**МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ**

**НАЦІОНАЛЬНА АКАДЕМІЯ ВНУТРІШНІХ СПРАВ**

**Навчально-науковий інститут права та психології**

**Кафедра інформаційних технологій**

105 РОКІВ
НАВС 2026

# КІБЕРПРОСТІР
# ЯК СФЕРА ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ:
# НОВІ ЗАГРОЗИ ТА МЕТОДИ РЕАГУВАННЯ

**Матеріали науково-практичного семінару**

(м. Київ, 26 березня 2026 року)

***Київ***
***2026***

УДК 004.056:351.74](477)(06)
К38

**Матеріали науково-практичного семінару за загальною редакцією:**

***Кудінов В.А.*** – кандидат фізико-математичних наук, доцент, завідувач кафедри інформаційних технологій навчально-наукового інституту права та психології Національної академії внутрішніх справ

**Рецензенти:**

***Галицька І. Є.*** – кандидат технічних наук, доцент, доцент кафедри математичних методів захисту інформації ННФТІ Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»

***Школьніков В.І.*** – завідувач кафедри кримінології та інформаційних технологій Національної академії внутрішніх справ, доктор філософії з галузі знань «Право», капітан поліції

*Матеріали схвалено та рекомендовано до друку на засіданні науково-методичної ради Національної академії внутрішніх справ (протокол № 5 від «19» травня 2026 року)*

*Усі матеріали надані в авторській редакції та виражають персональну позицію учасників круглого столу*

К38 **Кіберпростір як сфера правоохоронної діяльності: нові загрози та методи реагування**: матеріали наук.-практ. семінару (м. Київ, НАВС, 26 березня 2026 р.); за заг. редакцією В. А. Кудінова. Київ: Нац. акад. внутр. справ, 2026. 72 с.

У збірнику представлено стислий виклад доповідей і повідомлень, поданих на науково-практичний семінар на тему «Кіберпростір як сфера правоохоронної діяльності: нові загрози та методи реагування», який відбувся на базі навчально-наукового інституту права та психології Національної академії внутрішніх справ 26 березня 2026 року.

Для здобувачів вищої освіти, науково-педагогічних працівників закладів вищої освіти, практичних працівників органів та підрозділів системи МВС України.

УДК 004.056:351.74](477)(06)

**ЗМІСТ**

**МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ**
**НАЦІОНАЛЬНА АКАДЕМІЯ ВНУТРІШНІХ СПРАВ**
**Навчально-науковий інститут права та психології**
**Кафедра інформаційних технологій**

# П Р О Г Р А М А

проведення науково-практичного семінару на тему:

## «КІБЕРПРОСТІР ЯК СФЕРА ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ: НОВІ ЗАГРОЗИ ТА МЕТОДИ РЕАГУВАННЯ»

(*26 березня 2026 року*)

***Київ – 2026***

*Дата проведення:* **26 березня 2026 року**
*Початок роботи:* **15:00**
*Місце проведення:* Національна академія внутрішніх справ (м. Київ, пл. Солом'янська 1, ауд. 442) та ZOOM.
**Регламент:** доповіді – *до 5 хв.*; обговорення – *до 3 хв.*
**Відкриває захід** директор ННІ права та психології НАВС, кандидат юридичних наук, доцент **Кульчицька Оксана Вікторівна**.
**Вступне слово** завідувача кафедри інформаційних технологій ННІ права та психології НАВС, кандидата фізико-математичних наук, доцента **Кудінова Вадима Анатолійовича**.
**Модератор заходу:** доцент кафедри інформаційних технологій ННІ права та психології НАВС, кандидат технічних наук, доцент **Пакриш Олександр Євгенійович**.

## ДОПОВІДІ:

1. Студентка 107_СПД н.гр. **Артеменко Надія Олександрівна** «Кіберпростір та його ключові характеристики» (Швець М.М).
2. Студентка 101_СПД н.гр. **Шинкаренко Ангеліна Юріївна «**Формування системного механізму правоохоронної діяльності у кіберпросторі: ризик-орієнтований підхід та технологічна адаптація» (к.ф.-м.н. Кудінов В.А.).
3. Студентка 109_СПД н.гр. **Мартинюк Софія Володимирівна** «Цілі інформаційних та психологічних операцій в кіберпросторі» (Грищенко О.І).
4. Студент 102_СПД н.гр. **Шуляк Богдан Андрійович** «Кіберпростір у стані війни: посилення кримінальної відповідальності та нові алгоритми кіберзахисту» (к.ф.-м.н. Кудінов В.А.).
5. Студентка 202_СПС н.гр. **Гуменюк Вікторія Олегівна** «Кіберсталкінг – основні ознаки та протидія» (к.т.н. Пакриш О.Є.).
6. Студентка 201_СПС н.гр. **Король Тетяна Анатоліївна** «Психологічні методи маніпуляції в кіберпросторі та шляхи протидії» (к.ф.-м.н. Тарасенко В.П.).
7. Студент 109_СПД н.гр. **Масовець В'ячеслав Олександрович** «Використання соціальних мереж як інструменту впливу та маніпуляції в контексті національної безпеки» (Грищенко О.І).
8. Студентка 202_СПС н.гр. **Кривошеєва Діана Юріївна** «Грумінг – основні ознаки та протидія» (к.т.н. Пакриш О.Є.).
9. Студентка 208_СПД н.гр. **Горбаченко Вероніка Романівна** «Кібербезпека в соціальних мережах» (к.ф.-м.н. Кудінов В.А.)
10. Студентка 202_СПС н.гр. **Гілевич Камелія Валеріївна** «Дифамація (Defamation) – основні ознаки та протидія» (к.т.н. Пакриш О.Є.).

11. Студентка 102_СПРБ н.гр. **Ковальчук Світлана Миколаївна** «Кібербезпека держави в умовах гібридної війни» (к.ф.-м.н. Тарасенко В.П.).
12. Студентка 107_СПД н.гр. **Голікова Мілена Олексіївна** «Кібершпигунство, кібершахрайство та кібератаки» (Швець М.М.).
13. Студентка 117_СПД н.гр. **Савчин Євгенія Андріївна** «Кібербезпека як елемент стабільного функціонування держави» (к.ф.-м.н. Тарасенко В.П.).
14. Студентка 107_СПД н.гр **Борко Надія Олександрівна** «Еволюція кіберзагроз за останні роки у світі» (Швець М.М).
15. Студент 102_СПРБ н.гр. **Баклан Мирослав Анатолійович** «Кібербезпека в забезпеченні національної безпеки України» (к.ф.-м.н. Тарасенко В.П.).
16. Студентка 108_СПД н.гр. **Новицька Ірина Ігорівна** «Кібертероризм та його відмінність від звичайних кіберзлочинів» (Грищенко О.І).
17. Студентка 102_СПРБ н.гр. **Руснак Міла Олегівна** «Проблеми правового та дійового забезпечення кібербезпеки у світі та в Україні» (к.ф.-м.н. Тарасенко В.П.).
18. Студентка 101_СПРБ н.гр. **Кобилянська Кристіна Василівна** «Кібербезпека в діяльності правника: сучасні загрози та методи захисту інформації» (к.т.н. Корнейко О.В.).
19. Студентка 117_СПД н.гр. **Убога Сніжана Сергіївна** «Нові виклики та види кіберзлочинів: правовий аналіз та методи реагування крізь призму Конституції України» (к.ф.-м.н. Тарасенко В.П.).
20. Студентка 202_СПС н.гр. **Гой Катерина Володимирівна** «Використання штучного інтелекту для автоматизації кібератак та створення діпфейків» (к.т.н. Пакриш О.Є.).
21. Студентка 204_СПД н.гр. **Козіна Олена Вікторівна** «Використання штучного інтелекту у злочинних цілях: сучасні виклики та механізми протидії» (к.ф.-м.н. Кудінов В.А.).
22. Студентка 201_СПС н.гр. **Фертіль Анастасія Ігорівна** «Людський фактор у системі протидії кіберзлочинності: психологія злочинця, жертви та правоохоронця як взаємопов’язані елементи» (к.ф.-м.н. Тарасенко В.П.).

***Артеменко Надія Олександрівна***
студентка 107_СПД н.гр. ННІ права та психології НАВС

*Науковий керівник:*
***Швець Микола Миколайович***
викладач кафедри інформаційних технологій ННІ права та психології НАВС

# КІБЕРПРОСТІР ТА ЙОГО КЛЮЧОВІ ХАРАКТЕРИСТИКИ

***Кіберпростір*** – це складне багатовимірне середовище, яке утворюється в результаті взаємодії інформаційних технологій, комп'ютерних мереж, цифрових пристроїв та користувачів [1]. У найширшому розумінні кіберпростір можна визначити як сукупність інформаційних ресурсів, систем обробки даних, мереж зв'язку та цифрових комунікацій, які забезпечують створення, зберігання, передавання і використання інформації. Це віртуальне середовище, яке існує завдяки технічній інфраструктурі, але водночас має соціальний, економічний, політичний і культурний вимір. Сьогодні кіберпростір є невід'ємною частиною життя сучасного суспільства, оскільки він забезпечує функціонування держав, бізнесу, освіти, науки, медицини та повсякденної діяльності людей [2].

Поняття кіберпростору з'явилося у другій половині XX століття у зв'язку зі стрімким розвитком комп'ютерних технологій і глобальних мереж. З розвитком Інтернету та цифровізації практично всіх сфер життя значення кіберпростору значно зросло. Він перестав бути лише технічним середовищем і перетворився на окремий простір людської діяльності. У кіберпросторі відбуваються комунікації, обмін інформацією, фінансові операції, навчання, розваги, політичні процеси та навіть конфлікти. Тому сьогодні кіберпростір розглядається як важливий фактор розвитку суспільства та один із ключових елементів національної і міжнародної безпеки [3].

Однією з ключових характеристик кіберпростору є його **глобальність**. На відміну від традиційних середовищ, він не має чітких географічних меж. Користувачі з різних країн можуть взаємодіяти в режимі реального часу, незалежно від відстані. Це створює нові можливості для міжнародного співробітництва, економічної діяльності, освіти та культурного обміну. Водночас глобальність кіберпростору породжує і нові виклики, зокрема проблеми регулювання, безпеки, захисту даних та боротьби з кіберзлочинністю.

Іншою важливою характеристикою є **інтерактивність**. У кіберпросторі користувачі не лише отримують інформацію, а й активно її створюють, поширюють та змінюють.

Соціальні мережі, форуми, блоги, онлайн-платформи дозволяють кожному бути учасником інформаційного процесу. Це сприяє розвитку демократії, свободи слова та громадянської активності. Проте одночасно виникають ризики поширення фейкової інформації, маніпуляцій, інформаційних атак і психологічного впливу на суспільство.

Наступною характеристикою є **динамічність і швидкість розвитку**. Технології постійно вдосконалюються, з'являються нові сервіси, цифрові платформи, методи обробки інформації. Кіберпростір швидко змінюється, що потребує адаптації як від користувачів, так і від держав та організацій. Це також створює умови для інновацій, розвитку економіки, електронного урядування, дистанційної освіти та цифрових послуг.

Важливою рисою кіберпростору є **віртуальність**. Більшість процесів у ньому відбувається у цифровому середовищі, без фізичного контакту між учасниками. Це дозволяє здійснювати діяльність незалежно від місця перебування. Наприклад, люди можуть працювати дистанційно, навчатися онлайн, здійснювати покупки, спілкуватися і навіть отримувати медичні консультації. Віртуальність змінює традиційні форми взаємодії, створює нові соціальні та економічні моделі.

Ще однією ключовою характеристикою є **інформаційність**. Основним ресурсом кіберпростору є інформація, яка є цінністю, товаром і стратегічним ресурсом. Обсяг інформації постійно зростає, що потребує ефективних систем зберігання, обробки, аналізу та захисту даних. Розвиток штучного інтелекту, великих даних і хмарних технологій ще більше підсилює роль інформації.

Не менш важливою характеристикою є **відкритість і доступність**. Багато інформаційних ресурсів доступні широкому колу користувачів. Це сприяє розвитку освіти, науки, міжнародного співробітництва. Водночас відкритість створює ризики витоку конфіденційної інформації, кіберзлочинності, порушення авторських прав та приватності.

Кіберпростір також характеризується **мережевою структурою**. Він складається з великої кількості взаємопов'язаних елементів: серверів, мереж, програмного забезпечення, баз даних, користувачів. Така структура забезпечує стійкість і гнучкість, але одночасно створює складність управління та захисту. Порушення в одній частині мережі можуть впливати на інші системи.

Важливою характеристикою є **анонімність**. У кіберпросторі користувачі можуть приховувати свою особу, що сприяє свободі самовираження. Проте це також створює умови для шахрайства, кібербулінгу, незаконної діяльності. Тому питання ідентифікації та цифрової безпеки стають все більш актуальними.

Ще одна особливість – **уразливість і необхідність кібербезпеки**. Кіберпростір піддається різним загрозам: віруси, хакерські атаки, фішинг, кібершпигунство, інформаційні війни. Держави створюють системи кіберзахисту, розробляють закони, формують кіберполіцію для протидії цим загрозам. Захист інформації, критичної інфраструктури тощо є пріоритетними завданнями [4].

Також кіберпростір має *соціальний і культурний вимір*. Він впливає на спосіб життя, комунікацію, формування цінностей, культуру та ідентичність. Онлайн-спільноти, цифрові платформи, медіа змінюють традиційні форми взаємодії. З'являються нові професії, стилі життя, цифрові культури.

*Економічна складова* кіберпростору є надзвичайно важливою. Електронна комерція, онлайн-банкінг, цифрові валюти, стартапи та IT-сектор формують нову цифрову економіку. Бізнес активно використовує кіберпростір для розвитку, реклами, продажу та комунікації з клієнтами. Це сприяє глобалізації та економічному зростанню.

*Політичний аспект* також відіграє важливу роль. У кіберпросторі проводяться інформаційні кампанії, виборчі процеси, політична комунікація. Він стає інструментом впливу на громадську думку, міжнародні відносини, національну безпеку. Кіберпростір часто розглядається як новий простір протистояння між державами.

У сучасному світі кіберпростір є невід'ємною складовою розвитку суспільства. Він відкриває широкі можливості для інновацій, освіти, науки, економіки та соціальної взаємодії. Водночас він створює нові ризики та виклики, пов'язані з безпекою, етикою, правом і відповідальністю.

***Отже***, кіберпростір – це складне, глобальне, динамічне та багатофункціональне середовище, яке поєднує технології, інформацію та людську діяльність. Його ключовими характеристиками є глобальність, інтерактивність, динамічність, віртуальність, інформаційність, відкритість, мережевість, анонімність і уразливість. Розуміння сутності кіберпростору та його особливостей є важливим для ефективного використання сучасних технологій, забезпечення кібербезпеки та сталого розвитку суспільства в умовах цифрової трансформації.

