувати та розуміти вплив кібератак, інформаційної пропаганди та кібершпигунства на військові, політичні, економічні та соціальні процеси в країні.

1.3. Методологічні принципи та підходи дослідження кіберзлочинності в умовах російсько-української війни

Соціологічне дослідження кіберзлочинності в умовах російсько-української війни базується на ряді методологічних принципів та підходів, які враховують специфіку цього явища та його взаємозв'язок з воєнним

конфліктом. По-перше, у цьому підрозділі ми розглянемо, використання інтердисциплінарного підходу, оскільки кіберзлочинність включає в себе не лише технічні, але й соціальні аспекти. Соціологи співпрацюють з фахівцями з інформаційної безпеки, політичних вченими та іншими галузями для глибшого розуміння явища. Другим важливим принципом є контекстуалізація дослідження, що передбачає аналіз кіберзлочинності в контексті геополітичних, культурних та соціально-економічних реалій конфлікту між Росією та Україною. Крім того, використання як кількісних, так і якісних методів дослідження дозволяє отримати різноманітні дані про кіберзлочинність, включаючи статистичні дані, аналіз текстів, інтерв'ю з експертами та учасниками, історичний аналіз тощо. Ці підходи дозволяють соціологам отримати глибше розуміння природи та наслідків кіберзлочинності в умовах конфлікту, що допомагає розробляти ефективні стратегії протидії та зміцнення кібербезпеки в суспільстві.

У цьому дослідженні вже зараз ми спостерігаємо вияв інтердисциплінарного підходу, в нашому випадку він полягає у поєднанні соціології, та кримінологічної діяльності. Цей підхід допомагає нам розуміти соціальні контексти, структури та процеси, що можуть спричиняти виникнення кримінальної активності в мережі Інтернет, а також впливати на формування криміногенного середовища в кіберпросторі. З іншого боку, кримінологічний підхід надає нам засоби для аналізу злочинної поведінки, механізмів її виникнення та протидії. Поєднання цих двох підходів дозволяє нам отримати комплексне уявлення про причини, динаміку та наслідки кіберкримінальної активності в суспільстві, а також розробляти ефективні стратегії протидії та змінювати умови, які сприяють виникненню злочинності. Такий підхід дозволяє нам глибше розуміти складні соціальні проблеми та розвивати більш ефективні методи їх вирішення.

Контекстуалізація соціологічного дослідження кіберзлочинності в умовах війни передбачає розглядання кібератак у широкому соціально-політичному контексті конфлікту. Війна, особливо гібридна, зумовлює не

лише фізичні бойові дії, але й використання кіберпростору як інструменту для досягнення військових, політичних та інформаційних цілей. У такому контексті, соціологічне дослідження кіберзлочинності має за мету розкриття специфіки та особливостей таких атак у рамках військових конфліктів. Це означає аналіз мотивів та стратегій суб'єктів конфлікту, розуміння соціальних наслідків кібератак для цільового суспільства, а також вивчення взаємодії між кіберзлочинністю та іншими аспектами війни, такими як інформаційна війна, гібридна війна та політична маніпуляція. Контекстуалізація дослідження допомагає врахувати унікальні виклики та можливості, які виникають в умовах військового конфлікту, та сприяє розробці ефективних стратегій протидії та захисту від кіберзагроз.

Класифікація методів дослідження в гуманітарних науках базується на принципі якості та кількості, і включає три основні типи методології: кількісну, якісну та змішану. Кількісна методологія, часто відома як позитивістська, використовує кількісні дані для вивчення і аналізу соціальних явищ, наприклад, опитування, анкетування, статистичний аналіз. Якісна методологія, відома як інтерпретаційна, спрямована на розуміння глибинних аспектів соціальної реальності, використовуючи методи, такі як спостереження, інтерв'ю, фокус-групи. Змішана методологія поєднує якісні та кількісні підходи для отримання більш повного та комплексного розуміння досліджуваних явищ. Наприклад, дослідження кіберзлочинності в умовах війни може включати аналіз статистичних даних про кібератаки (кількісний підхід), а також глибинне інтерв'ю з експертами зі збройних сил або кібербезпеки (якісний підхід), щоб зрозуміти мотивації та стратегії злочинців [22].

В. Марков розробив методологічну схему аналізу кіберзлочинності, яка включає кроки зі збору та систематизації даних, встановлення причинно-наслідкових зв'язків, аналізу показників та побудови моделей на основі характеристик тенденцій. Цей підхід ускладнює виявлення факторів, що впливають на кіберзлочинність, та потребує перегляду кримінологічної

оцінки, але дозволяє краще контролювати зв'язки між різними видами кіберзлочинності та виробляти ефективні заходи її протидії [23].

Під час написання цієї роботи ми застосовували низку принципів і підходів, щоб забезпечити високий рівень наукової об'єктивності та всебічного аналізу досліджуваної теми. По-перше, ми керувалися принципом об’єктивності, що дозволило нам зберігати нейтральність і неупередженість у висновках, базуючись на достовірних даних та наукових фактах. Принцип розвитку допоміг нам враховувати динамічні зміни та еволюцію соціальних явищ у контексті досліджуваної теми. Ціннісний підхід дав можливість аналізувати соціальні явища через призму суспільних цінностей та їх впливу на поведінку людей.

Також ми використовувала принцип загального зв’язку, який підкреслює взаємозалежність і взаємозв’язок соціальних явищ і процесів, що сприяло глибшому розумінню складних соціальних систем. Системний підхід дозволив нам розглядати об'єкт дослідження як цілісну систему, що складається з взаємопов'язаних елементів, а структурно-функціональний підхід допоміг виявити роль і функції кожного з цих елементів у межах системи.

У межах соціології середнього рівня і соціології комунікацій, ми застосовували комунікативний підхід, що акцентує увагу на процесах обміну інформацією і взаємодії між індивідами та групами. Це дозволило нам краще зрозуміти механізми соціальної комунікації та їх вплив на суспільство.

В прикладному аспекті цього дослідження ми застосували метод контент-аналізу. Це якісний і кількісний метод дослідження текстової інформації, що дозволив мені аналізувати зміст і структуру комунікативних повідомлень, виявляти основні теми, тенденції та патерни в обговорюваних соціальних явищах. Завдяки цьому ми змогли глибше зрозуміти соціальні процеси та явища, що були предметом цього дослідження, і зробити обґрунтовані висновки та рекомендації [24].

Отже, у цьому розділі ми зосередилися на розгляді ключових понять нашого дослідження, включаючи «кіберзлочинність», «війна», «гібридна війна» та «кібербезпека» та інші. Провели аналіз генези цього питання, звернувшись до історичного контексту, щоб краще зрозуміти, як кіберзлочинність стала неодмінною складовою військових конфліктів. Виявлення зв'язків між цими поняттями виявилося ключовим для нашого розуміння сутності проблеми. осмислили методологічні принципи, які використовуються для вивчення кіберзлочинності в умовах війни. Виявлення зв'язків між цими поняттями допомогло нам уточнити нашу концептуальну базу та розкрити сутність проблеми кіберзлочинності в умовах війни. Це відкриває шлях до більш глибокого аналізу та розуміння впливу кібератак на військові операції та стратегічні процеси.

Отже, цей розділ надав нам теоретичну та методологічну основу для подальшого дослідження кіберзлочинності в умовах війни, що важливо для розробки ефективних стратегій захисту національної та міжнародної кібербезпеки.

Відтак ми вже визначили що кіберзлочин — це незаконні дії, що здійснюються за допомогою комп’ютерних систем, мереж або пристроїв, з метою отримання несанкціонованого доступу до інформації, її зміни, знищення або поширення. Війна — це збройний конфлікт між державами або великими соціальними групами з використанням військової сили, що супроводжується значними втратами та руйнуваннями. Стан соціологічного етапу дослідження кіберзлочинності під час російсько-української війни на сьогоднішній день перебуває на початковій стадії вивчення. Ця проблема є новою для соціології, що обумовлює потребу в більш глибокому аналізі і дослідженні. У дипломній роботі як поблема розглядається саме стан та кіберзлочинності в умовах російсько-української війни.

Основні принципи, що застосовувалися у роботі, включають принципи об’єктивності, розвитку, ціннісного підходу, загального зв’язку. Принцип об’єктивності забезпечує неупереджене та точне висвітлення фактів і подій.

Принцип розвитку враховує динамічність та еволюцію явищ і процесів. Ціннісний підхід підкреслює важливість моральних та етичних аспектів. Принцип загального зв’язку показує взаємозалежність соціальних явищ і процесів.

Методологічними підходами нашої роботи є системний, структурно-функціональний та комунікативний підходи.

