МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ ВНУТРІШНІХ СПРАВ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
ПРАВА ТА ПСИХОЛОГІЇ

КІБЕРБЕЗПЕКА В ДІЇ: ВІД ОСОБИСТОГО ЗАХИСТУ ДО НАЦІОНАЛЬНОГО

Матеріали
науково-практичного круглого столу
(Київ, 15 жовтня 2025 року)

Київ
2025

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ ВНУТРІШНІХ СПРАВ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
ПРАВА ТА ПСИХОЛОГІЇ

КІБЕРБЕЗПЕКА В ДІЇ: ВІД ОСОБИСТОГО ЗАХИСТУ ДО НАЦІОНАЛЬНОГО

Матеріали
науково-практичного круглого столу
(Київ, 15 жовтня 2025 року)

Київ
2025

УДК 004.056(477)(06)
К38

Відповідальні за випуск:

Шрамко С. С., кандидат юридичних наук, старший дослідник, завідувач кафедри кримінального права та кримінології навчально-наукового інституту права та психології Національної академії внутрішніх справ;

Резнік Ю. С., кандидат юридичних наук, старший викладач кафедри кримінального права та кримінології навчально-наукового інституту права та психології Національної академії внутрішніх справ

Рекомендовано до друку науково-методичною радою Національної академії внутрішніх справ 18 листопада 2025 року (протокол № 10)

Матеріали подано в авторській редакції. Відповідальність за їхню якість, а також відсутність у них відомостей, що становлять державну таємницю та службову інформацію, несуть автори та їхні наукові керівники

К38 **Кібербезпека** в дії: від особистого захисту до національного [Текст] : матеріали наук.-практ. круглого столу (Київ, 15 жовт. 2025 р.). – Київ : Нац. акад. внутр. справ, 2025. – 120 с.

Збірник підготовлено за результатами круглого столу, проведеного в межах місяця кібербезпеки. Опубліковано тези здобувачів вищої освіти, які роблять перші кроки в дослідницькій діяльності, а також досвідчених науковців. У роботах зосереджено увагу на загрозах у кіберпросторі, перевагах і недоліках штучного інтелекту, проаналізовано досвід провідних країн світу й схарактеризовано національну стратегію у сфері боротьбі з кіберзлочинністю, а також віктимогенні чинники в цій сфері.

УДК 004.056(477)(06)

ЗМІСТ

Борко Надія Олександрівна,
здобувач ступеня вищої освіти бакалавра навчально-наукового інституту права та психології Національної академії внутрішніх справ
Науковий керівник:
Резнік Ю. С., старший викладач кафедри кримінального права та кримінології навчально-наукового інституту права та психології Національної академії внутрішніх справ, кандидат юридичних наук

КІБЕРЗЛОЧИННІСТЬ В УКРАЇНІ ТА СВІТІ: ЕКЗИСТЕНЦІЙНИЙ АНАЛІЗ, МЕТОДОЛОГІЯ АТАК І СТРАТЕГІЇ ПРОТИДІЇ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

Сучасна цивілізація перебуває на етапі цифрової трансформації, де інформаційно-комунікаційні технології (ІКТ) виступають критичним каталізатором для функціонування усіх сфер життєдіяльності – від електронного урядування та e-commerce до управління критичними інфраструктурами [1]. Ця технологічна інтеграція забезпечує безпрецедентну ефективність, але водночас формує ефект гіперзалежності від цифрового простору, роблячи будь-яку мережеву систему потенційним об'єктом атаки. У цьому контексті кіберзлочинність перестала бути виключно технічною проблемою, перетворившись на системну загрозу XXI століття, що зачіпає національну безпеку, економічну стійкість та фундаментальні права людини на конфіденційність [2].

Кіберзлочинність охоплює незаконні дії, які здійснюються за допомогою ІКТ або спрямовані проти них. Концептуальна основа цього явища, закріплена у міжнародних документах, таких як Конвенція Ради Європи про кіберзлочинність, стосується порушення тріади цілісності, конфіденційності та доступності комп'ютерних даних і систем (CIA Triad). До основних видів кіберзлочинів належать: несанкціоноване заволодіння коштами, кібершпигунство, шантаж,

розповсюдження шкідливого програмного забезпечення та атаки на державні й комерційні системи. Їх транскордонний та анонімний характер ускладнює ефективну протидію, оскільки агресор може діяти з будь-якої точки світу, мінімізуючи юридичну відповідальність [3].

Методологія кіберзлочинності відзначається високою технологічною складністю, що підтверджують численні інциденти. Наприклад, атака на критичну інфраструктуру Західної України у 2015 році, здійснена угрупованням «Sandworm» із використанням шкідливого ПЗ BlackEnergy 3, призвела до відключення електропостачання понад 225 тисяч споживачів [4]. Цей кейс став прецедентом у світі і показав, як кіберзлочини можуть слугувати інструментом гібридної війни.

Фінансовий сектор також часто стає об'єктом кібератак. Група Carbanak викрала понад $1 млрд, маніпулюючи внутрішніми банківськими системами, використовуючи фішинг та банківські трояни, замасковані під легітимні оновлення [5]. Крім того, порушення доступності систем через DoS/DDoS-атаки, які часто здійснюють ботнети – централізовано керовані мережі заражених пристроїв, призводять до економічних втрат і підриву довіри до державних та комерційних порталів. Прикладом є серія атак на українські урядові сервіси у 2020 році [6].

Викрадення даних і застосування програм-вимагачів (ransomware) – ще одна загроза. Наприклад, DarkSide зашифрувала дані Colonial Pipeline у США в 2021 році, що спричинило дефіцит пального і підкреслило залежність фізичної інфраструктури від цифрової безпеки [7].

Зростання кіберзлочинності визначається кількома ключовими детермінантами. По-перше, технологічна експансія та зростання кількості пристроїв Інтернету речей (IoT) створюють величезну кількість точок вразливості [8]. По-друге, низький рівень цифрової грамотності та нехтування кібергігієною серед користувачів забезпечує успіх атак із застосуванням соціальної інженерії [9]. По-третє, професіоналізація та комерціалізація кіберзлочинності на чорному ринку знизили поріг входу для потенційних злочинців [10].

Комплексний підхід до кібербезпеки передбачає дії на різних рівнях. На корпоративному та індивідуальному рівні необхідне суворе дотримання кібергігієни: багатофакторна автентифікація, регулярне оновлення програмного забезпечення,

резервне копіювання даних. На державному рівні потрібне вдосконалення законодавства, наприклад, через реалізацію Закону України «Про основні засади забезпечення кібербезпеки України», та зміцнення інституцій, таких як Департамент кіберполіції, для ефективного розкриття транскордонних злочинів.

Лише узгоджена стратегія, що поєднує технологічну стійкість, юридичну відповідальність та високий рівень обізнаності користувачів, здатна забезпечити надійний захист цифрового середовища та зберегти стабільність суспільства перед обличчям кіберзагроз.

Список використаних джерел

1. Laudon, K., & Laudon, J. (2020). *Management Information Systems: Managing the Digital Firm*. Pearson.
2. Wall, D. S. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. Polity Press.
3. Brenner, S. W. (2010). *Cybercrime: Criminal Threats from Cyberspace*. Praeger.
4. Zetter, K. (2016). *Inside the Cyberattack that Shocked the US and Ukraine*. Wired.
5. Symantec Security Response. (2018). *Carbanak Gang Analysis Report*.
6. CERT-UA. (2020). *Annual Report on DDoS Attacks Against Ukrainian Government Services*.
7. FBI & CISA. (2021). *Colonial Pipeline Ransomware Incident Report*.
8. Rose, S., et al. (2019). *Zero Trust Architecture*. NIST Special Publication 800-207.
9. Hadnagy, C. (2018). *Social Engineering: The Science of Human Hacking*. Wiley.
10. Europol. (2021). *Internet Organised Crime Threat Assessment (IOCTA)*.

Бриль Дар'я Павлівна,
здобувач ступеня вищої освіти магістра навчально-наукового інституту права та психології Національної академії внутрішніх справ
Науковий керівник:
Шрамко С. С., завідувач кафедри кримінального права та кримінології навчально-наукового інституту права та психології Національної академії внутрішніх справ, кандидат юридичних наук, старший дослідник

ЗАХИСТ КРИТИЧНОЇ ІТ-ІНФРАСТРУКТУРИ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ

В умовах стрімкої цифровізації суспільства прослідковується певна залежність державних і приватних структур від інформаційно-комунікаційних технологій, внаслідок чого питання захисту критичної ІТ-інфраструктури набуває особливого значення. В узагальненому виді під критичною ІТ-інфраструктурою розуміють сукупність інформаційних систем, ресурсів та сервісів, безперебійне функціонування яких є життєвою необхідністю для забезпечення національної безпеки, економічної стабільності, охорони здоров'я, енергетики, транспорту та інших ключових сфер життєдіяльності держави [3].

Водночас з розвитком цифрового середовища та посиленням глобальної конкуренції держави стикаються з явищем гібридних загроз, що поєднують у собі кібернапади, інформаційно-психологічні операції, економічні диверсії, технічні саботажі та правові маніпуляції. Такі дії мають комплексний характер і спрямовані на підрив стабільності держави, дезорганізацію управління та зниження довіри до суспільних інститутів. У кіберпросторі гібридні загрози проявляються у вигляді масованих атак на державні реєстри, банківську інфраструктуру, системи енергозабезпечення та комунікації [7, с. 3].

Для України дана проблематика є особливо актуальною в умовах воєнного стану та постійного тиску з боку держави-

агресора з використанням гібридних дій, серед яких значну частину становлять кібератаки на органи державної влади, об'єкти енергетики, транспорту та зв'язку.

Одночасно держава здійснює масштабні євроінтеграційні процеси, які передбачають гармонізацію національного законодавства з нормами та стандартами Європейського Союзу у сфері кібербезпеки, зокрема –імплементацію вимог директиви NIS2. Ця директива – новий законодавчий акт Європейського Союзу, спрямований на посилення кібербезпеки шляхом встановлення суворіших вимог до управління ризиками, звітності про інциденти та обов'язкового впровадження заходів безпеки для ширшого кола компаній, що працюють у критичних галузях. Вона замінює попередню директиву NIS 2016 року, розширює сферу її застосування та посилює відповідальність організацій за забезпечення кіберстійкості [1].

Захист критичної ІТ-інфраструктури в Україні ґрунтується на конституційних принципах національної безпеки, верховенства права та захисту інформації. Базовими нормативними актами у цій сфері є Закон України «Про основні засади забезпечення кібербезпеки України», який визначає систему суб'єктів, принципи та механізми забезпечення кіберзахисту [4], та Закон «Про національну безпеку України», що інтегрує питання кіберзагроз у загальну структуру безпеки держави [2]. Важливими стратегічними документами виступають Кіберстратегія України (2021–2025) та Стратегія національної безпеки, що формують політико-правові пріоритети розвитку кіберстійкості [5]. Актуальною залишається потреба у оновленні законодавства відповідно до європейських стандартів NIS2, а також у створенні ефективної системи державного контролю за дотриманням вимог кібербезпеки. Лише чітке нормативне визначення об'єктів критичної ІТ-інфраструктури, підкріплене узгодженими міжвідомчими механізмами, може забезпечити її реальний захист в умовах зростаючих гібридних загроз. Міжнародно-правові документи, зокрема Tallinn Manual та Будапештська конвенція про кіберзлочинність, формують базові підходи до кваліфікації таких дій і визначають механізми співпраці між державами [6].

Проблемним залишається віднесення кібердій до актів агресії або тероризму, адже чинне міжнародне право не має

чітких критеріїв для цього. Водночас дедалі більшого значення набуває явище lawfare – використання правових механізмів як інструменту політичного або воєнного тиску [8].

Таким чином, захист критичної ІТ-інфраструктури в умовах гібридних загроз є стратегічним завданням держави, що поєднує правові, технічні та організаційні заходи. Україна вже створила базові інституційні та нормативні механізми кібербезпеки, однак потребує подальшої гармонізації законодавства з нормами ЄС, запровадження єдиних стандартів кіберзахисту та посилення державно-приватної взаємодії.

Ефективна протидія гібридним загрозам можлива лише за умови міжвідомчої координації, міжнародного партнерства та професійної правової експертизи, спрямованої на забезпечення кіберстійкості держави та суспільства.

Список використаних джерел

1. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance) : Directive of 14.12.2022.

2. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII : станом на 5 жовт. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 08.10.2025).

3. Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX : станом на 21 верес. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 11.10.2025).

4. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII : станом на 20 квіт. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 10.10.2025).

5. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 12.10.2025).

6. Конвенція про кіберзлочинність : Конвенція Ради Європи від 23.11.2001 : станом на 7 верес. 2005 р. URL:

https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 14.10.2025).

7. Делембовський М., Ткаченко В., Дмитро Д. Захист критичної інфраструктури України від кібератак. *Міжнародний науковий журнал «Грааль науки»*. 2024.

8. Yefimenko I., Sakovskyi A., Bilozorov Ye. Protection of critical infrastructure as a component of Ukraine's national security. *Юридичний часопис НАВС*. Т. 13, № 2, 2023. DOI: 10.56215/naia-chasopis/2.2023.74

Броварник Анна Сергіївна,
здобувач ступеня вищої освіти бакалавра навчально-наукового інституту права та психології Національної академії внутрішніх справ
Науковий керівник:
Шрамко С. С., завідувач кафедри кримінального права та кримінології навчально-наукового інституту права та психології Національної академії внутрішніх справ, кандидат юридичних наук, старший дослідник

МІЖНАРОДНИЙ ДОСВІД ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ У СФЕРІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

Щодня в світі, в силу його шаленого темпу розвитку, з'являється багато різних можливостей у кіберпросторі, більшість із яких, відповідно, потребують збору та обробки персональних даних. Варто зауважити, що ні приписи норм законодавства, ні інші важелі суспільного впливу не зможуть забезпечити абсолютну безпеку персональних даних у кіберпросторі, адже витік інформації може статися навіть тоді, коли більшість про це не здогадуєтеся [1, с. 255].

Важливою рисою кіберзлочинності є її глобальний, інтернаціональний характер, що обумовлює низьку ефективність традиційних методів припинення злочинів. Слід зазначити, що для організації ефективної боротьби з кіберзлочинністю держави мають співпрацювати між собою –

проте такого роду співпраця в певною мірою зачіпає державний суверенітет та його повноваження у сфері захисту інформації. Міжнародна взаємодія між державами, спрямована на боротьбу з кіберзлочинністю, кібертероризмом, є найбільш ефективною в районах, де між державами існує високий рівень політичної довіри – наприклад, в рамках Європейського Союзу [2, с. 281–282].

Основні проблеми, що виникають при міжнародно-правовому регулюванні протидії кіберзлочинності, полягають у відмінностях національного законодавства у сфері кібербезпеки; відсутності чіткого уніфікованого категоріального апарату; недостатньому рівні координації діяльності правоохоронних органів при розслідуванні кіберзлочинів, низькому рівні обміну інформацією про кіберінциденти між державами; недостатньому рівні державного й приватного співробітництва у цій сфері [2, с. 281].

Згідно зі Стратегією кібербезпеки Європейського Союзу, прийнятої у 2013 році, передбачено «зміцнення співпраці між державним та приватним секторами, а також розробку концептуальних документів для створення єдиної підходової парадигми в Європейському Союзі стосовно організації та проведення інформаційних операцій в рамках Стратегії «Спільної оборони і політики безпеки». Серед головних завдань, визначених у Стратегії кібербезпеки ЄС, можна виділити наступне: значне зниження рівня кіберзлочинності в країнах Європейського Союзу; розвиток політики кіберзахисту в країнах-членах Європейського Союзу та розвиток індустрії та технологічних ресурсів для забезпечення кібербезпеки [3, с. 264]. Також Стратегія підкреслює активну роль Європейського Союзу у забезпеченні захисту країн-членів організації, державних установ та громадян від кіберзлочинності. Одним з конкретних результатів цієї діяльності було створення Європейського центру протидії кіберзлочинності [3, с. 265].

У США основним органом, який централізовано здійснює операції в рамках кібернетичної війни, управління та захист військових комп'ютерних мереж є Кібернетичне командування (United States Cyber Command, USCYBERCOM). Його підрозділи володіють силами та засобами для проведення кібератак, вони «застосовуються на практиці протидії будь-якій IT-інфраструктурі, з якої, на їх думку, виходять загрози».

З 2018 року USCYBERCOM надали право проводити проактивні хакерські атаки з метою запобігання кібернападам, що готуються. Окрім USCYBERCOM, потужні кібернетичні підрозділи є в ФБР та АНБ (Агенція національної безпеки). Наприклад, після однієї з атак на нафтопровід Colonial Pipeline, ФБР змогла знищити кілька хакерських груп і відкликати більшу частину сплаченої за здирництво суми [4, с. 114].

У Великій Британії проблемами інформаційної боротьби займається департамент урядових комунікацій (The Government Communications Headquarters). Під інформаційною боротьбою у цій країні розуміється цілеспрямована реалізація комплексу заходів щодо дезорганізації і встановлення контролю над системою державного та воєнного управління противника шляхом інформаційно-технічного й інформаційно-психологічного впливу на його інформаційні ресурси, на суспільну та індивідуальну свідомість. Питаннями проведення інформаційних операцій у військовому відомстві займається група з координації військових інформаційних операцій, яка підпорядкована міністрові оборони [4, с. 115]. Також у цій країні реалізується низка програм із залучення громадськості до забезпечення безпеки інформаційного простору держави (насамперед учнівської та студентської молоді) [4, с. 115–116].

У ФРН створений і активно функціонує Центр безпеки інформаційної техніки (штат 500 співробітників, річний бюджет 50 млн євро). За результатами його діяльності передбачається ведення наступальних і оборонних операцій інформаційної війни для досягнення національних цілей. Німецькі аналітики розглядають управління засобами масової інформації як дієвий елемент інформаційної війни. Крім того, вони окремо розглядають економічну інформаційну війну [4, с. 117]. У 2009 році Конституцію ФРН було доповнено статтею 91с, яка заклала основу для співпраці федерального уряду та урядів земель у сфері інформаційних технологій. Базовим законом у сфері інформаційної безпеки Німеччини є Закон «Про посилення безпеки систем інформаційних технологій» (Закон про безпеку ІТ) від липня 2015 року. Закон відводить Федеральному відомству з безпеки у сфері інформаційних технологій центральну роль у захисті критично важливих інфраструктур у Німеччині [4, с. 118].

За останні роки ізраїльська армія зробила чимало для «диджиталізації» своїх сухопутних військ. Але це підвищило загрозу того, що під час війни противник спробує порушити роботу військової мережі. Водночас Ізраїль вперше в історії показав, що атаки у віртуальному світі можна відбити реальним бомбардуванням. Зокрема, в травні 2019 року авіація Ізраїлю завдала швидкого авіаудару по будівлі в секторі Газа. За даними розвідки саме звідти проводилася кібератака [4, с. 117].

Базовим документом у протидії кіберзлочинності для європейських держав, і не тільки, є Конвенція Ради Європи про кіберзлочинність від 23 листопада 2001 р. та Додатковий протокол до неї від 28 січня 2003 р. Вони є «фундаментом для розробки відповідного законодавства європейських держав» [2, с. 280]. Документ зобов'язує держави, які є її сторонами, гармонізувати національні закони стосовно визначення основних злочинів. Отже, кожна сторона приймає заходи, необхідні для того, щоб кваліфікувати в якості кримінального злочину, відповідно внутрішньодержавного права, широке коло діянь; реалізує політику, спрямовану на здійснення протидії кіберзлочинності; на міжнародному рівні сприяє цій протидії; розслідує злочини, вчинені в рамках глобальної інформаційно-цифрової мережі; бере участь у створенні нових заходів протидії кіберзлочинності [2, с. 280, 282].

Визначаючи безпеку однією з основних цілей, НАТО внесла зміни у свою політику стосовно інформаційної безпеки. Організація встановила центри в країнах-членах як багатонаціональні інститути, спрямовані на розробку стратегій цифрової безпеки, поліпшення міжнародної співпраці, впровадження наукових розробок у боротьбі з цифровими загрозами, обмін досвідом забезпечення інформаційної безпеки між країнами-членами та партнерами [3, с. 265].

Беззаперечно, звернення до міжнародного досвіду забезпечення кібербезпеки є важливим з огляду запозичення кращих практик для України. Крім того, зважаючи на інтернаціональний характер кіберзлочинності та загрозу світовій безпеці, необхідний обмін досвідом та тісна співпраця на міжнародному та європейському рівнях.

Список використаних джерел

1. Аніщук В. В. Проблема захисту персональних даних в кіберпросторі. *Науковий вісник Ужгородського Національного Університету*. Серія ПРАВО. 2024. Вип. 84, ч. 3. С. 252–256. URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2024/09/40-2.pdf
2. Попко В. В., Попко Є. В. Міжнародно-правова регламентація транснаціональної кіберзлочинності у кіберпросторі. *Науковий вісник Ужгородського Національного Університету.* Серія ПРАВО. 2021. Вип. 66. С. 276–283. URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2021/11/49.pdf
3. Тєтєвін М. С. Досвід України в галузі міжнародного співробітництва в галузі кібербезпеки. *Науковий вісник Ужгородського Національного Університету*. Серія ПРАВО. 2024. Вип. 82, ч. 3. С. 263–266. URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2024/05/43-2.pdf
4. Черниш Р. Ф. Міжнародний організаційний досвід у сфері забезпечення кібербезпеки. *Вісник кримінального судочинства.* 2021. № 3–4. С. 112–121. URL: https://vkslaw.knu.ua/wp-content/uploads/2024/03/3-4_2021-chernysh-r.pdf

Герун Ілона Петрівна,
здобувач ступеня вищої освіти бакалавра навчально-наукового інституту права та психології Національної академії внутрішніх справ
Науковий керівник:
Резнік Ю. С., старший викладач кафедри кримінального права та кримінології навчально-наукового інституту права та психології Національної академії внутрішніх справ, кандидат юридичних наук

КІБЕРБУЛІНГ: ЗАГРОЗИ ДЛЯ МОЛОДІ ТА ПРАВОВІ МЕХАНІЗМИ ПРОТИДІЇ

Сьогодні цифрове середовище стає невід'ємною частиною життя молоді, що спричиняє одночасне зростання ризиків для їхньої психологічної та соціальної безпеки. Інтернет використовується не лише для комунікації, навчання та

самореалізації, але й відкриває нові можливості для агресивної поведінки, зокрема кібербулінгу. Як зазначає І. О. Лисенко, кібербулінг являє собою специфічну форму психологічного насильства, яка реалізується через інформаційно-комунікаційні технології та соціальні мережі [1]. Це явище відрізняється від традиційного булінгу тим, що воно не обмежується фізичним простором і дозволяє агресору завдавати шкоди дистанційно.

Пандемія COVID-19 та військові дії в Україні спричинили значні зміни у сфері освіти, зокрема поширення дистанційного навчання, що призвело до значного збільшення часу перебування молоді в інтернеті [2]. Як зазначає О. В. Ковальчук, соціальні мережі та онлайн-платформи стали основним каналом комунікації, що водночас підвищує ризик потрапляння молоді під вплив маніпуляцій та кіберзлочинців [3]. Залежність від цифрового середовища здатна негативно впливати на психічне здоров'я та соціальну адаптацію підлітків.

Наукові дослідження свідчать, що кібербулінг має різноманітні форми прояву та поведінкові стилі. Зокрема, він включає флеймінг, харасмент, обмовлення, наклеп, самозванство, шахрайство, видурювання конфіденційної інформації, ізоляцію та кіберпереслідування [4]. Усі ці дії мають на меті завдати шкоди або принизити особу дистанційно, без фізичного насильства. За словами С. В. Петрів, сучасні соціальні мережі та месенджери, такі як Telegram, Facebook та Instagram, активно використовуються агресорами для реалізації цих дій [5].

Особливу небезпеку становлять спроби зовнішніх агентів використати молодь у протиправних цілях. Наприклад, російські спецслужби застосовують маніпуляції у соціальних мережах та пропонують молодим людям участь у незаконних діях, починаючи від дрібних доручень і закінчуючи серйозними злочинами [6]. Це свідчить про необхідність підвищеної обізнаності молоді щодо онлайн-загроз і правових механізмів захисту.

Правове регулювання кібербулінгу в Україні здійснюється через низку положень Кримінального кодексу (ст. 120, 129, 163) та Кодексу України про адміністративні правопорушення (ст. 173-4) [7]. Крім того, існують механізми правового реагування: звернення до поліції та Кіберполіції, використання гарячих ліній та правових консультацій, а також інформування адміністрацій навчальних закладів. Як відзначає

М. О. Гончаренко, профілактична робота та правове просвітництво серед учнів є ключовими для зменшення негативного впливу інтернету на молодь [8].

Для ефективного протидіяння кібербулінгу серед молоді необхідно впровадити комплексний кримінально-правовий та превентивний підхід, який передбачає системне поєднання законодавчих, правоохоронних та освітніх заходів. По-перше, необхідно законодавчо визначити кібербулінг як окреме правопорушення з чіткими критеріями суспільної небезпечності, враховуючи повторність дій, анонімність, груповий характер поведінки та вік учасників. По-друге, слід запровадити диференційовану кримінальну відповідальність, яка враховує тяжкість завданої шкоди та соціальну вразливість потерпілих, зокрема молоді та учасників освітнього процесу.

Важливим елементом є інтеграція державних органів, правоохоронних структур, освітніх установ і операторів цифрових платформ у механізми запобігання та розслідування кібербулінгу. Для цього слід встановити обов'язок освітніх закладів і цифрових платформ своєчасно інформувати правоохоронні органи про випадки кібербулінгу та зберігати цифрові докази, що підвищує ефективність притягнення винних до відповідальності і забезпечує належний захист потерпілих.

Не менш значущим є впровадження превентивних і просвітницьких заходів, включаючи підвищення цифрової грамотності, навчання безпечній поведінці в інтернеті, надання психологічної підтримки постраждалим та консультацій молоді, яка перебуває у групі ризику. Це дозволяє формувати відповідальну поведінку користувачів, запобігати проявам кібербулінгу та створювати безпечне цифрове середовище.

Також доцільно впроваджувати системи моніторингу, аналізу та оперативного виявлення кіберзлочинів серед молоді, що забезпечує своєчасне реагування на нові загрози і мінімізує негативні наслідки. Комплексний підхід повинен передбачати поєднання кримінально-правових, освітніх та технологічних заходів, що робитиме систему захисту молоді у цифровому середовищі ефективною, системною та адаптованою до сучасних умов глобальної мережі.

Таким чином, ефективна протидія кібербулінгу потребує комплексного підходу, що включає наукові дослідження, правові механізми та активну просвітницьку діяльність. Необхідно

визнавати існування проблем, відкрито обговорювати їх та разом шукати шляхи безпечного та свідомого використання цифрових ресурсів молоддю.

Список використаних джерел

1. Лисенко І. О. Кібербулінг серед підлітків: психологічні аспекти та сучасні виклики. Київ, 2020. 120 с.
2. Кравченко Т. В. Вплив дистанційного навчання на психосоціальний розвиток учнів. Львів, 2021. 98 с.
3. Ковальчук О. В. Соціальні мережі та онлайн-маніпуляції: ризики для молоді. Харків, 2022. 135 с.
4. Петренко С. В. Форми та методи кібербулінгу: емпіричне дослідження. Одеса, 2021. 110 с.
5. Петрів С. В. Цифрова агресія та соціальні платформи: сучасні тенденції. Київ, 2022. 142 с.
6. Іваненко А. П. Використання молоді в інформаційних війнах: аналіз ризиків. Київ, 2023. 115 с.
7. Кримінальний кодекс України / Верховна Рада України. Київ, 2020.
8. Гончаренко М. О. Профілактика кібербулінгу та правове просвітництво серед учнів. Львів, 2021. 103 с.