**Список використаних джерел:**

1. Кіберпростір. *Національний інститут стандартів і технологій (NIST)* : [сайт]. URL: https://csrc.nist.gov/glossary/term/cyberspace?utm_source=chatgpt.com.

2. Про розвиток кіберпростору та глобальні кіберзагрози. *Global Cybersecurity Index* : [сайт]. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf?utm_source=chatgpt.com.

3. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26 серп. 2021 р.№ 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013?utm_source=chatgpt.com.

4. Розвиток кіберзахисту – невід'ємна складова цифровізації України. *Міністерство цифрової трансформації України* : [сайт]. URL: https://thedigital.gov.ua/news/technologies/rozvitok-kiberzakhistu-nevidemna-skladova-tsifrovizatsii-ukraini.

***Шинкаренко Ангеліна Юріївна***
студентка 101_СПД н.гр. ННІ права та психології НАВС

*Науковий керівник:*
***Кудінов Вадим Анатолійович***
кандидат фізико-математичних наук, доцент, завідувач кафедри інформаційних технологій ННІ права та психології НАВС

# ФОРМУВАННЯ СИСТЕМНОГО МЕХАНІЗМУ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ У КІБЕРПРОСТОРІ: РИЗИК-ОРІЄНТОВАНИЙ ПІДХІД ТА ТЕХНОЛОГІЧНА АДАПТАЦІЯ

**Вступ.** Сучасний кіберпростір дедалі активніше перетворюється на самостійну сферу правоохоронної діяльності, у якій поєднуються технологічні, правові та безпекові виклики. Масштабна цифровізація державних інституцій, бізнесу та повсякденного життя громадян зумовлює стрімке зростання кількості кіберзагроз, що безпосередньо впливають на національну безпеку, публічний порядок і реалізацію прав людини. В умовах воєнного стану для України кіберпростір набуває особливого значення, оскільки кібератаки дедалі частіше використовуються як елемент гібридної війни. У зв'язку з цим аналіз кіберпростору як сфери правоохоронної діяльності, а також визначення нових загроз і методів реагування є вкрай актуальним науковим і практичним завданням.

У ході опрацювання джерел, присвячених загрозам кібербезпеці для малого бізнесу, зокрема аналітичних і практикоорієнтованих матеріалів, було встановлено, що такі явища, як фішинг, програми-вимагачі, шкідливе програмне забезпечення, DDoS-атаки та соціальна інженерія, мають масовий і системний характер. Аналіз цих загроз дозволяє зробити висновок, що вони виходять за межі приватного сектору та становлять небезпеку для всієї інформаційної інфраструктури держави. Для правоохоронної діяльності це означає ускладнення процесів виявлення кіберзлочинів, фіксації доказів, ідентифікації злочинців і притягнення їх до відповідальності, особливо з огляду на транснаціональний характер більшості таких правопорушень[1].

Значну увагу в межах дослідження було приділено аналізу рішень Ради національної безпеки і оборони України та інших нормативно-правових актів, що формують національну систему кібербезпеки. Їх вивчення дало змогу дійти висновку, що держава поступово визнає кіберпростір критично важливим елементом національної безпеки та визначає необхідність посилення захисту об'єктів критичної інформаційної інфраструктури.

Водночас для правоохоронних органів ці документи мають фундаментальне значення, оскільки визначають правові підстави реагування на кіберінциденти, міжвідомчу координацію та відповідальність за порушення вимог кіберзахисту [2].

Аналіз наукових праць, присвячених міжнародному співробітництву у сфері кібербезпеки, дозволив встановити, що ефективна протидія кіберзагрозам неможлива без системної взаємодії з міжнародними партнерами. Закон України «Про основні засади забезпечення кібербезпеки України», Стратегія кібербезпеки України, а також стратегічні документи Європейського Союзу й НАТО акцентують увагу на необхідності обміну інформацією про кіберінциденти, проведення спільних навчань і уніфікації підходів до цифрових розслідувань. Для правоохоронної діяльності це означає перехід від ізольованого реагування до колективної безпеки у кіберпросторі [3, с. 89-93].

**Пропозиції.** На основі проведеного аналізу вважаємо за доцільне розглядати кіберпростір не лише як технічне або інформаційне середовище, а як самостійну, динамічну сферу правового регулювання та правоохоронного впливу, яка потребує комплексного міждисциплінарного підходу. Кіберпростір фактично перетворюється на окремий «цифровий вимір» суспільних відносин, у якому формуються нові види злочинності, суб'єкти та способи протиправної діяльності, що не завжди можуть бути ефективно охоплені традиційними правовими механізмами.

Однією з ключових пропозицій є впровадження ризик-орієнтованої моделі реагування на кіберзагрози, яка передбачає перехід від реактивного до проактивного підходу у діяльності правоохоронних органів. Така модель має ґрунтуватися на постійному аналізі цифрових ризиків, визначенні найбільш уразливих секторів (державні інформаційні ресурси, фінансові установи, критична інфраструктура, соціальні мережі) та концентрації ресурсів на попередженні найбільш небезпечних кіберінцидентів ще до моменту їх реалізації.

З метою практичної реалізації зазначеного підходу пропонуємо створити та впровадити Державну міжвідомчу програму «Проактивна кібербезпека», основними елементами якої мають стати:

- використання аналітичних і предиктивних систем на основі великих даних для прогнозування кіберзагроз;
- автоматизований моніторинг аномальної активності в кіберпросторі;
- розробка єдиних стандартів реагування на кіберінциденти з урахуванням рівня загрози.

Окремої уваги потребує удосконалення механізмів збирання, фіксації та використання електронних доказів. Вважаємо за необхідне на законодавчому рівні закріпити спеціальні процесуальні процедури роботи з цифровими доказами, зокрема з даними, згенерованими або модифікованими системами штучного інтелекту, що дозволить підвищити їх допустимість і доказову цінність у кримінальному провадженні.

У межах дослідження також проаналізовано нові види кіберзагроз, пов’язані з використанням інструментів штучного інтелекту, зокрема таких систем, як ChatGPT та його аналоги. Встановлено, що зазначені технології можуть бути використані для автоматизованого фішингу, створення персоналізованих шахрайських повідомлень, масштабних інформаційно-психологічних операцій, генерації deepfake-контенту, а також для ускладнення ідентифікації осіб, причетних до вчинення злочинів.

У зв’язку з цим пропонуємо створити спеціалізовані підрозділи у структурі Національної поліції України, діяльність яких буде спрямована саме на протидію злочинам із використанням штучного інтелекту. Такі підрозділи повинні займатися:

- аналізом цифрових слідів, залишених AI-інструментами;
- виявленням ознак використання генеративних моделей у злочинній діяльності;
- розробкою методик ідентифікації deepfake-контенту;
- підготовкою фахівців нового покоління у сфері кіберрозслідувань, які поєднують знання права, кібербезпеки та штучного інтелекту.

Таким чином, запропоновані заходи спрямовані на формування системного, випереджального та технологічно адаптованого механізму правоохоронної діяльності у кіберпросторі, що дозволить ефективно реагувати на сучасні та майбутні виклики цифрової злочинності.

**Висновки.**

Таким чином, кіберпростір сьогодні є однією з ключових і водночас найбільш динамічних сфер правоохоронної діяльності. Проведений аналіз нормативно-правових актів, наукових досліджень і практичних матеріалів дозволяє дійти висновку, що ефективна протидія сучасним і майбутнім кіберзагрозам можлива лише за умови комплексного підходу, поєднання міжнародної співпраці, оновлення законодавства та впровадження нових методів реагування.

Особливого значення набуває врахування викликів, пов’язаних із розвитком штучного інтелекту, що потребує створення спеціалізованих правоохоронних механізмів та підрозділів.

Саме такий підхід здатен забезпечити кіберстійкість держави та ефективний захист правопорядку у цифровому середовищі.

**Список використаних джерел:**

1. 10 поширених загроз кібербезпеки, з якими стикається малий бізнес, і як їм запобігти. *ITEZ :* [сайт]. URL: https://itez.com.ua/blog/10-cybersecurity-threats-small-businesses-prevention.html (дата звернення: 24.03.2026).

2. Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації: Рішення Ради Національної безпеки і оборони України від 29 груд. 2016 р. (введено в дію Указом Президента України від 13 лют. 2017 р. № 32/2017). *Верховна Рада України* : [сайт]. URL: https://zakon.rada.gov.ua/laws/show/n0015525-16#Text.

3. Лисеюк А., Свінцицька Т. Розвиток міжнародного співробітництва у сфері кібербезпеки: нормативно-правові засади та перспективи. *Право та інноваційне суспільство*. 2024. № 2(23). С. 89–95.

***Мартинюк Софія Володимирівна***
студентка 109_СПД н.гр. ННІ права та психології НАВС

*Науковий керівник:*
***Грищенко Олег Ігорович***
старший викладач кафедри інформаційних технологій ННІ права та психології НАВС

## ЦІЛІ ІНФОРМАЦІЙНИХ ТА ПСИХОЛОГІЧНИХ ОПЕРАЦІЙ В КІБЕРПРОСТОРІ

Інформаційні та психологічні операції в кіберпросторі спрямовані на системну зміну поведінки, рішень і світоглядних орієнтирів цільових аудиторій через контроль інформаційного середовища та вплив на когнітивні процеси.

Інформаційні та психологічні операції в кіберпросторі в сучасних умовах трансформувалися в один із ключових інструментів геополітичного протиборства та гібридних конфліктів. Стрімка цифровізація суспільства, інтеграція інформаційно-комунікаційних технологій у всі сфери державного управління, економіки та соціальної взаємодії зумовили формування якісно нового середовища безпеки. Кіберпростір став не лише технічною інфраструктурою передачі даних, а й когнітивним середовищем, у межах якого відбувається формування суспільних установок, ціннісних орієнтирів і моделей поведінки. Саме тому вплив на інформаційне середовище дедалі частіше використовується як альтернатива або доповнення до традиційних військових засобів.

У доктринальному розумінні інформаційні операції (Information Operations) розглядаються як інтегрований комплекс заходів, спрямованих на вплив на інформаційні системи, процеси прийняття рішень та інформаційне середовище противника при одночасному захисті власного інформаційного простору [1].

Відповідні підходи системно закріплені в документах NATO та United States Department of Defense, де інформаційний компонент визначається як складова багатодоменних операцій. Психологічні операції (PSYOPS) є функціональною частиною ширшої системи інформаційного впливу й орієнтовані на зміну установок, переконань, емоційного стану та поведінки конкретних цільових аудиторій – військовослужбовців, цивільного населення, політичного керівництва, міжнародної спільноти [2].

Стратегічні цілі інформаційних та психологічних операцій у кіберпросторі мають комплексний характер. Передусім йдеться про дестабілізацію політичної системи противника шляхом підриву довіри до державних інститутів, судової системи, виборчих процедур, правоохоронних органів та збройних сил. Через поширення маніпулятивних наративів і дезінформації формується сумнів у легітимності владних рішень, що сприяє зростанню соціальної напруги та поляризації. Іншою ціллю є вплив на процеси стратегічного та оперативного прийняття рішень шляхом створення інформаційного тиску, формування хибних уявлень про реальний стан справ або нав'язування вигідного порядку денного [3].

Окремим напрямом є деморалізація особового складу збройних сил і цивільного населення. Поширення панічних настроїв, перебільшення втрат, дискредитація командування або маніпуляція фактами можуть істотно впливати на морально-психологічний стан суспільства. У цьому контексті кіберпростір дозволяє здійснювати точковий вплив через соціальні мережі, месенджери, а також через таргетовану рекламу з персоналізованим контентом. За оцінками аналітичних досліджень RAND Corporation, сучасні інформаційні кампанії дедалі більше спираються на аналіз великих масивів даних для ідентифікації вразливих груп і конструювання повідомлень, що максимально відповідають їхнім когнітивним особливостям [4].

Кіберпростір має низку характеристик, що роблять його особливо ефективним для реалізації інформаційно-психологічного впливу. Анонімність та складність атрибуції створюють сприятливі умови для прихованих операцій, оскільки доведення причетності конкретного суб'єкта є складним з технічної та правової точки зору. Глобальність цифрового середовища забезпечує охоплення міжнародної аудиторії практично без географічних обмежень. Висока швидкість поширення інформації та алгоритмічні механізми соціальних платформ сприяють вірусному ефекту, особливо щодо емоційно насиченого контенту. Використання бот-мереж, фабрик тролів, технологій deepfake та синтетичних медіа дозволяє створювати ілюзію масової підтримки певної позиції або дискредитувати конкретних осіб [5].

Психологічна складова таких операцій базується на глибокому розумінні когнітивних механізмів сприйняття інформації. Використовуються ефект підтвердження власних переконань, феномен інформаційних «бульбашок», механізми соціального доказу та емоційної поляризації [6].

Створення інформаційного перевантаження знижує здатність до критичного аналізу, а постійне повторення певних меседжів формує стійкі установки. Маніпуляція історичною пам'яттю, національною ідентичністю та культурними символами дозволяє поглиблювати розколи всередині суспільства та підсилювати конфліктні лінії.

У міжнародно-правовому вимірі питання застосування інформаційних і кібероперацій аналізуються в межах норм міжнародного права, зокрема в експертному дослідженні Tallinn Manual щодо застосування міжнародного права до кібероперацій [2]. Питання формування довіри, прозорості та заходів зміцнення безпеки в інформаційному просторі розглядаються також у документах OSCE. Аналітичні звіти European Union Agency for Cybersecurity систематизують сучасні кіберзагрози, включаючи інформаційні кампанії як елемент гібридних атак [3].

***Висновки.*** Інформаційні та психологічні операції в кіберпросторі мають стратегічну спрямованість і спрямовані на досягнення довгострокових політичних, військових та геоекономічних результатів. Їх кінцевою метою є контроль над інформаційним порядком денним, формування вигідної картини реальності та зміна поведінкових моделей цільових аудиторій без застосування військової сили. У сучасному безпековому середовищі ефективна протидія таким операціям потребує комплексного підходу: розвитку національних систем кіберзахисту, удосконалення стратегічних комунікацій, підвищення рівня медіаграмотності населення та активної міжнародної співпраці у сфері кібербезпеки.

**Список використаних джерел:**


1. NATO. *Allied Joint Doctrine for Information Operations (AJP-3.10).* URL: https://info.publicintelligence.net/NATO-IO.pdf.
2. Tallinn Manual. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* URL: https://ilmc.univie.ac.at/fileadmin/user_upload/p_ilmc/Bilder/Bewerbung/Case_2/Michael_N._Schmitt_-_Tallinn_Manual_2.0_on_the_International_Law_Applicable_to_Cyber_Operations-Cambridge_University_Press__2017_.pdf.
3. European Union Agency for Cybersecurity (ENISA). *ENISA Threat Landscape Report.* URL: https://www.enisa.europa.eu/topics/cyber-threats/threat-landscape.
4. RAND Corporation. *The Russian "Firehose of Falsehood" Propaganda Model.* URL: https://www.rand.org/pubs/perspectives/PE198.html.
5. Influence: The Psychology of Persuasion – Robert Cialdini. URL: https://ia803201.us.archive.org/7/items/ThePsychologyOfPersuasion/The%20Psychology%20of%20Persuasion.pdf.
6. Thinking, Fast and Slow – Daniel Kahneman. URL: https://dn790002.ca.archive.org/0/items/DanielKahnemanThinkingFastAndSlow/Daniel%20Kahneman-Thinking%2C%20Fast%20and%20Slow%20%20.pdf.