Системний підхід дозволяє розглядати кіберзлочинність як частину більшої соціальної системи. Структурно-функціональний підхід аналізує роль і функції окремих елементів у системі кіберзлочинності. Комунікативний підхід вивчає взаємодію між різними соціальними суб’єктами та інформаційними потоками.

У наступному ж розділі ми детально розглянемо теоретичні аспекти кіберзлочинності в умовах російсько-української війни, включаючи інформаційний та кібернетичний вимір конфлікту, зміст і форми кіберзлочинності в диджиталізованому суспільстві, а також заходи безпеки проти кіберзлочинності в умовах цього збройного протистояння.

РОЗДІЛ 2
ТЕОРЕТИЧНІ АСПЕКТИ ДОСЛІДЖЕННЯ КІБЕРЗЛОЧИННОСТІ В УМОВАХ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ

2.1. Інформаційний та кібернетичний вимір російсько-української війни.

Російсько-українська війна почалася ще після анексії Російською Федерацією Криму у 2014 році та початку збройного конфлікту на сході України, що призвело до руйнування соціальних структур, економічного стресу, масової міграції, втрат життів та травматизації населення, змінюючи українське суспільство, а також формуючи новий контекст військових дій, де використовуються сучасні технології, інформаційна війна та нестандартні методи бойових дій.

Початок повномасштабного вторгнення Російської Федерації спричинив різкі соціальні реакції як на внутрішньому, так і на міжнародному рівні. У внутрішньому контексті суспільство переживало шок і обурення перед ворожнечею, що загрожувала їхній безпеці та стабільності. Відбулися масові протести, активізувалися громадські рухи та партії, які вимагали реакції влади та підтримки від міжнародних партнерів. Медіа відігравали ключову роль у формуванні громадської думки, розкриваючи факти вторгнення та його наслідки.

Мирові лідери реагували різнопланово: засудження, введення санкцій, вимоги до Росії відступити від агресії. Міжнародні організації викликали до дії згуртованість та спільні зусилля у забезпеченні міжнародної безпеки та регіональної стабільності. Політичні дипломатичні зусилля були спрямовані на пошук мирного розв’язання конфлікту, у той час як військові стратегії передбачали відповідь на вторгнення та захист суверенітету та територіальної цілісності. Цей критичний момент став випробуванням для міжнародної співпраці та міжнародного порядку, а його наслідки продовжують впливати на геополітичну ситуацію у світі.

Війна має складну структуру, яка може включати різні складові, такі як військові операції, економічний тиск, інформаційна пропаганда, психологічний вплив і т. п. Структура війни може змінюватися в залежності від контексту і стратегії сторін конфлікту [22]. У контексті кіберпростору, особливо цікавою для нас є структура гібридної війни.

Характерною рисою гібридної війни є використання інформаційної зброї, що поєднується з сучасними технологіями для створення мережевих та мережоцентричних війн. Мережева війна здійснюється шляхом використання інформаційних переваг та організаційних здібностей, а не простою числовою або вогневою перевагою [25].

Російсько-українська війна має як інформаційний, так і кібервимір. Інформаційна війна передбачає поширення пропаганди та дезінформації з метою впливу на громадську думку та маніпулювання сприйняттям. З іншого боку, кібервимір, який включає кібератаки на критичну інфраструктуру, урядові системи та мережі зв’язку. У той самий час, російська пропаганда активно використовує соціальні мережі та засоби масової інформації для поширення дезінформації та маніпулювання громадською думкою. Що може вплинути на уявлення суспільства про конфлікт і його учасників.

О. Данильян та О. Дзьобань визначають проблему вірного сприйняття інформації, яка стає особливо актуальною для будь-якого суспільства на етапі інформаційної еволюції. Відбір найважливішої інформації, її правильне подання та тлумачення – важливі завдання для медіапростору, що може використовуватися для маніпулювання масовими переконаннями. Україна, зокрема, зіткнулася з інтенсивним інформаційним тиском з боку Росії ще до початку активних бойових дій. Цей інформаційний штурм зазнавав постійних модифікацій та підсилення з часом [2]. Як правильно відзначає І. Фещенко, ця війна, з одного боку, може здатися простою й примітивною, але з іншого боку, вона була довго планована, розроблена і успішно втілена [26]. Ми погоджуємося з думкою І. Фещенко, оскільки з одного боку, термін «інформаційна війна» вже відомий і розповсюджений, і може здатися простим

і примітивним для сприйняття. Проте, занурюючись у цю тему, стає очевидним, що вона дійсно вимагає довгого планування, розробки та вдалої реалізації. Аналізуючи складність та різноманітність методів, стратегій та технологій, використовуваних у такій війні, ми розуміємо, наскільки вона може бути великим викликом для національної та міжнародної безпеки.

Пропаганда – це один з ключових структурних елементів інформаційної війни. Вона використовується для поширення спеціально підготовленої інформації з метою впливу на громадську думку, формування певних переконань та підтримки конкретного порядку денного. Пропаганда може бути використана як військовими, так і невійськовими суб'єктами конфлікту з метою досягнення їхніх цілей.

Розділення суспільства за різними ідентичностями, зниження морально-вольової складової, спотворення світогляду та метасмислів, намагання збільшити протистояння між громадянським суспільством і державною владою, військово-політичним керівництвом та військовими, можуть мати серйозні наслідки для суспільства. Ці явища можуть виявлятися через інформаційно-психологічну складову, яка має на меті погіршити якість життя населення, впливати на громадську думку та суспільну свідомість.

Інформаційно-психологічні операції (ІПсО) стали необхідною частиною всіх сучасних воєнних дій. Проведення ІПсО перед самою боротьбою стало звичайною практикою. Інформаційно-психологічну операцію слід розглядати як систему узгоджених та взаємопов'язаних за метою, завданнями, об'єктами і часом інформаційних акцій, атак і заходів, що проводяться одночасно або послідовно за єдиними замислом і планом для вирішення завдань ІПсО на цільову аудиторію [27].

ІПсО тісно пов'язані з кіберпростором та кіберзлочинністю під час Російсько-української війни. Ця війна виявила, як критично важливою може бути інформаційна аспект у сучасних конфліктах, де кібератаки та маніпулювання інформацією стали невід'ємною частиною стратегії ведення війни. ІПсО використовується для маніпулювання суспільною думкою,

дезінформації, створення фейкових новин та інших методів, які мають на меті психологічно впливати на ворога та місцеве населення. Такий підхід до інформаційно-психологічних операцій дозволяє використовувати кіберпростір як ефективний інструмент в веденні сучасних воєнних конфліктів.

Фейки, які є однією з частин інформаційно-психологічних операцій (ІПсО), сприяють утворенню негативного іміджу осіб, інституцій чи організацій. В сучасному інфопросторі, де існує велика кількість повідомлень і швидке оновлення інформації, фейкова інформація може легко поширюватись і впливати на суспільство. Ці фейки можуть містити маніпулятивну інформацію, що ставить за мету підривати репутацію та спричиняти негативні емоції у громадськості. Такі операції здебільшого проводяться анонімно чи через використання вигаданих експертів та джерел, що ускладнює їх ідентифікацію та нейтралізацію. Громадські організації та владні структури в Україні активно працюють над виявленням та боротьбою із фейками, аналізуючи технології їх створення та механізми їх поширення для забезпечення інформаційної безпеки суспільства [28].

Під час вторгнення в Україну, Росія активно використовує фейки та маніпуляції з метою спотворення світогляду громадян. Наприклад, ще під час анексії Криму та подій на сході України, російські ЗМІ та пропагандистські ресурси активно поширювали дезінформацію про події, змальовуючи українську владу як агресивну та несправедливу, а російську інтервенцію як захист від «фашистів» і «українських націоналістів». Ця тактика не змінилась і сьогодні. Це сприяло збільшенню протистояння між громадянським суспільством та державною владою, створюючи напругу та конфліктність.

Також, російська інформаційно-психологічна складова використовується для маніпуляції військово-політичним керівництвом та військовими, створюючи штучні кризи та загострення для виправдання агресивних дій та розширення впливу в регіоні. Ще у листопаді 2023 року Українська влада стикнулася зі спробами російської дезінформації,

спрямованої на розпалення конфлікту між військовими та українською владою. Російські пропагандисти розповсюджували фейкові новини про внутрішній конфлікт між Президентом Зеленським та Головнокомандувачем Збройних сил Залужним. Їхні маніпуляції включали поширення фейкових відео та інсайдерських новин про звільнення Залужного, що призводило до напруження відносин та негативного ставлення громадськості до української влади. Така дезінформація мала на меті створити образ розбрату в українських військах та послабити довіру до уряду.