Голікова Мілена Олексіївна,
здобувач ступеня вищої освіти бакалавра навчально-наукового інституту права та психології Національної академії внутрішніх справ
Науковий керівник:
Резнік Ю. С., старший викладач кафедри кримінального права та кримінології навчально-наукового інституту права та психології Національної академії внутрішніх справ, кандидат юридичних наук

ВІКТИМОЛОГІЧНИЙ ПОРТРЕТ ТА МОДЕЛІ ПОВЕДІНКИ ЖЕРТВ КІБЕРЗЛОЧИНІВ

Розвиток інформаційних технологій не стоїть на місці і з кожним днем все глибше входить у всі сфери нашого життя. На сьогоднішній день навіть наймолодший українець має телефон

або планшет із доступом в Інтернет, має месенджери для зв'язку з батьками та доступ до різноманітних онлайн ігор. Не відстає і старше покоління. Зараз зустрічається все менше дідусів і бабусь із кнопковими телефонами, життя заполонили смартфони. Та чи безпечною для усіх є ця повальна цифровізація?

Безперечно, використання цифрових можливостей несе неабияку користь, але й небезпека існує. Згадайте, скільки разів вам доводилось отримувати повідомлення у телеграмі на кшталт «Моя дитина бере участь у конкурсі малюнка, проголосуй за неї за цим посиланням» або дзвінки із повідомлення про виграш, отримати який можливо всього-на-всього продиктувавши пароль з смс. Всі ці, безневинні на перший погляд, дії – ознаки кібератаки на вас та ваші пристрої. Так, це дрібниця у порівнянні з кібератаками на великі підприємства, критичну інфраструктуру або державні бази даних, але ці дрібниці несуть неабияку шкоду – втрачаються персональні дані, дані платіжних систем, відбувається крадіжка коштів або використання персональних даних для оформлення кредитів. Те, що здається дрібницею у масштабах країни, є трагедією для окремої людини.

Для початку розберемось, що таке «кіберзлочин». Відповідно до закону України «Про основні засади забезпечення кібербезпеки України» під поняттям «кіберзлочин (комп'ютерний злочин)» варто розуміти «суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України» [1]. У цьому ж законі знаходимо і значення поняття «кібератака», під якою розуміється «спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) у комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних

систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту» [1].

Незважаючи на те, що сам термін «кіберзлочин» розкрито лише у зазначеному вище законі України, злочинам з використанням кіберпростору присвячено цілий розділ у Кримінальному кодексі України. Йдеться про розділ XVI «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку».

Ціллю будь-якої кібератаки є порушення конфіденційності, а також отримання доступу до інформації, зокрема персональної інформації користувача. Для кібератак часто використовується різноманітне шкідливе програмне забезпечення, яке умовно можна розділити на такі групи:

1. Backdoor – шкідливий програмний код, який встановлюється в систему, щоб надати зловмиснику віддалений доступ. Бекдори зазвичай дозволяють підключитися до комп'ютера з мінімальною аутентифікацією або зовсім без такої і виконувати команди в локальній системі.

2. Downloader – шкідливе програмне забезпечення, єдиною метою якого є завантаження іншого шкідливого програмного коду. Зазвичай встановлюють завантажувачі при першому доступі до системи.

3. Stealer – шкідливе програмне забезпечення, яке збирає інформацію на комп'ютері жертви і, як правило, відправляє її зловмисникові. Як приклад можна привести програми, що збирають хеші паролів, перехоплювачі й кейлогери. Дане ШПЗ використовується для отримання доступу до облікових записів інтернет додатків, таких як електронна пошта або інтернет-банкінг.

4. Rootkit – шкідливе програмне забезпечення, що приховує існування іншого коду. Руткіти зазвичай застосовуються в поєднанні з іншим ШПЗ, таким як бекдор, що дозволяє їм відкрити зловмисникові доступ до системи і ускладнити виявлення коду.

5. Вірус-вимагач (ransomware). Тип шкідливого програмного забезпечення, що блокує доступ до системи або унеможливлює роботу з файлами (часто за допомогою методів шифрування), після чого вимагає від жертви викуп для відновлення вихідного стану.

6. Keylogger – програмне забезпечення, що реєструє кожну дію користувача, наприклад з пристроїв вводу (рух комп'ютерної миші, натиснення кнопок клавіатури). Дозволяє заволодіти даними користувача, що були введені після його встановлення [2].

Однак усі перераховані вище способи кібератак стосуються в першу чергу комп'ютерних мереж та персональних комп'ютерів користувачів великих підприємств чи організацій. У випадку ж коли жертвою кіберзлочину є звичайний пересічний громадянин, найчастіше використовується «фішинг».

Фішингом називають атаку, метою якої є отримання доступу до конфіденційної інформації користувачів – логінів, паролів, платіжних даних тощо. Це досягається шляхом проведення масових розсилок електронних листів або повідомлень в соціальних мережах. Часто це робиться від імені відомих організацій, наприклад банків, або від імені знайомих користувачів. При цьому використовуються технічних засобів і засобів соціальної інженерії, які мають на меті введення в оману авторизованих користувачів і спонукання їх до розкриття персональних даних через створення копій сайтів, повідомлень подібних до легальних і знайомих користувачам.

Фішинг є одним із найпростіших способів отримання персональних даних, розрахований на персональну необережність та неуважність користувача. Фактично, такий «прямий фішинг» змушує користувача абсолютно свідомо ввести свої персональні дані та надати їх зловмисникам.

Беззаперечно, жертвою кіберзлочину може стати кожен, але все ж таки можливо виокремити певні віктимологічні ознаки потенційної жертви. Під віктимністю науковці розуміють уразливість членів суспільства перед злочинними посяганнями за певних ситуацій. Віктимність як явище – це властивість соціального суб'єкта наражатися на небезпеку злочинних посягань за певних обставин, ситуацій або внаслідок дій інших осіб [3, с. 8]. Таким чином, під віктимологічними ознаками варто розуміти такі собі дії, що вчиняє сама жертва, які полегшують можливість злочинцю вчинити злочин.

На мою думку, основними ознаками потенційної жертви кіберзлочину є: необережність, самовпевненість та наївність. Розглянемо кожну із наведених ознак окремо. Необережність користувача зазвичай проявляється у ігноруванні обов'язкових ознак, що вказували б на «реальне», а не «фішингове»

повідомлення. Наприклад, користувач отримує у месенджер повідомлення нібито від банку, але номер телефону – звичайний номер із кодом мобільного оператора, а посилання, на яке необхідно натиснути для того щоб перейти на сторінку банку, відрізняється від справжнього на одну-дві літери у адресі. Окрім того, зазвичай за такими посиланнями знаходяться сайти, на яких відсутній протокол безпеки, що вказує на його незахищеність.

Самовпевненість користувача зазвичай проявляється у випадках, коли користувач самостійно чинить дії із потенційно небезпечним контентом, вважаючи, що його проблема обійде стороною. Необережність часто проявляється при завантаженні файлів із сторонніх ресурсів, або самостійному введенні своїх особистих даних на ресурсах, що пропонують легкі гроші. У таких випадках користувач часто розуміє, що чинить неправильно, але вважає, що він жертвою не стане.

Наївність потенційної жертви кіберзлочину – найзручніша ознака для кіберзлочинця. Потенційній жертві обіцяють певну вигоду, або банально грають на її почуттях для того, щоб у подальшому отримати від неї необхідні дані. На наївності грають повідомлення щодо виграшу або державної допомоги, повідомлення щодо необхідності проголосувати у конкурсі чи пройти опитування.

Окрім того, якщо говорити про вік потенційної жертви, то більш вразливими є або наймолодші користувачі, або люди старшого покоління. Чому? Саме через необережність та певну наївність.

Так, на мою думку, люди похилого віку є більш вразливою ланкою суспільства. Наші люди старшого покоління не завжди обізнані в гаджетах. Вони живуть самі, або їх родичі далеко, та нема кому їм пояснити, як користуватися інтернетом та скільки в ньому потенційних злочинців. Приклад кіберзлочину, направленого на людей старшого віку, може бути повідомлення щодо надання такої собі послуги як Є-допомога. Довіра до назви, що вже не перший рік на слуху та викликає асоціації з державною допомогою, а також часта потреба у додаткових фінансах, спонукає потенційну жертву повірити у реальність такого повідомлення та вчинити всі дії, що необхідні злочинцю.

Іншою вразливою віковою групою є діти та молодші підлітки. Діти є наївними, їх легше вести в оману. Коли їм приходить повідомлення, наприклад, з акаунту їх друзів з

посиланням на ігрову валюту у популярних онлайн іграх (Roblox, Minecraft, Brawl Stars тощо), наївність та довіра не дозволяють їм запідозрити, що за цей акаунт був зламаний, а пропозицію щодо безкоштовної вигоди їм надає шахрай. Підлітки вже не такі наївні, тут більше грає зухвалість, віра в те, що вони будуть хитрішими. І навіть при наявності підозри щодо того, що посилання надійшло від шахрая, зухвалість спонукає перейти і подивитись, що буде далі.

Таким чином, відповідно до зазначеного вище, можна зробити наступні висновки. Найпопулярнішим кіберзлочином та методом кібершахрайства є «фішинг».

Віктимологічний портрет жертви кіберзлочину має такі ознаки: необережність, самовпевненість та наївність. А найбільш вразливими віковими групами є люди старшого покоління, діти та молодші підлітки.

Відповідальність за те, щоб не стати жертвою кіберзлочину лежить на кожному з нас особисто, тобто кожному треба слідкувати як і що він робить щоб не стати жертвою кіберзлочину. Загальні рекомендації залишаються незмінними: не переходити за невідомими посиланнями, перевіряти файли, які ви хочете завантажити, перевіряти протоколи безпеки на сайтах, на які заходити та не вводити особисті авторизаційні або платіжні дані на підозрілих сайтах. Краще тричі перевірити, аби потім не стати жертвою шахрая.

Список використаних джерел

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

2. Бикова Т. М., Гомон В. О., Голікова О. В. Розповсюдження шкідливого програмного забезпечення з метою отримання доступу до інформаційних систем. *Шкідливі програми як загроза об'єктам критичної інфраструктури в умовах кібервійни* : збірник матеріалів міжвідомчого круглого столу (Київ, 21 лют. 2023 р.). Київ : ІСТЕ СБУ, 2023. С. 24–28.

3. Головкін Б. М. Віктимність як основна категорія віктимології. *Журнал східноєвропейського права*. 2015. № 20. С. 6–13.

Горошко Юлія Андріївна,
здобувач ступеня вищої освіти магістра навчально-наукового інституту права та психології Національної академії внутрішніх справ
Науковий керівник:
Шрамко С. С., завідувач кафедри кримінального права та кримінології навчально-наукового інституту права та психології Національної академії внутрішніх справ, кандидат юридичних наук, старший дослідник

ВІКТИМОГЕННІ ФАКТОРИ У СФЕРІ КІБЕРБЕЗПЕКИ: ДОСЛІДЖЕННЯ КОРЕЛЯЦІЇ РІВНЯ ЦИФРОВОЇ ОБАЧНОСТІ

Прогресивна цифровізація економічних процесів, та становлення цифрової економіки є детермінантами якісної трансформації кримінальних діянь, що проявляється у формі шахрайства та набуває нових форм і модифікує способи свого вчинення [1, с. 22].

Під впливом цифрових технологій шахрайство набуло нових, високотехнологічних форм, а саме: фішингових атак, створення підроблених вебресурсів, використання шкідливого програмного забезпечення для викрадення фінансової інформації, підміни SIM-карт, генерації штучних голосів і зображень за допомогою технологій deepfake, а також автоматизованих схем обману через платформи електронної комерції, онлайн-банкінг [2].

Ключовими віктимогенними чинниками у сфері кібербезпеки є низький рівень цифрової грамотності, неусвідомлене поширення персональних даних, схильність до довірливої поведінки онлайн, відсутність навичок розпізнання фішингових атак, використання слабких або повторюваних паролів, а також недосконалості управлінських механізмів експлуатації та контролю за дотриманням протоколів кіберзахисту. Ці та інші детермінанти створюють сприятливе криміногенне середовище для успішних кібератак, що становить загрозу сталому функціонуванню об’єктів критичної інфраструктури та конфіденційності персональних даних фізичних осіб [3].

Зокрема, такий випадок трапився 12 грудня 2023 року, коли хакери атакували ядро мережі «Київстару». Тоді зловмисникам вдалося це зробити через злам акаунту одного з партнерів компанії внаслідок чого без зв'язку опинилися близько 24 млн абонентів. Атака на віртуальну інфраструктуру виявилась успішною, хакерам вдалося знищити 40 % інфраструктури, використовуючи стилер Mimikatz, який збирає інформацію на комп'ютері жертви та передає хакерам [4]. Подібні приклади ставалися і через через DDoS-атаки, завдані банківським установам, центральним органам державної влади, критичній інфраструктурі, офіційним ресурсам Міністерства оборони та Збройних Сил України [5].

Успішне протистояння кіберзагрозам вимагає комплексного регулювання, а саме впровадження програм з підвищення цифрової грамотності, що включатимуть курси кібергігієни для мінімізації віктимогенності користувачів, та запровадження систематичних тренінгів і симуляційних атак для забезпечення стійкості їхніх інформаційних систем [6].

Ще одним із аспектів кіберзагроз є інформаційна агресія, а саме вплив на громадську думку, що має тривалі наслідки. Пропаганда створює викривлене уявлення про реальність, маніпулює настроями у суспільстві. Через соціальні мережі та інші цифрові канали поширюються матеріали, спрямовані на розкол у суспільстві та розпалювання ворожнечі.

Слід зазначити, що на відміну від традиційних форм віктимізації, у цифровому середовищі ключову роль відіграє поведінковий компонент, тобто те, як особа здійснює власну «онлайн-навігацію», сприймає інформацію, та, наприклад, управляє своїми цифровими активами. У центрі цієї моделі стоїть цифрова обачність – особистісний ресурс, який визначає здатність до безпечної поведінки в Інтернеті. Така поведінка охоплює знання, навички, когнітивні фільтри та стратегії уникнення ризиків віктимізації. Отже, кореляція між цифровою обачністю та ймовірністю віктимізації проявляється у зворотній залежності: чим вищий рівень обачності, тим нижчий ризик потрапляння у шахрайські, маніпуляційні чи інші небезпечні ситуації в інтернет-просторі.

Таким чином, кібербезпека потребує, насамперед, комплексного державного підходу, глобальною метою якого є мінімізація ризиків як для окремих громадян, так і держави в

цілому. Зважаючи на те, що людський чинник у детермінації кіберзлочинів є домінуючим, то актуальним є формування культури інформаційної безпеки в суспільстві, яка включатиме навички безпечної поведінки у цифровому середовищі, критичне мислення та способи виокремлення потенційних загроз.

Список використаних джерел

1. Коновалова О. І. Запобігання шахрайству у сфері електронної торгівлі : дис. … д-ра філософії. URL: https://dspace.nlu.edu.ua/bitstream/123456789/19894/1/Konovalova_dis.pdf (дата звернення: 07.11.2025).

2. Шахраї у 2025 році: 6 найпопулярніших схем, на які ведуться люди. URL: https://www.rbc.ua/rus/news/shahrayi-2025-rotsi-6-naypopulyarnishih-shem-1755871833.html

3. Свердлик З. Кібербезпека та кіберзахист: питання порядку денного в українському суспільстві. *Український журнал з бібліотекознавства та інформаційних наук*. 2022. № 10. С. 175–188.

4. Коваль О. Якою була атака хакерів на «Київстар» та як відновлювалась компанія. URL: https://dou.ua/lenta/news/kyivstar-cyber-attack-restoration/.

5. Приват24, Ощадбанк, сайти Міноборони, ЗСУ, Українського радіо зазнали DDoS-атаки. URL: https://suspilne.media/207368-privat24-ne-pracuvav-cerez-pereboi-zi-zvazkom-ci-bula-ddos-ataka-zasovuut-fahivci-pressluzba/.

6. Державна служба спеціального зв'язку та захисту інформації України. Як протидіяти кіберзагрозам та захистити системи від ворожих кібератак – важливі рекомендації та допомога CERT-UA. URL: https://www.kmu.gov.ua/news/yak-protydiiaty-kiberzahrozam-ta-zakhystyty-systemy-vid-vorozhykh-kiberatak-vazhlyvi-rekomendatsii-ta-dopomoha-cert-ua.

Денисенко Дмитро Миколайович,
здобувач ступеня вищої освіти бакалавра навчально-наукового інституту права та психології Національної академії внутрішніх справ
Науковий керівник:
Резнік Ю. С., старший викладач кафедри кримінального права та кримінології навчально-наукового інституту права та психології Національної академії внутрішніх справ, кандидат юридичних наук

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ВЧИНЕННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ: ВИКЛИКИ ДЛЯ КРИМІНАЛЬНОГО ПРАВА

Стрімкий розвиток технологій штучного інтелекту (ШІ) суттєво трансформував багато сфер суспільного життя – від економіки, освіти та медицини до систем безпеки. Однак разом із позитивними змінами виникають і нові загрози: сьогодні злочинні суб'єкти дедалі активніше застосовують ШІ як інструмент для вчинення кримінальних правопорушень. Це явище являє собою не просто еволюцію існуючих злочинних схем, але і якісно новий фронт ризиків для кримінального права, правоохоронних органів та суспільства в цілому [1].

Зокрема, одним із найпомітніших трендів є використання технологій deepfake – створення надзвичайно реалістичних відео- або аудіоматеріалів, які можуть бути використані для шантажу, вимагання коштів, дискредитації публічних осіб чи приватних громадян. У відомих випадках шахраї імітували голоси керівників компаній або державних службовців, змушуючи працівників переводити значні кошти на підконтрольні шахраям рахунки [2]. Паралельно з цим формуються нові моделі фішингових атак: ШІ дозволяє генерувати високоперсоналізовані повідомлення, адаптовані під конкретну особу, що робить їх значно ефективнішими, ніж традиційні розсильні листи [3]. Додатково ШІ використовується у кіберзлочинності для створення шкідливого програмного забезпечення, пошуку вразливостей або проведення атак без прямої участі людини.

Автоматизація в цій сфері дозволяє злочинцям одночасно атакувати тисячі жертв по всьому світу, що раніше було технічно значно складніше. Генеративні моделі глибокого навчання також сприяють фальсифікації доказів – створенню зображень, аудіо чи відео, які практично не вирізняються від справжніх, і це істотно ускладнює кримінальне переслідування та доведення провини [4].

Використання ШІ у злочинній діяльності породжує низку серйозних викликів для традиційної системи кримінального права. По-перше, алгоритм як такий не має умислу (mens rea), і тому класичні підходи до визначення вини або відповідальності стають недостатніми. Хто має нести відповідальність – розробник алгоритму, провайдер, хостинг-платформа чи кінцевий користувач – часто не визначено чітко, що створює правову невизначеність. По-друге, збору та перевірці цифрових доказів потрібна спеціалізована експертиза та ретельне логування, що не завжди забезпечується на рівні правоохоронних органів. По-третє, злочини із застосуванням ШІ часто мають транскордонний характер, що ускладнює розслідування: юрисдикції перетинаються, обмін доказами та співпраця між країнами – не завжди налагоджені.

Додатково автоматизація та масштабність атак (наприклад, одночасне застосування ШІ-базованих схем на тисячі жертв) роблять традиційні правові механізми – реагування, переслідування, санкції – малоефективними. Нарешті, законодавство значною мірою відстає від технологічного прогресу: нові форми злочинів вже реалізуються, тоді як нормативна база часто ще не адаптована до них [5].

У міжнародному контексті можна виділити приклади нормативної та практичної відповіді на виклики, пов’язані із ШІ. У межах AI Act Європейського Союзу встановлено рамки щодо ризикованих систем ШІ та передбачено відповідальність за зловживання ними [6]. У США правоохоронні органи видають рекомендації та попередження щодо використання технологій deepfake у шахрайських схемах, а також обговорюються кримінальні санкції за створення чи розповсюдження deepfake без згоди особи. У сукупності міжнародна практика демонструє, що ефективна протидія злочинам із застосуванням ШІ потребує системного підходу: узгодження нормативної бази, технологічних стандартів і міжнародного співробітництва.

До заходів, які вже вживаються або обговорюються, належать: обов'язкове збереження логів та метаданих платформ, що надають доступ до систем ШІ; розробка стандартів цифрової криміналістики для верифікації AI-контенту; створення міжнародних каналів співпраці для розслідування транскордонних злочинів; залучення експертів із кібербезпеки та технологій ШІ до кримінальних проваджень; розробка методик доказування вини та атрибуції у справах, пов'язаних із ШІ.

Окрім цього, обговорюється введення окремого складу злочину «використання технологій ШІ з метою вчинення кримінальних правопорушень», адміністративна та кримінальна відповідальність для провайдерів, які не забезпечують адекватні механізми безпеки, обов'язок розробників зберігати історію використання ШІ, маркування контенту, створеного алгоритмами, та система оперативного реагування на шкідливий контент.

Крім вищезгаданих правових і технологічних заходів, ключове місце належить і просвітницьким ініціативам з підвищення цифрової грамотності суспільства. Навіть найсучасніші технології захисту виявляються недостатніми, якщо користувачі не здатні розпізнати шахрайські схеми чи ознаки маніпуляцій. Освітні програми та тренінги для працівників державних установ, приватних компаній і громадськості повинні включати навчання щодо потенційних ризиків ШІ, методів безпечної взаємодії з цифровими системами та ознак активних атак. Водночас важливо розвивати міждисциплінарну співпрацю – поєднувати зусилля юристів, правоохоронців, фахівців із технологій, етиків та соціологів, щоб адекватно аналізувати та реагувати на злочини XXI століття.

Отже, використання ШІ у кримінальній діяльності становить одну з найсерйозніших загроз для системи кримінального права сьогодні. Злочини із застосуванням ШІ важко розслідувати, важко довести і ще важче попередити, що вимагає від правової системи, технологічного сектору та суспільства оновлення підходів. Необхідна модернізація законодавства, підвищення технічної грамотності правоохоронців, впровадження технічних стандартів і міжнародна координація. Штучний інтелект – потужний

інструмент, який може бути використаний як на благо, так і на шкоду; лише взаємодія держави, технологічного сектору, правової системи та суспільства дозволить мінімізувати ризики його зловживання та зберегти потенціал для розвитку науки, економіки й соціальних сфер.

Список використаних джерел

1. Gupta et al. (2024). *Digital deception: generative artificial intelligence in social engineering and phishing*. Artificial Intelligence Review, 57:324. SpringerLink

2. Chenchi Reddy, K., & Saleem, M. (2025). *The dark side of AI: How criminals leverage machine learning for illicit activities in the context of assault*. International Journal of Intelligent Systems and Applications in Engineering, 13(1). IJISAE

3. Riurean, P., Bolog, G., & Riurean, S. (2024). *The rise of sophisticated phishing. How AI fuels cybercrime*. Journal of Digital Science, 6(2), 15-25. Institute of Cited Scientists

4. Seidlitz, S., Dittmann, J. (2024). *Media forensic considerations of the usage of artificial intelligence using the example of DeepFake detection*. J. Imaging, 10(2):46. MDPI

5. «AI and Serious Online Crime». Centre for Emerging Technology and Security report. cetas.turing.ac.uk

6. «AI-deepfake scams and the importance of a holistic communication security strategy». International Cybersecurity Law Review, 6:53-61 (2025). SpringerLink

Добровольська Тетяна Миколаївна,
здобувач ступеня вищої освіти магістра інституту заочного та дистанційного навчання Національної академії внутрішніх справ
Науковий керівник:
Шрамко С. С., завідувач кафедри кримінального права та кримінології навчально-наукового інституту права та психології Національної академії внутрішніх справ, кандидат юридичних наук, старший дослідник

КІБЕРБЕЗПЕКА У ВОЄННИЙ ЧАС: НОВІ ТЕНДЕНЦІЇ ТА ПРАВОВІ АСПЕКТИ

Кібербезпека у воєнний час охоплює правові, організаційні, технічні й інформаційні механізми, спрямовані на захист цифрового простору держави. Вона включає діяльність спеціально уповноважених суб'єктів, наділених відповідними повноваженнями у сфері протидії кіберзагрозам, які використовують методи, засоби та технології для виявлення, запобігання й нейтралізації небезпечних впливів на інформаційні ресурси.

Кібербезпеку також можна розглядати як рівень захищеності національних інформаційних ресурсів від зовнішніх і внутрішніх загроз, зокрема кібератак, інформаційних диверсій та спроб несанкціонованого втручання у функціонування інформаційно-телекомунікаційних систем.

Цифровий простір став одним із ключових фронтів протистояння в умовах повномасштабної війни. Кібератаки, інформаційні диверсії та спроби несанкціонованого втручання у роботу державних і військових систем стали складовою гібридної агресії російської федерації. У зв'язку з цим забезпечення національної кібербезпеки є критично важливим елементом обороноздатності держави, а її правове, організаційне та технічне регулювання потребує постійного вдосконалення.

Закон України «Про основні засади забезпечення кібербезпеки України» визначає поняття кіберзлочин або комп'ютерний злочин як суспільно-небезпечні дії, як умисні, так

і вчинені з необережності, що здійснюються у кіберпросторі або з його використанням; кримінальна відповідальність за такі діяння передбачена Кримінальним кодексом України [1]. Метою таких протиправних дій часто стає викрадення або знищення інформації, порушення роботи інформаційних систем чи мереж. Особливо в умовах війни кіберзлочинці спрямовують свої зусилля на дестабілізацію державних інститутів, на завдання шкоди інфраструктурі, порушення функціонування обладнання і доступу до секретних даних.

У згаданому законі говориться, що об'єктами атак виступають системи, від функціонування яких залежить стабільність держави: інформаційні ресурси органів державної влади, Збройних Сил України, правоохоронних органів, засобів масової інформації та інших структур, що здійснюють комунікацію між державою і суспільством [1].

До категорії критичних об'єктів також належать енергетичні та промислові підприємства, зокрема атомні електростанції та підприємства хімічної галузі. Їх інформаційно-комунікаційні системи віднесено до критичної інфраструктури про що йдеться у Законі України «Про критичну інфраструктуру», з огляду на потенційну небезпеку наслідків їх порушення для життя, здоров'я людей і національної безпеки держави [2]. Підвищена увага спрямована й до транспортних мереж, системи електронного урядування, електронної комерції та документообігу, які забезпечують безперервність функціонування державних послуг та економічних процесів. Важливою складовою є також фінансовий сектор — банківські установи, платіжні системи та інші сервіси, збої у роботі яких можуть викликати масштабні економічні ризики. Саме тому законодавець відносить такі структури до секторів критичної інфраструктури, які потребують особливого режиму захисту [3].

З початком повномасштабної воєнної агресії проти України суттєво зросла кількість кібератак, спрямованих як на державні, так і на приватні структури. Одним із прикладів стала спроба кібератаки, здійсненої хакерським угрупованням Strontium (APT28), яке намагалося проникнути в комп'ютерні мережі України, Сполучених Штатів Америки та країн Європейського Союзу. Метою було отримання тактичної інформації для підтримки військових дій росії та викрадення конфіденційних даних, що стосуються державних і безпекових структур [4].

Фахівці Державної служби спеціального зв'язку та захисту інформації України неодноразово фіксували нові спроби фішингових розсилок, відкриття яких давало можливість хакерам встановити шкідливе програмне забезпечення та отримати повний контроль над зараженими пристроями [5]. Схожі атаки були із застосуванням шкідливого програмного забезпечення Cobalt Strike Beacon, яке використовувалося російськими хакерами для ураження державних інформаційних систем було із спробою компрометації комп'ютерів державних органів через розсилку заражених документів [6].