***Шуляк Богдан Андрійович***
студент 102_СПД н.гр. ННІ права та психології НАВС

*Науковий керівник:*
***Кудінов Вадим Анатолійович***
кандидат фізико-математичних наук, доцент, завідувач кафедри інформаційних технологій ННІ права та психології НАВС

# КІБЕРПРОСТІР У СТАНІ ВІЙНИ: ПОСИЛЕННЯ КРИМІНАЛЬНОЇ ВІДПОВІДАЛЬНОСТІ ТА НОВІ АЛГОРИТМИ КІБЕРЗАХИСТУ

Сьогодні діяльність підприємств, установ та організацій (незалежно від форми власності) залежить від стабільності кіберпростору, з яким вони працюють. ***Кіберпростір*** – це середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних (п. 11 ч. 1 ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України») [1].

Стабільність кіберпростору базується на трьох основних «китах»: 1) *стійкість* (здатність систем витримувати атаки, технічні збої або стихійні лиха та швидко відновлюватися); 2) *безпека* (захищеність даних і критичної інфраструктури від зламів, шпигунства та втручання); 3) *міжнародне право та норми* (відсутність міждержавних конфліктів у цифровій сфері та дотримання країнами «правил гри»).

Головним дестабілізуючим фактором усередині цієї системи є *кіберзлочинність* (сукупність кіберзлочинів) – це діяльність, де технології використовуються не для розвитку, а для отримання незаконної вигоди через вразливості систем та людей. Як відомо, *кіберзлочин (комп'ютерний злочин)* – це 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 (п. 8 ч. 1 ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України») [1]. Мета таких дій – це розкрадання або руйнування інформації в інформаційних системах і мережах. За даними офіційної статистики лише за останні 8 років кількість виявлених кіберзлочинів в Україні збільшилась майже в 7,5 разів [2].

В умовах війни кіберзлочини можуть здійснюватися з метою дестабілізації ситуації в країні, крадіжки необхідних (конфіденційних) даних, виведення з ладу державних інституцій, техніки, завдання іншої матеріальної шкоди. В наш час війна в кіберпросторі може завдати не меншої шкоди, аніж війна на полі бою. Від початку війни стало відомо про велику кількість кібератак на Україну. На країну припало близько 9,5% від загальної кількості постраждалих у європейському регіоні [3]. Наприкінці червня 2025 року очільник Мінцифри Михайло Федоров розповідав, що Україна щомісяця зазнає близько 100 тисяч кібератак [4]. У відповідь на зростання кіберзагроз, Президент України Зеленський Володимир 27 березня 2025 року підписав законопроєкт, який формує принципи з кіберзахисту держінформресурсів [5].

Відомо, що відповідальність за кіберзлочини передбачена розділом XVI «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» Кримінального кодексу України (далі – ККУ) [6], який містить станом на сьогодні 6 статей. Верховна Рада України на початку війни з метою удосконалення підстав та процесуальних механізмів притягнення до кримінальної відповідальності кіберзлочинців оперативно внесла зміни до кримінального та кримінально-процесуального законодавства [7, 8].

Закон України від 24 березня 2022 року № 2149-IX було розроблено з метою посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам у сучасному безпековому середовищі шляхом оптимізації положень статей 361, 361-1 ККУ [9]. Внесено зміни в термінологію цих статей. Стаття 361 ККУ викладена в новій редакції, якою розмежовується ступінь відповідальності за несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж в залежності від спричинених наслідків, а також посилені санкції за вчинення відповідного кримінального правопорушення [9]. Серед нових кваліфікованих юридичних складів злочину необхідно відмітити дії, вчинені під час дії воєнного стану (ч. 5 ст. 361 ККУ) [6]. Настільки суворі санкції за їх вчинення продиктовані поточною ситуацією в країні, адже особа, яка завдає шкоди національним інтересам України чи українцям у кіберпросторі, тим самим допомагаючи агресору у цій війні, не може нести відповідальності меншої, ніж військові злочинці [10]. Посилено санкції за вчинення кримінального правопорушення, передбаченого статтею 361-1 ККУ, щодо створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут [6, 10].

В роботі [10] висловлено побажання змінити термінологію назви розділу та інших статей з нього ж, де юридичні склади інших правопорушень також охоплюються поняттям «кіберзлочини», а також посилити відповідальність за збут або розповсюдження інформації з обмеженим доступом (ч. 1 ст. 361-2 ККУ).

Водночас стаття 361 ККУ передбачає, що втручання в роботу цих систем та мереж, не вважається несанкціонованим, якщо таке втручання вчинено відповідно до Порядку пошуку та виявлення потенційних вразливостей таких систем чи мереж [9, 10, 11]. Необхідність запровадження невідкладних змін в українському законодавстві для узаконення процедури Bug Bounty (залучення зовнішніх фахівців до пошуку помилок і вразливостей програмних продуктів, інформаційно-комунікаційних систем тощо) виникла ще до початку війни, після кібератак 14 січня 2022 року на сайти державних органів влади [10]. Станом на сьогодні ІТ-спільнота може легально тестувати державні інформаційні системи на наявність вразливостей, а держава має інструмент для значного підвищення ступеня захисту таких систем [12]. Кабінет Міністрів України ухвалив постанову від 03 грудня 2025 року № 1580, яка створює правову рамку для залучення «етичних хакерів» до пошуку вразливостей у системах, які обробляють державні інформаційні ресурси та інформацію з обмеженим доступом, а також на об'єктах критичної інформаційної інфраструктури [13]. Постанова встановлює чіткі правила для взаємодії між державою та спільнотою фахівців з кібербезпеки.

Відтепер пошук вразливостей здійснюватиметься за трьома основними напрямами: 1) CERT-UA, галузеві CSIRT та власники систем на постійній основі здійснюють збір та аналіз інформації про вразливості; 2) Державний центр кіберзахисту Держспецзв'язку проводить планове та позапланове сканування державних вебресурсів на наявність вразливостей, а також пошук вразливостей під час проведення оцінки стану захищеності систем; 3) залучення зовнішніх дослідників до пошуку вразливостей на визначених умовах [12, 13].

Порядок сканування на предмет вразливості державних інформаційних ресурсів, розміщених у мережі Інтернет, регламентується нормативно-правовим актом [14], а Порядок пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж регламентується нормативно-правовим актом [15].

В роботі [10] зазначено, що державним органам, підприємствам, місцевим жителям, які перебувають під час війни в зоні ризику варто звернути увагу на декілька точок контролю:

1. Залучати технічних спеціалістів (спеціалізовані компанії). Професіонали здатні ускладнити роботу ворогу через запровадження необхідних алгоритмів захисту, в тому числі організаційних. Варто відповідно проінструктувати працівників, які залучені до роботи із відповідними системами та мережами, адже багато атак досягають цілі лише через непродумані й необережні дії працівників.

2. Тим, хто перебуває в зоні кіберризику, варто слідкувати за відповідними повідомленнями на офіційних ресурсах Держспецзв'язку та CERT-UA. Ці органи публікують офіційні попередження не лише про можливі кіберзагрози, а й про те, як мінімізувати ризики.

3. Якщо ви стали жертвою кібератаки, повідомте про це тих, на кого така атака може поширитися. Для фізичних осіб – це контакти, з якими здійснюється активна комунікація. Для організацій – це співробітники, клієнти та контрагенти.

4. Найважливіше завдання кожного у момент виявлення атаки – інформувати офіційні суб'єкти забезпечення кібербезпеки України, CERT-UA та Кіберполіцію. Це дозволить не лише притягти до відповідальності винних, а й вжити невідкладних заходів з блокування шкідливих вебресурсів.

***Висновки.*** Сфера кіберпростору завжди потребувала посиленого захисту та змін. Відкрите вторгнення росії стимулювало вдосконалення чинного законодавства та гарантій безпеки у сучасному інформаційному середовищі. Розширено межі діяльності правоохоронних органів щодо розслідування кіберзлочинів, передбачених статями 361, 361-1 ККУ. Посилення санкцій та додаткова криміналізація окремих діянь здатні частково стримати потенційних злочинців від вчинення нових злочинів. Виправданим є й запровадження відповідальності за злочини, що скоєні у воєнний час [10].

Таким чином, основи законодавчих механізмів для ефективного кіберзахисту в кіберпросторі в умовах воєнного стану закладені. Завдання кожного – при виявленні кібератаки якнайшвидше запустити цей механізм, щоб у майбутньому подібних атак та збитків від них ставало дедалі менше [10].

**Список використаних джерел:**

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05 жовт. 2017 р. № 2163-VIII. *Відомості Верховної Ради України*. 2017. № 45. Ст. 403.

2. Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування. *Офіс Генерального прокурора* : [сайт]. URL: https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2 (дата звернення: 23.03.2026).

3. Кузьменко О. Україна посіла п'яте місце у світі та третє в Європі серед країн, які найчастіше ставали об'єктами кібератак (дата публікації: 17.10.2025). *Dev.ua* : [сайт]. URL: https://dev.ua/news/ukraina-posila-piate-mistse-u-sviti-ta-tretie-v-yevropi-sered-krain-iaki-naichastishe-stavaly-obiektamy-kiberatak-1760682433 (дата звернення: 23.03.2026).

4. Михайлов Д. Українські держресурси зазнають близько 100 тисяч кібератак щомісяця – Федоров (дата публікації: 18.06.2025). *Суспільне Новини* : [сайт]. URL: https://suspilne.media/1045747-ukrainski-derzresursi-zaznaut-blizko-100-tisac-kiberatak-somisaca-fedorov/ (дата звернення: 23.03.2026).

5. Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури : Закон України від 27 берез. 2025 р. № 4336-IX. *Відомості Верховної Ради*. 2025. № 35. Ст. 134.

6. Кримінальний кодекс України : Закон України від 05 квіт. 2001 р. № 2341-III. Відомості Верховної Ради України. 2001. № 25-26. Ст. 131. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text.

7. Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану : Закон України від 24 берез. 2022 р. № 2149-IX. *Голос України* від 02 квіт. 2022 р. № 74. URL: https://zakon.rada.gov.ua/laws/show/2149-20#Text.

8. 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 берез. 2022 р. № 2137-IX. *Голос України* від 21 берез. 2022 р. № 62. URL: https://zakon.rada.gov.ua/laws/show/2137-20#Text.

9. Пояснювальна записка до проєкту Закону України «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану». *Верховна Рада України* : [сайт]. URL: blob:https://itd.rada.gov.ua/62ada0aa-5fe7-4f2c-bd6e-30273eaced1e.

10. Боротьба з кіберзлочинністю в умовах дії воєнного стану: Закон 2149-IX. *ЮРЛІГА :* [сайт]. URL: https://jurliga.ligazakon.net/analitycs/210562_borotba-z-kberzlochinnstyu-v-umovakh-d-vonnogo-stanu-zakon-2149-ix (дата звернення: 23.03.2026).

11. Держспецзв'язку: В Україні узаконили Bug Bounty. Що це – і як допоможе? *Урядовий портал* : [сайт]. URL: https://www.kmu.gov.ua/news/derzhspeczvyazku-v-ukrayini-uzakonili-bug-bounty-shcho-ce-i-yak-dopomozhe (дата звернення: 23.03.2026).

12. Уряд легалізував Bug Bounty для державних систем. *Державна служба спеціального зв'язку та захисту інформації України* : [сайт]. URL: https://cip.gov.ua/ua/news/uryad-legalizuvav-bug-bounty-dlya-derzhavnikh-sistem (дата звернення: 23.03.2026).

13. Деякі питання пошуку та виявлення потенційних вразливостей в інформаційно-комунікаційних системах : Постанова КМУ від 03 груд. 2025 р. № 1580. URL: https://zakon.rada.gov.ua/laws/show/1580-2025-%D0%BF#Text.

14. Про затвердження Порядку сканування на предмет вразливості державних інформаційних ресурсів, розміщених у мережі Інтернет : Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 15 січ. 2016 р. № 20. *Верховна Рада України* : [сайт]. URL: https://zakon.rada.gov.ua/laws/show/z0196-16#n13.

15. Про затвердження Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж : Постанова КМУ від 16 трав. 2023 р. № 497. *Верховна Рада України* : [сайт]. URL: https://zakon.rada.gov.ua/laws/show/497-2023-%D0%BF#n10.

***Гуменюк Вікторія Олегівна***
студентка 202_СПС н.гр. ННІ права та психології НАВС

*Науковий керівник:*
***Пакриш Олександр Євгенійович***
кандидат технічних наук, доцент, доцент кафедри інформаційних технологій ННІ права та психології НАВС

## КІБЕРСТАЛКІНГ – ОСНОВНІ ОЗНАКИ ТА ПРОТИДІЯ

У сучасному інформаційному суспільстві Інтернет став невід'ємною частиною життя людини. Разом із його перевагами з'являються й нові загрози, однією з яких є ***кіберсталкінг***. Це форма онлайн-переслідування, що полягає у нав'язливому контролі, стеженні, залякуванні або психологічному тиску на людину за допомогою цифрових технологій. Кібersталкінг може проявлятися у різних формах. Найпоширенішими ознаками є регулярні небажані повідомлення або дзвінки, постійні коментарі в соціальних мережах, створення фейкових акаунтів для стеження чи контакту, а також поширення особистої інформації без згоди людини. Окрім цього, до проявів кібersталкінгу належать погрози, шантаж, образи та навіть спроби зламу особистих акаунтів. Усе це може спричиняти серйозні психологічні наслідки, такі як тривога, страх, емоційне виснаження та зниження самооцінки.

Важливо знати, як протидіяти кібersталкінгу та захистити себе. Насамперед не варто вступати в діалог із переслідувачем, оскільки це може лише посилити його дії. Необхідно зберігати всі докази переслідування: скріншоти повідомлень, листування, записи дзвінків. Слід блокувати порушника в соціальних мережах і месенджерах, змінювати паролі та налаштовувати конфіденційність акаунтів. Рекомендується обмежити публікацію особистої інформації у відкритому доступі. У разі серйозних погроз або тривалого переслідування важливо звернутися до адміністрації онлайн-платформ або правоохоронних органів. Це допоможе не лише зупинити порушника, а й притягнути його до відповідальності.