Російська пропаганда вже давно стала легендарною своєю одночасною геніальністю та безглуздістю до абсурду. Навіть після 2014 року вона активно переконувала українців у нашій второсортності та стирала культурні межі. Після повномасштабного вторгнення не раз дивувала нас «біолабораторіями».

Дані соціологічного дослідження, проведеного компанією «Active Group» 2 липня 2023 року, показують, що майже 60% українців спостерігають російську пропаганду в Інтернеті. За цим дослідженням, 18,5% респондентів стверджують, що бачать російську пропаганду дуже часто, а 40,4% – час від часу. Щодо спроб передавати правдиву інформацію про війну російським користувачам Інтернету, лише 16,8% опитаних роблять це постійно, а 22,7% – час від часу. Більшість респондентів (26,7%) навіть не намагаються доносити правду росіянам.

2.2. Зміст і форми кіберзлочинності в диджиталізованому суспільстві.

Давайте дослідимо, який зміст та конкретні форми кіберзлочинності найбільш поширені серед користувачів інтернету. Розгляд цієї теми окремо дозволить відобразити, як розвиток технологій впливає на злочинність в онлайн просторі та як соціум адаптується до цього явища.

Росія проводить постійні кібернетичні операції проти об’єктів критичної інфраструктури, приватного сектору і інформаційно-телекомунікаційних систем Збройних Сил України. Ці атаки включають:

1. Атаки, які завдають репутаційних втрат, але не завдають фізичної шкоди.

2. Розсилка спаму та фейкових новин для маніпулювання громадською думкою.

3. Ламання приватних сторінок або серверів для отримання конфіденційної інформації.

4. Атаки з метою порушення функціонування сайтів або комп'ютерних систем.

5. Атаки, що можуть призвести до відключення або помилок у роботі систем.

Для захисту мереж потрібно інвестувати в кібербезпеку та розвивати правила та стандарти для захисту у кіберпросторі. Тільки так можна протистояти кіберним загрозам і дефективним намірам дестабілізувати суспільство [29]. Виходячи з усього цього, Росія займається кібертероризмом, використовуючи цифрові технології як ефективний інструмент для розповсюдження хаосу та дестабілізації ситуації не лише в Україні, але й на власній території

Атаки на телефонні та інтернет мережі, а також сайти офіційних державних органів та банків, які набувають масштабів, подібних до атаки на Монобанк 21 січня, сприяють погіршенню якості життя населення через перерви у роботі цифрових сервісів та виток конфіденційної інформації, що порушує довіру громадян до цифрових технологій та впливає на їхню соціальну свідомість через ризик втрати особистих даних та фінансових збитків, що в свою чергу підірвує електоральні процеси в інших країнах через можливий втручання та маніпуляції у цифровому просторі, надаючи приклад технологічного впливу на суспільний розвиток та зміну соціальних уявлень.

Наприклад, за повідомленням Держспецзв'язку від 28 серпня 2023 року, в Україні зафіксували новий випадок хакерської атаки на органи юстиції та нотаріату. Хакери використовують електронні листи зі шкідливою програмою AsyncRAT, що надсилаються із вкладеннями у формі BZIP, GZIP чи RAR-

архівів. Відкриття таких файлів призводить до зараження комп'ютера шкідливою програмою, що надає віддалений доступ до пристрою.

Кіберполіція у своїх соціальних мережах повідомила про результати своєї діяльності у 2023 році: вони виявили понад 3600 кіберзлочинів. Понад 1700 осіб отримали підозру за більш ніж 3700 злочинів завдяки оперативному супроводу кіберполіції, що на 59% перевищує показники минулого року. Матеріали щодо 42 організованих злочинних груп, включаючи 7 злочинних організацій, було направлено до суду, що на 83% більше, ніж у 2022 році.

В 2023 році, у своєму коментарі для платформи United24 начальник Департаменту кібербезпеки СБУ Ілля Вітюк заявив про систематичні спроби ворога вплинути на інформаційний простір України. Одним із засобів цього впливу є використання ботоферм, які активно поширюють проросійські наративи в Інтернеті. За словами Вітюка, з моменту початку повномасштабного вторгнення Росії, СБУ вже заблокувала 76 таких ботоферм, які налічують понад 3 мільйони акаунтів.

У кіберпросторі розподіл праці відбувається у формі спеціалізованих функцій, де різні групи осіб виконують певні завдання залежно від їхніх навичок та цілей. Це включає хакерів, які здійснюють несанкціонований доступ до систем, фішерів, що використовують соціальні інженерні методи для отримання конфіденційної інформації, та кіберзлочинців-вірусологів, які створюють та розповсюджують шкідливе програмне забезпечення. Паралельно існують кіберзлочинці-шахраї, які використовують шахрайські схеми для обману користувачів, а також кіберзлочинці-ексторшеністи, які вимагають викуп за допомогою кібератак. Розподіл праці у кіберпросторі може бути детермінований не лише технічними здібностями, але й мотивацією та цілями, що стимулюють ці дії.

У контексті війни, кібершахрайство стає надзвичайно актуальною проблемою. Спільнота великих інформаційних потоків та неперевіреної інформації, що характерна для воєнного часу, створює сприятливі умови для кібершахраїв. Вони використовують цей хаос для викрадення конфіденційної

інформації, шахрайства та інших злочинних дій. Таке шахрайство може значно ускладнити вже складну ситуацію під час війни та створити додаткові виклики для суспільства і влади.

Результати масштабного опитування Національного банку та платформи відкритих даних Опендатабот вказують на те, що кожен дев'ятий українець став жертвою шахраїв з початку повномасштабного вторгнення. За цей період активність кібершахраїв в Україні значно зросла, і злочинці адаптували свої схеми до складної ситуації в країні, використовуючи фальшиві обіцянки фінансової допомоги від імені держави, міжнародних та благодійних організацій. Особливо часто молодь (вік 18-24 років) та люди пенсійного віку (65+) потрапляли під атаки шахраїв. Найбільш поширені способи обману включають покупку/продаж товарів в інтернеті (52,74%), фішингові посилання (18,57%), злом соцмереж (12,04%) та виманювання інформації телефоном (10,18%). Під час війни шахраї використовують тривогу та вразливість громадян, а найчастіше втрати коштів відбуваються через розголошення особистих даних, таких як номери карток чи паролі для інтернет-банкінгу.

2.3. Заходи безпеки кіберзлочинності в умовах російсько-української війни

Для того, щоб запобігти усьому, що було наведено у попередніх параграфах, країни активно розробляють засоби протидії кіберзлочинності. Це включає в себе створення та вдосконалення кібербезпекових стратегій, розвиток спеціалізованих кіберзахисних підрозділів та агентств, впровадження технологічних рішень для виявлення та блокування кібератак, а також підвищення кіберграмотності серед населення та бізнесу. Ці заходи спрямовані на забезпечення безпеки інформаційних систем, захисту приватності та персональних даних громадян, а також уникнення серйозних наслідків для соціальних, економічних та політичних сфер життя країн.

У своїй дисертації дослідниця Н. Козак пропонує комплекс заходів для виявлення слідів кібератак та їх протидії. Першим заходом є контроль цілісності програм, файлів даних та інших інформаційних ресурсів, які підлягають захисту. Другий захід включає аналіз діяльності користувачів і процесів, а також мережного трафіку в комп'ютерній мережі, над якою здійснюється контроль. Третій захід передбачає контроль фізичних форм нападу на елементи інформаційної системи, зокрема на відчужувані джерела збереження інформації. І нарешті, четвертий захід включає аналіз дій адміністраторів з перевірки попередніх інцидентів [30].

У 1994 році в Україні були здійснені перші кроки у напрямку протидії кіберзлочинам. Тоді до Кримінального кодексу 1960 року були внесені зміни, які стали основою для статті 198-1 «Порушення роботи автоматизованих систем». Ця стаття передбачала кримінальну відповідальність за умисне втручання у роботу автоматизованих систем, що призводило до перекручення або знищення інформації, розповсюдження програмних і технічних засобів для незаконного проникнення до систем і здатних спричинити шкоду.

У жовтні 2015 року, за підставою норм закону про ратифікацію Конвенції про кіберзлочинність, було утворено Управління по боротьбі з кіберзлочинністю в Міністерстві внутрішніх справ України, яке пізніше було перетворено на Департамент кіберполіції Національної поліції України. Кримінальний кодекс України містить розділ XVI, що стосується правопорушень у сфері цифрових технологій, таких як несанкціоноване втручання в роботу комп'ютерів та мереж, створення та розповсюдження шкідливих програм, порушення правил експлуатації комп'ютерів тощо. Кібербезпека полягає у захисті користувачів від кіберзагроз та в діяльності, спрямованій на захист цифрових систем від кримінальних правопорушень [31].