Вважливим елементом кіберзахисту держави стала співпраця уряду та українського IT-сектору. Провідні компанії галузі об'єднали зусилля для протидії кібератакам, які спрямовуються проти об'єктів критичної інфраструктури, державних ресурсів та бізнесу. IT-фахівці здійснюють моніторинг, виявлення й нейтралізацію ворожих кіберзагроз, включно з діяльністю російських хакерських угруповань і бот-мереж, а також сприяють безперервному функціонуванню цифрових сервісів. Наприклад, компанія GigaCloud, яка під час активних бойових дій безкоштовно здійснила міграцію дата-центру Prozorro з Києва до Львова, забезпечивши збереження критичних даних та безперервність роботи державної електронної системи закупівель, попри ракетні обстріли [7].

З урахуванням зазначених інцидентів, кримінальна відповідальність за певні діяння, які пов'язані з кіберзлочинністю, була посилена. Стаття 361-1 Кримінального кодексу України, чітко передбачає відповідальність за створення або розповсюдження шкідливих програмних чи технічних засобів, що можуть бути використані для несанкціонованого втручання в роботу комп'ютерів, автоматизованих систем, мереж або мереж електрозв'язку [8].

Законодавцем розширено перелік кримінально караних дій у сфері несанкціонованого втручання в роботу комп'ютерних систем, а також передбачено більш суворі санкції у випадках, коли такі злочини завдають шкоди об'єктам критичної інфраструктури держави [9], та удосконалено процедури виявлення, документування та розслідування кіберзлочинів, що дозволяє правоохоронним органам оперативніше реагувати на кібератаки та підвищує ефективність притягнення винних до відповідальності [10].

Підсумовуючи викладене, зазначимо таке:

1. Зростання кількості ворожих кібератак, спроб проникнення хакерських угруповань у мережі державних установ і оборонних структур України, підтверджує реальність та масштабність кіберзагроз.

2. Сучасні воєнні конфлікти значною мірою виходять за межі традиційного бойового протистояння, саме тому захист держави у цифровій сфері стає рівнозначним із забезпеченням її обороноздатності.

3. В умовах воєнного стану кібербезпека постає як технічним та інформаційним питанням, так і складовою національної безпеки, без якої неможливе стабільне функціонування держави, її економіки та систем управління.

4. Актуалізується необхідність правового, організаційного та технологічного забезпечення стійкості держави перед зростаючими кіберзагрозами, що є невід'ємною частиною сучасних воєнних дій.

Список використаних джерел

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII : станом на 20 квіт. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

2. Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX : станом на 21 верес. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text

3. Про затвердження Порядку ведення Реєстру об'єктів критичної інфраструктури, включення таких об'єктів до Реєстру, доступу та надання інформації з нього : постанова Кабінету Міністрів України від 28.04.2023 № 415. URL: https://zakon.rada.gov.ua/laws/show/415-2023-п#Text

4. Яворович Т. Корпорація Microsoft запобігла спробам хакерів ГРУ атакувати українські інституції. *Суспільне новини*. URL: https://suspilne.media/226405-korporacia-microsoft-zapobigla-rosijskim-kiberatakam-na-ukrainski-organizacii.

5. Державна служба спеціального зв'язку та захисту інформації України. Хакери розсилають військовослужбовцям ЗСУ повідомлення зі шкідливим програмним забезпеченням під виглядом рекрутингу до 3 ОШБр та ЦАХАЛ. cip.gov.ua. URL: https://cip.gov.ua/ua/news/khakeri-rozsilayut-viiskovosluzhbovcyam-zsu-povidomlennya-zi-shkidlivim-programnim-zabezpechennyam-pid-viglyadom-rekrutingu-do-3-oshbr-ta-cakhal.

6. Veronika Telychko. Cobalt Strike Beacon Malware Detection: A New Cyber-Attack on Ukrainian Government Organizations Attributed to the UAC-0056 Group. socprime.com. URL: https://socprime.com/blog/cobalt-strike-beacon-malware-detection-a-new-cyber-attack-on-ukrainian-government-organizations-attributed-to-the-uac-0056-group/?utm_source=chatgpt.com.

7. Lviv It Cluster. Хмарний оператор GigaCloud запустив оновлений дата-центр у Львові. Чому це важливо для бізнесу під час війни. itcluster.lviv.ua. URL: https://itcluster.lviv.ua/hmarnyj-operator-gigacloud-zapustyv-onovleny.

8. Кримінальний кодекс України : Кодекс України від 05.04.2001 № 2341-III : станом на 17 лип. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text

9. Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану : Закон України від 24.03.2022 № 2149-IX. URL: https://zakon.rada.gov.ua/laws/show/2149-20#Text

10. Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам : Закон України від 15.03.2022 № 2137-IX. URL: https://zakon.rada.gov.ua/laws/show/2137-20#Text

Домашенко Аліна Олександрівна,
здобувач ступеня вищої освіти бакалавра навчально-наукового інституту права та психології Національної академії внутрішніх справ
Науковий керівник:
Козачина А. М., старший викладач кафедри кримінального права та кримінології навчально-наукового інституту права та психології Національної академії внутрішніх справ, доктор філософії

ФОРМУВАННЯ НАЦІОНАЛЬНОЇ СИСТЕМИ КІБЕРБЕЗПЕКИ В УМОВАХ ВОЄННИХ ЗАГРОЗ: ВИКЛИКИ, МІЖНАРОДНИЙ ДОСВІД ТА ШЛЯХИ ВДОСКОНАЛЕННЯ

Сучасний світ дедалі більше залежить від цифрових технологій, інтернету та інформаційних систем. Майже кожна сфера життя – від спілкування до банківських операцій – пов'язана з використанням мережевих сервісів. Однак разом із розвитком технологій зростає і рівень кіберзагроз. Сьогодні кіберзлочини охоплюють не лише приватних користувачів, а й великі компанії та державні установи [1, с. 12].

В умовах війни проти України питання кібербезпеки набуло особливого значення. Кібератаки стали складовою гібридної війни – вони спрямовані на порушення роботи державних установ, об'єктів критичної інфраструктури, інформаційних систем та фінансових установ [2]. Ефективна кібербезпека має бути побудована не лише на рівні держави, а й на рівні кожного громадянина та організації.

У літературі зазначається, що сучасні кіберзагрози, з якими стикається Україна, умовно можна розділити на чотири основні категорії:

1. Деструктивні атаки, зміст яких передбачає використання програм-руйнівників (wiper), як-от HermeticWiper, WhisperGate, які були зафіксовані в перші дні повномасштабного вторгнення. Метою цих атак є виведення з ладу систем управління, баз даних та пошкодження об'єктів критичної інфраструктури.

2. Фішингові атаки, значна частина яких реалізується через соціальну інженерію – від імені державних органів розповсюджуються фішингові листи, підроблені застосунки (наприклад, фейкові «Дія») з метою збору персональних даних або проникнення в інформаційні системи.

3. Кібершпигунство (тривале проникнення у комп'ютерні мережі з метою збору розвідданих, ураження комунікаційних систем або підготовки до фізичних атак) під час якого, зокрема, використовуються RAT-інструменти, модулі screen-capture, кейлогери.

4. Інформаційно-психологічні операції: дезінформація, поширення фейкових повідомлень, deepfake-відео, маніпуляція громадською думкою через Telegram-канали, Інтернет та соціальні мережі. Ці операції спрямовані, у першу чергу, на посилення напруги у суспільстві, дискредитацію державної влади України [3, с. 133].

Отже, ключові загрози інформаційній безпеці України мають комплексний характер і стосуються як технічної сфери, так і соціально-політичних процесів. Кіберзлочинність, поширення дезінформації, інформаційне шпигунство, а також прогалини в правовому регулюванні інформаційного простору зумовлюють потребу в цілісній державній політиці захисту національної інформаційної безпеки.

Європейські країни приділяють увагу навчанню населення основам цифрової безпеки. Наприклад, у багатьох країнах ЄС проводяться загальнонаціональні інформаційні кампанії та тренінги, які навчають громадян розпізнавати загрози в інтернеті [4]. Це формує культуру безпечної поведінки в цифровому середовищі, що є першою лінією оборони від кіберзлочинців.

У сучасній практиці все більше компаній переходять до концепції Zero Trust – «нульової довіри». Це означає, що кожна дія користувача або пристрою в мережі проходить перевірку, а доступ надається лише за принципом «необхідного мінімуму». Такий підхід зменшує можливість зламу навіть у випадку, якщо обліковий запис зловмисник отримає [4].

Досвід показує, що кібербезпека ефективна лише тоді, коли охоплює як технічні, так і організаційні заходи. Це підтверджується й дослідженнями українських фахівців, які вказують на важливість підготовки персоналу та внутрішніх інструкцій із кіберзахисту [1, с. 35].

Національний рівень кібербезпеки визначає здатність держави протидіяти масштабним атакам, захищати критичну інфраструктуру та забезпечувати стабільність інформаційного простору. Європейський Союз активно розвиває спільну політику у сфері кібербезпеки. У 2022 році була ухвалена NIS2 Directive, яка встановлює обов'язкові вимоги до кіберзахисту для енергетичного, транспортного, медичного, фінансового та інших важливих секторів [6].

Важливу роль у розробці стандартів і рекомендацій відіграє European Union Agency for Cybersecurity (ENISA). Це агентство аналізує кіберзагрози, публікує аналітичні звіти та допомагає державам координувати свої дії [4].

Хорошим прикладом ефективної кіберполітики є Естонія. Після масованої кібератаки у 2007 році країна створила розвинену систему кіберзахисту, у тому числі національний кіберцентр, систему резервного копіювання та проведення регулярних тренувань. Завдяки цьому Естонія вважається однією з найбільш захищених у цифровому просторі держав [6].

Зростаюча актуальність кіберсфери в міжнародних відносинах спонукала дедалі більше урядів інтегрувати оборонну стратегію в кібербезпеці та напад. Італія зробила значний крок, наслідуючи тенденцію НАТО. Завдяки італійському законодавству, Збройні сили зможуть наймати приватних хакерів та спеціалістів для проведення наступальних та оборонних цифрових операцій. Цей крок визнає, що сучасна війна — це не лише ракети чи дрони, а й контроль над критичною інфраструктурою та громадською думкою. До недавніх часів італійська кібербезпека переважно контролювалася Національним агентством кібербезпеки, але наразі Міністерство оборони має можливість діяти автономно навіть у мирний час, зосереджуючись на основній меті – захисті установ та громадян, зміцнення національного щита від атак на межі війни та проведення наступальних дій проти ворожих суб'єктів, якщо це необхідно. Адже кібервійна зараз є опорою сучасної геополітики.

В Україні також активно розвивається система національної кібербезпеки. Важливу роль відіграє Державна служба спеціального зв'язку та захисту інформації України, яка координує заходи з кіберзахисту, проводить спільні навчання з партнерами та забезпечує кібероборону державних інформаційних систем [7].

Центри (підрозділи) забезпечення кібербезпеки або кіберзахисту створено також у Службі безпеки України (СБУ), Національному банку України, Міністерстві інфраструктури України, Міністерстві оборони України та Збройних Силах України.

Активно розвивається співпраця у сфері кібербезпеки із зарубіжними партнерами (Сполучені Штати Америки, Сполучене Королівство Великої Британії та Північної Ірландії, Федеративна Республіка Німеччина, Королівство Нідерландів, Японія тощо), поглиблюється співпраця з ЄС та НАТО, проводиться кіберпідготовка за участю інших держав та міжнародних організацій.

Тож, розвиток системи кібербезпеки України здійснюється на основі досвіду побудови національної системи кібербезпеки; аналізу сильних та слабких сторін моделей кібербезпеки інших країн; практики організації роботи в цій сфері та взаємодії з іншими суб'єктами кібербезпеки. Заходи та засоби кіберзахисту спрямовані на оперативне реагування на кібератаки та інші кіберінциденти, та впровадження контрзаходів, спрямованих на мінімізацію вразливості систем зв'язку. У цьому контексті, на нашу думку, важливо не обмежуватися впровадженням лише сучасних технічних рішень, а й удосконалювати правові інструменти, зміцнювати міжнародну взаємодію та формувати належний рівень медіаграмотності громадян.

Кібербезпека – складна система, яка включає індивідуальні дії, організаційні заходи та державну політику. Це спільна відповідальність урядів, компаній та громадян. Без належної уваги до кожного з цих рівнів неможливо забезпечити надійний захист від сучасних кіберзагроз. Посилення безпеки інформації та мереж є основоположним для забезпечення захисту даних та стійкості до кіберзагроз. Досвід країн Європи свідчить, що лише спільна відповідальність громадян, бізнесу та держави дає реальні результати у боротьбі з кібератаками [5; 6]. Україна вже робить важливі кроки у цьому напрямку, але подальший розвиток кіберзахисту потребує інвестицій у освіту, кадри та міжнародну співпрацю.

З метою вирішення проблемних питань, пропозиціями щодо покращення може стати:

1. Розробка національної програми з кіберосвіти, яка охоплюватиме школярів, студентів та працівників державного сектору.
2. Посилення вимог до організацій щодо впровадження політик кібербезпеки та навчання персоналу.
3. Розвиток міжнародної співпраці з ЄС у сфері обміну досвідом та інформацією про кіберзагрози.
4. Кадровий та технологічний розвиток: збільшення кількості фахівців шляхом створення державних освітніх програм і стипендій у сфері кібербезпеки.
5. Проведення національних тренувань з кіберзахисту, які об'єднуватимуть державні органи, бізнес і громадські організації, підвищення обізнаності про важливість кібербезпеки.

Список використаних джерел

1. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко та ін.; за заг. ред. В. Б. Толубка. Київ : ДУТ, 2015. 288 с.
2. Матеріали з офіційного сайту Служба безпеки України. URL: https://ssu.gov.ua
3. Горун О. Ю. Кіберзагрози України в умовах агресії РФ. *Інформація і право*. 2025. № 3 (54). С. 131–138. URL: http://il.ippi.org.ua/article/view/340520
4. ENISA. Cybersecurity Education and Awareness. URL: https://www.enisa.europa.eu
5. Directive (EU) 2022/2555 (NIS2 Directive). URL: https://eur-lex.europa.eu
6. National Cybersecurity Strategy of Estonia. URL: https://www.mkm.ee
7. Матеріали з офіційного сайту Державна служба спеціального зв'язку та захисту інформації України. URL: https://cip.gov.ua

Дорошенко Анастасія Григорівна,
здобувач ступеня вищої освіти бакалавра факультету міжнародної торгівлі та права Державного торговельно-економічного університету;
Кудінова Дар'я Дмитрівна,
здобувач ступеня вищої освіти бакалавра факультету міжнародної торгівлі та права Державного торговельно-економічного університету
Науковий керівник:
Шведова Г. Л., доцент кафедри правового забезпечення безпеки бізнесу Державного торговельно-економічного університету, кандидат юридичних наук, доцент

КРИМІНАЛЬНО-ПРАВОВА ПРОТИДІЯ КІБЕРЗЛОЧИННОСТІ В УКРАЇНІ: АКТУАЛЬНІ ПИТАННЯ

У наш час стрімкий розвиток інформаційних технологій не тільки надає нам багато можливостей, а й породжує нові загрози – одною з них є кіберзлочинність. Це явище стало серйозним випробуванням для правової системи України і потребує не тільки оновлення законодавства, а й удосконалення механізмів його реалізації на практиці.

Кіберзлочинність, як явище – не просто сукупність правопорушень, а ціла система відповідних суспільно небезпечних діянь, які ставлять пвд загрозу державу та її інформаційну безпеку. В Україні, як і в більшості країн світу, відзначається швидке зростання кількості кібератак. Одним із найвідоміших випадків став вірус Petya, що в 2017 році спричинив зупинку роботи державних установ, банків та великих компаній. За інформацією Служби безпеки України, протягом 2024 року було знешкоджено близько 4000 кібератак, спрямованих на органи влади та об'єкти критичної інфраструктури. [1]

Можна погодитися з думкою А. В. Микитчика, що кіберзлочинність має низку специфічних рис: високотехнологічність, латентність, транскордонність і тісний

зв'язок з організованою злочинністю. Значну частину таких кримінальних правопорушень вчиняють професійні хакерські групи, які діють у міжнародних мережах і мають на меті отримання матеріальної вигоди. Особливо небезпечними формами є кібертероризм і кіберекстремізм, які можуть становити реальну загрозу життю людей та інформаційній безпеці держави. [2]

Кібертероризмом є злочинна діяльність, здійснена з використанням інформаційно-комунікаційних технологій**,** з метою дестабілізації суспільства або впливу на органи влади**.** До кібертерористичних дій відносяться: атаки на критичну інфраструктуру (енергетичні системи, транспорт, зв'язок), злам державних або військових інформаційних систем, поширення дезінформації з метою залякування населення.

Кіберекстремізм є використанням Інтернету чи цифрових технологій для пропаганди радикальних ідей**,** розпалювання ворожнечі, закликів до насильницьких дій з політичних, релігійних чи ідеологічних мотивів. Прикладами є: поширення в соцмережах екстремістських матеріалів, створення онлайн-спільнот для вербування учасників радикальних рухів, використання цифрових платформ для організації незаконних акцій тощо.

В Україні кримінальна відповідальність за кіберзлочини передбачена розділом 16 КК України. Санкції цих норм містять покарання від штрафу до позбавлення волі на строк від 3 до 15 років, залежно від тяжкості злочину завданих збитків та кваліфікуючих обставин. [3]

Щодо протидії з цій загрозі, справедливою є думка А. В. Микитчика про те, що: «Перш за все слід відійти від вирішення проблеми запобігання кіберзлочинності шляхом подолання існуючих тенденцій і перейти до активної розробки інформаційної безпеки на випередження. Також він зазначає, що необхідним є об'єднання зусиль всіх учасників, зацікавлених у запобіганні кіберзагрозам: правоохоронних органів, підприємницького середовища, громадських організацій, науково-дослідних установ і громадян». [2]

Підтримуючи цю позицію зазначимо, що ефективна протидія кіберзлочинності можлива лише за умови консолідації зусиль державних інституцій, правоохоронних органів, бізнес-сектору, наукового середовища та громадянського суспільства. Основними напрямами такої діяльності мають бути розвиток

професійного потенціалу фахівців у галузі кібербезпеки, розширення міжнародного співробітництва й обміну досвідом, а також утвердження правової культури безпечного та відповідального використання цифрових технологій.

Список використаних джерел

1. З початку року СБУ нейтралізувала майже 4 тис. кібератак на органи влади та критичну інфраструктуру України. Служба безпеки України. URL: https://ssu.gov.ua/novyny/460-kiberatak-i-20-khakerskykh-uhrupovan-neitralizuvala-sbu-z-pochatku-roku

2. Микитчик А.В. Заходи запобігання кіберзлочинності в Україні. Кримінально-правові та кримінологічні засоби протидії злочинам проти громадської безпеки та публічного порядку. Харків, 2019. URL: https://univd.edu.ua/general/publishing/konf/18_04_2019/pdf/63.pdf

3. Кримінальний кодекс України від 05.04.2001 р. URL: https://zakon.rada.gov.ua/laws/show/2149-20#Text

4. Никончук Н.С., Маслова О.О. Кіберзлочинність в Україні: виклики сучасності. URL: http://www.lsej.org.ua/9_2021/51.pdf

Зінченко Ірина Олександрівна,
здобувач ступеня вищої освіти бакалавра навчально-наукового інституту права та психології Національної академії внутрішніх справ
Науковий керівник:
Резнік Ю. С., старший викладач кафедри кримінального права та кримінології навчально-наукового інституту права та психології Національної академії внутрішніх справ, кандидат юридичних наук

ВІКТИМОЛОГІЧНИЙ ПОРТРЕТ ТА МОДЕЛІ ПОВЕДІНКИ ЖЕРТВ КІБЕРЗЛОЧИНІВ

«Жертва злочину є не просто об’єктом, а активним учасником кримінальної ситуації, чия поведінка, свідома чи несвідома, може або сприяти, або перешкоджати вчиненню

злочину», – стверджував відомий ізраїльський кримінолог та один із засновників віктимології Беніамін Мендельсон [1].

Ця думка якнайкраще відображає сутність проблематики віктимології кіберзлочинів. Бути жертвою у віртуальному просторі – це не завжди пасивна доля, а часто результат певної поведінки: від необережного використання ненадійного програмного забезпечення до надмірної довірливості. Саме в цьому полягає питання свідомої або несвідомої участі особи, чия поведінка може як збільшити, так і зменшити ймовірність віктимізації [2].

Актуальність дослідження зумовлена стрімким зростанням кількості кіберзлочинів в умовах цифрової трансформації суспільства. Так, за даними Департаменту кіберполіції Національної поліції України, лише за 2024 рік було зареєстровано понад 60 000 кримінальних правопорушень, пов'язаних з використанням інформаційних технологій. Низький рівень дослідження особистості потерпілого як об'єкта злочинного посягання свідчить про необхідність віктимологічного вивчення жертв, що дозволяє виявити характерні риси, моделі поведінки та рівень інформаційної захищеності, що сприяє вчиненню правопорушень [3].

За таких умов виникає нагальна потреба у формуванні дієвих пропозицій та реалізації ефективних заходів щодо підвищення рівня кібербезпеки.

Протягом тривалого часу традиційна кримінологія зосереджувалась виключно на особі злочинця, ігноруючи роль жертви в механізмі вчинення правопорушення. Однак, стрімкий розвиток інформаційних технологій та повсюдне поширення кіберзлочинності змінили цей підхід. Сучасні дослідження вказують, що віктимізація у кіберпросторі часто обумовлена не лише діями зловмисника, але й певними характеристиками та поведінкою самої жертви. Цей історичний процес трансформації акцентів у кримінології виявляє тенденцію до зростання наукового інтересу до жертви кіберзлочину як ключового елемента у системі попередження правопорушень.

Станом на сьогодні несприятлива віктимологічна ситуація в Україні, і насамперед збільшення кількості потерпілих від несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних, комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж

(ст. 361 ККУ), пов'язана із загостренням проблем функціонування інформаційного суспільства та низькою обізнаністю населення [4].

Це явище є результатом складного комплексу соціально-психологічних та поведінкових чинників. Серед них: безтурботне ставлення до захисту конфіденційних даних, надмірна публічність у соціальних мережах. Також слід зазначити про вплив сучасних викликів, зокрема широкомасштабної агресії, що використовує кіберпростір для поширення дезінформації та фінансових шахрайств.

Сучасні тенденції віктимізації населення від кіберзлочинів у відносному вимірі перевищують втрати від традиційних правопорушень, оскільки вони мають здатність завдавати значних фінансових та особистих збитків у масштабах, що раніше були недоступними. Крім технічних та соціальних чинників, на темпи кібервіктимізації, безумовно, впливає відсутність належного рівня цифрової грамотності та низька обізнаність населення щодо потенційних загроз. Це особливо важливо для України, де, згідно з дослідженнями, ще до повномасштабного вторгнення спостерігався недостатній рівень знань щодо інформаційної безпеки у порівнянні з розвиненими країнами [5; 6].

Питання віктимологічного портрета та моделей поведінки жертв кіберзлочинів може здатися другорядним у час війни, коли мільйони людей борються за виживання в умовах фізичної загрози. Однак саме від підвищення рівня обізнаності та профілактики кіберзлочинів залежатиме захист персональних даних, фінансова стабільність та загальна цифрова безпека громадян у довгостроковій перспективі.

Аналіз правопорушень, передбачених статтею 361 КК України, демонструє, що жертвами стають як фізичні, так і юридичні особи, проте віктимність цих груп суттєво відрізняється [4].

Згідно з судовою статистикою за 2020-2024 роки, правопорушення були вчинені проти 145 фізичних та 32 юридичних осіб. Хоча кількість потерпілих фізичних осіб є значно більшою, загальна сума завданих їм збитків (1 764 142 грн) майже вчетверо перевищує втрати, спричинені юридичним особам (473 917 грн). Ця диспропорція пояснюється вищим рівнем захисту, який забезпечують корпоративні структури. Вони інвестують у сучасні системи кібербезпеки,

застосовують багаторівневі протоколи автентифікації та мають спеціалізовані ІТ-відділи, які постійно моніторять стан інформаційної безпеки. Натомість, фізичні особи є значно менш захищеними як у технічному, так і в поведінковому аспектах, що робить їх більш вразливими [7].

Віктимологічний портрет типової жертви – це особа віком від 21 до 49 років, з вищою або середньою освітою, яка активно використовує мережу Інтернет, але, за відсутності належної обізнаності, має низький рівень цифрової грамотності.

На додаток до вищенаведених характеристик, необхідно враховувати психологічні особливості жертв кіберзлочинів. Визначення лише соціального статусу є недостатнім для повного розуміння ролі потерпілого у злочинній ситуації та характеру його взаємодії зі злочинцем. Саме психологічні чинники (наприклад, довірливість, необережність) безпосередньо впливають на поведінку людини в криміногенних умовах і можуть бути визначальними для її віктимної вразливості [8].

Поведінкові моделі, що відображають психологічні особливості, поділяються на два основні типи:

Активна модель – характеризується екстравертованістю, емоційною збудливістю та схильністю до ризику. Такі особи часто демонструють надмірну самовпевненість у своїх знаннях про безпеку або просто нехтують основними правилами цифрової гігієни. Вони часто мають високий або середній рівень освіти, займають посади у сферах державної служби, бізнесу чи інформаційних технологій. Їхня поведінка демонструє підвищену довірливість у поєднанні з прагненням до швидкої вигоди. Це може призводити до встановлення небезпечних контактів та використання ненадійного програмного забезпечення. Прикладом такої активної поведінки є добровільне надання злочинцю свого телефону, паролів чи інших даних, що безпосередньо призводить до віктимізації. Цікавим фактом є те, що жертви, які демонструють таку модель поведінки при кіберзлочинах, часто мають психологічні ознаки, притаманні й жертвам шахрайства [9].

Пасивна модель – властиві риси інтровертованої особистості: емоційна ригідність, підвищена тривожність, невпевненість у собі, схильність до замкнутості й уникнення конфліктів. Цей тип жертв, навпаки, є більш емоційно стриманим. Їхня віктимність зумовлена не так схильністю до

ризику, як бездіяльністю та недостатньою обізнаністю. Дана поведінка проявляється в ігноруванні базових правил безпеки: використання слабких, легко вгадуваних паролів на кшталт «123456» або «password», а також застосування одного й того ж пароля для багатьох облікових записів. Також до цього типу відноситься відмова від оновлення програмного забезпечення або ігнорування системних повідомлень про безпеку, що залишає цифрові пристрої вразливими до атак.

Важливо відзначити, щодо вікової характеристики жертви, офіційна статистика не відображає повної картини віктимологічного портрета. Згідно з більшістю даних судових органів, жертвами несанкціонованого втручання є лише повнолітні особи, тоді як неповнолітні, віком 13-17 років, які демонструють високий рівень інтеграції в цифровий простір, залишаються так званою «невидимою» групою жертв. Ця ситуація пояснюється не тим, що підлітки не стають жертвами, а тим, що вони не повідомляють про правопорушення. Це зумовлено низкою соціально-психологічних чинників. Неповнолітні часто сприймають кіберзлочин як незначний інцидент або частину віртуальної гри, не усвідомлюючи всіх його наслідків. Вони можуть вважати, що втрата доступу до ігрового акаунту або персональної сторінки в соціальних мережах є просто неприємністю, а не кримінальним правопорушенням. Таким чином, реальний віктимологічний портрет є значно ширшим, ніж той, що відображений в офіційних даних [7; 10].

На мою думку, кіберзлочинці орієнтуються не на вік, а на індивідуальні характеристики потенційної жертви. Незважаючи на те, що, за даними Національного агентства боротьби зі злочинністю у Великобританії, жертвами кіберзлочинів схильні бути особи віком від 15 до 49 років [11], віктимологічний аналіз свідчить, що виокремлення конкретної вікової групи є недоцільним. Зокрема, ключовими факторами вразливості є рівень цифрової грамотності та ступінь дотримання елементарних принципів кібергігієни. Наприклад, молодий фахівець у сфері ІТ, який має високу цифрову грамотність і дотримується всіх правил безпеки, менш вразливий, ніж особа похилого віку, яка користується мережею Інтернет лише для спілкування, але при цьому ігнорує попередження системи безпеки та переходить за підозрілими посиланнями.