Особливо вразливою категорією до кібернасильства є жінки. Серед поширених форм – кібербулінг, мова ворожнечі, онлайн-переслідування, секстинг, аутинг та інші прояви. Такі дії можуть завдавати психологічної шкоди, підривати репутацію та навіть створювати фізичну загрозу. Запобігання цифровому насильству передбачає дотримання базових правил безпеки: захист персональних даних, уважність до онлайн-спілкування, вміння розпізнавати агресивну поведінку та формування відповідального ставлення до використання Інтернету.

Важливо також знати, куди звертатися за допомогою у разі загрози. Цифрові технології також можуть використовуватися і в межах домашнього насильства – для стеження, контролю або приниження. У таких випадках важливо знати свої права та звертатися до відповідних органів по допомогу.

У 2024 році в Європейському Союзі було прийнято директиву, спрямовану на боротьбу з насильством щодо жінок і домашнім насильством. Вона передбачає кримінальну відповідальність за онлайн-переслідування, домагання та розпалювання ненависті. Крім того, важливими міжнародними документами є Стамбульська, Будапештська та Лансаротська конвенції, які забезпечують захист прав жінок і дітей [1].

Щодо юридичної відповідальності за кіберсталкінг, слід зауважити, що стаття 32 Конституції України гарантує непорушність приватного життя. Законом України «Про основні засади забезпечення кібербезпеки України» запропоновано визначення відносно нової категорії злочинів – кіберзлочинів (комп'ютерних злочинів) – як суспільно небезпечних винних діянь у кіберпросторі та/або з його використанням, відповідальність за які передбачена законом України про кримінальну відповідальність та/або які визнано злочином міжнародними договорами України.

Відповідно до п. 14 ст. 1 Закону України «Про запобігання та протидію домашньому насильству» переслідування визначено окремою формою психологічного насильства, що включає словесні образи, погрози, зокрема щодо третіх осіб, приниження, переслідування, залякування, інші діяння, спрямовані на обмеження волевиявлення особи, контроль у репродуктивній сфері, якщо такі дії або бездіяльність викликали у постраждалої особи побоювання за свою безпеку чи безпеку третіх осіб, спричинили емоційну невпевненість, нездатність захистити себе або завдали шкоди психічному здоров'ю особи [2].

***Отже***, кіберсталкінг є серйозною загрозою в сучасному цифровому середовищі, що негативно впливає на психологічний стан і безпеку людини. Його своєчасне розпізнавання та усвідомлення можливих наслідків дозволяє ефективно протидіяти цьому явищу. Важливо дотримуватися правил онлайн-безпеки, не ігнорувати ознаки переслідування та вчасно звертатися по допомогу. Лише поєднання обізнаності, обережності та активних дій сприяє надійному захисту від кіберсталкінгу.

**Список використаних джерел:**

1. Карєв І. Ю., Фурашев В. М. Кібersталкінг: відображення у національному законодавстві. *Інформація і право*. 2021. № 1(36). С. 95–102. DOI: https://doi.org/10.37750/2616-6798.2021.1(36).238176 URL: https://il.ippi.org.ua/article/view/238176 (дата звернення: 26.03.2026).

2. Бежевець А. М., Шах К. І. Кібербулінг та кіберсталкінг в Інтернет-середовищі: порівняльно-правовий аналіз понять. *Інформація і право*. 2022. № 3(42). С. 49–54. DOI: https://doi.org/10.37750/2616-6798.2022.3(42).270100 URL: https://il.ippi.org.ua/article/view/270100 (дата звернення: 26.03.2026).

3. Кузан О., Кушніренко Н. Кіберсталкінг: проблеми та методи автоматичного виявлення. *Кібербезпека та комп'ютерно-інтегровані технології*. 2025. С. 7–12. URL: https://conference.wunu.edu.ua/index.php/kbkit/article/view/718 (дата звернення: 26.03.2026).

4. Красніков С. А. Кібергігієна як чинник запобігання кіберзагрозам. *Нове українське право*. 2024. № 6. С. 52–58. DOI: https://doi.org/10.51989/NUL.2024.6.8 URL: https://newukrainianlaw.in.ua/index.php/journal/article/view/689 (дата звернення: 26.03.2026).

***Король Тетяна Анатоліївна***
студентка 201_СПС н.гр. ННІ права та психології НАВС

*Науковий керівник:*
***Тарасенко Володимир Петрович***
кандидат фізико-математичних наук, доцент кафедри інформаційних технологій ННІ права та психології НАВС

## ПСИХОЛОГІЧНІ МЕТОДИ МАНІПУЛЯЦІЇ В КІБЕРПРОСТОРІ ТА ШЛЯХИ ПРОТИДІЇ

Сучасний етап розвитку інформаційного суспільства характеризується стрімким поширенням цифрових технологій та зростанням ролі кіберпростору у всіх сферах життєдіяльності людини. Інтернет, соціальні мережі, онлайн-платформи та цифрові комунікаційні сервіси стали невід'ємною частиною повсякденного життя. Вони виконують функції обміну інформацією, соціальної взаємодії, професійної діяльності, освіти та дозвілля. Водночас активна цифровізація суспільства спричинила появу нових соціально-психологічних викликів, серед яких особливе місце займають психологічні маніпуляції в кіберпросторі. Кіберпростір сьогодні виступає не лише середовищем комунікації, але й потужним інструментом впливу на свідомість людини. Інформація в цифровому середовищі поширюється надзвичайно швидко, що значно ускладнює її перевірку та критичне осмислення. Це створює сприятливі умови для використання різноманітних маніпулятивних технологій, спрямованих на формування певних установок, переконань та моделей поведінки користувачів.

Особливо актуальною ця проблема стала в умовах глобальних інформаційних процесів та інформаційних протистоянь, коли кіберпростір активно використовується для здійснення психологічного впливу на масову свідомість [1].

Психологічна маніпуляція у кіберпросторі визначається як прихований вплив на психіку людини з метою зміни її думок, установок або поведінки без її усвідомлення. Головною особливістю маніпуляції є її прихований характер, коли людина не завжди здатна розпізнати факт зовнішнього впливу. Маніпулятори активно використовують особливості когнітивних процесів, емоційні реакції, соціальні стереотипи та психологічні механізми сприйняття інформації [2].

Одним із найпоширеніших методів психологічної маніпуляції в кіберпросторі є **поширення дезінформації та фейкових новин**. Фейкові повідомлення створюються з метою введення користувачів в оману, формування панічних настроїв або впливу на громадську думку. Дослідники зазначають, що фейкові новини часто мають емоційно забарвлений характер і апелюють до страху, гніву або співчуття. Саме емоційна насиченість сприяє швидкому поширенню таких повідомлень у соціальних мережах, оскільки люди більш охоче діляться інформацією, яка викликає сильні емоції.

Іншим важливим методом маніпуляції є використання **когнітивних упереджень людини**. Когнітивні упередження – це систематичні помилки мислення, які виникають у процесі обробки інформації. Одним із найбільш відомих є ефект підтвердження, відповідно до якого люди схильні звертати увагу на інформацію, що підтверджує їхні попередні переконання, і ігнорувати інформацію, яка їм суперечить. Маніпулятори активно використовують цей механізм, створюючи інформаційні повідомлення, які відповідають очікуванням певної аудиторії. У результаті користувачі сприймають таку інформацію як правдиву, навіть не перевіряючи її достовірність.

У кіберпросторі широко застосовується також **ефект соціального доказу**. Люди схильні вважати правильними ті погляди або дії, які підтримує більшість. У соціальних мережах цей ефект підсилюється через використання великої кількості коментарів, лайків та репостів. Часто для цього використовуються фальшиві акаунти або автоматизовані програми (боти), які створюють ілюзію масової підтримки певної позиції. У результаті користувачі починають сприймати таку інформацію як більш достовірну та поширену.

Ще одним поширеним методом маніпуляції є **емоційний вплив**. Маніпулятивні повідомлення часто спрямовані на виклик сильних емоційних реакцій, таких як страх, обурення, тривога або співчуття. У стані сильного емоційного збудження людина менш схильна до критичного аналізу інформації та може швидше приймати імпульсивні рішення. Тому маніпулятивні повідомлення часто містять шокуючі заголовки, драматичні історії або емоційні заклики.

Суттєву роль у сучасних маніпуляціях відіграють **алгоритми соціальних мереж**, які формують інформаційні стрічки користувачів.

Алгоритми підбирають контент відповідно до інтересів та поведінки людини, що призводить до формування так званих «інформаційних бульбашок». У межах таких бульбашок користувачі отримують переважно інформацію, яка відповідає їхнім поглядам, що посилює вплив маніпулятивних повідомлень.

Особливу небезпеку становлять також **технології таргетованого впливу**, що базуються на аналізі персональних даних користувачів. Сучасні цифрові платформи здатні аналізувати поведінку людини в Інтернеті, її інтереси, уподобання та психологічні характеристики. На основі цих даних створюються персоналізовані повідомлення, які можуть мати значно більший вплив на конкретну аудиторію.

У зв'язку з поширенням психологічних маніпуляцій у кіберпросторі надзвичайно важливим стає питання ефективної протидії таким впливам. Одним із ключових напрямів є **розвиток критичного мислення**. Критичне мислення передбачає здатність аналізувати інформацію, оцінювати її достовірність, перевіряти джерела та робити обґрунтовані висновки. Люди з розвиненим критичним мисленням менш схильні піддаватися маніпуляціям та дезінформації.

Важливу роль відіграє також **підвищення рівня медіаграмотності населення**. Медіаграмотність передбачає знання про механізми створення та поширення інформації, розуміння особливостей роботи медіа та здатність відрізняти достовірну інформацію від маніпулятивної. Освітні програми з медіаграмотності сприяють формуванню відповідального ставлення до споживання інформації та розвитку інформаційної культури суспільства [2].

Ще одним важливим напрямом є **формування психологічної стійкості особистості**. Психологічна стійкість дозволяє людині зберігати емоційну рівновагу, адекватно оцінювати інформацію та не піддаватися панічним або маніпулятивним настроям. Розвиток емоційної саморегуляції, усвідомленості та здатності контролювати власні реакції сприяє зменшенню впливу психологічних маніпуляцій [3].

Не менш важливими є **технологічні та правові механізми протидії дезінформації**. Соціальні мережі та інтернет-платформи впроваджують системи перевірки інформації, маркування фейкових повідомлень, блокування ботів та підозрілих акаунтів. Разом із цим державні інституції розробляють нормативно-правові механізми регулювання інформаційного простору.

***Отже***, психологічні методи маніпуляції в кіберпросторі становлять серйозну загрозу для інформаційної безпеки суспільства та психологічного благополуччя людини. Вони базуються на використанні когнітивних упереджень, емоційних реакцій та соціально-психологічних механізмів впливу. Ефективна протидія таким маніпуляціям можлива лише за умови комплексного підходу, що поєднує розвиток критичного мислення, підвищення медіаграмотності, формування психологічної стійкості особистості та вдосконалення технологічних і правових механізмів інформаційної безпеки.

**Список використаних джерел:**

1. Почепцов Г. Г. Інформаційні війни: нові реалії та стратегії. Київ : Видавничий дім «Києво-Могилянська академія», 2015. 320 с.
2. Найдьонова Л. А. Медіапсихологія: основи рефлексивного підходу. Київ : Міленіум, 2015. 244 с.
3. Кокун О. М. Психологічна стійкість особистості в умовах сучасних викликів. Київ : Інститут психології ім. Г. С. Костюка НАПН України, 2017. 256 с.
4. Максименко С. Д. Генеза здійснення особистості. Київ : Видавництво ТОВ «КММ», 2006. 240 с.
5. Чепелєва Н. В. Особистість у кризових умовах: психологічні аспекти розвитку та адаптації. Київ : Педагогічна думка, 2012. 312 с.

***Масовець В'ячеслав Олександрович***
студент 107_СПД н.гр. ННІ права та психології НАВС

*Науковий керівник:*
***Грищенко Олег Ігорович***
старший викладач кафедри інформаційних технологій ННІ права та психології НАВС

## ВИКОРИСТАННЯ СОЦІАЛЬНИХ МЕРЕЖ ЯК ІНСТРУМЕНТУ ВПЛИВУ ТА МАНІПУЛЯЦІЇ В КОНТЕКСТІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

У сучасному глобалізованому світі інформаційний простір став не просто середовищем обміну даними, а повноцінним театром бойових дій. Соціальні мережі трансформувалися у потужні механізми управління суспільною свідомістю, що створює пряму загрозу національній безпеці. Особливої гостроти це питання набуває в умовах гібридної агресії, де маніпуляція фактами та підміна понять стають ефективнішими за традиційні види озброєння [1, с. 112].

Механізм впливу в соціальних мережах базується на використанні алгоритмів «інформаційних бульбашок» та специфічного феномену «зручності сприйняття» готової позиції. Для пересічного користувача самостійний аналіз складних процесів є когнітивно затратним. Лідер суспільної думки (ЛСД) пропонує готову, емоційно забарвлену картину світу, створюючи ілюзію правильності. Людина потрапляє в стан «делегованого мислення», де власна думка замінюється ретрансляцією тез медійного авторитету. Це призводить до «інтелектуального паразитизму», який дає відчуття приналежності до «правильної» групи без зайвих зусиль [2, с. 48].

Фундаментальним чинником успіху таких маніпуляцій є горизонтальна довіра та віральність. Маніпулятивні ідеї розповсюджуються за принципом «соціального доказу»: коли знайома людина рекомендує пост чи лідера думок, критичний фільтр користувача вимикається. Довіра до особистості автоматично переноситься на контент. Це запускає вірусний механізм, де неправдива ідея чи штучно створена аналогія поширюється з геометричною прогресією через приватні повідомлення та репости знайомих. У такий спосіб ворожі ІПСО маскуються під «поради від своїх», що робить їх практично невразливими для стандартних методів спростування [3, с. 157].

В умовах війни цей фактор підсилюється використанням «сірих зон» правового регулювання. Анонімність у соціальних мережах створює ілюзію безкарності для маніпуляторів. Це дозволяє безперешкодно розповсюджувати неправдиві ідеї, які формують ефект «цифрового страху». Коли через бот-мережі створюється видимість агресивної більшості, прихильники державної позиції можуть впадати у вимушену самоцензуру. Людина боїться висловити власну думку, бачачи удавану монолітність протилежного боку, що призводить до руйнування суспільної єдності [4, с. 92].

Вплив на людину через соцмережі часто ігнорує логіку, апелюючи до базових емоцій. Фактор освіти у цьому контексті є двосічним: маніпулятори використовують «ілюзію знання», надаючи прості відповіді на складні питання національної безпеки. Навіть високий рівень формальної освіти не рятує від маніпуляцій, якщо у громадянина відсутня навичка деконструювати маніпулятивні аналогії, які підміняють суть юридичних та політичних реалій. Використання мікротаргетингу дозволяє зламувати суспільну злагоду, спрямовуючи персоналізовані маніпуляції на конкретні групи населення [5, с. 212].