З початку війни в Україні кібербезпека країни стала предметом серйозної загрози через активність російських кіберзлочинців, які атакують державні установи, приватні компанії та громадян. Уряд України вживає

рішучих заходів для підвищення кібербезпеки, включаючи прийняття Закону No 2149-IX, що збільшує відповідальність за кіберзлочини, та Закону No 2137-IX, який спрощує процедуру розслідування таких злочинів. Мета цих ініціатив - зробити кіберпростір України безпечнішим і покарати злочинців, що намагаються завдати шкоди країні.

Професор кафедри протидії злочинності Харківського національного університету, Світлана Лучік, разом з курсантом 4 курсу, Русланом Папуцею, звертають увагу на те, що в українському кіберпросторі діє ціла ІТ-армія, яка об'єднує фахівців зі всього світу. Ця армія щодня відбиває кібератаки та успішно контрнаступає. За 9 місяців війни вона атакувала понад 13 тисяч російських онлайн-ресурсів, зокрема сайти групи Вагнера, порталу Госуслуги та офіційний сайт ворога. Крім того, було відбито понад 1300 кібератак з боку Росії. Така діяльність дозволила державним та урядовим установам, а також банкам продовжити нормальну роботу. Крім ІТ-армії, активну роль у кіберпросторі відіграє відома хакерська група Anonymous, яка, зокрема, зламала сайт ФСБ Росії та отримала доступ до значної кількості даних [32].

Контроль інформації та цинзура теж може використовуватись як захід кібербеспеки. КМІС, у липні 2022 року провело опитування, в якому задавалося питання про необхідність більш активного контролю держави над інформацією в Інтернеті. У лютому 2024 року це ж питання було повторено соціологами з метою вивчення зміни настроїв серед українців.

Більшість українців, а саме 60%, згодні були з тим, що держава повинна активніше контролювати інформацію в інтернеті для зміцнення захисту від ворога. Проте 30% вважали це обмеженням прав і свобод. До лютого 2024 року ситуація змінилася: 49% - вважають це спробою активнішого контролю держави обмеженням прав і свобод, а лише 44%.

Щодо використання Телеграм-каналів, лише 43% серед користувачів згодні з активнішим контролем, 46% вважають це обмеженням прав і свобод. Це свідчить про загальне зниження довіри громадян до дій влади.

Такі зміни настроїв можуть вплинути на кібербезпеку, особливо в умовах війни з Росією, тому що можуть виникнути перешкоди для ефективного контролю та реагування на кіберзагрози. Подібна ситуація спостерігалася у попередні роки після заборони російських соціальних мереж, коли більшість українців не довіряли владі та сприймали це як політичний інструмент. Такі зміни настроїв важливо враховувати при прийнятті рішень та комунікації з громадськістю для забезпечення довіри та підтримки громадян.

Ми, як соціологи, у свою чергу можемо запропонувати комплексний підхід до проблеми. Починаючи з аналізу соціального профілю кіберзлочинців та їх мотивацій, ми можемо розробити ефективні стратегії запобігання злочинності в соціумі. Це може включати в себе проведення анкетування та інтерв'ювання фахівців у галузі кібербезпеки, щоб зрозуміти основні загрози та вразливості, а також виявити потенційні точки входу для кіберзлочинців. Крім того, розвиток соціології кіберзлочинності може допомогти у створенні більш дієвих та адаптивних стратегій безпеки, заснованих на вивченні поведінки та менталітету кіберзлочинців. Це може включати в себе вдосконалення методів виявлення та аналізу кіберзлочинності, розробку соціально-педагогічних програм для підвищення кібербезпеки в суспільстві, а також співпрацю з правоохоронними органами та іншими зацікавленими сторонами для ефективної реалізації цих стратегій.

Таким чином у цьому розділі ми визначили інформаційний та кібернетичний виміри російсько-української війни, яка почалася з анексії Криму у 2014 році. Як цей конфлікт змінив українське суспільство, зруйнувавши соціальні структури та викликавши масову міграцію, втрату життів і травматизацію населення. Початок повномасштабного вторгнення у 2022 році спричинив різкі соціальні реакції та масові протести, медіа відіграли ключову роль у формуванні громадської думки. Ця війна має гібридний характер, використовуючи інформаційну зброю та кібератаки на критичну інфраструктуру для створення мережевих війн. Інформаційна війна включає пропаганду та дезінформацію для маніпулювання громадською думкою, в той

час як кібератаки спрямовані на урядові системи та мережі зв'язку. Пропаганда та інформаційно-психологічні операції (ІПсО) використовуються для створення негативного іміджу, маніпулювання суспільною думкою та погіршення якості життя населення.

Ми визначили, що в диджиталізованому суспільстві спостерігається зростання кіберзлочинності, особливо в контексті кібернетичних операцій Росії проти України. Ми розглядали різні форми цієї злочинності, такі як атаки на приватні дані, фейкові новини, спам, ламання сторінок та атаки на комп'ютерні системи. Масштаби цих атак вже призвели до серйозних наслідків, таких як виток конфіденційної інформації та відключення важливих мереж та сервісів. Ми також з'ясували, що захист від кіберзлочинності вимагає великих інвестицій у кібербезпеку та розвитку правил і стандартів для кіберпростору, щоб забезпечити безпеку мереж і захистити суспільство від кіберзагрозю.

Ми вже дослідили основні аспекти заходів безпеки кіберзлочинності в умовах російсько-української війни, включаючи розробку кібербезпекових стратегій, створення спеціалізованих кіберзахисних підрозділів, використання технологічних рішень для виявлення та блокування кібератак, підвищення кіберграмотності, і розвиток правової бази для боротьби з кіберзлочинами. Проаналізували існуючи кейси

Далі, перейдемо до третього, практичного розділу, де будуть наведені результати емпіричного дослідження, яке Це буде спрямоване на аналіз типів кіберзлочинів, основних мотивацій кіберзлочинців, їхніх методів діяльності та впливу на суспільство. Такий підхід дозволить нам отримати глибше розуміння проблеми кіберзлочинності в контексті війни та розробити більш ефективні стратегії протидії цьому явищу, що враховуватимуть не лише технічні аспекти, а й соціально-психологічні чинники, що визначають поведінку кіберзлочинців та їхні мотивації.

РОЗДІЛ 3
ЕМПІРИЧНЕ ДОСЛІДЖЕННЯ КІБЕРЗЛОЧИННОСТІ В УМОВАХ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ

3.1. Обґрунтування соціологічного дослідження кіберзлочинності в умовах російсько-української війни

В історії війн часто відзначається, що вони сприяють значним змінам у суспільстві, зокрема у розвитку технологій та еволюції форм злочинності. Російсько-українська війна не є винятком, особливо коли мова йде про кіберзлочинність. Це дослідження має на меті не лише виявлення та аналіз основних тенденцій у цьому контексті, але й розкриття різноманітності типів кіберзлочинів, їх виконавців та цілей в умовах військового конфлікту.

Кіберзлочинність у контексті війни виявляється в низці проявів, включаючи кібератаки на державні структури, критичну інфраструктуру, комунікаційні мережі та громадянське суспільство загалом. Це може бути виражене в різних формах: від кібершахрайства та кібершпигунства до впливових кібератак на ключові системи.

Основним завданням нашого дослідження є ретельний аналіз цих явищ для розуміння їхнього впливу на суспільство та розвиток кібербезпеки. Важливо виявити основні мотивації злочинців, такі як політична дестабілізація, економічні вигоди або просто хакерська активність, а також розкрити специфічні цілі кожного типу кіберзлочину. Дослідження також спрямоване на ідентифікацію патернів у злочинності під час війни, що може вказати на стратегії та тенденції у використанні кіберпростору для військових цілей.

Такий глибокий аналіз є важливим для розробки ефективних стратегій захисту, які враховують специфіку кіберзлочинності під час війни та забезпечують адекватний відповідь на ці виклики. Це дослідження також може мати значний внесок у зростання усвідомленості про кібербезпеку серед

суспільства та урядових структур, що є важливим кроком у підвищенні загального рівня захисту від кіберзагроз у воєнний час.

Головне завдання цього дослідження полягає в аналізі змін у кількості та типах кіберзлочинів, які сталися до та після повномасштабного вторгнення Росії в Україну. Цей період має особливе значення, оскільки він включає в себе період підготовки до конфлікту, саме вторгнення та його наслідки, які відобразилися на кіберзлочинності.