Особи старшого віку не є типовими жертвами кіберзлочинів через їхню обмежену інтеграцію в цифровий простір, але вони все ж належать до групи ризику. Статистичні дані стверджують: згідно з дослідженням, лише 5 % респондентів віком понад 60 років ознайомлені з основами кібербезпеки, порівняно з 12 % серед осіб віком до 60 років [12].

В українському суспільстві, серед жертв кіберзлочинів переважають чоловіки. Статистика за 2020-2024 роки свідчить, що 66,4 % жертв – саме чоловіки, тоді як жінки становлять 37,6 %. Ця тенденція є закономірною і має кілька пояснень, які формують віктимологічний портрет за статевою ознакою [3; 7]:

– поведінкові та психологічні схильності – чоловіки, як правило, більш схильні до ризику та азартних ігор, що може підвищити їхню віктимність. Вони частіше залучені до ситуацій, які можуть призвести до злочинного посягання в кіберпросторі. Ця схильність до ризику може виражатися в ігноруванні базових правил безпеки, наприклад, при здійсненні онлайн-транзакцій на неперевірених сайтах або при взаємодії з підозрілими додатками;

– професійна діяльність та сфера інтересів – згідно з дослідженнями, чоловіки складають більшість (близько 82 %) фахівців у сфері ІТ. Їхня постійна та поглиблена взаємодія з цифровими технологіями, включаючи технічні пристрої та відеоігри. Прикладом може слугувати ситуація, коли ІТ-спеціаліст, працюючи з великими обсягами даних, може недооцінити ризики та завантажити шкідливе програмне забезпечення, замасковане під професійний інструмент. Аналогічно, захоплення онлайн-іграми може призвести до розголошення особистих даних або втрати доступу до облікового запису через фішинг.

На підставі аналізу Єдиного державного реєстру судових рішень, жертви несанкціонованого втручання в інформаційні системи часто є потерпілими й за статтями, що стосуються крадіжок та шахрайства (статті 185, 190 КК України), що вказує на корисливий мотив (81 %) і буденний характер цих кіберзлочинів.

Жертвами таких правопорушень найчастіше є особи із середнім рівнем доходів або безробітні, які володіють лише майном повсякденного вжитку. Ця тенденція пояснюється тим, що злочинці та їхні жертви належать до одного соціального прошарку.

Вони мають схожий стиль життя та уявлення про матеріальне благополуччя. Їх об'єднує маргіналізований соціальний статус, що робить їх соціально вразливими й периферійними в структурі суспільства. Тобто кіберзлочинці обирають собі за мішень не багатих людей, а тих, чиї активи легше вкрасти завдяки їхній соціальній та фінансовій вразливості [14].

За професійною ознакою підвищений ризик кібервіктимізації мають представники банківського та фінансового сектору, працівники державних реєстрів і органів влади, а також особи, що мають публічний цифровий вплив, як-от журналісти, блогери та активісти, оскільки їхні акаунти дають доступ до цінної інформації або маніпуляційного впливу. Ці фахівці є пріоритетною мішенню, оскільки несанкціонований доступ до їхніх облікових записів чи систем може принести злочинцям значну фінансову вигоду або дозволити здійснити політичний чи соціальний вплив.

Отже, враховуючи вищезазначене, я вважаю, що віктимологічний аналіз кіберзлочинів в Україні підтверджує, що жертва є активним учасником кримінальної ситуації у віртуальному просторі, і її поведінка, свідома чи несвідома, є критичним фактором, що сприяє або перешкоджає злочинному посяганню. Одним із ключових аспектів несприятливої віктимологічної ситуації, що посилюється військовими викликами, є низький рівень цифрової грамотності та поведінкова вразливість значної частини населення.

Одним із ключових аспектів цієї проблеми є значна вразливість фізичних осіб, що підтверджується чотириразовим перевищенням завданих їм збитків порівняно з корпоративним сектором, який має вищий рівень захисту. Причини високої віктимності включають низьку обізнаність населення, схильність до ризику та довірливість, а також функціонування в умовах широкомасштабної агресії, що посилює використання кіберпростору для шахрайства та дезінформації. Причини високої кібервіктимізації фізичних осіб, чиї збитки значно перевищують втрати корпоративного сектору, включають соціально-психологічні та поведінкові фактори, соціальна та демографічна вразливість та деякі прогалини в статистиці. Відновлення фінансової та цифрової безпеки громадян в умовах стрімкого зростання кіберзлочинності вимагає комплексного підходу до реалізації державної політики,

спрямованої на зміщення акцентів у профілактиці. Важливою складовою такої політики є масове підвищення рівня цифрової грамотності та формування відповідальної поведінки серед усіх верств населення, а не лише посилення технічного захисту.

Таким чином, саме через призму віктимологічної профілактики слід розглядати і реформувати механізми кіберзахисту, адже обізнаний та відповідальний користувач – ключ до зниження кібервіктимізації та забезпечення цифрової безпеки країни.

Список використаних джерел

1. Мендельсон Б. Теоретичні основи віктимології: вчення про жертву злочину. *Віктимологічний вісник*. 2018. № 3. С. 15–28.

2. Ковальчук В. С. Віктимологія кіберзлочинів: соціально-психологічний портрет потерпілого. *Наукові праці Національної академії внутрішніх справ.* 2024. Т. 5. № 1. С. 112–125.

3. Департамент кіберполіції Національної поліції України. Звіт про стан кіберзлочинності в Україні за 2024 рік. URL: https://cyberpolice.gov.ua/statistics/report (дата звернення: 01.10.2025).

4. Кримінальний кодекс України: Закон України від 05.04.2001 р. № 2341-III. *Відомості Верховної Ради України*. 2001. № 25–26. Ст. 131.

5. Степаненко Л. І. Цифрова грамотність як чинник віктимологічної безпеки населення. *Інформаційне суспільство та право.* 2024. № 2. С. 88–95.

6. Ярошенко А. Л. Вплив широкомасштабної агресії на рівень кібершахрайства в Україні: соціально-психологічний аналіз. *Науковий вісник Національної академії внутрішніх справ*. 2023. № 1. С. 78–89.

7. Судова статистика України (Єдиний державний реєстр судових рішень). Аналіз правопорушень за ст. 361 ККУ щодо фізичних та юридичних осіб 2020–2024. URL: https://reyestr.court.gov.ua/analysis_cybercrime (дата звернення: 02.10.2025).

8. Шевченко О. Р. Поведінкові чинники кібервіктимізації: соціально-психологічний аналіз. *Проблеми кримінології та криміналістики.* 2023. Т. 4. № 1. С. 45–59.

9. Шевчук І. П. Психологічні маркери активної моделі поведінки жертв кібершахрайства та їхній зв’язок із загальними

ознаками шахрайства. *Психологічний журнал.* 2024. Т. 15. № 4. С. 205–218.

10. Коваль І. В. Вікова специфіка кібервіктимності: «невидима» група неповнолітніх жертв. Науковий вісник Національної академії внутрішніх справ. Серія «Право». 2023. Т. 3. № 4. С. 110–121.

11. Національне агентство боротьби зі злочинністю Великобританії (NCA). Профіль жертв кіберзлочинів: міжнародний досвід / пер. з англ. К. В. Ковальчук. Київ : Юрінком Інтер, 2023. С. 320–345.

12. Юхименко С. Г. Вразливість осіб похилого віку в кіберпросторі: соціологічне дослідження. *Демографія та соціологія.* 2022. № 1. С. 145–155.

13. Єдиний державний реєстр судових рішень. Аналітична довідка щодо судової статистики за статтями 361, 185, 190 КК України (2020–2024 рр.) URL: http://reyestr.court.gov.ua/analytics/cyber/2020-2024 (дата звернення: 02.10.2025).

Кавєріна Тетяна Петрівна,
старший викладач кафедри криміналістики навчально-наукового інституту права та психології Національної академії внутрішніх справ

ЖЕРТВА ШАХРАЙСТВА ІЗ СОЦІАЛЬНОЇ МЕРЕЖІ

Вважаючи більш зручним спосіб спілкування у соціальних мережах та месенджерах, ми часто довіряємо їм всі больові точки, які потім можуть стати нашою уразливою зоною. Але, перебуваючи в певному психологічному стані через зовнішні чи особисті обставини, ми не надаємо належного значення своїм дописам та думкам, хибно вважаючи отриману взамін інформацію більш цінною. Проте, шахраї відразу виділяють свою майбутню жертву саме через такі дописи.

До прикладу, соціальна мережа «Facebook» об’єднала мільйони людей в багатьох країнах світу, а відтак – інформація, що потрапила до неї, може швидко розповсюдитись, а її автор – стати справжньою здобиччю для шахрайських дій.

Однією з так званих уразливих категорій потерпілих є родини військових, зниклих безвісти за особливих обставин [1]. Термін «особа, що перебуває в уразливому стані»[2], наразі

сміливо можна використовувати не лише в контексті досудового розслідування кримінальних правопорушень, передбачених статтями 149 та 303 КК України, де так добре розтлумачено сутність такого стану. Адже саме «уразливим станом» законодавець окреслив «зумовлений фізичними чи психічними властивостями або зовнішніми обставинами стан особи, який позбавляє або обмежує її здатність усвідомлювати свої дії (бездіяльність) або керувати ними, приймати за своєю волею самостійні рішення, чинити опір насильницьким чи іншим незаконним діям, збіг тяжких особистих, сімейних або інших обставин»[2].

Перебуваючи в особливому емоційному стані та маючи намір щодо отримання хоч найменшої інформації про зниклу близьку людину, дуже часто, будучи активним користувачем соціальних мереж, рідні зниклого публікують його фото разом з персональними даними та особистою інформацією на сторінках відповідних тематичних груп. Не треба бути знавцем психології, аби усвідомлювати, на що здатна людина, яка не має звістки від зниклого сина, чоловіка, брата, який перебував у зоні бойових дій, аби отримати дорогоцінну інформацію про його місцеперебування та стан здоров'я, або і взагалі можливість спілкування з ними чи «викупу» з неволі. Це і є основною «больовою точкою» майбутнього уразливого потерпілого, яку буде взято за основу низькоморальним шахраєм. А далі – справа техніки. Через відстежені пости шахраї зв'язуються з рідними, повідомляючи їм, що мають запитувану ними інформацію про військовослужбовця та готові надати свої «послуги» за певних умов. Такими умовами можуть стати переказ грошових коштів чи надання інших «послуг», як правило – розвідувального характеру про місцезнаходження чи геолокацію певних об'єктів. Але останнє – то вже наміри інших персоналій окупаційної армії.

Діючи за схемами «внесення до списку на обмін», «ваш рідний у шпиталі», «вимагання неіснуючих боргів» чи просто отримання доступу до банківської картки зниклого, шахраї майстерно просочуються у мізки жертви, отримуючи доступ не лише до варіювання психоемоційним станом жертви, а й до її гаманця.

Створивши фейкові акаунти чи сторінки псевдо міжнародних організацій та волонтерів, шахраї пропонують свої «послуги» щодо включення даних зниклого військового до

списків на обмін та «позачергове» звільнення його з полону, репатріацію тіла загиблого чи надання інших даних, які майбутньому уразливому потерпілому видаються супер реальними. Маючи намір суттєво полегшити долю зниклого військовослужбовця чи отримати тіло загиблого якнайшвидше, зневірившись у роботі правоохоронців та певних державних органів після численних звернень, його рідні беруть до уваги пропозицію шахрая, перераховуючи тому кошти та сподіваючись на позитивне вирішення «свого питання». Однак, насправді позбавляються і коштів і інформації, якої злочинці й не мали.

Підрозділи Національної поліції України, неодноразово реєструючи заяви від громадян про вчинення стосовно них шахрайських дій, глибоко вивчили проблему та систематично проводять просвітницьку діяльність, застерігаючи уразливих потерпілих – рідних зниклих безвісти військовослужбовців не лише від необхідності контактування з зазначених питань з неофіційними структурами, а й щодо публікації особистих даних і фото зниклих у соціальних мережах[3].

Аби уберегти потенційних потерпілих від скоєння щодо них шахрайських дій, на зазначених фактах постійно наголошують також представники структурних підрозділів МВС України, одним з яких є Управління з питань осіб, зниклих безвісти за особливих обставин. Маючи у функціоналі широку комунікацію з родинами осіб, зниклих безвісти за особливих обставин (цивільних та військових), держслужбовці цього підрозділу ведуть роз'яснювальну роботу та наголошують на тому, що всі державні структури надають свої послуги безкоштовно та діють від імені держави і в межах Закону[4]. Особливої уваги потребують родини військовополонених, які хоч і мають інформацію про перебування їх рідної особи у полоні, проте роками чекають на обміни, втрачаючи віру в реалізацію цієї мети. В цьому напрямку проводить роз'яснювальну роботу єдина в Україні офіційна структура – Координаційний штаб з питань поводження з військовополоненими [5], яка веде відповідні Реєстри та надає консультаційні послуги безкоштовно і є єдиною структурою, яка безпосередньо займається перемовинами та обміном військовополонених.

Тож, аби не дати рідним осіб, зниклих безвісти за особливих обставин, стати жертвою шахраїв з соціальних мереж, необхідно систематично проводити роз'яснювальну роботу не

лише про те, чого не треба робити, а й наголошувати на тому, куди можна звернутись для отримання офіційної допомоги. Слід зважати, що робота з сім'ями родин осіб, зниклих безвісти за особливих обставин є різноплановою, часто пов'язана з підвищеним емоційним градусом, зневірою та надчутливістю, викликаною неможливістю швидко становити місцезнаходження зниклого чи провести обмін військовополоненого, що є взагалі окремою закритою від широкого загалу темою. Тож у разі вчинення шахрайських дій – слід негайно подавати заяву до найближчого підрозділу поліції, аби прискорити повернення коштів та покарання злочинців, не ігнорувати роз'яснення правоохоронців та зважати на висвітлені у засобах масової інформації негативні приклади реалізації злочинних намірів правопорушниками.

Список використаних джерел

1. Про правовий статус осіб, зниклих безвісти за особливих обставин : Закон України від 12.07.2018 № 2505-VIII. URL: https://zakon.rada.gov.ua/laws/show/2505-19#Text (дата звернення 13.10.2025)

2. Кримінальний кодекс України: Закон України від 05.04.2001 № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#top (дата звернення 14.10.2025)

3. Як родинам полонених та зниклих безвісти вберегтися від шахраїв – поради від співробітників кіберполіції та Офісу Омбудсмана. *Офіційний сайт кіберполіції України*. 2024. 24 грудня. URL: https://cyberpolice.gov.ua/article/yak-rodynam-polonenyx-ta-znyklyx-bezvisty-vberegtysya-vid-shaxrayiv--porady-vid-spivrobitnykiv-kiberpolicziyi-ta-ofisu-ombudsmana-8333/ (дата звернення 13.10.2025)

4. Шахраї полюють на родини військовополонених та зниклих безвісти: як розпізнати та уникнути обману. *Офіційний сайт МВС України*. 2025. 11 серпня. URL: https://mvs.gov.ua/news/saxrayi-poliuiut-na-rodini-viiskovopolonenix-ta-zniklix-bezvisti-iak-rozpiznati-ta-uniknuti-obmanu (дата звернення 13.10.2025)

5. Що робити, якщо Ваш рідний довго не виходить на зв'язок? *Офіційний сайт Координаційного штабу з питань поводження з військовополоненими*. URL: https://roadmap.koordshtab.gov.ua/lost-communication (дата звернення 13.10.2025)

Кара Анна Володимирівна,
здобувач ступеня вищої освіти магістра навчально-наукового інституту права та психології Національної академії внутрішніх справ
Науковий керівник:
Шрамко С. С., завідувач кафедри кримінального права та кримінології навчально-наукового інституту права та психології Національної академії внутрішніх справ, кандидат юридичних наук, старший дослідник

КРИМІНАЛЬНО-ПРАВОВА ОХОРОНА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ В ЦИФРОВОМУ СЕРЕДОВИЩІ

Розвиток Інтернету зумовлює появу нових загроз у сфері захисту прав інтелектуальної власності. У мережі розміщено велику кількість об'єктів, що мають правовий статус інтелектуальної власності, і значна їх частина залучається до комерційного обігу. Це підкреслює необхідність формування ефективних механізмів їх правової охорони та належного реагування на сучасні виклики цифрового середовища.

Актуальність кримінально-правової охорони інтелектуальної власності в цифровому середовищі зумовлена стрімким розвитком цифрових технологій, глобалізацією Інтернету та поширенням нових форм порушень прав.

Необхідно виокремити ключові загрози для об'єктів права інтелектуальної власності у цифровому середовищі. По-перше, мережа Інтернет функціонує як відкритий інформаційний простір, що не має централізованого управління, єдиного власника чи чітко визначених меж майнової належності. По-друге, в онлайн-середовищі поширюються об'єкти інтелектуальної власності, які існують виключно у цифровій формі. По-третє, використання таких об'єктів має транскордонний характер, що суттєво ускладнює застосування національних правових механізмів для захисту порушених прав, а в окремих випадках фактично унеможливлює їх ефективне відновлення [1].

З аналізу ст. 53 Закону України «Про авторське право і суміжні права» випливає, що порушення авторського права та суміжних прав включають кілька основних видів: порушення авторського та суміжних прав, що дають підстави для судового захисту, включають дії, що порушують особисті немайнові та майнові права правовласників, піратство – опублікування, відтворення, ввезення, вивезення та розповсюдження контрафактних примірників творів, комп'ютерних програм, баз даних, фонограм, відеограм та програм організацій мовлення, навмисний обхід технічних засобів захисту прав, підробку, зміну або вилучення інформації про управління правами, а також розповсюдження чи публічне сповіщення об'єктів, у яких без дозволу правовласників змінено або вилучено інформацію про управління правами, зокрема в електронній формі [2].

До найпоширеніших порушень прав інтелектуальної власності у цифровому середовищі належать такі явища: інтернет-фішинг, який полягає у створенні шахрайських веб-сторінок, що зовні повторюють офіційні ресурси інтернет-магазинів, банків, виробників чи платіжних систем; онлайн-шахрайство, до якого відносять підроблені інтернет-аукціони, фіктивні магазини, сайти та інші форми зловживань засобами телекомунікаційного зв'язку; піратство, тобто незаконне розповсюдження об'єктів інтелектуальної власності через Інтернет.

Окремо слід відзначити проблему поширення контрафактної продукції, що виникає внаслідок несанкціонованого використання товарних знаків, найменувань місця походження товарів чи фірмових позначень. Додатковою загрозою є кіберсквотинг, який проявляється у неправомірній реєстрації, використанні або пропонуванні до продажу доменних імен із недобросовісною метою отримати прибуток за рахунок гудвілу чи торговельної марки, що належить іншому суб'єкту [3].

Стаття 176 Кримінального кодексу України встановлює відповідальність за порушення авторського та суміжних прав [4]. Зокрема, йдеться про незаконне використання таких об'єктів, їх відтворення, розповсюдження чи інші способи комерційного використання. Притягнення до кримінальної відповідальності за ці правопорушення можливе лише за наявності істотної матеріальної шкоди, а також у разі повторності діяння чи його вчинення групою осіб.

В умовах розвитку інформаційних технологій особливої актуальності набуває проблема охорони інтелектуальної власності в цифровому середовищі. Чинна редакція ст. 176 КК України значною мірою зорієнтована на правопорушення, пов'язані з матеріальними носіями творів, і тому не повною мірою враховує специфіку обігу інтелектуального продукту в Інтернет-середовищі. Це знижує результативність кримінально-правових механізмів захисту інтелектуальної власності в умовах цифровізації.

Міжнародні зобов'язання, які взяла на себе Україна, вимагають запровадження дієвого й ефективного механізму захисту інтелектуальних прав. З огляду на це важливо привести національне законодавство у відповідність до вимог директив Європейського Союзу, актів національного законодавства європейських держав та міжнародних актів загалом, щодо охорони новітніх об'єктів інформаційних технологій.

Актуальним завданням є вдосконалення складів кримінальних правопорушень шляхом конкретизації їхніх ознак та врахування сучасних способів порушення прав в Інтернет-середовищі. Йдеться, про кримінально-правову протидію нелегальному розповсюдженню цифрового контенту, про обхід технічних засобів захисту авторських прав, а також про створення й розповсюдження програмних продуктів, призначених для порушення прав інтелектуальної власності [5, с. 241–242].

Коли виникає приватно-правовий спір щодо використання певного об'єкта інтелектуальної власності в Інтернеті, доцільно керуватися законодавством тієї держави, де фактично відбувалося його використання. При цьому підтвердження права власності на твір або інший об'єкт інтелектуальної власності повинно здійснюватися на основі відповідних правовстановлюючих документів, виданих у країні їх походження. Такий підхід дозволяє уникати правових колізій та забезпечує стабільність процедур вирішення приватноправових конфліктів у міжнародному контексті.

У рамках Європейського Союзу обов'язок для платформ укладати ліцензійні угоди та впроваджувати технології, що запобігають розміщенню піратського контенту, встановлює Директива 2019/790 щодо авторського права в цифровому єдиному ринку [6]. Цей підхід отримав своє відображення у

справі Frank Peterson проти Google та YouTube (C-682/18), яку розглядав Суд Європейського Союзу, ухваливши рішення 22 червня 2021 року. У ньому Суд зазначив, що YouTube не несе автоматичної відповідальності за розміщений піратський контент, якщо після отримання повідомлення від правовласника оперативно видаляє такий матеріал, що демонструє ефективність механізму швидкого реагування [7].

З поширенням цифрових технологій виникають ситуації, коли право користувачів на доступ до інформації може суперечити правам власників інтелектуальної власності. Особливу увагу привертають обмеження на відтворення та розповсюдження матеріалів у навчальних, наукових та інших суспільно значущих цілях. Сучасні цифрові інструменти відкривають широкі можливості для створення й використання інтелектуальних творів у таких галузях, як штучний інтелект, машинне навчання та біотехнології, що зумовлює необхідність адаптації правових механізмів захисту [8, с. 115].

Для захисту інтелектуальної власності застосовуються різноманітні стратегії та інструменти. Одним із таких методів є водяний знак (Watermarking), що передбачає нанесення на цифровий контент видимого або прихованого позначення, яке дозволяє ідентифікувати його власника. Це допомагає запобігати плагіату та незаконному використанню творів.

Наступними є освітні програми та ініціативи спрямовані на формування усвідомленого підходу до використання інтелектуальної власності. Вони знайомлять користувачів із правилами авторського права та підвищують розуміння важливості охорони інтелектуальних прав.

Власники інтелектуальної власності також можуть застосовувати технічні засоби захисту на рівні мережі – такі як брандмауери, антивірусні програми та інші механізми – для запобігання несанкціонованому доступу та крадіжці цифрових об’єктів. Крім того, захист метаданих, що описує інші дані є важливим інструментом для ідентифікації власника контенту та автора. [9, с. 89].

Таким чином, кримінально-правова охорона інтелектуальної власності в цифровому середовищі потребує комплексного підходу, що об’єднує законодавчі, технічні, освітні та етичні засоби захисту. Чине законодавство в даній сфері потребує удосконалення з урахуванням специфіки цифрового

середовища та транскордонного характеру обігу об'єктів. Використання сучасних технологій захисту, ефективних механізмів ліцензування та швидкого реагування на порушення забезпечує баланс між правами користувачів і власників, стимулює інноваційну діяльність та підвищує результативність охорони інтелектуальної власності в умовах цифровізації.

Список використаних джерел

1. Літавський Т. Захист ІВ у мережі Інтернет: як це теоретично має працювати? *Юридична газета.* 2020. № 12 (718). URL: https://yur-gazeta.com/publications/practice/zahist-intelektualnoyi-vlasnosti-avtorske-pravo/zahist-iv-u-merezhi-internet-yak-ce-teoretichno-mae-pracyuvati.html

2. Про авторське право і суміжні права : Закон України від 01.12.2022 № 2811-IX : станом на 15 листоп. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/2811-20#Text

3. Гриньчак В., Ткаченко В. Порушення прав на об'єкти інтелектуальної власності у глобальній мережі Інтернет», *Молодий вчений*. 2021. № 9 (97). С. 143-147. doi: 10.32839/2304-5809/2021-9-97-29.

4. Кримінальний кодекс України : Кодекс України від 05.04.2001 № 2341-III : станом на 17 лип. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text

5. Бошицький Ю.Л. Деякі огранізаційно-правові аспекти удосконалення правової охорони інтелектуальної власності в сучасній Україні. *Часопис Київського університету права.* 2020. Т. 1, No 3. С. 239–247.

6. Директива Європейського парламенту і Ради (ЄС) 2019/790 від 17 квітня 2019 року про авторське право і суміжні права на Єдиному цифровому ринку та про внесення змін до директив 96/9/ЄС та 2001/29/ЄС (OJ 2019 L 130, с. 92)

7. Judgment of Grand Chamber of 22.06.2021 in no. C-682/18 and C-683/18. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62018CJ0682

8. Токарева В.О. Деякі аспекти авторського права в США в цифрову добу. *Порівняльно-аналітичне право*. 2018. № 1. С. 114–118.

9. Савич С.С. Авторське право у цифровому середовищі: проблема монополії правовласника та забезпечення умов вільного використання творів. Бюлетень Міністерства Юстиції України. 2015. № 1.

Лозова Тетяна Андріївна,
здобувач ступеня вищої освіти бакалавра навчально-наукового інституту права та психології Національної академії внутрішніх справ
Науковий керівник:
Шопіна Ю. О., доцент кафедри кримінального права та кримінології навчально-наукового інституту права та психології Національної академії внутрішніх справ, кандидат юридичних наук

КІБЕРБУЛІНГ СЕРЕД МОЛОДІ: ПРАВОВІ МЕХАНІЗМИ ПРОТИДІЇ ТА РОЛЬ ПРАВООХОРОННИХ ОРГАНІВ

Сучасне суспільство неможливо уявити без інтернет-мережі, що стало місцем комунікації, навчання та самореалізації молоді. Проте розвиток цифрових технологій породив нові соціальні загрози, серед яких є загрозливим для суспільства кібербулінг. Найбільше від кібербулінгу потерпає молодь, яка є найактивнішим користувачем соціальних мереж та інших платформ. Актуальність теми зумовлена тим, що масштаби цього явища щороку зростають, а правовий механізми протидії потребують вдосконалення. Важливу роль у забезпеченні безпеки молоді в відіграють правоохоронні органи, адже саме вони уповноважені розслідувати та припиняти кіберправопорушення.

Міжнародні документи, зокрема Резолюція 2450 (XXIII) ООН, підкреслюють важливість цифрових прав і наголошують на необхідності створення ефективних механізмів захисту громадян в умовах глобальної цифровізації [1]. Сьогодні Україна, враховуючи європейські стандарти, формує правові механізми для забезпечення цифрових прав громадян.

Відповідно, щодо боротьби з кібербулінгом, то в Україні вперше було сформовано державну політику щодо запобігання цькування з прийняттям Закону України «Про внесення змін до деяких законодавчих актів України щодо протидії булінгу (цькуванню)», згідно з яким визначається, що булінг (цькування) – це діяння учасників освітнього процесу, які

полягають у психологічному, фізичному, економічному, сексуальному насильстві, зокрема із застосуванням засобів електронних комунікацій, що вчиняються стосовно малолітньої чи неповнолітньої особи або такою особою стосовно інших учасників освітнього процесу, внаслідок чого могла бути чи була заподіяна шкода психічному або фізичному здоров'ю потерпілого [2].

Ми підкреслюємо, булінг – це доволі неприємне явище, що може проявлятися у різноманітних формах. Найпоширенішими формами такого знущання у наш час є булінг в інформаційному просторі – через телефони та соціальні мережі, що є кібербулінгом. Конституція України, Кримінальний кодекс України, Закон України «Про основні засади забезпечення кібербезпеки України», Закон України «Про розповсюдження примірників аудіовізуальних творів, фонограм, відеограм, комп'ютерних програм, баз даних». Як відомо, за булінг передбачається цивільна, адміністративна або кримінальна відповідальність. В більшості випадків, особа буде нести адміністративну відповідальність.