***Отже***, протидія маніпуляціям у соцмережах потребує не лише технологічних рішень, а й нових підходів у правоохоронній діяльності та стратегічних комунікаціях. Захист національної безпеки сьогодні неможливий без усвідомлення кожним громадянином своєї ролі у віральному поширенні інформації. Формування культури індивідуальної інформаційної гігієни є невід'ємною частиною сучасної державної доктрини безпеки.

**Список використаних джерел:**

1. Горбулін В. П. Як перемогти росію у війні майбутнього. Київ : Брайт Букс, 2020. С. 112–118.

2. Почепцов Г. Когнітивні війни. Київ : Видавничий дім «Києво-Могилянська академія», 2019. С. 45–52.

3. Чалдині Р. Психологія впливу. Харків : Клуб сімейного дозвілля, 2016. С. 154–160.

4. Золотар О. А. Інформаційна безпека людини в умовах цифровізації: правовий аспект. Київ : АртЕк, 2021. С. 89–94.

5. Вайлі К. Mindf*ck: Як Cambridge Analytica будувала модель для зламу свідомості. Харків : Фабула, 2021. С.210–215.

***Кривошеєва Діана Юріївна***
студентка 202_СПС н.гр. ННІ права та психології НАВС

*Науковий керівник:*
***Пакриш Олександр Євгенійович***
кандидат технічних наук, доцент, доцент кафедри інформаційних технологій ННІ права та психології НАВС

## ГРУМІНГ: ОСНОВНІ ОЗНАКИ ТА ПРОТИДІЯ

У сучасному цифровому середовищі стрімкий розвиток інформаційних технологій створює не лише нові можливості для комунікації, але й нові загрози, серед яких особливу небезпеку становить явище грумінгу. ***Грумінг*** – це процес встановлення довірливих відносин із дитиною або підлітком з метою подальшої експлуатації, найчастіше сексуального характеру. Зловмисники використовують психологічні маніпуляції, щоб поступово підпорядкувати жертву та отримати контроль над нею.

Актуальність теми зумовлена зростанням кількості випадків онлайн-грумінгу, особливо в соціальних мережах, месенджерах та ігрових платформах. Діти та підлітки є найбільш уразливою категорією через недостатній життєвий досвід, довірливість та потребу у спілкуванні й підтримці. Це робить їх легкою мішенню для маніпуляцій з боку злочинців.

Проблему грумінгу досліджують як вітчизняні, так і зарубіжні науковці. Зокрема, Н. О. Симоненко [3] аналізує кримінально-правові аспекти захисту дітей у кіберпросторі, а В. В. Сенько [4] – психологічні механізми впливу на неповнолітніх. Зарубіжні дослідники, такі як E. Whittle [1] та S. Webster [2], вивчають поведінкові стратегії грумерів і способи їх виявлення в онлайн-середовищі.

Грумінг має чітко визначені етапи, які дозволяють ідентифікувати загрозу. На першому етапі відбувається встановлення контакту: зловмисник представляється однолітком або людиною, яка викликає довіру. Далі формується емоційний зв’язок – жертву підтримують, вислуховують, створюють ілюзію близькості.

Наступним кроком є ізоляція дитини від оточення, коли її переконують зберігати спілкування в таємниці. На завершальному етапі відбувається експлуатація – вимагання інтимних фото, відео або зустріч у реальному житті.

Основними ознаками грумінгу є надмірна увага до дитини з боку незнайомця, швидке встановлення довірливих відносин, використання компліментів та подарунків, поступовий перехід до інтимних тем, а також спроби ізолювати жертву від друзів і родини. Важливим сигналом небезпеки є прохання зберігати таємницю спілкування або надсилати особисту інформацію.

Психологічними чинниками, що сприяють ефективності грумінгу, є потреба підлітків у визнанні, самотність, низька самооцінка та відсутність достатнього контролю з боку дорослих. Зловмисники активно використовують емпатію, маніпуляції почуттями та страхами, а також поступове підвищення рівня довіри.

Для протидії грумінгу необхідно застосовувати комплексний підхід. Насамперед важливо підвищувати рівень цифрової грамотності дітей та підлітків, формувати у них критичне мислення та навички безпечної поведінки в Інтернеті. Дітей слід навчати не довіряти незнайомцям онлайн, не розголошувати особисту інформацію та повідомляти дорослих про підозріле спілкування.

Важливу роль відіграють батьки та педагоги, які повинні підтримувати довірливі відносини з дітьми, цікавитися їх онлайн-активністю та пояснювати можливі ризики. Також доцільно використовувати технічні засоби захисту: налаштування конфіденційності, батьківський контроль, фільтрацію контенту.

***Отже***, грумінг є серйозною загрозою в сучасному цифровому середовищі, що потребує підвищеної уваги з боку суспільства. Основними ознаками грумінгу є маніпулятивна поведінка, швидке встановлення довіри та поступове втягнення жертви в небезпечну взаємодію. Ефективна протидія можлива лише за умови поєднання освітніх, психологічних і технічних заходів, а також активної участі дорослих у забезпеченні безпеки дітей. Формування обізнаності та відповідальної поведінки в Інтернеті є ключовим чинником запобігання цьому явищу.

**Список використаних джерел:**

1. Whittle H., Hamilton-Giachritsis C., Beech A., Collings G. A review of online grooming: Characteristics and concerns // Aggression and Violent Behavior. 2013.

2. Webster S., Davidson J. B. B. European Online Grooming Project: Final Report. 2012.

3. Симоненко Н. О. Кримінальна відповідальність за «грумінг». *Правова держава*. 2022. № 45. С. 120–127. URL: https://pd.onu.edu.ua/article/view/254367 (дата звернення: 26.03.2026).

4. Сенько В. В. Актуальні питання кібергрумінгу в Україні. *Аналітично-порівняльне правознавство*. 2022. № 2. С. 244–249. DOI: https://doi.org/10.24144/2788-6018.2022.02.48. URL: https://journal-app.uzhnu.edu.ua/article/view/261901 (дата звернення: 26.03.2026).

***Горбаченко Вероніка Романівна***
студентка 208_СПД н.гр. ННІ права та психології НАВС

*Науковий керівник:*
***Кудінов Вадим Анатолійович***
кандидат фізико-математичних наук, доцент, завідувач кафедри інформаційних технологій ННІ права та психології НАВС

# КІБЕРБЕЗПЕКА В СОЦІАЛЬНИХ МЕРЕЖАХ

У сучасних умовах цифровізації суспільства соціальні мережі стали невід'ємною частиною повсякденного життя людини: ми ділимося фотографіями, отримуємо інформацію про різноманітні події, спілкуємося з рідними та друзями. Проте разом зі зручністю зростає ризик і небезпека – зломи акаунтів, крадіжки особистих даних та фішинг [1].

У сучасному світі важко уявити життя без соціальних мереж та платформ, таких як Facebook, Instagram, TikTok, Telegram та безліч інших. Водночас акаунти користувачів містять значну кількість особистої інформації, яка потребує надійного захисту [2]. Злам акаунтів і витік особистих даних є реальною загрозою, оскільки зловмисники можуть скористатися цим задля шахрайства або інших протиправних дій. Слід врахувати, що багато користувачів, незважаючи на ці численні випадки, все ж недооцінюють загрози, вважаючи що їх це омине, але насправді будь-хто може стати жертвою кіберзлочинців. Тому треба пам'ятати декілька правил, які можуть мінімізувати ризик витоку даних [3].

Перш за все, необхідно звернути увагу на ознаки можливого злому. Наприклад: якщо у профілі з'являються публікації або повідомлення, яких ви не створювали та не публікували в мережі особисто; якщо рідні, друзі, підписники отримують від вас підозрілі повідомлення; або якщо ви отримуєте повідомлення від певної платформи про витік даних. Ці всі основні ознаки є підставою терміново змінити пароль, попередити друзів та рідних та звернутися до служби підтримки платформи. Якщо ж є підозра, що ваші фінанси також під загрозою, потрібно повідомити банк і звернутися до правоохоронних органів.

Особливу загрозу становить фішинг – один з найпоширеніших методів кіберзлочинності, що полягає у виманюванні конфіденційної інформації шляхом використання підроблених сайтів або повідомлень. Зараз ця схема є дуже актуальною, тому основним захистом від цього є попередня уважна перевірка всіх посилань, сайтів та листів, особливо якщо вони містять надмірно привабливі пропозиції або спам.

Ефективним засобом підвищення рівня безпеки є використання двофакторної автентифікації. Передбачає такий захист, як: додатковий пароль, SMS-повідомлення, FaceID або інші методи підтвердження. Крім того, для кожної соціальної мережі за можливості рекомендується створювати окрему електронну пошту для того аби захистити профіль від спаму та фішингових атак.

Важливим елементом кібезахисту є використання надійних паролів. Є певні вимоги щодо створення їх, аби знизити можливість злому: унікальність для кожного облікового запису, щонайменше 12 символів, великі та малі літери, цифри, спеціальні символи тощо. Використання простих або однакових паролів значно підвищує ймовірність злому. Також слід ретельно та обережно ставитися до нових контактів у соцмережах, оскільки фейкові акаунти можуть поширювати шкідливий та небезпечний контент і формувати інформаційні бульбашки.

Окремої уваги потребує проблема кібербулінгу (кіберхуліганство). Вона полягає у систематичному переслідуванні, образах або приниженні користувачів. Тому у разі виникнення подібних ситуацій доцільно відразу блокувати кривдників, зберігати про всяк випадок докази їх дій та повідомляти адміністрацію певної платформи про неправомірну поведінку.

Значною загрозою для безпеки користувачів є надмірне розкриття персональної інформації: особисті дані (дата народження, плани на відпустку чи навіть здавалося би якась дрібниця) можуть бути використані злочинцями для шахрайства, що вже казати про обережність приватних розмов чи відвертих фотографій. Тому важливо обмежувати публічний доступ до таких відомостей і не розкривати їх у соціальних мережах, месенджерах, а інколи й навіть у приватних розмовах.

Для забезпечення належного рівня кібербезпеки важливо дотримуватися базових принципів так званої кібергігієни. Це передбачає регулярне оновлення програмного забезпечення та операційних систем, перевірку файлів на віруси, використання мережевих екранів та надійного антивірусного програмного забезпечення, а також контроль активних сесій і сторонніх пристроїв. Якщо ж є хоч найменший сумнів – відразу вживати всі необхідні міри для подальшого забезпечення контролю та захисту над своїми особистими даними. А кібергігієна допомагає мінімізувати ризики порушення безпеки, а також дозволяє залишатися в курсі нових кіберзагроз.

Особливої актуальності питання кібербезпеки набуває в умовах воєнного стану в Україні. Суворо дотримуватися правил мають військові, держслужбовці та працівники критичних секторів. Рекомендується мінімізувати використання месенджерів і соціальних мереж для службового спілкування, вимикати геолокацію на пристроях, не розголошувати важливу інформацію стороннім особам, максимально обмежувати публікацію контенту військової тематики і користуватися лише тими сервісами, які застосовують наскрізне шифрування [4].

Для журналістів і публічних осіб також важливо застосовувати додаткові заходи захисту, зокрема впроваджувати двофакторні перевірки на всіх платформах, ставити надійні паролі, використовувати VPN і зашифровані канали для комунікацій [3].

***Отже***, важливо розуміти, що кібезбезпека в соціальних мережах – це не разовий захід, а постійний процес. Бо усвідомленість і відповідальне ставлення до обробки і поширення інформації у соцмережах є ключовим фактором забезпечення безпеки в сучасному цифровому середовищі.

**Список використаних джерел:**


1. Офіційний сайт кіберполіції України. URL: https://cyberpolice.gov.ua/
2. Безпека соцмереж та месенджерів. *BRAMA Кібер* : [сайт]. URL: https://stopfraud.gov.ua/cybersecurity-in-communication/bezpeka-sotsmerezh-mesendzheriv-i783 (дата звернення: 25.03.2026).
3. Рекомендації для медіа з підвищення рівня безпеки. *ІЖ «Кібербез»* : [сайт]. URL: https://cybersec.net.ua/statti/941-rekomendatsii-dlia-media-z-pidvyshchennia-rivnia-kiberbezpeky.html (дата звернення: 25.03.2026).
4. Соцмережі та месенджери: у кіберполіції дали поради військовим. *UKRINFORM* : [сайт]. URL: https://www.ukrinform.ua/rubric-ato/3888578-socmerezi-ta-mesendzeri-u-kiberpolicii-dali-poradi-vijskovim.html (дата звернення: 25.03.2026).



***Гілевич Камелія Валеріївна***
студентка 202_СПС н.гр. ННІ права та психології НАВС

*Науковий керівник:*
***Пакриш Олександр Євгенійович***
кандидат технічних наук, доцент,
доцент кафедри інформаційних технологій ННІ права та психології НАВС


## ДИФАМАЦІЯ (DEFAMATION) – ОСНОВНІ ОЗНАКИ ТА ПРОТИДІЯ

У сучасному світі інформаційних технологій, де обмін даними відбувається миттєво, питання захисту репутації особистості набуває особливої значущості. Однією з ключових загроз у цій сфері виступає ***дифамація*** – поширення неправдивих або перекручених відомостей, що здатні завдати шкоди честі, гідності або діловій репутації людини чи організації [1].

Актуальність дослідження зумовлена тим, що розвиток цифрових платформ і соціальних мереж значно полегшив доступ до публічного висловлення думок, однак одночасно створив передумови для масового поширення неправдивої інформації. В умовах інформаційного перевантаження користувачі не завжди здатні критично оцінювати отримані повідомлення, що сприяє поширенню дифамаційних матеріалів.

У науковому дискурсі дифамація розглядається як комплексне явище, що поєднує правові, соціальні та психологічні аспекти. Вона знаходиться на перетині свободи слова та обов'язку не завдавати шкоди іншим, що робить її складною для регулювання. Особливу увагу дослідники приділяють проблемі балансу між правом на висловлення думки та відповідальністю за неправдиву інформацію.

Під дифамацією розуміють поширення відомостей, які не відповідають дійсності та негативно впливають на репутацію особи.

У правовій практиці традиційно виділяють дві форми цього явища: письмову (наклеп), яка фіксується у матеріальному вигляді, та усну (образливі висловлювання), що передається вербально.

Аналізуючи сутність дифамації, можна виділити низку ключових ознак, без яких вона не може бути встановлена.

- Передусім, йдеться про факт доведення інформації до інших осіб. Якщо відомості залишаються приватними, вони не утворюють складу правопорушення.
- Другою важливою ознакою є недостовірність – інформація має бути неправдивою або такою, що суттєво спотворює реальність.
- Не менш важливим є негативний характер поширених відомостей. Вони повинні принижувати честь, гідність або підривати ділову репутацію.
- Крім того, обов'язковою умовою є можливість ідентифікації особи, про яку йдеться. Якщо неможливо встановити, кого саме стосується інформація, склад дифамації відсутній.
- Завершальною ознакою є наявність шкоди – моральної, психологічної або матеріальної.