Війна не тільки призводить до змін у політичній та економічній сферах, але має істотний вплив і на соціальний аспект життя суспільства. Аналіз кіберзлочинності у контексті війни дозволить виявити найбільш поширені види кіберзлочинів, щоб розробити ефективні стратегії їх протидії та залучити до цього процесу всіх зацікавлених учасників суспільства. Це дослідження має на меті звернути увагу на проблему кіберзлочинності в умовах війни та мотивувати соціологів приділити цій проблемі більше уваги, враховуючи її новизну як напрямку дослідження в соціології.

Розуміння змін у кіберзлочинності дозволяє розробити більш ефективні стратегії захисту та реагування, враховуючи збільшення кількості кібератак на державні структури, що може вказувати на потребу у посиленні кібербезпеки в цих сферах. Такий аналіз також допомагає виявити тенденції та патерни, які можуть бути використані для прогнозування майбутніх атак та розробки превентивних заходів. Розуміння мотивацій злочинців, таких як збагачення, нанесення шкоди інфраструктурі, дестабілізація країни, дозволяє краще розуміти їхні цілі та ризики для різних сфер суспільства. Врахування залучення іноземних змі у кіберзлочинність може вказувати на міжнародні аспекти кібератак та необхідність співпраці з іншими країнами у сфері кібербезпеки. Знання про типи жертв, таких як громадяни, держустанови, компанії, дозволяє спрямувати заходи захисту на найбільш вразливі групи та об'єкти.

Проведення контент-аналізу новин є обґрунтованим та важливим методом для мого дослідження. Перш за все, цей метод дозволяє об'єктивно

оцінити кількісні та якісні зміни в злочинності, враховуючи різні аспекти кіберзлочинності, такі як типи атак, об'єкти впливу, мотивації злочинців та їх методи. Крім того, аналіз новин дозволяє виявити можливі тенденції та зв'язки між конфліктом та кіберзлочинністю, що сприятиме у формулюванні обґрунтованих висновків.

Використання контент-аналізу також важливе з точки зору систематизації та структурування великої кількості інформації з різних джерел новин, що дозволяє отримати повніше та об'єктивніше уявлення про зміни в кіберзлочинності під час війни. Крім того, цей метод дозволяє побудувати аналітичні моделі та виявити складні взаємозв'язки, які можуть залишитися непоміченими в інших методах дослідження.

3.2. Результати соціологічного дослідження кіберзлочинності в умовах російсько-української війни

У цій роботі представлені результати дослідження, яке базується на контент-аналізі новинної онлайн платформи «ФАКТИ»(fakty.com.ua) за період з червня 2020 року по лютий 2022 року та з березня 2022 року до сьогодні. У ході аналізу було вивчено 180 повідомлень про кіберзлочини. Для кодування даних ми використали такі категорії, як тип злочину, злочинець, мотивація та жертва. Платформа «ФАКТИ» була обрана через її високу популярність та репутацію надійного джерела новин, що дозволяє отримати достовірну та актуальну інформацію про кіберзлочини в Україні.

Перед початком повномасштабного вторгнення було зафіксовано загалом 61 випадок кіберзлочинів. Ці випадки можна розділити на три типи: кібершахрайство (26 випадків), кібератаки (4 випадки) та розповсюдження незаконного контенту (виготовлення та розповсюдження порнографії) (36 випадків).

2. Виконавець злочину:

- Один злочинець: 8 випадків
- Один хакер: 18 випадків

- Група хакерів: 13 випадків
- Злочинне угруповування: 22 випадки

3. Мотивація злочину:

- Збагачення: 57 випадків
- Нанесення шкоди пристрою: 4 випадки

4. Жертва:

- Громадяни України: 55 випадків
- Іноземці: 2 випадки
- Держустанови: 4 випадки

Загальна картина показує, що більшість злочинів були вчинені окремими злочинцями або групами хакерів, які мали різні мотивації. Основний мотив - збагачення. Щодо жертв, найбільше постраждали громадяни України, що вказує на внутрішній характер цих кіберзлочинів, а також національну спрямованість дій злочинців. Нанесення шкоди пристрою є менш поширеним мотивом, що може свідчити про те, що більшість злочинів спрямовані на отримання матеріальної вигоди, а не на специфічне завдання шкоди технічним засобам.

Після початку повномоштабного вторгнення дінаміка змінилась. Зафіксовано наступні дані щодо типів кіберзлочинів, їх виконавців, мотивації та жертв:

1. Тип кіберзлочину:
   - Кібершахрайство: 13 випадків
   - Кібератаки: 38 випадків
   - Незаконний контент: 21 випадок
   - Розповсюдження фейків: 47 випадків
   - Загалом: 119 випадків
2. Виконавець злочину:
   - Один злочинець: 11 випадків
   - Один хакер: 43 випадки
   - Група хакерів: 12 випадків

- Злочинне угруповування: 15 випадків
- Іноземні змі: 38 випадків

3. Мотивація злочину:

- Збагачення: 33 випадки
- Нанесення шкоди пристрою: 9 випадків
- Нанесення шкоди інфраструктурі: 27 випадків
- Дестабілізація країни: 50 випадків

4. Жертва злочину:

- Громадяни України: 101 випадок
- Іноземці: 2 випадки
- Держустанови: 11 випадків
- Компанії: 5 випадків

Порівнюючи дані, можна зробити кілька висновків:

1. Загальна кількість кіберзлочинів:

- Перед вторгненням: 61 випадок
- Після вторгнення: 119 випадків Зафіксовано помітне збільшення кількості кіберзлочинів після початку повномасштабного вторгнення, що свідчить про інтенсифікацію кібератак та злочинної активності в цілому.

2. Типи кіберзлочинів:

- Кібершахрайство: зменшення з 26 до 13 випадків
- Кібератаки: зростання з 4 до 38 випадків
- Незаконний контент: зростання з 36 до 21 випадку
- Розповсюдження фейків: зростання з 0 до 47 випадків Після вторгнення найбільше зростання зафіксовано в категоріях кібератак та розповсюдження фейків, що може вказувати на активну інформаційну та технічну війну.

3. Виконавці злочину та їх мотивація:

- Один злочинець: збільшення з 8 до 11 випадків
- Один хакер: збільшення з 18 до 43 випадків
- Група хакерів: збільшення з 13 до 12 випадків

- Злочинне угруповування: збільшення з 22 до 15 випадків
- Іноземні змі: збільшення з 0 до 38 випадків Після вторгнення помітно збільшення кількості злочинів, вчинених окремими хакерами та іноземними змі, що може свідчити про залучення зовнішніх сил у кібератаки на країну.

4. Жертви злочину:

- Громадяни України: збільшення з 55 до 101 випадку
- Іноземці: збільшення з 2 до 2 випадків
- Держустанови: збільшення з 4 до 11 випадків
- Компанії: зростання з 0 до 5 випадків Після вторгнення найбільше збільшення зафіксовано у категорії громадян України, що може свідчити про зростання загрози для національної кібербезпеки та інфраструктури країни.

Загальна динаміка після вторгнення показує інтенсивне зростання кіберзлочинів, залучення іноземних хакерів та злочинців, а також збільшення активності в розповсюдженні фейків та кібератаках на різноманітні сфери українського суспільства.

3.3. Напрями вдосконалення боротьби з кіберзлочинністю в умовах російсько-української війни

Умови війни створюють нові виклики і загрози в сфері кіберзлочинності, що вимагає перегляду підходів до її протидії. У цьому розділі ми пропонуємо розглянути напрями вдосконалення стратегій боротьби з кіберзлочинністю в контексті російсько-української війни, звертаючи увагу на те, що соціологічний підхід може допомогти зрозуміти соціальні та культурні виміри цієї проблеми та врахувати їх у розробці ефективних заходів протидії.

Участь громадськості в боротьбі з кіберзлочинністю в умовах війни відіграє ключову роль у формуванні ефективної стратегії протидії цим загрозам. Перш за все, необхідно підвищити рівень обізнаності серед громадян щодо можливих кіберзагроз та способів їх уникнення. Це може бути здійснено

шляхом проведення освітніх кампаній, воркшопів та тренінгів, на яких люди отримають необхідні знання та навички для захисту своєї кібербезпеки.

Крім того, мобілізація суспільства у цьому питанні передбачає активну участь громадських організацій та соціальних активістів у співпраці з владними структурами. Наприклад, організації можуть створювати інформаційні ресурси, які будуть надавати консультації з кібербезпеки, розповсюджувати інформацію про актуальні загрози та надавати підтримку постраждалим від кібератак.

Крім того, важливо залучати молодь до цієї проблеми, оскільки вони часто володіють високим рівнем технічної грамотності та можуть бути ключовими учасниками у створенні нових інноваційних рішень для захисту від кіберзагроз.