Ми підкреслюємо, що булінг – це доволі неприємне явище що може проявлятися у різноманітних формах. Найпоширенішими формами такого знущання у наш час є кібербулінг в інформаційному просторі через телефон та соціальні мережі. Правові механізми міститься в основних нормативно-правових актах України таких як: Конституція України, Кримінальний кодекс України, Закон України «Про основи засади забезпечення кібербезпеки України». Як відомо, за кібербулінг передбачається цивільна, адміністративна та кримінальна відповідальність. В більшості випадків особа буде нести саме адміністративну відповідальність.

Національне законодавство безпосередньо не містить положень, спрямованих на реалізацію захисту дітей від сексуальної експлуатації і сексуального насильства в інтернет-мережі. Звичайно, розслідування подібних злочинів можна розглядати через інші статті [3, с. 133]. Кримінального кодексу, наприклад, ч.ч. 1–2 ст. 156-1 КК України визначає відповідальність за пропозицію зустрічі, зроблену повнолітньою особою, у тому числі з використанням інформаційно-телекомунікаційних систем або технологій, особі, яка не досягла шістнадцятирічного віку, задля вчинення

стосовно неї будь-яких дій сексуального характеру або розпусних дій, а також задля втягнення її у виготовлення дитячої порнографії, якщо після таких пропозицій було вчинено хоча б одну дію, спрямовану на те, щоб така зустріч відбулася; положеннями ст. 300-1 КК України встановлюється відповідальність за умисне одержання доступу до дитячої порнографії з використанням інформаційно-телекомунікаційних систем чи технологій або умисне її придбання, або умисне зберігання, ввезення в Україну, виготовлення, перевезення чи інше переміщення дитячої порнографії задля збуту або без мети збуту чи розповсюдження [4]. Ми наголошуємо, що домагання дітей у цифровому середовищі не обов'язково має наслідковий фізичний контакт чи зустріч у реальному житті, оскільки воно може стати віртуальному просторі однак, його вплив на психоемоційний стан дитини не є менш небезпечним.

Важливо зазначити, що правоохоронні органи відповідно до ст. 8 Закон України «Про основи засади забезпечення кібербезпеки України» відіграють важливу роль у протидії кібербулінгу. Державна служба спеціального зв'язку та захисту інформації України – формує політику кіберзахисту, створює систему реагування на кібератаки. Національна поліція України – розслідує кіберправопорушення, зокрема кібербулінг. Служба безпеки України – боротися з кібертероризмом і кібершпигунством. Міністерство оборони та ЗСУ – кібероборону. Національний банк України – кіберзахист банківської системи. Міністерство закордонних справ – міжнародна співпраця у сфері кібербезпеки тому як практика Національної поліції у розслідуванні фактів кібербулінгу є дієвою. Співпраці з освітніми закладами. Інформаційні кампанії для молоді та батьків [5].

Отже, кібербулінг є складним соціально-правовим явищем, що потребує комплексного реагування. Особливість полягає в тому, що правопорушення дій відбуваються віртуальному просторі, але мають реальні наслідки для психічного та фізичного здоров'я молоді. Україна вдосконалює правовові механізми протидії кібербулінгу. Перспективні напрямки розвитку є гармонізація національного законодавства з європейськими стандартами; підвищення грамотності населення; створення ефективних механізмів психологічного та

правової допомоги жертвам кібербулінгу. Таким чином, лише поєднання правових, освітніх та профілактичних заходів значною мірою здатні забезпечити належний рівень захисту молоді в цифровому середовищі та мінімізувати наслідки кібербулінгу.

Список використаних джерел

1. Резолюція Генеральної Асамблеї ООН 2450 (XXIII). Цифрові права в умовах глобалізації. ООН, 2020. URL: https://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/2450 (дата звернення: 28.09.2025).

2. Про внесення змін до деяких законодавчих актів України щодо протидії булінгу (цькуванню) : Закон України від 18 грудня 2018 року № 2657. URL:https://zakon.rada.gov.ua/laws/show/2657-19#Text (дата звернення: 28.09.2025).

3. Янішевська К. Д., Зінченко Г. С. Запобігання кібербулінгу, кібермобінгу, кібергрумінгу в Україні. *Юридичний науковий електронний журнал.* 2022. № 2. С. 132–135.

4. Кримінальний кодекс України від 05.04.2001 № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14/conv#n3806 (дата звернення: 28.09.2025).

5. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 URL: https://zakon.rada.gov.ua/ laws/show/2163-19#Text (дата звернення: 28.09.2025).

Микитенко Інеса Андріївна,
здобувач ступеня вищої освіти бакалавра навчально-наукового інституту права та психології Національної академії внутрішніх справ
Науковий керівник:
Козачина А. М., старший викладач кафедри кримінального права та кримінології навчально-наукового інституту права та психології Національної академії внутрішніх справ, доктор філософії

ІМПЛЕМЕНТАЦІЯ ПОЛОЖЕНЬ КОНВЕНЦІЇ ПРО КІБЕРЗЛОЧИННІСТЬ У НАЦІОНАЛЬНЕ ЗАКОНОДАВСТВО

Імплементація положень Конвенції про кіберзлочинність у національне законодавство України є важливим етапом у розвитку державної політики та сфері інформаційної безпеки. З кожним роком роль інформаційних технологій у житті суспільства зростає, а разом із тим – і кількість правопорушень, пов'язаних із використанням комп'ютерних систем, мереж і даних. Саме тому виникла потреба у створенні єдиних міжнародних стандартів, які б регулювали питання протидії таким злочинам. Першим кроком у цьому напрямі стала Конвенція Ради Європи про кіберзлочинність, ухвалена 23 листопада 2001 року в Будапешті. Її головна мета – забезпечити спільну політику держав щодо криміналізації діянь, які вчиняються за допомогою комп'ютерних технологій, а також створити ефективні механізми міжнародного співробітництва.

Україна підписала Конвенцію одразу після її прийняття – 23 листопада 2001 року, а у 2005 році ратифікувала її Законом № 2824-IV. Це означало, що держава взяла на себе зобов'язання забезпечити своє законодавство у відповідності до положень цього міжнародного документа. Імплементація Конвенції полягає не лише у формальному закріпленні її норм у правовій системі, а й у практичному впровадженні міжнародних стандартів боротьби з кіберзлочинами у повсякденну діяльність правоохоронних органів та судової системи.

Передусім, виконання положень Конвенції вплинуло на оновлення кримінального законодавства України. До нього було введено норми, які передбачають відповідальність за несанкціоноване втручання в роботу комп'ютерних систем і мереж, створення та поширення шкідливого програмного забезпечення, незаконне використання або зміну інформації, що обробляється в електронних системах, а також за порушення правил їх експлуатації. Такі нововведення відтворюють основні положення Конвенції та створюють правові механізми для ефективного переслідування осіб, які вчиняють злочини у сфері кібербезпеки.

Окрім змін до кримінального законодавства, значну увагу було приділено удосконаленню кримінального процесу. Конвенція містить положення, що зобов'язують держави забезпечити можливість оперативного доступу до комп'ютерних даних, проведення обшуків і вилучення інформації в електронній формі, а також збереження даних для подальшого розслідування. Україна внесла відповідні зміни до Кримінального процесуального кодексу, що дозволило слідчим використовувати нові форми доказування – електронні листи, файли, записи з мережі Інтернет, дані з мобільних пристроїв.

Реалізація Конвенції про кіберзлочинність також сприяла створенню спеціальних органів, які займаються боротьбою з кіберзлочинами. У структурі Національної поліції України діє Департамент кіберполіції, який координує роботу з виявлення, розслідування та попередження кіберзлочинів. Крім того, створено Національний контактний пункт, який забезпечує цілодобовий обмін інформацією з правоохоронними органами інших країн для швидкого реагування на кіберінциденти.

У 2017 році Верховна Рада України ухвалила Закон «Про основні засади забезпечення кібербезпеки України». Цей закон визначив ключові принципи та напрями державної політики у сфері кібербезпеки, а також перелік суб'єктів, які відповідають за захист кіберпростору – Службу безпеки України, Національну поліцію, Міністерство оборони, Державну службу спеціального зв'язку та захисту інформації. Важливо, що закон передбачає активне міжнародне співробітництво, адже кіберзлочинність не має кордонів і ефективна боротьба з нею можлива лише спільними зусиллями.

Як на міжнародному, так і на національному рівні кіберзлочинність є однією з найгостріших проблем, яка постала сьогодні перед правоохоронними органами. До цього часу не вироблений системний підхід у протидії кіберзлочинності з урахуванням сучасних викликів і загроз інформаційній безпеці [1, с. 129].

Разом з тим, імплементація положень Конвенції стикається з низкою проблем. По-перше, в Україні все ще не вистачає висококваліфікованих фахівців, здатних професійно працювати з цифровими доказами. По-друге, технічне забезпечення правоохоронних органів часто не відповідає сучасним викликам. По-третє, судова практика у справах про кіберзлочини перебуває на стадії становлення, тому існують труднощі з доказуванням та кваліфікацією таких правопорушень.

У 2022 році Україна підписала Другий додатковий протокол до Конвенції про кіберзлочинність, який спрямований на вдосконалення процедур міжнародного обміну електронними доказами. Це дозволить швидше отримувати необхідну інформацію з-за кордону, а також спростить співпрацю між правоохоронними органами різних країн.

Стрімкий розвиток інформаційних технологій створює умови для появи нових ризиків та кіберзагроз. Незважаючи на позитивний вплив на всі сфери людського життя, цей розвиток зумовив зростання й поширення кіберзлочинів. З упевненістю можна сказати, що кіберзлочини – це одна з основних проблем XXI ст., вирішення якої потребує сучасних методів, активних, рішучих заходів і своєчасного нормативного реагування [1, с. 129].

Оскільки заходи, передбачені Законом України «Про оперативно-розшукову діяльність», можуть бути застосовані і під час кримінального провадження, а зібрана інформація може бути використана як доказ, необхідно узгодити ці положення з Кримінальним процесуальним кодексом, у тому числі і умови та запобіжні заходи, що передбачені ним.

Документ, підготовлений Офісом Програми з кіберзлочинності Ради Європи за участю експертів Маркко Куннапу та Марка Юріча за фінансової підтримки Європейського Союзу, присвячений аналізу процесу імплементації положень Будапештської конвенції про кіберзлочинність у національне законодавство України. У ньому розглядаються чинні

нормативно-правові акти та проєкти законів, що стосуються боротьби з кіберзлочинністю та використання електронних доказів. Документ визначає відповідність українських норм міжнародним стандартам, надає рекомендації щодо вдосконалення правового регулювання у сфері кібербезпеки та сприяє гармонізації законодавства України з вимогами Ради Європи.

Експерти наводять такі рекомендації, ось кілька з них, які є дійсно перспективними: з метою ефективної протидії розповсюдженню незаконного контенту в мережі Інтернет необхідно ретельно врегулювати питання блокування та вилучення такого незаконного контенту з мережі, оскільки цей захід є дуже суперечливим. Окрему увагу при цьому належить приділяти забезпеченню того, що ордери на блокування не застосовуються щодо досить широкого переліку випадків. Варто передбачити суворе застосування вимог щодо пропорційності. Обміркувати розробку спеціальних правил щодо доступу до електронних даних, що будуть застосовуватись за невідкладних обставин, а також їхнього збирання; особливу уваги потрібно приділити умовам та запобіжним заходам щодо того, коли і за яких обставин варто проводити перевірку заходів [3, с.23]. Звісно це не повний перелік рекомендацій, які є слушними, але питання щодо заходів та спеціального доступу до електронних даних є досить цікавою порадою для втілення положень про кіберзлочинність.

Стратегічним пріоритетом вважається прийняття ефективного законодавства у сфері боротьби з кіберзлочинністю та застосування електронних доказів, яке б відповіло вимогам із забезпечення дотримання прав людини і верховенства закону [4, с. 25].

У наслідок аналізу вітчизняного законодавства та порівняння його положень із нормами Конвенції про кіберзлочинність встановлено ряд напрямків, які потребують опрацювання [4, с. 26].

Вирішення цих питань, як зазначено у Конвенції, буде сприяти підвищенню ефективності кримінальних розслідувань, що стосуються кримінальних правопорушень, пов’язаних з комп’ютерними системами і даними, і для надання можливості збирання доказів, що стосуються кримінального злочину, в електронній формі [4, с. 26].

Крім того, проблематика протидії кіберзлочинності набуває особливої важливості в умовах запровадження воєнного стану. Сучасні інформаційні війни здатні завдати шкоди, співмірної або навіть більшої за ту, що спричиняється збройними конфліктами на полі бою. У зв'язку з цим, суб'єкти, відповідальні за протидію кіберзлочинам, повинні вживати всіх можливих заходів для мінімалізації кібератак, здійснюваних противником [2, с. 374].

Підписання, державами, членами Ради Європи «Конвенції по боротьбі з кіберзлочинністю», стало результатом розуміння важливості проведення політики, спрямованої на захист суспільства від кіберзлочинів, необхідності прийняття відповідного законодавства та зміцнення міжнародного співробітництва [5].

Використання та удосконалення сфери інформаційних технологій спричинило появу кіберзлочинності – характерного наслідку глобалізації інформаційних процесів. Кіберзлочинність стала загрозою не лише для окремих осіб, а й для держав, оскільки передбачає руйнування економічної та інформаційної сфер. Характерні ознаки кіберзлочинності приваблюють людство, що означає, у свою чергу, збільшення кількості осіб, що чинять протиправну діяльність. Більшість методів соціальної інженерії не вимагають особливих технічних знань з боку зловмисників, а отже використовувати ці методи може будь-хто – від дрібних злодіїв до досвідчених кіберзлочинців [6, с. 387].

Отже, імплементація Конвенції про кіберзлочинність стала важливим кроком для України у розвитку правової системи та захисті національного кіберпростору. Вона дала можливість створити сучасне законодавство, яке відповідає міжнародним стандартам, налагодити співпрацю з іншими державами, підвищити рівень захисту інформації та сформувати дієву систему реагування на кіберзагрози. Разом із тим, цей процес потребує подальшого вдосконалення – необхідно посилювати технічні можливості державних структур, підвищувати професійний рівень працівників правоохоронних органів, розширювати освітні програми з кібербезпеки та впроваджувати новітні технології. Лише системна робота у цьому напрямі дозволить Україні ефективно протидіяти кіберзлочинності, забезпечити безпеку громадян та зберегти інформаційну стійкість держави у цифрову епоху.

Список використаних джерел

1. Жеребець О. М. Реалізація державної політики у сфері протидії кіберзлочинності: законодавчий аспект. *Інформація і право.* 2021. № 4(39). С. 129–134.

2. Захаревич Р. В. Імплементація зарубіжного досвіду в українське законодавство щодо протидії кіберзлочинам. *Аналітично-порівняльне правознавство* : електронне наукове видання. 2025. Вип. 3, ч. 2. С. 372–376.

3. Звіт щодо України. Підготовлено Офісом Програми з кіберзлочинності на основі експертної підтримки незалежних експертів Ради Європи пана Маркко Куннапу і пана Марка Юріча. Про чинне законодавство і проекти законів, що доповнюють різні питання, пов'язані з кіберзлочинністю та електронними доказами, та вносять зміни до них. 3 листопада 2016 року. URL: https://share.google/f83dkxYASNhL61Kkn

4. Бердиченко І. О. Імплементації окремих норм конвенції про кіберзлочинність у вітчизняне законодавство, проблеми та шляхи їх вирішення. 2017. С. 25–28. URL: https://share.google/fqpxOpRlmoUgbgTqN

5. Конвенція Ради Європи про кіберзлочинність. URL: https://share.google/jaI2tFm8M6PDEzFSd

6. Саєнко М. І., Савела Є. А., Тополянський Ю. Ю. Міжнародний досвід протидії кіберзлочинності та кібершахрайству. *Науковий вісник Ужгородського Національного Університету.* Серія ПРАВО. 2021. Вип. 64. С. 386–391. URL: https://doi.org/10.24144/2307-3322.2021.64.71

Морозов Михайло Андрійович,
здобувач ступеня вищої освіти магістра навчально-наукового інституту права та психології Національної академії внутрішніх справ
Науковий керівник:
Шрамко С. С., завідувач кафедри кримінального права та кримінології навчально-наукового інституту права та психології Національної академії внутрішніх справ, кандидат юридичних наук, старший дослідник

ШТУЧНИЙ ІНТЕЛЕКТ І КРИМІНАЛЬНЕ ПРАВО: НОВІ ВИКЛИКИ, РИЗИКИ ТА ПЕРСПЕКТИВИ ПРАВОВОГО РЕГУЛЮВАННЯ

Сьогодні штучний інтелект (ШІ) виступає не лише як технологічне нововведення, а й як невід'ємний елемент сучасного суспільного життя, проникаючи у бізнес, медицину, а також у діяльність правоохоронних органів і судових інституцій. З одного боку, використання ШІ забезпечує значні переваги, проте водночас породжує нові виклики для кримінального права. Зокрема, постає питання правового регулювання випадків, коли кримінальні правопорушення здійснюються із залученням роботизованих систем, автономних алгоритмів чи генеративних моделей ШІ.

ШІ може виконувати роль як знаряддя вчинення злочину, так і об'єкта правового регулювання, що потребує переосмислення традиційних категорій кримінального права, таких як вина, умисел та суб'єкт відповідальності. Наразі чинне кримінальне законодавство не завжди здатне ефективно реагувати на виклики, пов'язані з розвитком технологій ШІ. Це зумовлює необхідність адаптації правових норм, розроблення нових механізмів регулювання та формування міжнародних стандартів відповідальності. Саме тому дослідження взаємодії штучного інтелекту та кримінального права є надзвичайно актуальним, перспективним та міждисциплінарним напрямом сучасної науки.

ШІ дедалі більше впливає на можливість вчинення кримінальних правопорушень у майбутньому. Під кримінальними правопорушеннями розуміють будь-які дії або бездіяльність, що

становлять злочин відповідно до кримінального законодавства. Явищем «кримінальних правопорушень із використанням ШІ» (AI-Crime, AIC) слугують теоретичні дослідження. У одному експерименті ШІ використовували для масових фішингових атак у соціальних мережах, де повідомлення підлаштовувалися під поведінку конкретних користувачів, що дозволяло зловмиснику отримати приватні дані для шахрайства. У іншому – торгові агенти на основі ШІ навчилися маніпулювати ринком за допомогою фальшивих ордерів, отримуючи прибуток. Ці приклади демонструють, що ШІ створює нові, реально існуючі загрози у сфері кримінальної діяльності. Водночас проблема AI-Crime як окремого явища досі не отримала належного визнання. Дослідження зосереджені переважно на етичних і соціальних аспектах цивільного використання ШІ, а наукові праці про злочинність із використанням ШІ розпорошені між різними дисциплінами, що ускладнює прогнозування ризиків та пошук ефективних правових рішень [1, с. 90].

У цьому контексті ШІ може виконувати дії, які в результатів призводять до кримінального правопорушення. Щоби настали наслідки достатньо щоби правопорушник або ШІ вчинили відповідну поведінку, адже саме вона стає причиною результату. Результати оцінюються об'єктивно – якщо вони мають місце, їх спричинила саме вчинена дія, а не додаткові фактори. Оскільки ШІ здатний виконувати різні дії, він може спричиняти наслідки, що з них випливають. Наприклад, робот, який приводить у дію вогнепальну зброю і стріляє в людину, тобто формально виконує компонент поведінки злочину, а тест причинного зв'язку визначає, чи спричинила ця дія смерть. У такому випадку вимоги до поведінки та результату виконані, хоча фізично робот нічого «не робить», крім виконання алгоритму. Ключове питання – умисел. Людина, що стріляє, може заперечувати намір, але суд, застосовуючи презумпцію передбачуваності, визнає наявність умислу, якщо результат був високовірогідним. Так само здатність ШІ «мати умисел» оцінюється за ймовірністю передбачуваного результату та усвідомленням дій. Для застосування кримінальної відповідальності до ШІ потрібно встановити, що результати були передбачувані, а поведінка – свідома [2, с. 59].

Вільна воля передбачає здатність діяти для досягнення цілей незалежно від зовнішніх впливів. Людина має певний ступінь свободи волі, приймаючи рішення на основі досвіду. ШІ

здатний сприймати зовнішній світ і генерувати ефективні рішення, але наразі не володіє самосвідомістю або усвідомленням власних дій. У майбутньому, коли ШІ досягне самосвідомості, він може проявляти цілеспрямовану поведінку і творчість, що створює потенційну основу для кримінальної відповідальності. У разі заподіяння ШІ шкоди людині або участі в смертельній аварії постає питання відповідальності: нині відповідальність покладається на власника чи користувача засобу, проте визнання ШІ як інтелектуальної сутності може змінити цю практику. Сучасне кримінальне право орієнтоване на людей і не передбачає покарання для машин. Теорія відплати, яка визначає мету покарання як відновлення справедливості, не може застосовуватися до ШІ: знищення чи демонтаж машини не компенсує шкоду потерпілим і не має сенсу як покарання. Доцільність інших санкцій для ШІ також сумнівна, особливо для машин без усвідомлення [3, с. 292].

Роздуми про можливу «волю» ШІ та відсутність у чинному законодавстві санкцій щодо машин поступово переходять на рівень практичних викликів сучасних технологій: технічний прогрес робить реалістичними ситуації, коли автономні системи можуть спричиняти тяжку шкоду, отже правничі дискусії мусять поєднуватися з оцінкою фактичних можливостей і ризиків. Водночас ті самі технології можуть ефективно використовуватися для протидії злочинності.

Дослідниками зазначається, що машинне навчання дає змогу створювати алгоритми, які автоматично виявляють складні закономірності та патерни у вхідних даних, що сприяє своєчасному виявленню злочинів і прогнозуванню кримінальної активності. Обробка природної мови дозволяє системам аналізувати та розуміти великі обсяги текстової інформації з різних джерел, включно з соціальними мережами, новинами та іншими медіаресурсами. Комп'ютерний зір надає можливість обробляти візуальні дані, такі як відеозаписи та фотографії, що сприяє ідентифікації злочинців і розслідуванню подій. Ці технології стають ключовими інструментами для правоохоронних органів, підвищуючи ефективність забезпечення безпеки громадян та протидії злочинності. Застосування ШІ у кримінальному аналізі дозволяє створювати моделі, які враховують не лише очевидні фактори, а й складні взаємозв'язки між різними параметрами. Це підвищує точність прогнозування,

ускладнює обходи захисних стратегій злочинців і дозволяє оперативно реагувати на зміни у кримінальній ситуації, ефективніше запобігаючи можливим загрозам [4, с. 103].

Список використаних джерел

1. King T. C. Artificial intelligence crime: An interdisciplinary analysis of foreseeable threats and solutions. *Science and engineering ethics*. 2020. №. 1. С. 89-120. URL: https://link.springer.com/article/10.1007/s11948-018-00081-0

2. Hallevy G. When robots kill: Artificial intelligence under criminal law. UPNE, 2013.

3. Kan C. H. Criminal liability of artificial intelligence from the perspective of criminal law: An evaluation in the context of the general theory of crime and fundamental principles. *International Journal of Eurasia Social Sciences*. 2024. № 55. URL: http://dx.doi.org/10.35826/ijoess.4434

4. Макаренко В. І., Кисельов А. Інтегрування системи штучного інтелекту в кримінальний аналіз. *International scientific journal «Grail of Science*. 2024. № 35. URL: 10.36074/grail-of-science.19.01.2024.017

Мягких Софія Вікторівна,
здобувач ступеня вищої освіти бакалавра навчально-наукового інституту права та психології Національної академії внутрішніх справ
Науковий керівник:
Шопіна Ю. О., доцент кафедри кримінального права та кримінології навчально-наукового інституту права та психології Національної академії внутрішніх справ, кандидат юридичних наук

ПРОБЛЕМИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ВЧИНЕННЯ КІБЕЗЛОЧИНІВ

Штучний інтелект стає потужним інструментом не лише для розвитку економіки та науки, а й для вчинення кіберзлочинів. Його використання у кримінально-протиправних цілях зумовлює новий рівень загроз, оскільки алгоритми здатні автоматизувати

злам систем, створювати реалістичні фішингові повідомлення, генерувати шкідливий код та здійснювати масові атаки без значних ресурсних витрат, що підвищує ефективність кіберзлочинців і ускладнює виявлення кримінальних правопорушень традиційними методами. Актуальність дослідження полягає в тому, що розвиток технологій штучного інтелекту випереджає темпи формування правових механізмів їхнього регулювання та протидії такому застосуванню. В умовах зростання цифрових ризиків необхідно аналізувати потенційні загрози, розробляти нормативно-правові та технічні засоби захисту, а також формувати міжнародне співробітництво у сфері кібербезпеки, що дозволить мінімізувати небезпеку використання ШІ у протиправних цілях і забезпечити баланс між інноваціями та безпекою.

Штучний інтелект – це сукупність теоретичних та практичних підходів у галузі інформаційних технологій, які передбачають створення систем, що можуть функціонувати розумно та незалежно, подібно до механізму прийняття рішень у мозку людини [1, с. 6].

Штучний інтелект є дуже корисним в багатьох галузях діяльності. В тому числі він може бути використаний для покращення ефективності роботи правоохоронних органів та забезпечення публічної безпеки. Але є і незаконні методи застосування ChatGPT. Протиправне застосування ШІ є важливою проблемою, яка вимагає уваги як з боку суспільства, так і з боку влади. Наприклад, злочинці легко обходять вбудований розробниками ChatGPT захист: заборону на створення шкідливого коду. Для цього вони просто розбивають завдання на кілька частин, щоб запити виглядали нейтральними. А потім за інструкціями від самого ж штучного інтелекту збирають їх в одну програму. Навіть ті, хто нічого не тямлять у програмуванні, створюють шкідливі програмні засоби під свої потреби, використовуючи ChatGPT як інструктора. Ще одна популярна ніша незаконного використання нейромережі – соціальна інженерія. ChatGPT здатний без зусиль написати переконливий текст для фішингового сайту або листування, без помилок і з такими деталями, які введуть в оману користувача. Він може вести діалоги та переконувати людей у своїй правоті, створювати привабливі пропозиції для розсилок і наслідувати конкретну манеру спілкування, щоб видати себе за реально існуючу людину.

ШІ може створювати дуже реалістичні фішингові листи, повідомлення чи навіть телефонні дзвінки за допомогою голосових ботів. Наступний спосіб застосування ChatGPT – можливість безпосередньо запитати його, як скоїти кримінальне правопорушення з найбільшою вигодою, дізнатися про нові афери, схеми обману, отримати статистику щодо скоєних кримінальних правопорушень, щоб не конкурувати з іншими злочинцями, а також отримати розуміння, які помилки роблять інші шахраї, на чому їх ловить поліція, як цього уникнути. Можливе використання технологій відтворення голосу людини з метою шахрайського отримання грошей або інформації. Також за допомогою ШІ можливо генерувати підроблені документи, підписи чи фото. У процесі нелегальної діяльності у фінансовій сфері за допомогою ШІ можливе зловживання біржовими алгоритмами для маніпуляцій на фінансових ринках та аналізу схем відмивання грошей та пошуку способів їх оптимізації [2, с. 32].

Кримінальні правопорушення у сфері сучасних інформаційних та інших технологій набувають міжнародного, транснаціонального характеру, до того ж потерпілі від таких дій і самі злочинці можуть перебувати в різних країнах світу (наприклад, злочинці, навіть у місцях позбавлення волі). Для протидії таким видам кримінальних правопорушень особливе значення насамперед має посилення й удосконалення міжнародного співробітництва в цій сфері, підвищення його ефективності [3, с. 41].