Слід також розмежовувати дифамацію та оціночні судження. Останні є суб'єктивним вираженням думки і не можуть бути перевірені на істинність. Саме тому вони, як правило, не підпадають під юридичну відповідальність, якщо не містять відвертих образ або мови ненависті.

Особливого поширення дифамація набула в умовах цифрового середовища. Соціальні мережі, Інтернет-форуми та новинні ресурси дозволяють миттєво поширювати інформацію серед великої аудиторії. Це значно ускладнює процес контролю та спростування неправдивих відомостей.

Онлайн-дифамація характеризується низкою специфічних особливостей.

*По-перше*, це можливість анонімного поширення інформації, що знижує рівень відповідальності користувачів.

*По-друге*, швидкість розповсюдження значно перевищує традиційні канали комунікації.

*По-третє*, навіть після видалення інформації її копії можуть залишатися в мережі тривалий час.

З психологічної точки зору дифамація має серйозні наслідки для особистості. Жертви можуть переживати стрес, тривогу, втрату впевненості в собі та соціальну ізоляцію. У деяких випадках це призводить до депресивних станів і порушення міжособистісних зв'язків. Репутаційні втрати також можуть мати довготривалі наслідки для професійної діяльності.

Водночас важливо враховувати і психологію поширювачів дифамації. Часто такими мотивами виступають заздрість, бажання самоствердження, агресія або прагнення маніпулювати громадською думкою [2, 3].

У цифровому середовищі ці мотиви підсилюються ефектом безкарності та відсутністю безпосереднього контакту з жертвою.

Правове регулювання дифамації передбачає можливість захисту порушених прав через суд [4]. Особа має право вимагати спростування неправдивої інформації, відшкодування моральної шкоди та захисту своєї репутації. Водночас ефективність такого захисту часто ускладнюється складністю доведення факту поширення та встановлення особи порушника.

Протидія дифамації потребує комплексного підходу [5]. Насамперед, важливу роль відіграє підвищення рівня медіаграмотності населення. Люди повинні вміти аналізувати інформацію, перевіряти джерела та критично оцінювати отримані повідомлення.

Не менш важливою є правова обізнаність громадян щодо своїх прав і можливостей їх захисту. Усвідомлення відповідальності за поширення неправдивих відомостей може зменшити кількість таких правопорушень.

На рівні особистості доцільно дотримуватися інформаційної гігієни: не поширювати неперевірені дані, уникати емоційних реакцій на провокаційні повідомлення та використовувати лише надійні джерела інформації.

На рівні держави важливими є вдосконалення законодавства, ефективна робота судової системи та співпраця з цифровими платформами щодо видалення неправдивого контенту.

***Таким чином***, дифамація є складним багатовимірним явищем, що поєднує правові та психологічні аспекти. Вона становить серйозну загрозу для репутації особистості та стабільності суспільних відносин. Ефективна протидія цьому явищу можлива лише за умови поєднання правових механізмів, розвитку критичного мислення та відповідального ставлення до інформації.

**Список використаних джерел:**

1. Скорописова Н. І. Визначення поняття «дифамація» в країнах континентальної Європи. *Правова держава*. 2021. № 43. С. 104–111. DOI: https://doi.org/10.18524/2411-2054.2021.43.240987.
2. Каблак П. І. Дифамація як спосіб незаконного впливу на суддів та права людини: пошук рівноваги. *Актуальні проблеми держави і права* : зб. наук. праць. Одеса : Юридична література, 2014. С. 326–332.
3. Кузьмін Р. Р. Дифамація як засіб протидії кримінальному провадженню в Україні та інших країнах: порівняльний аналіз. *Наукові праці Національної академії внутрішніх справ*. 2013. URL: https://elar.navs.edu.ua/jspui/handle/123456789/4682 (дата звернення: 26.03.2026).
4. Вовк В. М. Цивільно-правова відповідальність за дифамацію у соціальних мережах. *Науковий вісник Ужгородського національного університету*. Серія: Право. 2025. № 90(2). DOI: https://doi.org/10.24144/2307-3322.2025.90.2.4.
5. Пономаренко О. М. Дифамація: як правильно обрати ефективний спосіб захисту? (на підставі аналізу практики ЄСПЛ та Верховного Суду). Харків, 2023. URL: https://dspace.hnpu.edu.ua/handle/123456789/13668 (дата звернення: 26.03.2026).

**Ковальчук Світлана Миколаївна**
Студентка 102_СПРБ н.гр. ННІ права та психології НАВС

*Науковий керівник:*
***Тарасенко Володимир Петрович***
кандидат фізико-математичних наук, доцент кафедри інформаційних технологій ННІ права та психології НАВС

## КІБЕРБЕЗПЕКА ДЕРЖАВИ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

У кожній сфері нашого життя відбулося швидке поширення і модернізація цифрових технологій, які стали невід’ємною частиною сучасного буття. Вони сприяли появі нових загроз для державної безпеки в інформаційному просторі, які на даний момент мають надзвичайно великий вплив в умовах війни. Найнебезпечнішою загрозою є кібератака, яка може повністю зупинити функціонування державних інституцій та здійснити вплив на інформаційний простір України, який відіграє важливу роль у формуванні обізнаності громадян щодо подій, які відбуваються на полі бою.

***Кібербезпека*** – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [1]. Це є одним із факторів гібридної війни, яка включає також традиційні, економічні і політичні форми впливу.

Кібератака є однією з основних загроз нашого часу і вона вважається інформаційною війною, яка супроводжується впливом на органи влади та поширенням дезінформації.

Фахівці Ситуаційного центру забезпечення кібербезпеки СБУ у червні 2022 року попередили та нейтралізували у національному кіберпросторі 147 критичних кіберінцидентів та кібератак. Це відбулося шляхом безпосереднього аналізу понад 50 000 критичних подій інформаційної безпеки, виявлених у поточному місяці.

Основними типами виявлених кіберзагроз (хакерських атак) були:

- з'єднання з командно-контрольними серверами (C&C Server);
- спроби втручання, несанкціонованої авторизації (Intrusion / Login Attempts);
- спроби експлуатації вразливостей (Vulnerability Exploitation);
- ураження шкідливим програмним забезпеченням (Malware Infection);
- атаки на веб-додатки (Web App Attack);
- збір інформації, сканування (Information Gathering / Scanning) та інші [2].

У даній статті показується, що дезінформація є стратегічним інструментом впливу на суспільство. Автори наголошують, що поширення спотвореної або неправдивої інформації дозволяє противнику контролювати сприйняття громадян та формувати потрібні настрої, що може сприяти дестабілізації внутрішньої політичної ситуації. Особливо підкреслюють роль медіа та соціальних мереж, які слугують каналами для швидкого розповсюдження дезінформації. Завдяки високій швидкості поширення контенту навіть незначні фейки можуть набирати масовий резонанс. Це є доказом того, що підвищення медіаграмотності населення та швидке реагування на такі кампанії є критично важливими ддя захисту держави в сучасному просторі [3].

Для забезпечення кращого захисту існує кіберполіція, яка є спеціалізованим підрозділом у структурі Національної поліції України, що здійснює безпосереднє реагування на кіберзлочини та протидію загрозам у кіберпросторі. Цей Департамент відповідає за реалізацію державної політики щодо запобігання та розкриття злочинів, пов'язаних з використанням інформаційних технологій і телекомунікацій, зокрема кібератак, шахрайств, фішингу та інших правопорушень.

Їхня діяльність також включає міжнародну співпрацю з правоохоронними органами інших країн, спільних операціях проти кіберзлочинних угруповань [4].

***Таким чином***, ефективний захист держави в кіберпросторі вимагає комплексного підходу, бо лише поєднання технологічних, правових та освітніх заходів дозволяє мінімізувати ризики маніпуляцій та забезпечити інформаційну безпеку держави.

**Список використаних джерел:**

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05 жовт. 2017 р. № 2163-VIII. *Відомості Верховної Ради України*. 2017. № 45. Ст. 403.

2. У серпні поточного року СБУ заблокувала 43 кібератаки на українські органи влади. *СБУ* : [сайт]. URL: https://ssu.gov.ua/novyny/u-serpni-potochnoho-roku-sbu-zablokuvala-43-kiberataky-na-ukrainski-orhany-vlady.

3. Disinformation as a Weapon: Media Tactics and Psychological Warfare in the Ukrainian Conflict. URL: https://sjps.fsvucm.sk/index.php/sjps/article/view/584.

4. *Кіберполіція* : [сайт]. URL: https://cyberpolice.gov.ua/.

***Голікова Мілена Олексіївна***
студентка 107_СПД н.гр. ННІ права та психології НАВС

*Науковий керівник:*
***Швець Микола Миколайович***
викладач кафедри інформаційних технологій ННІ права та психології НАВС

## КІБЕРШПИГУНСТВО, КІБЕРШАХРАЙСТВО ТА КІБЕРАТАКИ

Сучасний світ більше не уявляється без диджиталізації, кожен з нас поступово, але невпинно входить до цифрового середовища. Однак не варто забувати, що цифровий світ несе не тільки можливості, але й нові загрози. Кібершпигунство, кібершахрайство та кібератаки – це різні грані сучасних інформаційних війн та злочинності. Розуміння їхньої природи є першим кроком до надійного захисту власних даних та національної безпеки.

Всі ці три поняття є різновидами кіберзлочинів та направлені на різні об’єкти нашого життя. Нагадаємо, що відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» (далі – Закон), ***кіберзлочином*** (або комп’ютерним злочином) називають 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].

Дане поняття дозволяє нам зрозуміти, що приставка «кібер-» вказує на те, що певне суспільно небезпечне діяння скоєно з використанням комп'ютерів, комунікаційних систем, електронних комунікацій, мережі Інтернет тощо. Розглянемо кожен із цих різновидів окремо і почнемо із кібершпигунства.

Відповідно до зазначеного вище Закону, під терміном «***кібершпигунство***» розуміють шпигунство, що здійснюється у кіберпросторі або з його використанням. Якщо казати більш простими словами, це незаконне отримання конфіденційної інформації або розвідувальних даних за допомогою комп'ютерних технологій [2].

Основними «жертвами» таких злочинів можуть стати великі корпорації, сегрегатори даних, фінансові, медичні та урядові установи, тобто ті організації, які володіють великими масивами конфіденційної інформації або ж інформації з обмеженим доступом. Злочинці, що вчиняють кібершпигунство, можуть мати різноманітну мотивацію, включаючи економічні вигоди, політичні цілі або здійснення шантажу.

Захист від кібершпигунства повинен бути реалізований на всіх рівнях. Починаючи від спеціалізованих тренінгів для співробітників і персоналу (наприклад, навчання з кібербезпеки і заходи з розпізнавання підозрілих активностей), закінчуючи підвищенням рівня захищеності серверів, на яких зберігають дані та співпрацею з професіоналами у сфері кібербезпеки.

Наступним видом кіберзлочинів є ***кібершахрайство***. Фактична кінцева ціль кібершахраїв майже така сама, як і у кібершпигунів – отримання персональних даних. Єдина різниця у тому, що кібершпигуни діють непомітно, а кібершахраї – відкрито, а часто навіть нахабно [3].

Злодії, які займаються викраденням даних, зазвичай, отримують особисту інформацію, таку як паролі, номери ID, кредитних карток або номери соціального страхування, та використовують ці дані від імені жертви. Викрадена конфіденційна інформація може бути використана для різних незаконних цілей, зокрема для отримання кредитів, здійснення онлайн-покупок або для отримання доступу до медичних та фінансових відомостей жертви.

Розрізняють наступні найпопулярніші методи кібершахрайства: фішинг, вішинг (телефонне шахрайство), смішинг (або смс-фішинг), байтінг, а також «кетфішинг».

*Фішинг* – це один з різновидів шахрайства в Інтернеті з метою отримання незаконного доступу до конфіденційних даних користувачів. Для фішингу часто застосовуються підробні веб-сторінки, а також шкідливе програмне забезпечення.

*Вішинг* – вид шахрайства, при якому зловмисники за допомогою телефонного зв'язку змушують людину повідомити їм свої конфіденційні банківські або персональні дані або стимулюють до здійснення певних дій зі своїм банківським рахунком або банківською картою. Найчастіше шахраї маскуються під служби підтримки банку або ж телефонного оператора.

*Смішинг (або смс-фішинг)* – злочинна схема спрямована на перехід користувачем за шкідливим посиланням з SMS-повідомлення. Це може бути посилання від ніби-то банку, або ж повідомлення із зламаного акаунта із проханням «проголосувати за дитину у конкурсі».

*Байтінг* – це техніка соціальної інженерії (метод маніпуляції діями людини), яку використовують зловмисники, при якій жертві підкидають що-небудь, щоб вона почала діяти.

Основними методами захисту від кібершахраїв є і залишається обізнаність та обережність. Варто завжди перевіряти підозрілі посилання, використовувати надійні рішення безпеки для своїх акаунтів та остерігатись підозрілих та занадто привабливих пропозицій.

Під терміном «***кібератака***» відповідно до Закону розуміють 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) в 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. Якщо говорити простіше, то кібератака – це спроба несанкціонованого доступу, пошкодження чи знищення комп’ютерних систем, мереж, програм або інформації [4].

Ці атаки можуть бути спрямовані на отримання конфіденційної інформації, завдання шкоди або порушення нормального функціонування цифрових систем. Кібератаки можуть здійснюватися з використанням вірусів, фішингу, DDoS-атак та інших методів, які використовуються для незаконного доступу чи завдання шкоди в цифровому середовищі.

На сьогоднішній день, в рамках існування гібридної війни із рф, кібератаки становлять найбільшу загрозу для національної безпеки нашої країни. Кібератаки відбуваються мало не кожного дня. Деякі із них агресивні DDoS-атаки, деякі непомітні із використанням вірусів або фішингу. Кіберпідрозділи Національної поліції та Служби безпеки України старанно стоять на сторожі, готові відбивати атаки ворога кожного дня.

***Отже***, в роботі розкрито поняття трьох різновидів кіберзлочинів, а саме: кібершпигунство, кібершахрайство та кібератаки. Наведено основні методи захисту від них.

**Список використаних джерел:**

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. *Законодавство України : офіц. вебпортал ВРУ*. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 19.02.2026).
2. Кібершпигунство. *StopFraud* : [сайт]. URL: https://stopfraud.gov.ua/cybersecurity-in-work/kibershpygunstvo-i315 (дата звернення: 19.02.2026).
3. Кібершахрайство: фішинг, вішинг, смішинг, бейтінг. *Kopirait* : [сайт]. URL: https://kopirait.com.ua/kibershahrajstvo-fishyng-vishyng-smishyng-bejting/ (дата звернення: 19.02.2026).
4. Кібератака. *StopFraud* : [сайт]. URL: https://stopfraud.gov.ua/cybersecurity-in-wartime/kiberataka-i270 (дата звернення: 19.02.2026).