Наприклад, проект «Інтернет безпечний для всіх» може організувати вебінари та круглі столи з експертами у галузі кібербезпеки для різних груп населення. Соціальні мережі також можуть бути ефективним засобом мобілізації громадськості, де розповсюджуватимуться корисні поради та інформація про небезпечні ситуації в кіберпросторі. Соціально-культурний аналіз у контексті кіберзлочинності включає в себе не лише виявлення соціокультурних чинників, що впливають на поширення цих злочинів серед різних соціальних груп, а й розуміння їхнього впливу на здатність суспільства в цілому адаптуватися та реагувати на ці виклики. Наприклад, дослідження може виявити, що підлітки з певних соціальних середовищ, де переважає низький рівень освіти та доступу до інформації, є більш схильні до використання кіберзлочинності через бажання вираження своєї соціальної позиції чи отримання матеріальної вигоди. Таке розуміння дозволить розробляти спеціальні програми та ініціативи з профілактики кіберзлочинності серед молоді, які б були ефективними та прийнятними для даної соціокультурної групи.

Додатково, соціокультурний аналіз може виявити особливості у сприйнятті кіберзлочинності в різних культурних середовищах. Наприклад, в

деяких культурах певні види кіберзлочинності можуть бути більш прийнятними або несприйнятними з певних моральних або етичних поглядів. Розуміння цих особливостей допоможе адаптувати стратегії боротьби з кіберзлочинністю до конкретного культурного контексту та зберегти ефективність заходів у міжкультурному спілкуванні та співпраці.

Таким чином, соціально-культурний аналіз не лише допомагає зрозуміти причини поширення кіберзлочинності серед різних соціальних груп, а й спрямовує на розробку та впровадження узгоджених та ефективних заходів протидії цій проблемі з урахуванням специфіки соціокультурного контексту.

Міжнародна співпраця є критично важливим аспектом у боротьбі з кіберзагрозами в військовому контексті. Забезпечення ефективного міжнародного співробітництва та обміну інформацією між країнами дозволяє вчасно виявляти та реагувати на кібератаки, які можуть мати важливе стратегічне значення у військових операціях. Наприклад, міжнародні партнерства у сфері кібербезпеки дозволяють обмінюватися інформацією про нові загрози та розроблені технології оборони, що підвищує загальний рівень захисту від кіберзагроз.

Співпраця соціології з іншими галузями, такими як інформаційні технології, правоохоронні органи та військові структури, є необхідним елементом комплексного реагування на кіберзагрози. Наприклад, соціологічні дослідження можуть допомогти розуміти психологічні та соціальні аспекти кіберзлочинності, що в свою чергу допоможе у розробці ефективних стратегій протидії та попередження таких злочинів. Крім того, співпраця з інформаційними технологіями дозволяє використовувати передові технології для виявлення та блокування кібератак, а співпраця з правоохоронними органами та військовими структурами забезпечує ефективне реагування на кіберзагрози відповідно до закону та стратегічних цілей безпеки країни.

Такий інтегрований підхід до боротьби з кіберзлочинністю дозволяє ефективно використовувати ресурси та знання різних галузей для створення

комплексних та забезпечених стратегій захисту від кіберзагроз у військовому контексті.

Отже, ми визначили необхідність адаптації стратегій боротьби з кіберзлочинністю під нові умови війни, зосереджуючись на соціологічному підході як ключовому чиннику у розумінні соціальних та культурних вимірів цієї проблеми. Залучення громадськості та міжнародна співпраця стають важливими стратегічними напрямами, спрямованими на підвищення обізнаності, мобілізацію суспільства та обмін інформацією між країнами. Такий підхід дозволяє створювати комплексні та ефективні заходи протидії кіберзлочинності, поєднуючи в собі ресурси та знання різних галузей, які спрямовані на захист від кіберзагроз у військовому контексті.

Ми визначили, що російсько-українська війна спричинила значні зміни у кіберзлочинності, особливо щодо кібератак на державні структури, критичну інфраструктуру, комунікаційні мережі та громадянське суспільство. Наше дослідження виявило різноманітність типів кіберзлочинів, їхніх виконавців та цілей в умовах військового конфлікту. Контент-аналіз новин виявився обґрунтованим методом, що дозволив об'єктивно оцінити зміни в кіберзлочинності та побудувати аналітичні моделі для формулювання обґрунтованих висновків та стратегій протидії кіберзагрозам у воєнний часу.

У цьому дослідженні було проаналізовано динаміку кіберзлочинності в Україні перед і після початку російсько-української війни. За допомогою контент-аналізу новинної платформи «ФАКТИ» було виявлено, що після вторгнення кількість кіберзлочинів значно збільшилась, зокрема кількість кібератак і розповсюдження фейків. Виконавцями злочинів в основному стали окремі хакери та групи хакерів, залучення іноземних змі також помітно зросло. Основним мотивом залишається збагачення, проте збільшується кількість злочинів з метою нанесення шкоди інфраструктурі та дестабілізації країни. Громадяни України стали основною жертвою кіберзлочинів, що свідчить про зростання загрози для національної кібербезпеки. Загальна динаміка після вторгнення свідчить про інтенсифікацію кібератак та активність злочинців у

віртуальному просторі, що становить серйозну загрозу для країни та її громадян.

Ми розробили ряд заходів для вдосконалення стратегій боротьби з кіберзлочинністю в контексті російсько-української війни, враховуючи соціологічний підхід до розуміння соціальних та культурних вимірів проблеми. Участь громадськості виявляється ключовою у формуванні стратегій протидії цим загрозам через підвищення обізнаності громадян, мобілізацію громадських організацій та активну участь молоді. Проекти, як «Інтернет безпечний для всіх,» спрямовані на надання знань та навичок з кібербезпеки, а також залучення соціальних мереж для поширення інформації та корисних порад. Соціально-культурний аналіз допомагає розуміти специфіку соціокультурного контексту та адаптувати стратегії до цих особливостей. Міжнародна співпраця та інтеграція соціології з іншими галузями, такими як інформаційні технології та правоохоронні органи, забезпечують комплексний підхід до захисту від кіберзагроз у військовому контексті, що сприяє ефективній реакції та збереженню безпеки країни.

ВИСНОВКИ

У цьому дослідженні ми детально аналізували проблему кіберзлочинності під час російсько-української війни, використовуючи соціологічний підхід для розуміння складних динамік, що виникають у цьому контексті. Наша робота зосереджувалась на розгляді кібернетичної організації суспільства під час воєнного конфлікту, включаючи аналіз мотивацій та стратегій кіберзлочинців, їхнього впливу на суспільство та можливих наслідках для кібербезпеки та міждержавних відносин.

У процесі дослідження ми визначили та уточнили поняття «кіберзлочинність» та «суспільство в умовах війни», дослідили їхній ґенезис у соціологічному контексті, обґрунтували методологічні принципи та підходи дослідження, а також проаналізували інформаційний та кібернетичний аспекти війни.

Використали контент-аналіз на основі моніторингу медіа ресурсів для визначення кількості згадок про кіберзлочини до початку війни та після, а також для виявлення їх різновидів та змін у мотиваціях, що ведуть до таких злочинів. Аналіз медійних джерел дозволив встановити, що під час війни спостерігається помітне збільшення згадок про кіберзлочини, особливо з боку державних та недержавних акторів. Різновиди кіберзлочинів, які найчастіше згадувалися, включали кібератаки на інфраструктуру, фінансові шахрайства, кібершпигунство та дезінформацію через соціальні мережі та медіа. Зміна мотивацій також була відзначена, де під час війни спостерігалося більше використання кіберзлочинів як засобу військової стратегії, політичного впливу та дестабілізації суспільства. Такий аналіз дозволяє краще розуміти динаміку кіберзлочинності в контексті військових конфліктів та розробляти ефективні стратегії боротьби з цими загрозами.

У дослідженні було проаналізовано 180 повідомлень про кіберзлочини з онлайн платформи «ФАКТИ» за період з червня 2020 року до сьогодні. Перед початком повномасштабного вторгнення було зафіксовано 61 випадок

кіберзлочинів, які можна розділити на кібершахрайство, кібератаки та розповсюдження незаконного контенту. Більшість злочинів вчинені окремими злочинцями або групами хакерів з мотивацією збагачення, а найбільше постраждали громадяни України.