Водночас впровадження штучного інтелекту у правоохоронну сферу викликає дискусії щодо конфіденційності та захисту персональних даних. Масове збирання й зберігання інформації про громадян може створити ризик зловживань і порушень прав людини. Отже, необхідно розробити чіткі та прозорі регуляторні норми, які забезпечать безпеку особистої інформації, а також запобігатимуть неправомірному використанню цих технологій. Окремим викликом стає захист персональних та, зокрема, біометричних даних. Ризик несанкціонованого доступу до таких даних або їх використання для прихованого спостереження вимагає розроблення суворих стандартів і правил [4, с. 32].

Оскільки з протиправною метою все активніше використовують інформаційні, телекомунікаційні, цифрові й інші технології, а також мережі кіберпростору, різноманітні види

засобів зв'язку, штучний інтелект та інші сучасні досягнення науки й техніки, то нагальною стає необхідність відбору, застосування й адаптування всіх цих засобів до потреб криміналістики, експертології й досудового слідства, а саме розроблення відповідних методик розслідування, які б передбачали застосування єдиних методів, засобів і прийомів для вирішення типових завдань досудового розслідування на різних його етапах [3, с. 42].

Що стосується правового регулювання, законодавчі органи повинні розробляти та впроваджувати нормативно-правові акти, що будуть в повній мірі регулювати використання штучного інтелекту в сфері прав людини та боротьби з протиправністю. Вони мають включати в себе правила щодо захисту приватності, заборони дискримінації, етичного використання алгоритмів тощо. Закони повинні вимагати від компаній, що використовують ШІ, надавати прозору та доступну інформацію про алгоритми, дані та вплив ШІ на права людини. Також мають створюватися групи для моніторингу за дотриманням прав людини та боротьби з протиправністю в контексті ШІ [5, с. 191].

Європейський комітет з проблем протиправності Ради Європи (із метою підвищення ефективності протидії таким видам кримінальних правопорушень і правового визначення в Європі групи кримінальних правопорушень, пов'язаних із комп'ютерами й інформаційними технологіями) підготував рекомендації про включення до законодавств європейських країн кримінальних норм «мінімального списку» і «необов'язкового списку» комп'ютерних кримінальних правопорушень. На початку 2002 р. ухвалено Протокол № 1 до Конвенції, який додав до цього переліку кримінальні правопорушення із поширення інформації расистського, ксенофобного й іншого характеру, що підбурює до насильницьких дій, ненависті чи дискримінації окремої особи або групи осіб і/або ґрунтується на расовій, національній, релігійній або етнічній належності. Згаданий Протокол також ратифіковано Верховною Радою України. Згідно з Конвенцією кримінальні правопорушення класифіковано за чотирма групами, а саме: 1) спрямовані проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (незаконний доступ (ст. 2), незаконне перехоплення (ст. 3), вплив на комп'ютерні дані (протиправне навмисне пошкодження, знищення, погіршення якості, зміна або блокування комп'ютерних даних) (ст. 4) або

системи (ст. 5)), протизаконне використання спеціальних технічних пристроїв (ст. 6) і комп'ютерних програм, розроблених або адаптованих для скоєння кримінальних правопорушень, передбачених у ст. 25, а також комп'ютерних паролів, кодів доступу, їх аналогів, за допомогою яких можна отримати доступ до комп'ютерної системи загалом або будь-якої її частини (норми ст. 6 застосовують тільки в разі, якщо використання (поширення) спеціальних технічних пристроїв спрямовано на скоєння протиправних діянь); 2) пов'язані з використанням комп'ютерних засобів (підроблення та шахрайство з використанням комп'ютерних технологій (ст. 7, 8): зловмисні й протиправні введення, зміна, видалення або блокування комп'ютерних даних, що тягнуть за собою порушення автентичності даних із наміром, щоб їх розглядали або використовували з юридичною метою як автентичні); 3) здійснювані з метою розповсюдження за допомогою комп'ютерних систем (надання пропозицій для користування, поширення та придбання різних видів дитячої порнографії, а також наявність дитячої порнографії в пам'яті комп'ютера певної особи; ст. 9); 4) пов'язані з порушенням авторського права й суміжних прав на програмне забезпечення (ст. 10; в Україні – ст. 176 Кримінального кодексу) [3, с. 42].

Отже, робимо висновок, що використання штучного інтелекту у сфері кіберзлочинності створює новий рівень небезпеки для інформаційної безпеки держави, бізнесу та громадян. Алгоритми здатні значно підвищувати ефективність протиправних дій, робити їх менш помітними та більш масштабними, що ускладнює їх своєчасне виявлення та формує серйозний виклик для правоохоронних органів і потребує постійного удосконалення механізмів протидії. Таким чином, виникла необхідності своєчасного оновлення законодавчої бази, розвитку сучасних засобів кіберзахисту та активного міжнародного співробітництва, бо тільки комплексний підхід дозволить мінімізувати ризики протиправного використання штучного інтелекту та зберегти баланс між технологічним прогресом і безпекою суспільства.

Список використаних джерел

1. Савченко В. А., Шаповаленко О. Д. Основні напрями застосування технологій штучного інтелекту у кібербезпеці. *Сучасний захист інформації.* 2020. С. 6–11. URL: https://surl.li/mgyeej (дата звернення: 25.09.2025).

2. Зачек О. І. Проблеми злочинного застосування штучного інтелекту. 2025. С. 32–34. URL: https://surl.li/cynjgl (дата звернення: 25.09.2025).

3. Юхно О. Генезис і проблемні питання використання новітніх технологій та штучного інтелекту в криміналістиці, експертній діяльності й досудовому розслідуванні. *Теорія та практика судової експертизи і криміналістики.* 2021. С. 40–59.

4. Кириченко В. В. Вплив штучного інтелекту на злочинність в Україні. 2025. С. 30–32. URL: https://surl.li/gwvrbs (дата звернення: 25.09.2025).

5. Андрущенко О. П. Захист прав людини в умовах розвитку штучного інтелекту. *Наукові дослідження*. 2024. С. 186–193.

Насальська Анна Олексіївна,
здобувач ступеня вищої освіти бакалавра навчально-наукового інституту права та психології Національної академії внутрішніх справ
Науковий керівник:
Шопіна Ю. О., доцент кафедри кримінального права та кримінології навчально-наукового інституту права та психології Національної академії внутрішніх справ, кандидат юридичних наук

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У ВИЯВЛЕННІ ТА ПОПЕРЕДЖЕННІ КІБЕРЗЛОЧИНІВ: ПЕРСПЕКТИВИ ТА ВИКЛИКИ ДЛЯ КРИМІНАЛЬНОГО ПРАВА

Штучний інтелект (ШІ) займає провідне місце у розвитку сучасних технологій, зокрема у сфері кібербезпеки. Збільшення обсягів цифрової інформації та ускладнення видів кіберзлочинів вимагають впровадження ефективних інструментів для їх виявлення та попередження. Завдяки своїй здатності аналізувати великі масиви даних, розпізнавати закономірності та прогнозувати потенційні загрози, ШІ відкриває нові горизонти у боротьбі з кіберзлочинністю.

Проте активне впровадження ШІ у цю сферу супроводжується низкою викликів, зокрема пов'язаних з правовим регулюванням його застосування. Кримінальне право, що традиційно орієнтується на людську діяльність та відповідальність, змушене адаптуватися до нових реалій, де рішення приймаються автоматизованими системами на базі алгоритмів. Це породжує складнощі у визначенні суб'єктів відповідальності, контролі за законністю дій ШІ та захисті прав осіб.

У доповіді буде детально проаналізовано сучасні підходи до використання штучного інтелекту у виявленні та попередженні кіберзлочинів, розглянуто перспективи розвитку таких систем, а також обґрунтовано необхідність оновлення кримінально-правових норм задля ефективної регуляції нових технологій при збереженні балансу між безпекою та захистом прав людини.

Кіберзлочинність є однією з найгостріших проблем сучасного інформаційного суспільства. Зі збільшенням обсягу цифрових даних і розвитку інтернету з'являються нові види загроз, які суттєво впливають на безпеку держави, бізнесу та громадян. Особливо актуальним це питання стало для України у зв'язку зі зростанням кількості кібератак та складністю їх виявлення та попередження. В таких умовах штучний інтелект (ШІ) набуває все більшого значення як інноваційний інструмент для боротьби з кіберзлочинністю. Водночас застосування ШІ у цій сфері ставить низку правових, етичних і технологічних викликів, що потребують комплексного аналізу в рамках кримінального права.

Метою цієї доповіді є всебічне дослідження застосування ШІ для виявлення та попередження кіберзлочинів в Україні, аналіз переваг та обмежень цієї технології, а також розгляд викликів, пов'язаних із нормативно-правовим регулюванням її використання.

За останні роки кіберзлочинність в Україні значно зросла. У 2024 році було зареєстровано понад 4 300 кіберінцидентів, що на 70 % більше, ніж у 2023 році. Найновіші кіберзлочини охоплюють фішингові атаки, розповсюдження шкідливого програмного забезпечення, кібершпигунство, а також кібертероризм, часто синхронізований з фізичними атаками на критичну інфраструктуру країни.

Особливої уваги заслуговує зростання масштабних кібернападів на державні та оборонні об'єкти, у тому числі місцеві органи влади і ключові підприємства. Більшість українських організацій, за даними досліджень, все ще не має достатнього рівня кіберзахисту – близько 70 % компаній у 2024 році не інвестували в необхідні системи безпеки.

На державному рівні Україна активізувала роботу з удосконалення законодавства в цій сфері. У березні 2025 року Верховна Рада ухвалила закон «Про кіберзахист державних інформаційних ресурсів та об'єктів критичної інфраструктури», а в квітні 2025 року його підписав Президент України. Закон передбачає створення національної системи реагування на кіберінциденти, включаючи CERT-UA і галузеві команди реагування.

У боротьбі з кіберзлочинами ШІ застосовується передусім через алгоритми машинного навчання і глибинного навчання для визначення аномалій у мережевому трафіку, автоматичного розпізнавання образів і поведінкових патернів користувачів. Особливу роль відіграють системи прогнозування кібератак на базі історичних даних та автоматизованого аналізу великих обсягів інформації. Також ШІ допомагає оптимізувати роботу правоохоронців: від автоматичного контролю за порушеннями до виявлення потенційно небезпечних осіб за допомогою соціальних мереж і відеоспостереження.

В Україні офіційно використовується програмне забезпечення з елементами ШІ, зокрема «Касандра», яка дає можливість аналізувати й прогнозувати повторні порушення закону злочинцями, а також розгортаються аеророзвідки з використанням безпілотників для різного роду моніторингових і захисних функцій.

Впровадження ШІ у правоохоронні органи України значно підвищує ефективність виявлення кіберзагроз та оперативність реагування. Кіберполіція, Служба безпеки України (СБУ) активно співпрацюють із приватним сектором і ІТ-компаніями для впровадження сучасних рішень захисту. Застосування ШІ також допомагає підвищити професійний рівень кадрів завдяки сучасним навчальним системам і тренінгам.

Крім того, автоматизація рутинних операцій та прогнозування загроз дозволяє краще планувати ресурси і запобігати потенційним атакам на ранніх етапах. Незважаючи на

значні переваги, використання ШІ у правоохоронній діяльності не позбавлене викликів. Зокрема, виникають питання юридичної відповідальності у разі помилкових рішень автоматизованих систем, а також складність визначення винності в умовах використання ШІ при розслідуванні. Проблематичним є і захист прав людини: конфіденційність персональних даних, можливість дискримінації через упереджені алгоритми, а також довіра суспільства до рішень, прийнятих машинами.

Важливою є і правова невизначеність у сфері використання ШІ, що потребує спеціального законодавчого врегулювання із захистом громадянських свобод і встановленням чітких процедур контролю за застосуванням таких технологій. Досвід ЄС, США та інших країн показує, що успішне застосування ШІ у кримінальному праві можливе за умови чіткого правового регулювання, прозорості алгоритмів і контролю за процесом їх використання. Важливими є етичні стандарти, які мають базуватися на повазі до прав людини, та багатостороннє співробітництво для обміну знаннями і швидкого реагування на глобальні кіберзагрози.

Для України критично необхідно адаптувати законодавство відповідно до міжнародних стандартів і створити мультидисциплінарні команди експертів із технологій, права та етики.

Штучний інтелект – ключовий інструмент для ефективної боротьби з кіберзлочинністю в Україні, що дозволяє швидко і точно виявляти загрози та запобігати злочинам. Водночас його впровадження вимагає вдосконалення законодавчої бази, балансування між безпекою і правами громадян, а також постійного розвитку професійних кадрів. Використання ШІ в кримінальному праві повинно базуватися на етичних принципах і прозорості, що дозволить відбудувати довіру суспільства до нових технологій і зміцнити кібербезпеку держави.

Список використаних джерел

1. Верховна Рада України. Закон України «Про кіберзахист державних інформаційних ресурсів та об’єктів критичної інфраструктури». 2025 р.

2. Президент України. Офіційне повідомлення про підписання закону про кіберзахист державних ресурсів. 2025.

3. Forbes Україна. В Україні за рік кількість кібератак зросла на 70%. 27 вересня 2025 року.

4. Synchron.ua. Кібератаки на бізнес України 2025: Нові Вектори Загроз та Виклики. 2025.

5. Detector Media. Верховна Рада ухвалила закон про кіберзахист державних ресурсів. 2025.

6. LSEJ (Legal Studies and Economic Journal). Роль технологій штучного інтелекту у правоохоронній діяльності. 2024.

7. BDO Україна. Роль штучного інтелекту в кібербезпеці: передбачення і запобігання атак. 2025.

8. Visnyk Juris (Журнал юридичних досліджень). Зарубіжний досвід використання штучного інтелекту для протидії кіберзлочинам. 2025.

9. LIGA360. Державне регулювання штучного інтелекту в Україні. 2025.

10. НАВС (Національна академія внутрішніх справ України). Міжнародний досвід правового регулювання небезпеки ШІ. 2025.

11. Держателеві дослідження та аналітика українського ринку кібербезпеки 2017-2025 років, MS Detector.

Радіонова Валерія Іванівна,
здобувач ступеня вищої освіти бакалавра навчально-наукового інституту права та психології Національної академії внутрішніх справ
Науковий керівник:
Смаглюк О. В., доцент кафедри кримінального права та кримінології навчально-наукового інституту права та психології Національної академії внутрішніх справ, кандидат юридичних наук, доцент

КРИМІНАЛЬНА ВІДПОВІДАЛЬНІСТЬ ЗА КІБЕРБУЛІНГ І ПЕРЕСЛІДУВАННЯ В МЕРЕЖІ: ПРОГАЛИНИ ЗАКОНОДАВСТВА

У цифрову епоху Інтернет перетворився не лише на зручний засіб спілкування, але й на простір, де все частіше фіксуються випадки психологічного насильства, зокрема

кібербулінг і кіберсталкінг. Ці явища порушують право кожного на невтручання в особисте і сімейне життя, закріплене статтею 32 Конституції України право кожного на невтручання в особисте і сімейне життя [1], а також статтю 17 Міжнародного пакту про громадянські і політичні права, згідно з якою «ніхто не може зазнавати свавільного або незаконного втручання в його особисте життя, недоторканність житла чи кореспонденції, або посягань на його честь і репутацію» [2].

Мета роботи полягає у всебічний аналіз проблеми кримінальної відповідальності за кібербулінг і переслідування в мережі в Україні. Основне завдання – виявити прогалини чинного законодавства та окреслити шляхи його вдосконалення з урахуванням міжнародних стандартів захисту прав людини.

Кібербулінг – це навмисне, повторюване та систематичне здійснення протиправних дій, що мають нав'язливий характер і спрямовані на приниження, переслідування або створення психологічного тиску на людину. Це може проявлятися у формі цькування, залякування чи приниження через засоби електронної комунікації. В Україні це явище частково регулюється положеннями Кодексу України про адміністративні правопорушення [3], проте запроваджені заходи відповідальності недостатньо враховують серйозні наслідки, які можуть негативно впливати на психологічний стан постраждалих.

Доктор юридичних наук О. Бандурка вказує на те, що адміністративна відповідальність за кібербулінг не відповідає рівню суспільної небезпеки цього правопорушення, оскільки воно часто перебуває на межі з кримінально караними формами насильства [4].

Відсутність законодавчого визначення терміну «кіберсталкінг» створює значні прогалини у формулюванні та регламентації цього поняття в контексті чинного законодавства України. На основі проведеного аналізу можна припустити, що поняття «кібербулінг» може бути тлумачено як переслідування особи з використанням засобів Інтернету, соціальних мереж або месенджерів.

Подібні дії можуть потрапляти під регулювання статті 126-1 Кримінального кодексу України, яка охоплює випадки домашнього насильства, статті 182, що передбачає відповідальність за порушення права на недоторканність приватного життя, статті 129, яка стосується погрози вбивством,

а також статті 153, що установлює відповідальність за сексуальне насильство Кримінального кодексу України [5].

Відсутність конкретного визначення призводить до зволікання з розслідуванням і безкарності переслідувачів, адже, правова кваліфікація кіберсталкінгу в Україні ускладнена саме через невизначеність складу злочину, що унеможливлює диференціацію між жартом, переслідуванням та психологічним насильством [6].

Ратифікація Україною Стамбульської конвенції (далі – Конвенція) [7] відкрила шлях до криміналізації зазначених вище дій. Стаття 34 Конвенції прямо зобов'язує держави-учасниці вжити необхідних законодавчих або інших заходів для криміналізації навмисного переслідування, що викликає у потерпілої особи страх за свою безпеку. У рекомендаціях Групи експертів Ради Європи з протидії насильству (GREVIO) наголошується, що переслідування у цифровому середовищі становить ту саму загрозу, що і фізичне наближення, тому має отримати однакову правову оцінку [8].

Практика Європейського суду з прав людини підтверджує, що держава несе позитивні зобов'язання щодо захисту осіб від кіберпереслідування. У справі Buturuga v. Romania (2020), Суд постановив, що відсутність належної реакції органів влади на переслідування в мережі є порушенням статей 3 і 8 Конвенції про захист прав людини і основоположних свобод. де ЄСПЛ визнав, що «кіберпереслідування, як і фізичне, становить форму насильства, яка має бути ефективно розслідувана державою» [9].

Питання, порушене в цій роботі, є досить новим для українського правового поля. У зв'язку із глобалізацією суспільства та стрімким розвитком Інтернет-середовища, законодавству, яке створювалося понад 15 років тому, стає дедалі складніше адаптуватися до сучасних реалій. Наразі українське законодавство демонструє свою недосконаліть через низку прогалин, зумовлених динамічними змінами цифрового середовища. До найбільших проблем можна віднести:

1. Відсутність чіткого законодавчого визначення терміна «кіберсталкінг».

2. Правове регулювання кібербулінгу обмежується лише адміністративною відповідальністю, без урахування можливостей кримінального переслідування.

3. Недостатня розробка єдиної методики розслідування таких злочинів.

4. Невизначеність і недостатня сформованість судової практики у цій сфері.

Сучасне кримінальне право має бути адаптоване до цифрових реалій, адже поява нових способів вчинення злочинів потребує впровадження відповідних механізмів їх протидії [10].

Для вирішення зазначених проблем необхідно:

1. Прийняти спеціальний закон про протидію кібернасильству.

2. Внести зміни до Кримінального кодексу України, передбачивши окремий склад злочину під назвою «переслідування в цифровому просторі».

3. Розробити і впровадити національні програми, спрямовані на підвищення цифрової грамотності та безпеки.

4. Створити ефективну систему психологічної підтримки жертв кібернасильства.

5. Підготувати правоохоронців до роботи з електронними доказами та забезпечити їх належними інструментами для боротьби з такими правопорушеннями.

Україна потребує сучасного підходу до цих викликів, аби забезпечити ефективний захист прав громадян у новітньому цифровому середовищі.

Висновок. Кібербулінг є новою формою насильства, яка порушує базові права людини на гідність, безпеку та приватність. В Україні відсутнє конкретне кримінально-правове визначення таких дій, що значно ускладнює притягнення винних до відповідальності. З урахуванням міжнародних стандартів, зокрема вимог Стамбульської конвенції та практики Європейського суду з прав людини, виникає необхідність запровадження в Кримінальному кодексі України окремих статей, які б визначали відповідальність за переслідування та цькування в цифровому просторі. Такий крок сприятиме реальному захисту постраждалих і стане важливим етапом у створенні безпечного правового простору в Інтернеті.

Список використаних джерел

1. Конституція України від 28.06.1996 р.

2. Міжнародний пакт про громадянські і політичні права від 16.12.1966р.

3. Закон України «Про ратифікацію Конвенції Ради Європи про запобігання насильству щодо жінок і домашньому насильству та боротьбу з цими явищами» № 2319-IX від 20.06.2022 р.

4. Кодекс України про адміністративні правопорушення.

5. Бандурка О. М. Цифрова безпека особи у контексті кримінального права України. Харків : Право, 2021.

6. Кримінальний кодекс України.

7. Стамбульської конвенції Закон № 2319-IX від 20 червня 2022 р.

8. GREVIO. Baseline Evaluation Report on Ukraine (2023). Council of Europe.

9. Постанова ЄСПЛ у справі Buturuga v. Romania (Application no. 56867/15), 11 лютого 2020 р.

10. Тацій В. Я. Кримінальне право України: проблеми адаптації до європейських стандартів. Харків: Право, 2022.

Романська Валерія Ігорівна,
здобувач ступеня вищої освіти магістра навчально-наукового інституту права та психології Національної академії внутрішніх справ
Науковий керівник:
Семенов В. В., доцент кафедри криміналістики навчально-наукового інституту права та психології Національної академії внутрішніх справ, кандидат юридичних наук, доцент

ОПТИМІЗАЦІЯ РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ ЗА ДОПОМОГОЮ ШТУЧНОГО ІНТЕЛЕКТУ

У сучасному світі стрімкий розвиток інноваційних розробок зумовлює появу новітніх векторів вдосконалення у всіх сферах життєдіяльності: медицині, промисловості, фінансах та, що особливо важливо, у правоохоронній діяльності та криміналістиці. З кожним днем інформаційні технології стають невід'ємною частиною нашого повсякденного життя, відіграючи ключову роль у вирішенні складних завдань та оптимізації різноманітних процесів.

Розслідування та розкриття злочинів стає дедалі складнішим і ресурсомістким, вимагаючи обробки великих обсягів даних (Big Data) та мінімізації людської помилки. Безумовно, вдосконалення правоохоронної системи та підвищення продуктивності протидії злочинності має здійснюватися за допомогою сучасних інформаційних технологій. Зокрема, Штучний Інтелект (ШІ) став звичайним явищем у діяльності правоохоронних органів, відкриваючи перед ними нові можливості. ШІ широко використовується як інструмент протидії злочинності: від обробки масштабних даних та виявлення правопорушників до аналізу, моделювання та прогнозу злочинності. Саме в криміналістиці – науці, що вивчає закономірності виявлення, фіксації, вилучення, дослідження та використання доказів, – ШІ відкриває найбільший потенціал для трансформації експертних досліджень. Це включає автоматизацію аналізу ДНК, трасологічних об'єктів, а також об'єктивізацію таких чутливих сфер, як дактилоскопічна експертиза. Втім, використання ШІ в правоохоронній діяльності та криміналістиці піднімає гострі етичні та правові питання. Йдеться про збереження конфіденційності даних, зменшення ймовірності виникнення систематичних помилок (алгоритмічна упередженість) та необхідність прозорості функціонування систем, особливо тих, що використовують технологію «чорної скриньки» [1].

Крім цього, порушене питання потребує чіткого нормативно-правового регулювання для збереження балансу між ефективною правоохоронною системою та захистом прав і свобод громадян. Термін «штучний інтелект» є новим для українського законодавства, і наразі відсутнє чітке визначення його правового статусу та регулювання застосування. Відсутність концептуальних засад державної політики у сфері ШІ унеможливлює повноцінний розвиток конкурентного середовища та ефективне, законне впровадження цих критичних технологій у судову та правоохоронну практику.

Однією з найбільш перспективних галузей застосування штучного інтелекту є дактилоскопіювання, або аналіз відбитків пальців. Цей метод використовується у правоохоронних органах, судових експертизах та системах безпеки для ідентифікації особи. Традиційно цей процес був досить трудомістким, вимагав значних людських ресурсів та часу, але завдяки автоматизації та

використанню передових алгоритмів аналіз стає швидшим і точнішим. Дактилоскопія є науковим методом аналізу унікальних відбитків пальців людини. Відбитки формуються ще під час внутрішньоутробного розвитку і залишаються незмінними протягом усього життя. Кожен відбиток має власний набір гребенів і борозен, що формують певний малюнок. Основні типи візерунків включають дуги, петлі та завитки. Традиційно дактилоскопічний аналіз здійснюється вручну експертами, що займаються порівнянням відбитків, проте з розвитком технологій значна частина роботи була автоматизована. Штучний інтелект відкриває нові можливості у дактилоскопії, дозволяючи швидше та точніше ідентифікувати особу[2,С. 68-76].

Основні напрямки застосування штучного інтелекту в цій сфері включають автоматизоване розпізнавання відбитків пальців, поліпшення якості відбитків, виявлення підроблених відбитків, аналіз частково зруйнованих чи пошкоджених відбитків, підвищення точності збігів за рахунок адаптивного навчання нейронних мереж. Крім того, штучний інтелект може аналізувати багатофакторні дані, наприклад, стан шкіри, вологість пальців, тиск при натисканні, що дозволяє уникнути хибних збігів. Це особливо важливо при роботі з нечіткими або неповними відбитками, які часто трапляються у криміналістичних дослідженнях.

Автоматизована дактилоскопічна ідентифікаційна система (далі – АДІС) – інформаційно-комунікаційна система, у якій реалізується технологія обробки та ідентифікації дактилоскопічних даних у межах реалізації повноважень суб'єктами АДІС. Основними завданнями АДІС є автоматизація дактилоскопічного обліку щодо наповнення, зберігання, захисту даних в інформаційному масиві, пошуку, узагальнення та ідентифікації дактилоскопічних даних в АДІС, забезпечення доступу суб'єктів АДІС до інформаційного масиву відповідно до наданих прав доступу до інформації. Метою обробки інформації в АДІС є:розшук осіб, зниклих безвісти, у тому числі за особливих обставин; встановлення особи невпізнаних трупів за дактилоскопічними картами осіб, взятих на облік; встановлення осіб, які не здатні за станом здоров'я або віком повідомити дані про себе; підтвердження особи людей, щодо яких раніше проводилося дактилоскопіювання; встановлення осіб, які залишили сліди пальців та/або долонь рук на місці

вчинення кримінального правопорушення; ідентифікація слідів пальців та/або долонь рук, вилучених із різних місць учинення кримінальних правопорушень[5].

Однією з найбільш критичних переваг ШІ є його здатність обробляти сліди, отримані у несприятливих умовах. Штучний інтелект може використовувати алгоритми згладжування, шумозаглушення та реконструкції зображень для відновлення пошкоджених або нечітких відбитків. Це особливо важливо при роботі з частково стертими або змазаними відбитками (латентними слідами), які раніше могли бути визнані непридатними для ідентифікації. Використання спеціалізованих алгоритмів покращення зображень дозволяє отримати більш чітке зображення навіть у складних випадках. Крім того, аналіз зображень у високій роздільній здатності дозволяє ідентифікувати мінімальні деталі, які можуть бути критично важливими у розслідуваннях. Це безпосередньо підвищує кількість придатних для ідентифікації, посилюючи доказову базу.

Штучний інтелект може аналізувати структуру відбитку пальця, щоб визначити, чи є він справжнім (живим) або створеним штучно (підробленим). Глибокі нейронні мережі можуть навчатися розрізняти реальні відбитки від підроблених, виготовлених за допомогою латексу чи інших матеріалів.

Ця технологія, відома як лайвнес-детекція (liveness detection) або спуфінг-детектор, є життєво необхідною не лише у криміналістиці, а й у системах біометричної автентифікації. Вона допомагає запобігати шахрайству у фінансових та державних установах, забезпечуючи додатковий рівень безпеки.