***Савчин Євгенія Андріївна***
студентка 117_СПД н.гр. ННІ права та психології НАВС

*Науковий керівник:*
***Тарасенко Володимир Петрович***
кандидат фізико-математичних наук, доцент кафедри інформаційних технологій ННІ права та психології НАВС

## КІБЕРБЕЗПЕКА КРИТИЧНОЇ ІНФРАСТРУКТУРИ: ВИКЛИКИ ІННОВАЦІЙ І ЗАГРОЗ ЦИФРОВИХ ТЕХНОЛОГІЙ

Захист критичної інфраструктури від кіберзагроз є однією з ключових умов забезпечення стабільності та безпеки сучасних держав. Критична інфраструктура включає такі сектори, як енергетика, водопостачання, транспорт, телекомунікації, охорона здоров’я, фінансові послуги та державне управління. Ці системи забезпечують функціонування суспільства і будь-яке порушення їхньої роботи може призвести до значних соціальних та економічних наслідків, таких як перебої в наданні послуг, загроза для життя людей та економічні втрати. Тому кібербезпека відіграє критичну роль у захисті систем від потенційних кіберзагроз.

*Метою* даного дослідження є вивчення основних принципів і підходів до захисту критичної інфраструктури в умовах сучасних кіберзагроз.

*Основні завдання* включають аналіз існуючих ризиків, вивчення методів захисту операційних і інформаційних технологій, що використовуються в управлінні критичними об’єктами, та оцінка можливостей застосування новітніх технологій, таких як ШІ і Інтернет речей, для покращення кіберзахисту.

Дослідження базується на аналізі наукових публікацій, державних документів та звітів з кібербезпеки, а також на вивченні практичних випадків кіберінцидентів, що впливали на критичну інфраструктуру. У роботі використовуються методи порівняльного аналізу, систематизації даних та моделювання можливих сценаріїв кібератак.

## Основні загрози критичної інфраструктури

Критична інфраструктура, яка забезпечує ключові функції держави та суспільства, все більше піддається загрозам у цифровому просторі. Це пов'язано із зростаючою залежністю від інформаційних технологій і підключених до Інтернету систем, які керують різними процесами. Кіберзагрози стають серйозним викликом для захисту енергетичних мереж, транспорту, фінансових систем та телекомунікацій. Найпоширенішими загрозами є цифрові атаки, вразливість промислових систем управління (SCADA), а також кібератаки з боку національних та міжнародних злочинних угрупувань [1].

## Цифрові атаки на енергетичні системи, транспорт, фінанси та комунікації

Одним із найсерйозніших викликів для об'єктів критичної інфраструктури сьогодні залишаються кібератаки на енергетичний сектор. Електричні мережі, газотранспортні системи, нафтопереробні підприємства та інші енергетичні об'єкти часто стають цілями хакерів. Порушення їхньої роботи може спричинити масштабні відключення електроенергії, що, у свою чергу, впливає на функціонування інших важливих сфер – транспорту, зв'язку та фінансів. Яскравим прикладом є кібератака на енергосистему України у 2015 році, яка призвела до знеструмлення сотень тисяч споживачів.

Не менш вразливою є транспортна інфраструктура. Йдеться як про громадський транспорт, так і про міжнародні перевезення. Втручання в системи управління залізничним, авіаційним чи морським транспортом може викликати серйозні логістичні перебої, розриви постачальних ланцюгів і навіть створити небезпеку для людей. Наприклад, кібератака на компанію Maersk у 2017 році спричинила значні порушення у глобальних морських перевезеннях та завдала суттєвих фінансових втрат.

Фінансова сфера, яка є основою світової економіки, також постійно перебуває під загрозою. Хакери можуть атакувати банки, фондові біржі та платіжні системи з метою викрадення коштів, знищення інформації або маніпуляцій на ринку. Одним із найвідоміших інцидентів стала атака на Bangladesh Bank у 2016 році, коли зловмисники намагалися викрасти близько мільярда доларів, з яких їм вдалося отримати 81 мільйон.

Телекомунікаційна інфраструктура, що забезпечує зв'язок між різними галузями, також є вразливою до кіберзагроз. Атаки на ці системи можуть призвести до збоїв у зв'язку, порушення роботи Інтернету або використання мереж для шпигунства. Особливо ризикованими є мобільні та широкосмугові мережі, які мають застарілі протоколи безпеки або недоліки в архітектурі.

### Атаки з боку національних та міжнародних кіберзлочинців

Одним із найбільших джерел загроз для критичної інфраструктури є дії національних та міжнародних кіберзлочинних угруповань. На відміну від одиночних хакерів або хактивістів, організовані угрупування можуть мати значні фінансові та технічні ресурси. Вони часто діють за підтримки держав або як незалежні злочинні організації, що переслідують фінансову, політичну або навіть військову мету. Державні актори можуть використовувати кібератаки як інструмент геополітичного тиску або шпигунства. Такі атаки можуть бути спрямовані на порушення роботи інфраструктури, знищення інформації або навіть викликати паніку та хаос у суспільстві. Міжнародні кіберзлочинці також мають свої інтереси в атаках на критичну інфраструктуру. Це можуть бути атаки з метою вимагання грошей, саботаж або викрадення важливих даних. Злочинні угруповання часто використовують такі методи, як фішинг, соціальна інженерія та ін'єкції шкідливого ПЗ для проникнення в системи. Таким чином, основні загрози для критичної інфраструктури включають цифрові атаки на ключові сектори економіки, вразливість SCADA-систем, а також дії організованих кіберзлочинних угрупувань. В умовах зростаючих кіберризиків уряди та організації повинні постійно вдосконалювати свої системи захисту, аби запобігти катастрофічним наслідкам [2].

### Розширення кіберстратегій на міжнародному ринку

В сучасному глобалізованому світі загроза кібератак на критичну інфраструктуру не обмежується кордонами однієї країни. Кіберзлочинці та державні актори можуть організовувати атаки на інфраструктуру в будь-якій точці світу, тому країни повинні активно співпрацювати для забезпечення кібербезпеки. Одним із ключових трендів останніх років є розширення міжнародної співпраці у сфері кіберзахисту. Організації, такі як НАТО, Європейський Союз та ООН, активно працюють над створенням спільних стратегій боротьби з кіберзагрозами. Наприклад, НАТО визнала кіберпростір п'ятою сферою військових дій, що означає, що альянс готовий реагувати на кібератаки так само, як і на фізичні загрози. Держави-члени НАТО співпрацюють у сфері кіберзахисту, обмінюються інформацією про загрози та проводять спільні навчання з кібербезпеки. Крім того, створюються міжнародні альянси для боротьби з кіберзлочинністю.

Один із таких прикладів – Європейське агентство з кібербезпеки (ENISA), яке координує зусилля держав-членів ЄС у захисті критичної інфраструктури від кіберзагроз. Також розвиваються стандарти та норми, які регулюють поведінку держав у кіберпросторі, зокрема в рамках Будапештської конвенції з кіберзлочинності. У зв'язку з поширенням нових видів загроз, таких як кібершпигунство, атаки на ланцюжки постачання та дезінформація, міжнародна співпраця стає критично важливою. Впровадження узгоджених кіберстратегій дозволяє забезпечити краще реагування на загрози, а також покращити обмін технологіями та досвідом між державами [3].

## Практичні заходи щодо підвищення рівня кібербезпеки

В умовах постійного зростання кіберзагроз організації мають вживати комплексних заходів для захисту критичної інфраструктури. До ключових підходів належать етичний хакінг (тестування на проникнення), який дозволяє своєчасно виявляти та усувати вразливості, а також впровадження систем моніторингу й реагування, що допомагають швидко виявляти атаки та мінімізувати їх наслідки. Не менш важливим є навчання персоналу, адже людський фактор часто стає причиною інцидентів. Регулярні тренінги та формування культури кібербезпеки сприяють підвищенню обізнаності працівників і зменшенню ризику успішних атак [4].

## Висновок та перспективи

У сучасному світі кіберзагрози мають глобальний характер, тому ефективна протидія їм потребує міжнародної співпраці. Атаки можуть здійснюватися з будь-якої країни, тому взаємодія між державами, міжнародними організаціями та бізнесом є необхідною для обміну інформацією, проведення спільних навчань і координації дій під час інцидентів. Таке партнерство сприяє зниженню вразливості критичної інфраструктури та підвищенню рівня її захисту.

Майбутнє кіберзахисту пов’язане з розвитком новітніх технологій, таких як штучний інтелект, блокчейн і хмарні сервіси. Вони допомагають посилити безпеку, але водночас створюють нові ризики. Тому організаціям важливо не лише реагувати на загрози, а й діяти на випередження, впроваджуючи інноваційні рішення та постійно вдосконалюючи системи захисту.

## Список використаних джерел:


1. Білявська Ю, Шестак Я. Кібербезпека та кібергігієна: нова ера цифрових технологій. *Commodity science. Technologies. Engineering*. 2022. Т. 43. № 3. С. 47–59. URL: https://doi.org/10.31617/2.2022(43)04.
2. Гончар С. Ф. Особливості забезпечення кібербезпеки об’єктів критичної інфраструктури. *Моделювання та інформаційні технології*. 2017. Вип. 80. С. 27–32. URL: http://nbuv.gov.ua/UJRN/Mtit_2017_80_6.
3. Дрейс Ю. О. Аналіз базової термінології та негативних наслідків кібератак на інформаційно-телекомунікаційні системи об'єктів критичної інфраструктури держави. *Український журнал досліджень інформаційної безпеки*. 2017. Т. 19. № 3. С. 214–222. URL: https://doi.org/10.18372/2410-7840.19.11900.
4. Марущак А. І. Інформаційно-правові аспекти протидії кіберзлочинності. *Інформація і право*. 2018. Т. 1. № 24. С. 127–132. URL: https://doi.org/10.37750/2616-6798.2018.1(24).273217
5. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. *Законодавство України : офіц. вебпортал ВРУ*. URL: https://zakon.rada.gov.ua/laws/show/2163-19.

***Борко Надія Олександрівна***
студентка 107_СПД н.гр. ННІ права та психології НАВС

*Науковий керівник:*
***Швець Микола Миколайович***
викладач кафедри інформаційних технологій ННІ права та психології НАВС

## ЕВОЛЮЦІЯ КІБЕРЗАГРОЗ ЗА ОСТАННІ РОКИ У СВІТІ

Сучасна спільнота значною мірою залежить від цифрових технологій у всіх аспектах життя – в економіці, державному управлінні, медицині, енергетиці та транспорті. Ця залежність робить інформаційні системи вразливими до кіберзагроз, які еволюціонували від локальних технічних інцидентів до глобальних викликів національній та міжнародній безпеці. Кіберзлочинність набуває організованих і спрямованих форм, керованих економічними, політичними та стратегічними мотивами. Сучасні дослідження підкреслюють, що кібербезпека є невід'ємним компонентом національної безпеки. Зокрема, фахівці, такі як Росс Андерсон (Університет Кембриджа) та Пітер Ньюман (Лондонська школа економіки), аналізують методи протидії кібератакам та розвиток технологій захисту інформаційних систем [1, 2].

На початковому етапі формування кіберзагроз, до 2010 року, домінували традиційні шкідливі програми: комп'ютерні віруси, мережеві черв'яки і трояни, що поширювалися через електронну пошту або мережеві підключення й зазвичай мали на меті продемонструвати технічні можливості або забезпечити широке розповсюдження серед користувачів. Яскравим прикладом є вірус ILOVEYOU (2000 р.), який масово розсилав власні копії електронною поштою у формі «листа любові» і вразив мільйони комп'ютерів у світі. Його успіх пояснювався здатністю звести користувачів до відкриття вкладення, оскільки повідомлення виглядало як персональна кореспонденція і багато отримувачів не підозрювали про загрозу. Це підкреслило нагальну потребу в застосуванні антивірусного програмного забезпечення та навчанні користувачів правилам безпечної поведінки в Інтернеті [3].

Іншим випадком є вірус Mydoom (2004 р.), який ширився мережею Інтернет і спричинив уповільнення роботи великих мереж. Цей інцидент додатково продемонстрував ризики, пов'язані з автоматизованим розповсюдженням шкідливих програм, і вказав на необхідність регулярного оновлення програмних систем [4].

У період приблизно з 2010 року по 2015 рік кіберзлочини дедалі частіше мали виражений фінансовий характер. Зловмисники почали систематично використовувати фішинг, викрадення банківських даних, створення ботнетів та DDoS-атаки задля отримання фінансової вигоди або доступу до конфіденційної інформації. Масові фішингові кампанії надсилали підроблені повідомлення від імені банків або великих інтернет-магазинів аби змусити користувачів розкривати паролі та логіни. Унаслідок цього організації були змушені впроваджувати багаторівневі системи автентифікації та проводити навчання персоналу з виявлення підозрілих листів. Індустріальне шпигунство й крадіжки технологій у великих корпораціях підкреслили стратегічну важливість захисту корпоративної інформації й інтелектуальної власності [5, 6].

Починаючи з 2016 року, особливу увагу привернули програми-вимагачі, що шифрують дані на пристроях жертв і вимагають викуп за їх відновлення. Найпомітнішою з таких атак стала кампанія WannaCry, яка розпочалась 12 травня 2017 року й уразила понад 200 000 комп’ютерів щонайменше в 150 країнах, технічно блокуючи доступ до даних та вимагаючи викуп у криптовалюті. Це була одна з наймасштабніших атак в історії, коли один шкідливий код спричинив глобальні збої в системах охорони здоров’я, транспорті, енергетиці та бізнесі через недостатнє встановлення оновлень безпеки операційних систем [5, 7].

Невдовзі, у червні 2017 року, з’явилася атака, відома як Petya/NotPetya, яка формально мала ознаки програм-вимагачів, однак фактично була спрямована на масове знищення даних, а не на отримання викупу. Шкідливий код поширювався через оновлення програмного забезпечення, блокував доступ до систем у численних організаціях, у тому числі в корпоративних структурах та фінансових установах. Протягом кількох днів ця атака паралізувала роботу банків, телекомунікаційних мереж та інших великих систем, завдавши значних економічних збитків і продемонструвавши, як кіберзагрози можуть впливати на економіку та критичну інфраструктуру [6, 8].

У наступні роки кіберзагрози дедалі частіше використовувалися як засіб політичного та економічного тиску. Основними мішенями стали державні реєстри, енергетичні компанії, банки, транспортні та медичні установи. Масові DDoS-атаки блокували доступ до важливих урядових порталів, викликаючи тимчасові перебої в наданні суспільно значущих послуг. Хоча конкретні назви деяких інцидентів не завжди були оприлюднені, загальні тенденції вказують на наявність подібних подій у період 2020–2022 років і посилили необхідність підвищення кіберстійкості критичної інфраструктури [7, 8, 9].