Після початку вторгнення збільшилась загальна кількість кіберзлочинів до 119 випадків. Відбулися зміни у типах злочинів, виконавцях, мотивації та жертвах. Найбільше зростання відзначено в кібератаках та розповсюдженні фейків, а також у вчиненні злочинів іноземними змі. Збільшення злочинів, спрямованих на дестабілізацію країни, свідчить про активну інформаційну та технічну війну. Також після вторгнення зросла кількість злочинів, вчинених окремими хакерами та іноземними змі.

Отже, дослідження показує інтенсифікацію кіберзлочинності та зміни в її характері після початку повномасштабного вторгнення.

Рекомендації щодо боротьби з кіберзлочинністю в умовах війни ґрунтуються на декількох напрямах дій. По-перше, це підвищення обізнаності громадськості через освітні кампанії та тренінги. Далі, мобілізація громадянського суспільства для активної участі в цих процесах є ключовою. Також важлива співпраця з міжнародними партнерами для обміну інформацією та розробки спільних стратегій. Не менш важливим є інтеграція соціологічного підходу для зрозуміння соціальних та культурних вимірів проблеми. Такий комплексний підхід сприятиме ефективній боротьбі з кіберзлочинністю у військовому контексті.

СПИСОК ЛІТЕРАТУРИ

1. Єнін М. Н., Коржов Г. О. Мережева комунікація: ризики та перспективи (на основі соціологічних опитувань громадської думки в країнах євросоюзу) . *Вісник НТУУ «КПІ». Політологія. Соціологія. Право.* 2021. Вип. 1 (49). С. 22-29.

2. Данильян О.Г., Дзьобань О.П. Інформаційна війна у медіапросторі сучасного суспільства. В*існик НЮУ імені Ярослава Мудрого. Серія: Філософія, філософія права, політологія, соціологія.* 2020. Вип. 3 (54). С. 11-29.

3. Ларкін М. О., Артьомов Є. О. Кримінологія як окремий розділ соціології. *Часопис Академії адвокатури України*. 2015. Т. 8, № 3. С. 51-55.

4. Кирбят'єв О.О. Комп'ютерні злочини: реалії сучасності, проблеми боротьби з ними та ймовірні шляхи їх вирішення. *Вісник Запорізького національного університету.* 2010. № 1. С. 165-170.

5. Кіберзлочинність та електронні докази. Cybercrime and digital evidence : навч. посібник / Б. М. Головкін та ін.; за ред. О. Денькович, Г. Шмельцер. Львів : ЛНУ ім. Івана Франка, 2022. 298 с.

6. Васильковський І. І. Поняття «кіберзлочинність» та «кіберзлочини»: стан та співвідношення. *Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика).* 2018. № 1-2 (10-11). С. 276-282.

7. Тарасюк К.В. Прокурорський нагляд при розслідуванні комп'ютерних злочинів. *Комп'ютерноінтегровані технології: освіта, наука, виробництво.* 2012. № 10. С. 178-181.

8. Голіна В., Головкін Б. Кримінологія: Загальна та Особлива частини : навчальний посібник. Харків : Право, 2014. 511 с.

9. Бондаренко О.С., Рєпін Д.А. Кіберзлочинність в Україні: причини, ознаки та заходи протидії. *Порівняльно-аналітичне право.* 2018. № 1. С. 246-248.

10. Гнатюк С. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи. *Ukrainian Scientific Journal of Information Security*. 2013. № 2 (19). С. 118-129.

11. Діордіца І. В. Кримінально-правова сутність кібершпигунства. *Реалії та перспективи розбудови правової держави в україні та світі:* матеріали III міжнар. наук.-практ. конф., м.Суми, 2020. С. 66-69.

12. Матвієнків С., Головчинський Н. Теоретико-методологічні засади дослідження поняття «війна». *Вісник Прикарпатського університету. Політологія.* 2020. Вип. 14. С. 103-113.

13. Требін М.П. «Гібридна» війна як нова українська реальність. *Український соціум*. 2014. № 3. С. 113-127.

14. Малик Я. Інформаційна війна і Україна. *Демократичне врядування.* 2015. Вип. 15. URL: file:///D:/%D0%97%D0%B0%D0%B3%D1%80%D1%83%D0%B7%D0%BA%D0%B8%20%D1%81%20%D1%85%D1%80%D0%BE%D0%BC%D0%B0/DeVr_2015_15_3%20(1).pdf (дата звернення: 09.04.2024).

15. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII; станом на 19.05.2018. URL: http://zakon3.rada.gov.ua/laws/show/2163-19 (дата звернення: 09.04.2024).

16. Требін М. П. Соціологія війни П. О. Сорокіна. *Вісник Національного університету «Юридична академія України імені Ярослава Мудрого». Серія: Соціологія*. Харків, 2016. № 3. С. 95-107.

17. Павленко І.О. Світоглядні характеристики суб'єктів миру та війни. *Гуманітарний вісник ЗДІА*. 2015. № 60. С. 114-126.

18. Лепський М., Щербань О., Бублєєв В. Класифікація переговорів в умовах війни. *Науково-теоретичний альманах Грані*. 2022. Т. 25, № 4. С. 43-49.

19. Кононов І.Ф. Соціологія в умовах кризи і війни: проблема методологічної спроможності. *Вісник Луганського національного*

університету імені Тараса Шевченка: Соціологічні науки. 2016. № 5 (302), травень. С. 5-54.

20. Пилипенко Я. С. Демаркація понять «воєнний конфлікт», «збройний конфлікт» та «війна». *Вісник НТУ «КПІ». Політологія. Соціологія. Право.* 2017. № 1/2 (33/34). С. 143-146.

21. Європіна І. В. Види протиправних діянь у сфері новітніх інформаційних технологій. *Вісник Академії адвокатури України.* 2010. Т.3. С. 129-136.

22. Гембарук О.В. Зміст та структура концепту «війна» у сучасній блогосфері. *Modern problems of science, education and society. Proceedings of the 9th International scientific and practical conference. SPC «Sci-conf.com.ua». Kyiv, Ukraine. 2023.* P. 981-988. URL: https://sci-conf.com.ua/ix-mizhnarodna-naukovo-praktichna-konferentsiya-modern-problems-of-science-education-and-society-6-8-11-2023-kiyiv-ukrayina-arhiv/ (дата звернення: 09.04.2024).

23. Марков В. В. Статистичне дослідження показників кіберзлочинності: методологічний аспект. *Право і безпека.* 2013. № 2 (49). С. 136-140.

24. Гоблик В. В., Щербань Т. Прикладна соціологія: логістика і методи дослідження : навчальний посібник. Мукачево : РВВ МДУ, 2021. 108 с.

25. Магда Є.М. Гібридна війна: сутність та структура феномену. *Міжнародні відносини: Серія «Політичні науки».* 2014. № 4. С. 9-10.

26. Фещенко І. В. Інформаційна війна як органічна складова сучасного збройно-політичного конфлікту. *Філософія та політологія в контексті сучасної культури.* 2021. Т. 13, № 1. С. 96-103.

27. Юзова І.Ю. Аналіз організації та ведення інформаційно-психологічних операцій при веденні гібридної війни. *Збірник наукових праць Харківського національного університету Повітряних Сил*. 2020. № 2 (64). С. 40-44.

28. Ратушна Т. О. Фейки як маніпулятивна технологія формування громадської думки. *Актуальні проблеми філософії та соціології : Науково-практичний журнал*. Одеса, 2021. Вип. 29. С. 71-76.

29. Бараненко Р.В. Кібератаки як одна з форм кібертероризму. *Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки.* 2021. С. 45-51.

30. Козак Н.С. Кіберзлочинність: сутність, специфіка та заходи протидії. *Південноукраїнський правничий часопис*. 2016. № 2. С. 63-67.

31. Єрмак О. В., Гордієнко М. В. Щодо питання про сучасний стан протидії кіберзагрозам в Україні. *Кримінально-виконавча система України та її роль у розбудові правової і соціальної держави:* матеріали VI науково-практичної конференції курсантів, студентів, слухачів та молодих дослідників (м. Чернігів, 27 листопада 2020 р.). Чернігів : Академія ДПтС, 2020. С. 42-46.

32. Лучик С. Д., Папуця Р. О. Кібербезпека як складова національної безпеки України: реалії війни. *Державно-правові засади формування безпекового середовища в Україні: сучасні виклики* : Всеукр. наук. конф. МВС України, ОДУВС. Одеса, 2023. С. 49-52.

33. Бабанін С. В. Кіберзлочинність. Комп'ютерна злочинність. *Велика українська юридична енциклопедія.* Харків, 2019. Т. 18. С. 207.

34. Василенко О. В. Основні світові тенденції розвитку озброєння та військової техніки для ведення війн у майбутньому. *Наука і оборона*. 2009. № 4. С. 18-22.