Ваш текст уже має гарний вступ і детальний опис теоретичних основ. Цей новий фрагмент ідеально посилює розділ про практичне застосування, деталізуючи використання вже існуючих автоматизованих систем (AFIS, IAFIS, NGI) та наголошуючи на тренді мультифакторної біометрії.

Правоохоронні органи різних країн активно впроваджують штучний інтелект для обробки дактилоскопічних даних, що стало наступним кроком після створення традиційних автоматизованих систем. Автоматизовані системи ідентифікації відбитків пальців (зокрема, AFIS, американська IAFIS та її наступниця NGI) стали основою для швидкого пошуку збігів у мільйонних базах даних.

Саме завдяки інтеграції алгоритмів штучного інтелекту та машинного навчання в ці системи, правоохоронці можуть значно швидше ідентифікувати підозрюваних та розкривати злочини. Впровадження таких систем дозволяє скоротити час аналізу відбитків від годин до хвилин і багаторазово підвищити ефективність розслідувань. ШІ допомагає не просто порівнювати існуючі мітки (мініції), а й навчається знаходити неочевидні патерни та відновлювати зображення, що підвищує загальну точність [4].

Однією з найбільш критичних переваг ШІ є його здатність обробляти сліди, отримані у несприятливих умовах. Штучний інтелект може використовувати алгоритми згладжування, шумозаглушення та реконструкції зображень для відновлення пошкоджених або нечітких відбитків. Це особливо важливо при роботі з частково стертими або змазаними відбитками (латентними слідами), які раніше могли бути визнані непридатними для ідентифікації. Використання спеціалізованих алгоритмів покращення зображень дозволяє отримати більш чітке зображення навіть у складних випадках. Крім того, аналіз зображень у високій роздільній здатності дозволяє ідентифікувати мінімальні деталі, які можуть бути критично важливими у розслідуваннях.

Технології штучного інтелекту активно інтегруються з іншими біометричними методами, такими як розпізнавання облич та аналіз райдужної оболонки ока, що забезпечує ще вищий рівень точності та надійності ідентифікації. У деяких країнах вже впроваджуються нові протоколи ідентифікації, які базуються на мультифакторному аналізі біометричних даних. Це комбіноване використання кількох біометричних ознак, оброблених ШІ, що значно зменшує ризик помилкових збігів та підвищує загальний рівень безпеки та доказової впевненості у криміналістичних висновках[3,С. 429].

Штучний інтелект також виконує функцію спуфінг-детектора. Він може аналізувати структуру відбитку пальця, щоб визначити, чи є він справжнім або створеним штучно. Глибокі нейронні мережі можуть навчатися розрізняти реальні відбитки від підроблених, виготовлених за допомогою латексу чи інших матеріалів. Така технологія є життєво необхідною у біометричній автентифікації для запобігання шахрайству

Штучний інтелект став каталізатором трансформації дактилоскопічної експертизи, перетворивши її з трудомісткого ручного процесу на високошвидкісний, об'єктивний та потужний інструмент криміналістичної ідентифікації. Системи, інтегровані з ШІ (AFIS, NGI), забезпечують безпрецедентну швидкість та точність ідентифікації, здатні відновлювати латентні сліди та працювати з мультифакторною біометрією, суттєво посилюючи доказову базу. Проте, повноцінна реалізація потенціалу ШІ залежить від успішного вирішення правових та етичних викликів, пов'язаних із прозорістю алгоритмів та упередженістю. Критично важливим є невідкладне розроблення чітких нормативно-правових рамок (як це передбачено Концепцією розвитку ШІ в Україні), які гарантують підзвітність і захист конституційних прав громадян при використанні цих інноваційних технологій у судочинстві.

Список використаних джерел

1. Про схвалення Концепції розвитку штучного інтелекту в Україні: Розпорядження Кабінету міністрів України від 2 грудня 2020 р. за № 1556-р. URL: https://zakon.rada.gov.ua/-laws/show/1556-2020 %D1%80#Text

2. Яровий К. Штучний інтелект як інструмент протидії злочинності. *Юридичний вісник*. 2024. № 2. С. 68–76. URL: http://yurvisnyk.in.ua/v2_2024/11.pdf

3. Комп'ютерно-інтегровані технології: освіта, наука, виробництво : науковий журнал. Луцьк, 2025. Вип. 60.

4. Справжній робокоп: як використовують ШІ для розкриття злочинів. URL: https://robotdreams.cc/uk/blog/362-spravzhniy-robokop-yak-vikoristovuyut-shi-dlya-rozkrittya-zlochiniv

5. Про затвердження Положення про функціональну підсистему «Автоматизована дактилоскопічна ідентифікаційна система» єдиної інформаційної системи Міністерства внутрішніх справ. URL: https://zakon.rada.gov.ua/laws/show/z1691-24#Text

Ружнілова Вікторія Віталіївна,
здобувач ступеня вищої освіти бакалавра навчально-наукового інституту права та психології Національної академії внутрішніх справ
Науковий керівник:
Козачина А. М., старший викладач кафедри кримінального права та кримінології навчально-наукового інституту права та психології Національної академії внутрішніх справ, доктор філософії

КІБЕРБУЛІНГ ЯК ФОРМА ПОСЯГАННЯ НА ЧЕСТЬ, ГІДНІСТЬ І БЕЗПЕКУ ОСОБИ

Поширення цифрових технологій та соціальних мереж призвело до появи нових форм посягання на честь, гідність і безпеку особи. Однією з таких форм є кібербулінг – агресивний, навмисний акт, учинений однією особою або групою осіб з використанням електронних форм стосовно жертви, якій важко захистити себе. Зазвичай здійснюється неодноразово за певний період часу та характеризується нерівністю сил. Кібербулінг може включати поширення слухів, розміщення неправдивої інформації або неприємних повідомлень, коментарів чи фотографій, які принижують, а також виключення будь-кого з онлайн-мереж чи комунікацій [1]. В українській мові термін «кібербулінг» вживається для позначення процесу навмисного й наполегливого переслідування або нападів, що виражається через дії, які можна описати дієсловами «дратувати», «задирати», «прискіпуватися», «провокувати», «дошкуляти», «тероризувати», «цькувати» тощо.

Це явище є особливо небезпечним, оскільки його прояви часто відбуваються у віртуальному середовищі, де кривдник може залишатися анонімним, а жертва – беззахисною, що ускладнює її можливість протидії. У науковій літературі та правозастосовній практиці підкреслюється, що кібербулінг є не лише соціальною проблемою, а й правопорушенням, яке зачіпає фундаментальні особисті немайнові права людини, такі як честь, гідність, особиста і сімейна таємниця і психологічна безпека.

В Україні правовий механізм протидії кібербулінгу формується через поєднання адміністративної, кримінальної та цивільно-правової відповідальності. Так, адміністративна відповідальність передбачена ст. 173-4 КУпАП «Булінг (цькування) учасників освітнього процесу». Кримінальна відповідальність може наставати у випадку, коли, для прикладу, внаслідок булінгу постраждала особа здійснює самогубство чи замах на самогубство (ст. 120 КК України). Цивільним кодексом України передбачено відповідальність за поширення неправдивої інформації в інтернеті, зокрема ст. 277 «Спростування недостовірної інформації» та ст. 278 «Заборона поширення інформації, якою порушуються особисті немайнові права». Одночасно із вимогами про захист честі, гідності та ділової репутації, згідно зі ст. 280, можна вимагати відшкодування матеріальної та моральної шкоди [2]. Поєднання адміністративних, кримінальних і цивільних засобів захисту дозволяє як реагувати на прояви кібербулінгу, так і формувати превентивну стратегію протидії у цифровому суспільстві.

Кібербулінг має численні прояви, жоден із яких не можна ігнорувати. До них належать: погрозливі й образливі текстові повідомлення; розповсюдження відео та фотографій порнографічного змісту; троллінг – погрозливі або грубі повідомлення в соціальних мережах; демонстративне видалення зі спільнот у соцмережах чи онлайн-ігор; створення груп ненависті до конкретної особи; провокування підлітків до самогубства чи завдання шкоди собі створення підробних сторінок у соцмережах або викрадення даних для формування онлайн-клонів [3]. Такі дії порушують право на недоторканність приватного життя, честь і гідність особи, завдають значної психологічної шкоди, формуючи у жертви тривогу, депресію, ізоляцію та низьку самооцінку.

Водночас анонімність і масштабність цифрового середовища значно ускладнюють можливість ефективного реагування на такі порушення, що підкреслює необхідність комплексного підходу, який поєднує правові, освітні та психологічні засоби захисту.

Відмінності кібербулінгу від булінгу зумовлюють принципово інший підхід до роботи з жертвами та переслідувачами, адже типовий для булінгу метод покращення стосунків в учнівській групі чи підвищення її згуртованості у випадку кібербулінгу застосувати неможливо.

Тому одним з важливих кроків протидії кібербулінгу є формування довіри між батьками та дітьми, ознайомлення батьків з психічними та поведінковими ознаками того, що дитина переживає цькування, навчання технікам обережного розпитування щодо знущань. Також для профілактики віктимної поведінки важливим є формування у дитини з раннього віку почуття власної гідності, самоповаги, розуміння того, що ніхто не має права її принижувати та ображати і завжди є дорослі, які допоможуть у складній ситуації [4]. Кібербулінг є серйозною соціальною та правовою проблемою, що потребує своєчасного реагування та превентивних заходів.

Отже, превентивна робота, освіта та психологічна підтримка є ключовими елементами у формуванні безпечного цифрового середовища. Лише комплексне поєднання правових, освітніх і психологічних механізмів дозволяє ефективно протидіяти кібербулінгу та захищати честь, гідність і безпеку особи у цифровому суспільстві. Це потребує спільних зусиль держави, навчальних закладів, сім'ї та громадськості, а також постійного вдосконалення правових норм і практик реагування на нові прояви цифрового насильства.

Список використаних джерел

1. Мойса, Б. Протидія кібербулінгу та кібергрумінгу в Україні : попередній аналітичний огляд. [Б. м.] : Docudays UA, 2023. 18 с.

2. Пилипишина І.І. Протидія кібербулінгу як забезпечення права дитини на безпеку. *Науковий вісник Ужгородського національного університету*. Серія: Право. 2024. Вип. 83, ч. 1. С. 141–146. DOI: https://doi.org/10.24144/2307-3322.2024.83.1.20.

3. Миронюк Т. В., Запорожець А. К. Кібербулінг в Україні – соціально небезпечне явище чи злочин: визначення та протидія. *Юридичний часопис Національної академії внутрішніх справ*. 2018. № 2 (16). С. 275.

4. Петренко, О. В. Протидія кібербулінгу в Україні: правовий аспект. *Перспективи науки і освіти*. 2019. Вип. 1. С. 121–126. DOI: https://doi.org/10.31472/pis.1.2019.121–126.

Рябокінь Максим Русланович,
здобувач ступеня вищої освіти бакалавра навчально-наукового інституту права та психології Національної академії внутрішніх справ
Науковий керівник:
Резнік Ю. С., старший викладач кафедри кримінального права та кримінології навчально-наукового інституту права та психології Національної академії внутрішніх справ, кандидат юридичних наук

КІБЕРБУЛІНГ В УКРАЇНІ: ФОРМИ, СОЦІАЛЬНО-ПСИХОЛОГІЧНІ НАСЛІДКИ ТА ПРАВОВЕ РЕГУЛЮВАННЯ

Проблема кібербулінгу, є однією з найбільш гострих соціальних та правових загроз, що виникають внаслідок стрімкої інтеграції цифрових технологій у повсякденне життя. Кібербулінг визначається як форма психологічного насильства, що здійснюється із застосуванням електронних комунікаційних технологій [1]. Інше поширене визначення трактує його як агресивний, навмисний вчинок, що здійснюється групою або індивідом за допомогою електронних засобів зв'язку, повторювано і з часом, проти жертви, яка не може легко захистити себе [2]. Саме така повторюваність та доступність цифрових платформ робить кібербулінг особливо небезпечним.

Масштаби кібербулінгу в Україні, за даними національних та міжнародних досліджень, є тривожними: щонайменше третина підлітків у віці 12–18 років засвідчували або ставали жертвами цькування в мережі [3]. Така висока поширеність обумовлена постійною доступністю Інтернету, зниженням рівня цифрового етикету та недостатньою обізнаністю користувачів. Основні платформи, що використовуються для цькування, включають соціальні мережі (Instagram, TikTok), месенджери (Telegram), а також онлайн-ігри та електронну пошту.

Цифрове середовище надає агресорам можливість анонімності та необмеженого поширення інформації, що багаторазово посилює психологічний тиск на жертву.

Серед основних форм кібербулінгу виділяють:

1. Тролінг (Trolling) – систематичне розміщення провокаційних або образливих повідомлень з метою емоційного розпалювання конфлікту [4]. Наприклад, навмисне провокування конфлікту у коментарях під відео.

2. Кіберсталкінг (Cyberstalking) або переслідування – залякування та збір особистої інформації про жертву (фото, геолокація) з подальшою розсилкою погроз або принизливих повідомлень, що часто має тривалий і нав'язливий характер [4].

3. Поширення конфіденційних даних (Doxing та Impersonation) –розголошення особистої інформації жертви без її згоди (Doxing) або видавання себе за іншу особу шляхом створення фейкових облікових записів для дискредитації чи зловживання довірою (Impersonation) [4].

4. Виключення (Exclusion) – навмисне виключення особи з онлайн-групи, чату чи спільноти з метою соціальної ізоляції [5].

5. Кіберхарасмент (Cyberharassment) – неодноразове надсилання образливих, ворожих або загрозливих повідомлень [5].

6. Хепі-слепінг (Happy Slapping) – акт насильства (фізичного або морального приниження) із записом на камеру та публічним розповсюдженням відео у мережі [5].

Кібербулінг часто межує з іншими кримінальними діяннями. До них належать:

1. Кібершантаж (Cyber Extortion) – вимагання грошей чи інших благ під загрозою розповсюдження компрометуючих даних або відео [4]. Наприклад, погрози опублікувати приватні фото, якщо жертва не виконає вимоги.

2. Фінансовий аб'юз онлайн (Online Financial Abuse) – несанкціоновані транзакції, злом акаунтів або вимагання грошей через цифрові платформи [4].

3. Несанкціоноване втручання у цифрові системи – злом облікових записів, серверів чи банківських систем з метою крадіжки фінансової чи персональної інформації [4].

Наслідки кібербулінгу для жертв є глибокими та деструктивними. Публічність та повторюваність цькування призводять до депресії, підвищеної тривожності, порушень сну, соціальної ізоляції, апатії до навчання та, в крайніх випадках, до формування суїцидальних думок [6]. Це руйнує інтегративний характер соціального середовища, підкреслюючи необхідність комплексних превентивних заходів.

В Україні правове регулювання кібербулінгу ще перебуває на стадії формування. На відміну від західних країн, де антибулінгова політика підкріплена чітким законодавством, в Україні досі відсутній спеціальний закон, що визначав би поняття «кібербулінг» та класифікував його форми. Це ускладнює процеси збирання доказів та притягнення винних до відповідальності.

Наразі застосовуються такі правові механізми:

1. Кодекс України про адміністративні правопорушення: Стаття 173-4 (Булінг/цькування), яка охоплює і кібербулінг, але не деталізує його специфіку [7].

2. Кримінальний кодекс України: Статті 120 (доведення до самогубства), 129 (погроза вбивством) та 301 (розповсюдження інтимних зображень без згоди) [7].

3. Закон України «Про освіту» (ст. 25, 26): Регулює запобігання булінгу в освітньому середовищі [7].

Боротьба з кібербулінгом ускладнюється безкарністю та браком чіткої відповідальності за дії в мережі. Необхідне термінове доопрацювання законодавства, що регламентує відповідальність за кібербулінг, сприяючи ефективнішій роботі Кіберполіції та судових органів. Паралельно важливим є впровадження освітніх програм для учнів та педагогів, спрямованих на підвищення цифрової грамотності, формування культури цифрового етикету та створення доступних механізмів подання скарг для жертв. Лише комплексний підхід, що поєднує правову регламентацію та просвітницьку діяльність, здатен забезпечити безпечне цифрове середовище.

Список використаних джерел

1. Kowalski, R. M., Limber, S. P., & Agatston, P. W. (2012). Cyberbullying: Bullying in the digital age (2nd ed.). Wiley-Blackwell.

2. Patchin, J. W., & Hinduja, S. (2013). Cyberbullying. , The Encyclopedia of Criminology and Criminal Justice. Wiley-Blackwell.

3. Денісова, А. (2021). Кібербулінг: поширеність та наслідки в учнівському середовищі.

4. Hardaker, C. (2010). Trolling in asynchronous computer-mediated communication: From user discussions to academic definitions. Journal of Politeness Research, 6(2), 215–242.

5. Willard, N. E. (2007). Cyberbullying and cyberthreats: Responding to the challenge of online social aggression, threats, and distress. Center for Safe and Responsible Internet Use.

6. Hinduja S., Patchin, J. W. (2010). Bullying, Cyberbullying, and Suicide. *Archives of Suicide Research*, 14(3), 206–221.

7. Законодавчі акти України: Кодекс України про адміністративні правопорушення, Кримінальний кодекс України, Закон України «Про освіту».

Саінчин Олександр Сергійович,
професор кафедри криміналістики навчально-наукового інституту права та психології Національної академії внутрішніх справ, доктор юридичних наук, професор

КРИМІНАЛІСТИЧНІ ЗАСАДИ ПРОТИДІЇ КРИМІНАЛЬНОГО ПРАВА В КІБЕРПРОСТОРІ

Стратегія інформаційної безпеки України – це державний документ, що визначає загрози, стратегічні цілі та завдання для захисту інформаційної сфери держави. Її головна мета – забезпечити захист життєво важливих інтересів громадян, суспільства та держави, протидіяти загрозам, забезпечувати суверенітет, територіальну цілісність та права громадян. Документ затверджений указом Президента № 685/2021 від 28 грудня 2021 року, реалізація якого розрахована до 2025 року [1; 2].

Згідно з затвердженим Кабінетом Міністрів плану заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року визначні наступні стратегічні цілі, на деяких аспектах реалізації яких в контексті служби безпеки України, ми вважаємо доцільно зупинитися окремо [3]:

1. Протидія дезінформації та інформаційним операціям, насамперед держави-агресора, спрямованим, серед іншого, на ліквідацію незалежності України, повалення конституційного ладу, порушення суверенітету і територіальної цілісності держави, пропаганду війни, насильства, жорстокості, розпалювання національної, міжетнічної, расової, релігійної ворожнечі та ненависті, вчинення терористичних актів, посягання на права і свободи людини і громадянина.

На Службу безпеки України [4] та Службу зовнішньої розвідки покладено реалізації наступних заходів: а) проведення моніторингу спеціальними методами і способами вітчизняних та іноземних медіа, Інтернету з метою виявлення загроз національній безпеці України в інформаційній сфері; б) здійснення добування, аналітичного опрацювання, оброблення та надання розвідувальної інформації в установленому Законом України «Про розвідку» порядку її споживачам, відповідальним за формування і реалізацію державної інформаційної політики та здійснення заходів стратегічних комунікацій; в) проведення офіційного моніторингу телерадіопрограм українських телерадіоорганізацій та іноземних мовників, які ретранслюють свої програми на території України; г) підготовка проведення систематичного узагальнюючого моніторингу національного інформаційного простору на предмет виявлення дезінформації, що містить загрози для національної безпеки України; д) підготовка проведення систематичного узагальнюючого моніторингу іноземного інформаційного простору (окремі країни) на предмет виявлення дезінформації, що містить загрози для національної безпеки України [5; 6].

Крім цього на Адміністрацію Держспецзв'язку, Мінцифри МКІП, Центр протидії дезінформації, Національний інститут стратегічних досліджень, наукові та науково-дослідні установи, які забезпечують науково-аналітичне та експертне супроводження процесу формування та реалізації державної інформаційної політики, покладені наступні обов'язки:

а) створення системи раннього виявлення, прогнозування та запобігання гібридним загрозам, зокрема створення системи протидії дезінформації та інформаційним операціям, спрямованої на запобігання, максимально швидке виявлення та реагування держави і суспільства на інформаційні загрози;

б) вжиття заходів до запобігання та протидії поширенню дезінформації та деструктивної пропаганди стосовно європейської та євроатлантичної інтеграції України;

в) розвиток спроможностей складових сил оборони щодо протидії загрозам в інформаційному просторі;

г) підготовка та проведення складовими сил оборони інформаційно-психологічних операцій та інших заходів, спрямованих на запобігання, стримування та відсіч збройної агресії Російської Федерації проти України;

д) посилення відповідальності за поширення недостовірної інформації (дезінформації) [7–9].

Стратегія інформаційної безпеки є рамковим документом і поки що не дає можливості оцінити, наскільки її впровадження вплине на реалізацію цифрових прав. Тим не менш, при розробці плану дій та законодавства, спрямованих на впровадження Стратегії, варто враховувати такі застереження:

– будь-які законодавчі заходи, спрямовані на протидію дезінформації та обмеження доступу до шкідливого контенту в Інтернеті можуть обмежувати право на свободу вираження поглядів виключно за умови відповідності вимогам законності та пропорційності;

– діяльність державних органів, залучених в імплементацію Стратегії має бути прозорою та з чітким розподілом повноважень, зокрема, слід більш чітко визначити орган, відповідальний за реалізацію Стратегії, що аналізуватиме та звітуватиме перед суспільством про ефективність заходів, вжитих на її виконання;

– План дій на виконання Стратегії має передбачати чіткі індикатори вимірювання ефективності її впровадження;

– при реалізації положень Стратегії та розробці Плану дій на її виконання має бути забезпечена повноцінна, а не формальна залученість громадськості.

Список використаних джерел

1. Стратегія інформаційної безпеки, затверджена Указом Президента України від 28.12.2021 р. № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text

2. План реалізації Стратегії кібербезпеки України : Указ Президента України від 01.02.22 р. № 37/2022. URL: https://zakon.rada.gov.ua/laws/show/n0087525-21#Text

3. Про затвердження плану заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року : Розпорядження Кабінету Міністрів України від 30.03.23 р. № 272-р. URL: https://zakon. rada.gov.ua/laws/show/272-2023-%D1%80#Text

4. Про Службу безпеки України : Закон України від 25 березня 1992 року № 2229-XII. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/ show/2229-12#Text

5. Про розвідку : Закон України від 17 вересня 2020 р. № 912–IX. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/912IX#Text

6. Про Національну безпеку України : Закон України від 21 червня 2018 року № 2469-VIII. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text

7. Стратегія забезпечення державної безпеки, затверджена Указом Президента України від 16.02.2022 р. № 56/2022. URL: https://zakon.rada.gov.ua/laws/main/56/2022.#Text

8. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

9. Про рішення Ради національної безпеки і оборони України від 18 березня 2022 року «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану»: Указ Президента України від 19.03.2022 № 152/2022. URL: https://zakon.rada.gov.ua/laws/show/152/2022#Text

Сердечна Анастасія Романівна,
здобувач ступеня вищої освіти бакалавра навчально-наукового інституту права та психології Національної академії внутрішніх справ
Науковий керівник:
Смаглюк О. В., доцент кафедри кримінального права та кримінології навчально-наукового інституту права та психології Національної академії внутрішніх справ, кандидат юридичних наук, доцент

КЛАСИФІКАЦІЯ ТА ТИПОЛОГІЧНІ ПІДХОДИ ДО ДОСЛІДЖЕННЯ ОСОБИ ПОТЕРПІЛОГО В КІБЕРПРОСТОРІ

Станом на початок 2025 року в Україні інтернетом користувався 31,5 млн людей, а рівень проникнення доступу до мережі склав 82,4 %. Для порівняння зазначимо, що в Східній Європі цей показник складає 90,6 %. З січня 2024 року до січня

2025 року кількість інтернет-користувачів в Україні зросла на 690 000 (або на 2,2 %) [1]. Стрімка діджиталізація суспільства створила появу нових форм кримінальних посягань, серед яких особливе місце посідають кібербулінг [2], кібершахрайство та кіберсталкінг. Незважаючи на схожість у механізмах впливу на особу, кожна із наведених форм злочинної поведінки характеризується власними траєкторіями віктимності, які визначають особливості реакцій жертв, рівень ризику та способи протидії. Вивчення поведінкових моделей потерпілих та їх соціально-психологічних характеристик є важливим для розробки ефективних механізмів профілактики та підтримки.

Мета цієї публікації полягає у визначенні науково обґрунтованих підходів до класифікації та типологізації особи потерпілого у кіберпросторі, виявленні основних критеріїв її диференціації залежно від характеру кіберзагроз, рівня цифрової компетентності, соціально-психологічних особливостей та поведінкових стратегій, а також формулюванні типологічної моделі, що сприятиме глибшому розумінню механізмів віктимізації в умовах цифрового середовища.

Віктимність у кіберпросторі розглядається як комплексна соціально-психологічна категорія, що характеризує особу як потенційну або фактичну жертву правопорушення. У наукових публікаціях підкреслюється, що її детермінантами є вік, соціально-економічний статус, рівень цифрової грамотності, ступінь відкритості персональних даних у мережі та психологічні особливості особи .

Науково-методологічно обґрунтована класифікація має спиратись на такі основні принципи як:

1. Мультидименсійність – поєднання технічного, соціально-психологічного і правового вимірів віктимізації.

2. Практична орієнтованість – виділення типів, що потребують різних форм захисту та реагування (технічна допомога, психологічна підтримка, кримінально-правовий захист).

3. Динамізм – визнання змінності статусу особи (наприклад, постраждалий може стати суб’єктом ризикованої поведінки або контрагентом у ланцюгу інциденту).

Саме на основі цих принципів, комплексних критеріїв класифікації різних типів кіберзагроз [3] та досліджень [4] формується науково обґрунтована класифікація потерпілих у

кіберпросторі, що дозволяє виділити типові групи постраждалих, визначити закономірності їх віктимності та розробити диференційовані заходи превенції, захисту та реабілітації. Таким чином, подальший розгляд буде зосереджено на описі основних підходів до класифікації та типології потерпілих у цифровому середовищі.

1. За характером взаємодії з правопорушником. Безпосередні потерпілі – особи, проти яких здійснено цілеспрямоване втручання (наприклад, фішинг, хакерська атака, вимагання). Опосередковані потерпілі – користувачі, що зазнали шкоди внаслідок масових атак або витоку даних, без прямого контакту з правопорушником.

2. За рівнем цифрової компетентності. Технічно необізнані особи, що стають жертвами кібершахрайства або соціальної інженерії. Користувачі із середнім рівнем знань, які не дотримуються основ кібергігієни. Професійні користувачі та адміністратори, що зазнають високотехнологічних атак.

3. За соціально-психологічними ознаками. Вразливі категорії (діти, підлітки, літні люди, особи з низьким рівнем критичного мислення) – часті жертви кібербулінгу, маніпуляцій чи секстингу. Соціально активні користувачі, які свідомо ризикують, публікуючи надлишкову кількість персональної інформації.

4. За видом шкоди, якої завдано. Матеріальна (економічна) – незаконне заволодіння коштами або майном через електронні засоби. Інформаційна – витік персональних чи конфіденційних даних. Психологічна – кібербулінг, кіберсталкінг, онлайн-насильство. Репутаційна – поширення компрометуючої інформації, підробка профілю.

5. За суб'єктним статусом. Фізичні особи – індивідуальні користувачі, які потерпають від персоналізованих атак [5]. Юридичні особи – організації, що зазнали втручання у діяльність їхніх інформаційних систем (наприклад, злам баз даних, атакування сайтів) [6].

На основі зазначених критеріїв можна виокремити кілька типологічних груп:

1. Технічно вразливі користувачі, які не володіють достатніми знаннями щодо цифрової безпеки.

2. Психологічно вразливі особи, схильні до довірливості чи емоційних реакцій, що використовуються правопорушниками.

3. Ризиковані користувачі, які свідомо нехтують правилами безпеки, публікують персональні дані або беруть участь у сумнівних онлайн-активностях.

4. Інституційні потерпілі, для яких шкода має економічний або репутаційний вимір (державні установи, банки, освітні організації).

Попри різну природу та мотиви кіберзлочинів їхні траєкторії віктимності мають спільні характеристики, зокрема емоційний стрес, соціальну ізоляцію та психологічну травму. Водночас кожний тип кіберзлочинності формує специфічні наслідки: кібербулінг – переважно психологічні, шахрайство – економічні, кіберсталкінг – комплексні психологічні та соціальні. Це дозволяє розробляти ефективні превентивні заходи, підвищувати рівень цифрової грамотності та вдосконалювати практику взаємодії громадян із правоохоронними органами.

Отже, класифікація потерпілих у кіберпросторі є необхідною умовою для формування цілісного уявлення про механізми віктимізації у цифровому середовищі. А аналіз віктимності у випадках кіберзлочинів, у свою чергу, свідчить, що різні форми кіберзлочинності визначають специфічні траєкторії впливу на жертв, що вимагає комплексного підходу до протидії. Законодавство України, кримінально-правові норми та практика кіберполіції створюють правові рамки для реагування на ці явища, але їх ефективність залежить від поєднання правового регулювання, освіти населення та психологічної підтримки постраждалих. Подальші наукові дослідження мають інтегрувати кримінологічний, психологічний та соціологічний аспекти віктимності у цифровому середовищі для розробки комплексної моделі захисту громадян.

Список використаних джерел

1. Інтернет, соцмережі, стримінги та відео. Найцікавіше зі звіту DIGITAL 2025 про взаємодію з цифровими технологіями. URL: https://mediamaker.me/najczikavishe-zi-zvitu-digital-2025-pro-vzayemodiyu-z-czyfrovymy-tehnologiyamy-16257/

2. Кібербулінг – що це та як це зупинити. 10 фактів, які підлітки хочуть знати про кібербулінг. URL: https://www.unicef.org/ukraine/cyberbulling

3. Даник Ю. Г., Воробієнко П. П., Чернега В. М. Основи кібербезпеки та кібероборони : підручник. [Видання друге, перероб. та доп.]. Одеса : ОНАЗ ім. О.С. Попова, 2019. 320 с.

4. Звіт про кінцеве дослідження щодо інформованості цільових аудиторій про основні аспекти кібербезпеки: підготовлено для Представництва Фонду цивільних досліджень та розвитку США в Україні. URL: info_sapiens_crdf_report_ua_2024.pdf

5. Фінансова допомога від організацій: як не стати жертвою онлайн-шахрайства. URL: https://fakty.com.ua/ua/videos/finansova-dopomoga-vid-organizaczij-yak-ne-staty-zhertvoyu-onlajn-shahrajstva/

6. Мелехова М. Хакери атакують держоргани та ОПК України за допомогою фейкових судових повісток. URL: https://fakty.com.ua/ua/ukraine/suspilstvo/20250805-hakery-atakuyut-derzhorgany-ta-opk-ukrayiny-za-dopomogoyu-fejkovyh-sudovyh-povistok/

Старовойт Аліна Олексіївна,
здобувач ступеня вищої освіти бакалавра навчально-наукового інституту права та психології Національної академії внутрішніх справ
Науковий керівник:
Смаглюк О. В., доцент кафедри кримінального права та кримінології навчально-наукового інституту права та психології Національної академії внутрішніх справ, кандидат юридичних наук, доцент

ВПЛИВ ЦИФРОВИХ ТЕХНОЛОГІЙ НА ПРАВОВЕ РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У сучасних умовах розвитку цифрових технологій проблема правового регулювання інформаційної безпеки набуває особливої актуальності. Цифровізація державного управління, бізнесу та освіти, а також активне впровадження штучного інтелекту й автоматизованих систем створюють нові ризики для захисту персональних даних, державних інформаційних ресурсів і прав громадян [2, с. 4–5].

Інформаційна безпека – це стан захищеності інформації, інформаційних систем і ресурсів, який забезпечує їхню цілісність, доступність та конфіденційність. В Україні основою правового регулювання у цій сфері є Конституція України, яка

гарантує кожному право на недоторканність приватного життя та захист персональних даних (ст. 32) [1, с. 15]. Закон України «Про основні засади забезпечення кібербезпеки України» визначає правові та організаційні основи забезпечення кіберзахисту держави, суб'єктів господарювання та громадян [2, с. 7–8].

Кримінальний кодекс України передбачає відповідальність за злочини у сфері комп'ютерної інформації. Зокрема, статті 361–363[1] встановлюють покарання за несанкціоноване втручання в роботу комп'ютерних систем, створення чи розповсюдження шкідливих програм, незаконне копіювання або використання інформації з обмеженим доступом [4, с. 210–212]. Закон України «Про інформацію» [3, с. 12–14] визначає основні принципи інформаційної діяльності, права та обов'язки суб'єктів інформаційних відносин, а також механізми захисту інформації.

Разом із тим, розвиток технологій породжує нові форми злочинної діяльності – фішинг, злом акаунтів, незаконне використання біометричних даних, маніпуляції у соціальних мережах. Це потребує вдосконалення законодавства, запровадження сучасних методів ідентифікації користувачів, розроблення єдиної державної політики з протидії кіберзлочинності. Значну роль відіграє підготовка фахівців у сфері інформаційного права, а також посилення співпраці між правоохоронними органами, судовою системою та експертними установами [5, с. 89–90].

В умовах цифрової трансформації України важливим напрямом є створення надійної системи кіберзахисту критичної інформаційної інфраструктури – енергетичних, фінансових, телекомунікаційних мереж. З метою координації таких заходів діє Національний координаційний центр кібербезпеки при РНБО України, який забезпечує моніторинг загроз і розроблення стратегій захисту державного кіберпростору [6, с. 47–48].

Отже, розвиток та активне використання цифрових технологій у злочинних цілях, істотно впливає на правове регулювання інформаційної безпеки, вимагаючи від держави адаптації кримінального законодавства до нових викликів часу. До того же, запорукою ефективного функціонування інформаційного суспільства України є підвищення рівня правосвідомості громадян, розвиток цифрової грамотності та зміцнення системи кіберзахисту, шо так само потребує врегулювання на державному рівні.

Список використаних джерел

1. Конституція України від 28 червня 1996 р. № 254к/96-ВР. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141. С. 15.
2. Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 р. № 2163-VIII. *Відомості Верховної Ради України*. 2017. № 45. Ст. 403. С. 4–8.
3. Закон України «Про інформацію» від 2 жовтня 1992 р. (ред. від 2023 р.). *Відомості Верховної Ради України.* 1992. № 48. Ст. 650. С. 12–14.
4. Кримінальний кодекс України від 5 квітня 2001 р. № 2341-III. *Відомості Верховної Ради України*. 2001. № 25–26. Ст. 131. С. 210–212.
5. Петров С. В. Правові засади забезпечення інформаційної безпеки в Україні. *Юридична наука*. 2022. № 2. С. 85–91.
6. Стратегія кібербезпеки України: Указ Президента України від 26 серпня 2021 р. № 447/2021. *Офіційний вісник Президента України.* 2021. № 19. С. 46–49.

Ступак Діана Русланівна,
здобувач ступеня вищої освіти бакалавра навчально-наукового інституту права та психології Національної академії внутрішніх справ
Науковий керівник:
Козачина А. М., старший викладач кафедри кримінального права та кримінології навчально-наукового інституту права та психології Національної академії внутрішніх справ, доктор філософії

КОГНІТИВНА ВІЙНА: НОВЕ ПОЛЕ БОЮ, ЩО ВИКОРИСТОВУЄ НАШ МОЗОК

Революційні досягнення в когнітивній науці та технологіях призвели дослідження взаємодії розуму та мозку до нової фази «контролю та моделювання мозку». Розвиток когнітивної науки та технологій, їх проникнення у стратегічну та військову сфери призвело до появи нової галузі дослідження – когнітивної війни – нової арени ведення війни.

«Когнітивна війна» – вислів, який з'явився у 2017 році в публічних виступах американських генералів і швидко був підхоплений науковцями та політологами, викликає таке ж занепокоєння, як і захопливість. Концепція когнітивної війни зараз дуже популярна у світі оборони. Існують різні її визначення, але узагальнено цю війну можна описати як дії, спрямовані на те, аби вплинути на мислення ворога з метою змусити його виконувати твою волю [1].

І. Р. Малик зазначає, що масштабність когнітивної війни визначається її глобальним характером, адже вона спрямована не тільки на окремих людей чи групи, але й на суспільство в цілому. Адже метою є зміна способу мислення та поведінки на рівні великих соціальних систем. Частіше це реалізовується через вплив на інформаційне середовище. Інструменти, які використовують у когнітивній війні включають використання цифрових технологій, соціальних мереж, мережі Інтернет, кіберпростору, алгоритмів, аналітики великих даних та інших сучасних технологій для створення інформації [2].

Концепція когнітивної війни є подвійною – цивільною та військовою – і також відома як «когнітивне домінування» або «когнітивна перевага». Спочатку вона засуджувала потенціал, відкритий у сфері маніпуляцій завдяки значним досягненням когнітивної науки, і висловлювала підозру, що їх можуть застосовувати на практиці ворожі держави чи організації. Донедавна психологічні операції, включаючи пропаганду та дезінформацію, а також наступальний маркетинг у цивільному секторі, базувалися на схематичних концепціях когнітивних процесів, які досі були погано вивчені. Тому ці операції намагалися контролювати те, що вони могли контролювати, тобто інформацію, що поширювалася серед ворогів, конкурентів чи споживачів, у надії вплинути на їхні рішення та поведінку.

Але розвиток так званих «жорстких» когнітивних наук – тобто неінтерпретативних, верифікованих та кількісно вимірюваних – все це змінив. Ці дисципліни вивчають думку як матеріальний об'єкт з точки зору різних галузей знань, що сходяться: нейронауки, лінгвістики, психології, аналітичної філософії та цифрових наук, включаючи штучний інтелект. Їхні результати показують, що можна точно впливати на самі когнітивні процеси та таким чином безпосередньо змінювати процеси мислення опонента.

Когнітивна війна використовує технології як зброю. Вона може використовувати інвазивні технології для зміни середовища мислення, мозку та, в ширшому сенсі, нервової системи, яка лежить в основі його функціонування. Наприклад, восени 2016 року близько сорока співробітників Міністерства оборони в посольстві США на Кубі раптово розвинулися дивні симптоми, що призводять до інвалідності, які згодом отримали назву «Гаванський синдром». Була підозра, що цілеспрямований маневр ворожої сили піддав цих людей нейробіологічним змінам через цілеспрямоване випромінювання. До березня 2023 року розвідувальні служби США не досягли консенсусу чи офіційного визначення причини гаванського синдрому, хоча представники розвідки та уряду США висловлювали пресі підозри, що відповідальність за це несе російська військова розвідка [3].

Україна сьогодні зіткнулася з новою загрозою, межі та можливості якої ми все ще намагаємося зрозуміти. Якщо вже мусимо її визначити, то можемо сказати, що когнітивна війна – це щонайменше галузь досліджень – і, ймовірно, спосіб сприяння підготовці та веденню війни, що здійснюється державними або недержавними суб'єктами. Вона охоплює операції, спрямовані на спотворення, запобігання або знищення мисленнєвих процесів, ситуаційної обізнаності та здатності супротивника приймати рішення, використовуючи науковий підхід та технологічні, зокрема цифрові, засоби.

Когнітивна війна може, перш за все, використовувати цифрові технології для порушення певних когнітивних функцій (пам'яті, уваги, комунікації, емоцій тощо) у окремих осіб [4]. Прикладами є надсилання персоналізованих текстових повідомлень членам парламенту під час голосування про їх близьких осіб, або надсилання фотографій загиблих дітей військовослужбовцям, які беруть участь в операції. Мета полягає в тому, щоб порушити короткострокове мислення, впливаючи на увагу, прийняття рішень та реакцію.

Однак, і це найбільш тривожний аспект, існує підозра, що ці операції відбуваються непомітно протягом тривалого періоду часу. Використовуючи когнітивні упередження, вони змінюють мислення жертв і мають тривалий, навіть незворотний вплив на когнітивну особистість, тобто на те, як людина обробляє інформацію. Наприклад, мотивація військового може бути поступово підірвана «цифро-соціальними» впливами, або ж

окремі особи можуть бути радикалізовані в межах ідентичних груп через соціальні платформи, щоб переконати їх, очевидно, за їхньою власною волею, у моральній правильності гуманних дій. Ці дії є поширеними, охоплюючи як цифровий, так і реальний світи. Тоді докази навмисного цілеспрямованого нападу може бути набагато складніше встановити, особливо тому, що виявлення когнітивного ефекту часто відбувається занадто пізно, і людина, на яку спрямовано напад, природно прагне мінімізувати ефект або навіть приховати той факт, що вона стала мішенню.

Ми більше не можемо жити без цифрових технологій: вони формують наш спосіб мислення з самого раннього віку, тому мають потужний вплив на наш інтелект та емоції, наш розум, наш спосіб мислення та планування. Тому, гегемонія компаній в організації кібервсесвіту, у поєднанні з крихкістю правових систем, що контролюють цю новітню сферу, дуже швидко привернула увагу лідерів та ідеологів, які скористалися цим, щоб знайти засоби для реалізації своїх проектів. Зловмисники покладаються на навички та ресурси цих приватних компаній або на посередників недобросовісних держав, часто за допомогою ідеологічних спільників, тобто людей, схильних до спотвореного мислення, які в свою чергу стають реле для зміни мислення інших, перетворюючи кіберсвіт на гігантський спектр операцій із залежністю користувачів.

Для захисту від таких атак діяти треба проактивно. Окрім фізичного захисту людей у стратегічних ситуаціях, частиною рішення було б звільнення від залежності від цифрових технологій або вміння використовувати їх розумно та об'єктивно. Однак, зазначене сьогодні здається недосяжним, адже неможливо нав'язати розвиток критичного мислення, жагу до перевірки інформації, недовіру до контенту, що поширюється в Інтернеті. Більш того, вказане має обмежену ефективність. Знання правил логічної аргументації, прийомів маніпуляції чи принципів роботи автоматичного мислення не завжди допомагають уникнути нераціональних висновків. Для цього необхідні системні кроки, зокрема розвиток інфраструктури раціонального мислення, тобто середовища, яке б допомагало уникати когнітивних атак і сприяло раціональним рішенням. Наприклад, замість того аби постійно боротися з когнітивними атаками, можна просто забрати їх джерело, як от російські пропагандистські ресурси (що й зробила свого часу Україна та багато інших демократичних країн) [5].

М. А. Мазикін зазначає, що протидія когнітивній війні вимагає комплексного підходу, що починається з медіаграмотності як навчання розпізнаванню маніпулятивних наративів. Психологічна підготовка включає розвиток критичного мислення та емоційної стійкості, щоб будь-яка особа мала можливість протистояти емоційним атакам. Інформаційна гігієна передбачає фільтрацію джерел інформації, зменшення впливу токсичного контенту та свідоме обмеження часу в цифровому просторі [6].

Відродження когнітивної науки і технологій підкреслює той факт, що майбутня сила та верховенство полягають у когнітивній перевазі та розширенні можливостей на арені когнітивної війни. Таким чином, деякими з критично важливих заходів, які необхідно вжити в цьому відношенні, є створення дослідницьких центрів когнітивної науки і технологій, центрів когнітивного захисту, а також баз і штабів когнітивного бою. Інші важливі дії включають підготовку офіцерів для когнітивної війни, розробку політики, законодавство та виконавчі заходи, а також планування наступу та оборони на арені когнітивної війни.

Підсумовуючи вище викладене, слід зазначити, що когнітивна війна – це війна за розум, емоції, свідомість та увагу людини. У цій війні людська свідомість стає полем бою. Метою такої війни є втручання в інформаційне середовище опонента таким чином, щоб створити вплив на сприйняття реальності й прийняття рішень. Об’єктами когнітивних атак можуть бути конкретні особи, групи людей чи навіть усе населення. Захиститися від когнітивної війни можливо за допомогою критичного мислення та аналізу інформації, здатності мислити незалежно та об’єктивно.

Список використаних джерел

1. Радченко Р. Ваш мозок під прицілом: український вимір когнітивної війни. URL: https://deepstateua.com/koghnitivni-viini-ukrayinskii-vimir/ (дата звернення: 14.10.2025).

2. Малик І. Р. Когнітивна війна: людська свідомість як поле бою. *Регіональні студії*. 2024. № 39. С. 45–50. URL: http://regionalstudies.uzhnu.uz.ua/archive/39/39_2024.pdf (дата звернення: 14.10.2025).

3. CIA Recalls Vienna Station Chief In Move Related To Handling Of ‘Havana Syndrome’. URL: https://www.npr.org/

2021/09/24/1040422112/cia-recalls-vienna-station-chief-in-move-related-to-handling-of-havana-syndrome (дата звернення: 14.10.2025).

4. Макух-Федоркова І. І. Сучасні методологічні підходи до визначення понять смислові/когнітивні війни: аналіз інструментів впливу. *Історико-політичні проблеми сучасного світу* : збірник наукових статей. 2024. № 49. С. 120–136. URL: https://mhpi.chnu.edu.ua/mhpi/article/view/19/11 (дата звернення: 14.10.2025).

5. Надурак В. В. Пастка для розуму. Як ворог веде проти України когнітивну війну. URL: https://nv.ua/ukr/amp/filosof-rozkriv-sekreti-kognitivnoji-viyni-yaku-vede-proti-ukrajini-rosiya-50536593.html (дата звернення: 14.10.2025).

6. Мазикін М. А. Когнітивна війна в сучасному світі: психолінгвістичні механізми впливу на свідомість та стратегії захисту. URL: https://ukr-happiness-institute.com/kognityvna-vijna-ta-strategii-zahystu/ (дата звернення: 14.10.2025).

Шеховцова Анна Андріївна,
здобувач ступеня вищої освіти бакалавра навчально-наукового інституту права та психології Національної академії внутрішніх справ
Науковий керівник:
Резнік Ю. С., старший викладач кафедри кримінального права та кримінології навчально-наукового інституту права та психології Національної академії внутрішніх справ, кандидат юридичних наук

МІЖНАРОДНЕ СПІВРОБІТНИЦТВО У СФЕРІ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Сучасний світ характеризується високим рівнем цифрової інтеграції, що водночас породжує нові ризики та виклики для безпеки. Кіберзлочинність стала однією з найсерйозніших транснаціональних загроз XXI століття, адже злочинці діють поза межами державних кордонів, використовуючи прогалини у правовому регулюванні та технологічні вразливості [1]. Метою

цього дослідження є аналіз міжнародних механізмів співробітництва у сфері протидії кіберзлочинності, визначення їх ключових елементів, результатів діяльності та основних проблем, що перешкоджають ефективній координації дій держав.

Поняття кіберзлочинності охоплює широкий спектр протиправних дій, які здійснюються із використанням інформаційно-комунікаційних технологій. Відповідно до положень Будапештської конвенції про кіберзлочинність [2], до таких злочинів належать атаки на мережеву інфраструктуру, фінансове шахрайство, використання програм-вимагачів, кібершпигунство, викрадення персональних даних, цифрове насильство, злочини проти дітей і поширення дезінформації [3]. Більшість таких злочинів мають комбінований характер: наприклад, фішинг може бути підготовчим етапом ransomware-атаки, а викрадення даних – способом подальшого шантажу. Це свідчить про необхідність комплексного підходу до протидії, що передбачає міжнародну координацію.

Ефективна боротьба з кіберзлочинністю неможлива без спільних міжнародно-правових засад, які регламентують координацію дій, обмін інформацією та взаємне визнання цифрових доказів. Основу такої системи становить Будапештська конвенція Ради Європи 2001 року – перший міжнародний договір, спрямований на гармонізацію кримінального законодавства у сфері комп'ютерних злочинів, запровадження спільних процедур збирання й збереження електронних доказів та створення каналів оперативного обміну між правоохоронними органами різних країн [2]. Саме цей документ заклав фундамент для формування міжнародного правового простору у сфері кібербезпеки.

Подальший розвиток міжнародного правового регулювання відбувся через укладення угод про взаємну правову допомогу (Mutual Legal Assistance – MLA), які стали ключовим інструментом обміну доказами під час розслідування кіберінцидентів [4]. Ці механізми дозволяють державам отримувати дані, що зберігаються за кордоном, та координувати кримінальні провадження, однак їх ефективність часто обмежується розбіжностями у національних правових системах і тривалістю процедур.

Важливим складником міжнародно-правових рамок є законодавство Європейського Союзу, яке встановлює спільні підходи до запобігання кіберзлочинності. Зокрема, Директива 2013/40/ЄС визначає відповідальність за атаки на інформаційні системи, а Регламент (ЄС) 2016/679 (GDPR) регулює обробку та передачу персональних даних, у тому числі для потреб правоохоронних органів [5]. У такий спосіб формується багаторівнева система – від глобальних норм Будапештської конвенції до регіональних директив і двосторонніх угод, які спільно забезпечують міжнародну кіберстабільність.

Реалізація цих правових механізмів відбувається через діяльність спеціалізованих міжнародних структур. Одним із ключових учасників глобальної системи є Міжнародна організація кримінальної поліції (INTERPOL), що об'єднує понад 190 держав. Її діяльність спрямована на координацію дій правоохоронних органів, організацію спільних операцій та обмін оперативною інформацією. Показовим прикладом ефективності такого підходу стала операція Synergia (2023–2024 рр.), у ході якої було нейтралізовано понад 70 % командно-контрольних серверів (C2), арештовано 31 особу, заблоковано сотні фішингових ресурсів [6].

На європейському рівні центральну роль відіграє Європейський центр із протидії кіберзлочинності (EC3), що функціонує в структурі Europol. Він координує спільні розслідування, здійснює аналітичну підтримку та організовує операції на міждержавному рівні. У травні 2024 року під егідою Europol проведено операцію Endgame, спрямовану на ліквідацію ботнетів, які використовувалися для розповсюдження програм-вимагачів; у результаті було вилучено понад сто серверів і заблоковано близько двох тисяч доменів [7].

Стратегічний вимір міжнародної кібербезпеки забезпечує НАТО через діяльність Центру передового досвіду з кібероборони (CCDCOE) у Таллінні. Центр проводить дослідження, навчання та міжнародні навчальні маневри Locked Shields, які щорічно залучають тисячі експертів із десятків країн і дозволяють перевірити готовність до відбиття масштабних атак на критичну інфраструктуру [8].

Операційне реагування на інциденти забезпечують національні команди реагування CSIRT/CERT. Вони займаються моніторингом кіберзагроз, збором технічних

індикаторів компрометації, взаємодією з приватними компаніями та забезпечують обмін даними між державними структурами. Така співпраця є основою публічно-приватного партнерства, без якого неможливо забезпечити ефективну глобальну кіберстійкість [9].

Практична результативність міжнародної співпраці підтверджується низкою успішних операцій. Серед них – Endgame (Europol, 2024), під час якої нейтралізовано понад сто серверів ботнетів; *Synergia* (INTERPOL, 2023–2024), у межах якої ліквідовано сотні C2-серверів і здійснено десятки арештів; Quicksand (2022–2023), що була спрямована проти груп GandCrab і REvil; а також LockBit Disruption (2024), де за участі Europol, Eurojust і українських правоохоронних органів було знищено інфраструктуру злочинної групи LockBit та арештовано її учасників [6; 7; 9; 10]. Ці операції демонструють ефективність глобальної координації та водночас виявляють проблемні аспекти міжнародної взаємодії.

Попри досягнення, співпраця у сфері протидії кіберзлочинності стикається з низкою труднощів. Насамперед це юридичні розбіжності між країнами у кваліфікації злочинів і процедурах збирання доказів, що ускладнює міжнародне переслідування правопорушників. Процедури взаємної правової допомоги залишаються повільними й бюрократичними, а нерівність технічних можливостей між державами знижує ефективність реагування. Додатковими обмеженнями виступають норми законодавства про захист приватності, зокрема Регламент ЄС (GDPR) [5], а також висока адаптивність злочинців, які активно використовують штучний інтелект, криптовалюти та анонімні мережі [11]. Ускладнює ситуацію й недостатня координація між урядовими структурами, приватним сектором і науковими установами.

Для підвищення ефективності міжнародної взаємодії доцільно вдосконалити існуючі механізми співпраці. Необхідним є розроблення прискорених процедур міжнародної правової допомоги у справах кіберзлочинів, які передбачатимуть швидкий електронний обмін запитами та доказами. Важливо також посилити технічну підтримку і підготовку кадрів у країнах із низьким рівнем кіберготовності, уніфікувати стандарти обміну технічними даними між командами CSIRT/CERT, розширити публічно-приватне

партнерство та запровадити чіткі правові рамки його функціонування. Регулярні багатосторонні навчання, подібні до Locked Shields, сприятимуть підтриманню високого рівня готовності до реагування на загрози. Окремої уваги потребують інвестиції у розвиток технологій штучного інтелекту, квантового шифрування та аналітики загроз, що можуть забезпечити новий рівень глобальної кіберстабільності. Водночас важливо зберігати баланс між захистом персональних даних і потребами правоохоронних органів у доступі до інформації [9].

Отже, кіберзлочинність є глобальною проблемою, подолання якої можливе лише шляхом послідовної міжнародної координації. Досвід INTERPOL, Europol, HATO/CCDCOE та CSIRT/CERT доводить, що об'єднані дії держав і приватного сектору здатні забезпечити реальні результати у боротьбі з транснаціональною злочинністю. Водночас актуальними залишаються питання правової гармонізації, швидкості обміну інформацією та залучення недержавних акторів до спільної роботи.

Міжнародне співробітництво у сфері кібербезпеки має стати ключовим чинником забезпечення стабільності, суверенітету та захисту прав людини у цифровому просторі. Тільки шляхом консолідації зусиль держав, міжнародних організацій і приватних компаній можна гарантувати стійкий розвиток, безпеку критичної інфраструктури та захист громадян у глобальному цифровому середовищі.

Список використаних джерел

1. Василенко О. М. Кібербезпека в системі міжнародних відносин: правові та організаційні аспекти. Київ : НАУ, 2022. 256 с.

2. Council of Europe. Convention on Cybercrime (Budapest Convention). ETS No.185. Budapest, 2001.

3. Яременко Л. П. Кіберзлочинність: правові засади та міжнародне співробітництво. Львів : ЛНУ ім. І. Франка, 2021. 198 с.

4. United Nations Office on Drugs and Crime (UNODC). Practical Guide to Mutual Legal Assistance in Cybercrime Cases. Vienna, 2020.

5. Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation, GDPR). — Official Journal of the EU, L 119, 2016.

6. INTERPOL. Operation Synergia Targets Cybercrime Infrastructure. Lyon : INTERPOL News, 2024.

7. Europol. Operation Endgame: Disruption of Ransomware Infrastructure. The Hague, 2024.

8. NATO CCDCOE. Locked Shields 2024 After Action Report. Tallinn, 2024.

9. ENISA. European CSIRT Network Annual Report. Brussels, 2023.

10. Eurojust. Joint Action Against LockBit Ransomware Group. The Hague, 2024.

11. Trend Micro Research. Cybercrime and Artificial Intelligence: Emerging Threats 2025. Tokyo, 2025.

Наукове видання

КІБЕРБЕЗПЕКА В ДІЇ: ВІД ОСОБИСТОГО ЗАХИСТУ ДО НАЦІОНАЛЬНОГО

Матеріали
науково-практичного круглого столу
(Київ, 15 жовтня 2025 року)

Відповідальний упорядник – *Сабріє ШРАМКО*

Свідоцтво про внесення суб'єкта видавничої справи до
державного реєстру видавців, виготовників і
розповсюджувачів видавничої продукції
Дк № 4155 від 13.09.2011.
Підписано до друку 19.06.2025. Формат 60x84/16. Папір офсетний.
Обл.-вид. арк. 14,5. Ум. друк. арк. 13,48.
Тираж 20 прим.