35. Волошин О. Г., Поліщук В. В. Кіберзлочинність як форма ведення гібридної війни. *Актуальні проблеми криміналістики та судової експертології* : матеріали міжвідом. наук.-практ. конф. 2018 р. Київ, 2018. С. 105.

36. Бурячок В. Л. Кібернетична безпека – головний фактор сталого розвитку сучасного інформаційного суспільства. *Сучасна спеціальна техніка.* 2011. № 3 (26). С. 104-114.

37. Ткачук Н. Кібертероризм як новий виклик національній безпеці. *Протидія терористичній діяльності: міжнародний досвід і його*

актуальність для України : матеріали міжнар. наук.-практ. конф. Київ : Національна академія прокуратури України, 2016. С. 340-342.

38. Владленова І. В., Кальницький Е. А. Кіберзлочинність як виклик інформаційному суспільству. *Гілея: науковий вісник : збірник наукових праць.* 2013. Вип. 77. С. 142-146.

39. Бойченко О. В., Ончурова О. О. Кібертероризм у складі сучасних проблем національної безпеки. *Фортеця права*. 2010. № 2. С. 57.

40. Бурячок В. Л. Основи формування державної системи кібернетичної безпеки : монографія. Київ : НАУ, 2013. 432 с.

41. Малик Я. Інформаційна війна і Україна. Демократичне врядування. 2015. Вип. 15. URL: http://nbuv.gov.ua/UJRN/DeVr_2015_15_3 (дата звернення: 09.04.2024).

42. Марков В. В. Статистичне дослідження показників кіберзлочинності: методологічний аспект . Право і безпека. 2013. № 2 (49). С. 136.

43. Keeley L. H. War Before Civilization. Oxford University Press, 1996. 245 p.

ДОДАТКИ

Додаток А

Програма соціологічного дослідження

на тему: **«Кіберзлочинність в умовах російсько української війни»**

І. Методологічна частина

Обґрунтування проблеми дослідження. Останні роки спостерігається швидкий прогрес у цифрових технологіях, що призвело до зростання загрози кіберзлочинності на всіх рівнях — від особистих до державних та корпоративних систем. Цей розвиток створює нові можливості для кіберзлочинців і вимагає постійного оновлення захисних методів. Війна в Україні додатково збільшує цю загрозу, зумовлюючи не тільки зростання кібератак, але й підвищення їхньої складності та масштабу. Умови війни спонукають обидві сторони використовувати кіберзброю для маніпуляції інформацією, дестабілізації противника та завдання шкоди його інфраструктурі. Тому важливість ефективного кіберзахисту надзвичайно висока як для держави, так і для приватних суб'єктів, і потребує постійного удосконалення та розвитку заходів захисту.

Проблемною ситуацією вважаємо те, що кіберзлочинність стає все більш складною та небезпечною, особливо у зв'язку з воєнним конфліктом. Збільшення обсягу кібератак і зростання їхньої складності створюють серйозні виклики для кібербезпеки держави та громадянського суспільства.

Об’єкт дослідження. Повідомлення про кіберзлочин.

Предмет дослідження. Зміни в кількості злочинів, їх типах, злочинцях, мотиваціях та жертвах до та після початку повномасштабного вторгнення.

Мета дослідження. Розробити стратегії розвитку протидії кіберзлочинам за допомогою соціології.

Завдання дослідження:

- Виявлення змін у кількості та типах кіберзлочинів до та після початку повномасштабного вторгнення.

- Аналіз мотивацій, які підштовхують злочинців до вчинення кіберзлочинів, і визначення змін у цій сфері в контексті військового конфлікту.
- Порівняння тенденцій кіберзлочинності до та після повномаштабного військового вторгнення.

Інтерпретація основних понять дослідження:

1. Кіберзлочинність - це широке поняття, яке включає в себе будь-які злочинні дії, які вчиняються через комп'ютерні мережі або інтернет. Це може бути від крадіжки даних до дестабілізації країн чи організацій через технічні засоби.
2. Війна - у контексті кіберзлочинності війна може відображати не тільки фізичний конфлікт між країнами, але й боротьбу у кіберпросторі за вплив, безпеку, та ресурси, що може включати кібератаки, шпигунство, дезінформацію тощо.
3. Кібершахрайство - вид кіберзлочинності, який орієнтований на отримання матеріальної вигоди через обман або злам системи. Це може бути фінансові шахрайства, включаючи фішинг, обманні платіжні системи тощо.
4. Кібератака - активна спроба зламати, пошкодити або зруйнувати комп'ютерні системи чи мережі. Кібератаки можуть бути спрямовані на знищення даних, перешкоджання роботі систем чи навіть крадіжку конфіденційної інформації.
5. Фейк - дезінформація або вигадана інформація, що розповсюджується через інтернет з метою введення в оману або створення негативного впливу на суспільство чи індивідів.
6. Хакер - технічно обізнана особа, яка має навички в проникненні в комп'ютерні системи для різних цілей, від тестування безпеки до злочинних дій, таких як крадіжка даних або виклик шкоди.

ІІ. Методична частина

Обґрунтування вибіркової сукупності. Обрання вибіркової сукупності для аналізу новинної онлайн платформи «ФАКТИ» за період з червня 2020 року по лютий 2022 року та з березня 2022 року до сьогодні обґрунтоване кількома важливими аспектами. По-перше, ця платформа відома своєю високою популярністю та репутацією надійного джерела новин, що гарантує отримання достовірної та актуальної інформації про кіберзлочини в Україні. Такий вибір джерела дозволяє забезпечити найбільш репрезентативні дані для дослідження. По-друге, обрані періоди - з червня 2020 року по лютий 2022 року та з березня 2022 року до сьогодні, охоплюють значну частину часового проміжку, що дозволяє виявити тенденції та зміни у кіберзлочинності на різних етапах часу, зокрема під час війни та після повномасштабного вторгнення**.**

Обґрунтування методу дослідження. Контент-аналіз дозволяє систематично та об'єктивно вивчати великі обсяги текстової інформації, що в даному випадку відображається в повідомленнях про кіберзлочини на платформі «ФАКТИ». Цей метод дозволяє структуровано виявляти та аналізувати певні категорії даних, такі як типи злочинів, характеристики злочинців, їхні мотивації та об'єкти нападів. Такий підхід дозволяє отримати детальну та об'єктивну інформацію для подальшого дослідження.

Контент-аналіз є об'єктивним методом, оскільки базується на аналізі фактичних текстів, що публікуються на відомій новинній платформі. Це дозволяє уникнути впливу особистих поглядів аналітика чи дослідника на результати дослідження та забезпечити достовірність отриманих даних.

Додаток Б

Результати дослвдження

Тип кібер злочину	Кібершахрайство	Кібератаки	Незаконий контент		Загалом
	21	4	36		61
Злочинець	Один хакер	Група хакерів	Один злочинець	Злочинне угруповування	
	8	18	13	22	
Мотивація	Збагачення	Нанесення шкоди пристрою			
	57	4			
Жертва	Грамодяни україни	Іноземці	Держустанови		
	55	2	4		

Тип кібер злочину	Кібершахрайство	Кібератаки	Незаконий контент	Расповсюдження фейків	Загалом
	13	38	21	47	119
Злочинець	Один хакер	Група хакерів	Один злочинець	Злочинне угруповуі	Іноземні змі
	11	43	12	15	38
Мотивація	Збагачення	Нанесення шкоди п	Нанесення шкоди і	Дестабілізація країни	
	33	9	27	50	
Жертва	Грамодяни україни	Іноземці	Держустанови	Компанії	
	101	2	11	5	

Декларація
академічної доброчесності
здобувача ступеня вищої освіти ЗНУ

Я, Лобанова Ангеліна Романівна, студентка IV курсу бакалаврату, денної форми навчання, факультету соціології та управління, спеціальність 054 «Соціологія», адреса електронної пошти angelinaberkyt777@gmail.com:

- підтверджую, що написана мною кваліфікаційна робота на тему «Соціологічний аналіз кіберзлочинності в умовах російсько-української війни» відповідає вимогам академічної доброчесності та не містить порушень, що визначені у ст. 42 Закону України «Про освіту», зі змістом яких ознайомлений/на;
- заявляю, що надана мною для перевірки електронна версія роботи є ідентичною її друкованій версії;
- згодна на перевірку моєї роботи на відповідність критеріям академічної доброчесності у будь-який спосіб, у тому числі за допомогою інтернет-системи, а також на архівування моєї роботи в базі даних цієї системи.

03.06.2024 А.Р. Лобанова

Науковий керівник,
д.філос.н., професор,
професор кафедри соціології
03.06.2024 М.А. Лепський