Від 2023 року атаки стали менш помітними, більш тривалими та цілеспрямованими. Часто застосовуються методи компрометації через ланцюги постачання програмного забезпечення або через підрядників і постачальників корпоративних сервісів.

Зловмисники можуть перебувати всередині внутрішніх мереж великих організацій протягом місяців, збираючи дані або порушуючи роботу систем. Такі складні й приховані операції перебувають у фокусі дослідників, які прогнозують їх подальше зростання та потребу в більш досконалих засобах захисту [1, 2, 9].

Кіберзлочинність не має географічних обмежень: сервери, з яких здійснюються атаки, можуть фізично розташовуватися в одній частині світу, тоді як жертви – в іншій, що ускладнює розслідування та притягнення винних до відповідальності. Міжнародні організації координують обмін інформацією та спільні зусилля для протидії кіберзлочинності [10].

Кіберзагрози виявляються у банківських системах, державних установах, енергетиці, промислових мережах та медичних закладах. Вони впливають на рух фінансових потоків, безпеку персональних і корпоративних даних та функціонування критичної інфраструктури. У найближчому майбутньому прогнозується подальше ускладнення та підвищення прихованості цих загроз: ймовірне зростання застосування складних алгоритмів шифрування, методів соціальної інженерії та атак через ланцюги постачання. Дослідники вважають, що ефективною відповіддю стануть інтегровані системи захисту інформації, навчання користувачів основам кібергігієни та міжнародна співпраця з обміну даними про загрози [1, 2, 7, 8, 9].

***Отже***, еволюція кіберзагроз у період 2000–2025 років демонструє поступовий перехід від простих вірусів до фінансово мотивованих атак, від програм-вимагачів до стратегічно спрямованих операцій, а далі – до прихованих і цілеспрямованих втручань. Сучасні кіберзагрози впливають на економіку, безпеку держав і міжнародні відносини. Протидія їм можлива лише за умов комплексного підходу, що поєднує технічні, правові та організаційні заходи, навчання користувачів і міжнародну співпрацю [1–10].

**Список використаних джерел:**

1. Anderson, R. Security Engineering: A Guide to Building Dependable Distributed Systems. 3rd ed. Chichester: Wiley, 2020. 560 p.

2. Newman, P. Cybersecurity and Global Politic**s**. London: LSE Press, 2019. 312 p.

3. Greenberg, A. Inside the ILOVEYOU Virus. *Wired*, 14 May 2000. URL: https://www.wired.com/story/iloveyou-virus/ (дата звернення: 20.02.2026).

4. Symantec Security Response. Mydoom Virus Analysis, 2004. URL: https://www.symantec.com/security-center/writeup/2004-012104-0911-99 (дата звернення: 15.02.2026).

5. Wired. Inside the WannaCry Ransomware Attack, 12 May 2017. URL: https://www.wired.com/story/wannacry-ransomware-attack/ (дата звернення: 20.02.2026).

6. Greenberg, A. Petya/NotPetya Ransomware Explained, 27 June 2017. URL: https://www.wired.com/story/petya-malware-attack-outbreak-june-2017/ (дата звернення: 17.02.2026).

7. The Guardian. WannaCry and Global Cybersecurity Threats, 30 Dec 2017. URL: https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware (дата звернення: 20.02.2026).

8. The Guardian. Petya ransomware attack strikes companies across Europe and US, 27 June 2017. URL: https://www.theguardian.com/world/2017/jun/27/petya-ransomware-attack-strikes-companies-across-europe (дата звернення: 10.02.2026).

9. ENISA. ENISA Threat Landscape 2023. European Union Agency for Cybersecurity, 2023. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 (дата звернення: 20.02.2026).

10. CERT-UA. Звіти про кібератаки на Україну 2016–2022, 2017–2022. URL: https://cert.gov.ua/ua/news (дата звернення: 20.02.2026).

***Баклан Мирослав Анатолійович***
студент 102_СПРБ н.гр. ННІ права та психології НАВС

*Науковий керівник:*
***Тарасенко Володимир Петрович***
кандидат фізико-математичних наук, доцент кафедри інформаційних технологій ННІ права та психології НАВС

## КІБЕРБЕЗПЕКА В ЗАБЕЗПЕЧЕННІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

В сучасних умовах розвитку інформаційних технологій кіберпростір став важливим елементом національної безпеки нашої держави. Сучасні виклики також реалізуються у цифровому середовищі, що вимагає належного рівня кіберзахисту. Важливу роль також відіграє інформаційний вплив, зокрема пропаганда, націлена на дестабілізацію суспільства.

В Законі «Про основні засади забезпечення кібербезпеки України» визначено терміни: ***кібербезпека*** – це захист інтересів людини та громадян під час використання кіберпростору, своєчасне виявлення, запобігання і нейтралізація загроз національній безпеці України у кіберпросторі; ***кіберпростір*** – середовище (віртуальний простір), яке надає можливість комунікації або реалізації суспільних відносин з використанням мережі Інтернет.

Головним кординаційним центром кібербезпеки є Рада національної безпеки і оборони України, що здійснює контроль за діяльністю суб'єктів, які забезпечують кібербезпеку, реагування на кіберінциденти та реалізацію Стратегії кібербезпеки України з урахуванням положень Директиви Європейського Союзу щодо мережевої та інформаційної безпеки.

Кабінет Міністрів України забезпечує захист прав і свобод громадян, національних інтересів України у кіберпросторі та боротьбу з кіберзлочинністю.

Суб'єктами, які безпосередньо здійснюють кіберзахист у межах своєї компетенції є: місцеві адміністрації, органи місцевого самоврядування, правоохоронні органи, військові формування, Національний банк України та оператори критичної інфраструктури [1].

*Критична інфраструктура* – це сукупність інформаційно-телекомунікаційних систем держави, які забезпечують безпеку держави і громадян. До них належать державні електронні ресурси, де зберігається інформація, яка є власністю держави, несанкціоновані дії можуть створювати загрозу національній безпеці [3].

Дослідники Онищенко С. та Глушко А. виявили лише за січень 2022 року 6,8 мільйонів підозрілих кіберподій. Реалії сьогодення прискорили нарощення кібервійськ задля захисту критичної інформації від кібератак. Вже з перших днів війни добровольча ІТ-армія України налічувала 175 тис. учасників від усього світу, зокрема від SpaceX до Anonimus. Парадокс полягає в тому, що жодній країні не вдалось залучити таку добровільну підтримку. Безумовно є кібервійська у Збройних силах України, які на початок повномаштабної війни перебували на етапі формування [2].

У 2023-2024 роках ситуація ускладнилась за даними звіту Оперативного центру реагування на кіберінциденти Державного центру кіберзахисту Держспецзв'язку: кількість кіберінцидентів зросла на 62,5% у порівнянні з 2022 роком. Служба безпеки України щомісяця реєструє понад тисячу кібератак російського походження, спрямованих на державний сектор та суспільство. Основна мета – вплив на суспільно-політичну ситуацію в країні [4].

***Отже***, кібербезпека є важливою складовою національної безпеки України. Умови зростаючих загроз у цифровому просторі зумовлюють розвиток кібербезпеки держави. В умовах повномаштабної війни особливого значення набуває захист критично важливої інформації та протидія інформаційно-психологічним впливам агресора.

**Список використаних джерел:**

1. Про основні засади забезпечення кібербезпеки України: Закон України від 05 жовт. 2017 р. № 2163-VIII. *Відомості Верховної Ради (ВВР)*. 2017. № 45. Ст. 403. URL: https://zakon.rada.gov.ua/laws/show/2163-19#top.

2. Дубов Д. В, Ожеван М. А. Кібербезпека: світові тенденції та виклики для України. С. 25. URL: https://niss.gov.ua/sites/default/files/2011-06/kyber_bezpeka-aab17.pdf.

3. Кіра С. О. Кібербезпека як частина національної безпеки України в умовах війни. С. 2. Львівська політехніка. URL: https://lsej.org.ua/5_2023/55.pdf.

4. Скіцько О. І., Ширшов Р. А. Актуальні питання забезпечення кібербезпеки об'єктів критичної інфраструктури. *Юридичний науковий електронний журнал.* 2024. № 10. С. 312–315. URL: https://lsej.org.ua/10_2024/73.pdf.

***Новицька Ірина Ігорівна***
студентка 108_СПД н.гр. ННІ права та психології НАВС

*Науковий керівник:*
***Грищенко Олег Ігорович***
старший викладач кафедри інформаційних технологій ННІ права та психології НАВС

## КІБЕРТЕРОРИЗМ ТА ЙОГО ВІДМІННІСТЬ ВІД ЗВИЧАЙНИХ КІБЕРЗЛОЧИНІВ

Як відомо, ***тероризм*** – це суспільно небезпечна діяльність, яка полягає у свідомому, цілеспрямованому застосуванні насильства шляхом захоплення заручників, підпалів, убивств, тортур, залякування населення та органів влади або вчинення інших посягань на життя чи здоров'я ні в чому не винних людей або погрози вчинення злочинних дій з метою досягнення злочинних цілей [1]. При цьому під боротьбою з тероризмом розуміється діяльність щодо запобігання, виявлення, припинення, мінімізації наслідків терористичної діяльності. Так, зокрема, метою антитерористичної операції є проведення комплексу скоординованих спеціальних заходів, спрямованих на попередження, запобігання та припинення терористичної діяльності, звільнення заручників, забезпечення безпеки населення, знешкодження терористів, мінімізацію наслідків терористичної діяльності [1].

Розглянемо, що таке ***кібертероризм***. Це форма терористичної діяльності, що здійснюється із використанням інформаційно-комунікаційних технологій, комп'ютерних мереж та цифрових систем з метою залякування населення, впливу на органи державної влади, дестабілізації суспільного порядку або завдання шкоди національній безпеці. Таким чином, кібертероризм – це терористична діяльність, що здійснюється у кіберпросторі або з його використанням [2].

На відміну від традиційного тероризму, де використовуються фізичні засоби насильства (вибухи, захоплення об’єктів, напади), кібертероризм реалізується у віртуальному просторі, але його наслідки можуть мати цілком реальний характер.

У сучасному світі більшість процесів управління державою, економікою, фінансовою системою, транспортом, зв’язком та медициною здійснюється за допомогою інформаційних систем. Саме ця цифровізація створює нові можливості для злочинців і терористичних організацій. Якщо раніше для виведення з ладу електростанції потрібно було фізично проникнути на об’єкт, то сьогодні теоретично достатньо отримати несанкціонований доступ до автоматизованої системи управління.

*Об’єктами кібертероризму* можуть бути:

– державні інформаційні ресурси та електронні реєстри;

– банківські та фінансові системи;

– енергетичні компанії та системи електропостачання;

– транспортні мережі (залізниця, авіація, метро);

– системи водопостачання та газопостачання;

– медичні інформаційні системи;

– засоби масової інформації та комунікаційні платформи.

Ключовою характеристикою кібертероризму є його цілеспрямованість. Він не є випадковим зламом або спонтанною атакою. Це заздалегідь спланована операція, яка має конкретну політичну або ідеологічну мету. Терористичні угруповання можуть використовувати кібератаки для тиску на уряд, вимагання певних рішень, дестабілізації політичної ситуації або демонстрації власної сили.

До основних методів кібертероризму належать: 1) DDoS-атаки – масове надсилання запитів на сервер з метою його перевантаження та блокування доступу до сайту чи сервісу; 2) впровадження шкідливого програмного забезпечення – вірусів, троянів, шпигунських програм або програм-вимагачів, які шифрують дані та блокують роботу систем; 3) злам і модифікація офіційних вебсайтів – розміщення неправдивої інформації або пропагандистських матеріалів; 4) крадіжка конфіденційних даних громадян, службових документів, державних таємниць; 5) втручання в роботу промислових систем управління, що може призвести до аварій, зупинки виробництва або техногенних катастроф.

Особливість кібертероризму полягає в тому, що він може здійснюватися дистанційно, без фізичної присутності злочинця. Це ускладнює процес розслідування та притягнення до відповідальності, адже атака може здійснюватися з території іншої держави або через мережу анонімних серверів.

Кібертероризм суттєво відрізняється від звичайних кіберзлочинів.

*По-перше*, різниться мотивація. Звичайні кіберзлочини здебільшого мають економічний характер: шахрайство з банківськими картками, фішинг, продаж викрадених даних, злам акаунтів.

Їхня мета – отримання фінансової вигоди або особистої користі. Кібертероризм же спрямований на досягнення політичних або ідеологічних результатів.

*По-друге*, відрізняється масштаб наслідків. Кіберзлочин може завдати шкоди окремій людині або компанії. Кібертерористична атака здатна вплинути на життя тисяч або навіть мільйонів людей, паралізувати діяльність державних органів чи цілих секторів економіки.

*По-третє*, різний рівень суспільної небезпеки. Кібертероризм розглядається як загроза національній безпеці. Його наслідками можуть бути масові відключення електроенергії, транспортний колапс, паніка серед населення, порушення роботи лікарень. Звичайні кіберзлочини, хоча й небезпечні, зазвичай не мають настільки масштабного впливу.

*По-четверте*, відмінність у суб'єктах. Кіберзлочинцями часто є окремі хакери або злочинні угруповання, що діють задля прибутку. Кібертероризм може бути пов'язаний із діяльністю організованих терористичних організацій, екстремістських рухів або навіть використовуватися як інструмент гібридної війни між державами.

Ще однією важливою особливістю є психологічний ефект. Кібертерористична атака може супроводжуватися поширенням дезінформації, фейкових повідомлень про небезпеку, що викликає паніку та недовіру до державних інституцій. Таким чином, навіть без фізичних руйнувань досягається головна мета тероризму – страх і хаос. У зв'язку з поширенням кібертероризму держави створюють спеціальні служби кібербезпеки, розробляють стратегії захисту інформаційної інфраструктури, співпрацюють на міжнародному рівні. Велику роль відіграє також підвищення цифрової грамотності населення, адже людський фактор часто стає причиною успішних атак.

***Отже***, кібертероризм – це складне і багатогранне явище сучасності, яке поєднує інформаційні технології та терористичну діяльність. Його відмінність від звичайних кіберзлочинів полягає в політичній або ідеологічній меті, масштабності наслідків, високому рівні суспільної небезпеки та стратегічному характері впливу. У цифрову епоху він становить одну з найсерйозніших загроз для держав, суспільства та міжнародної безпеки.

**Список використаних джерел:**

1. Про боротьбу з тероризмом : Закон України від 20 берез. 2003 р. № 638-IV. *Відомості Верховної Ради України.* 2003. № 25. Ст. 180. URL: https://zakon.rada.gov.ua/laws/show/638-15.

2. Про основні засади забезпечення кібербезпеки України : Закон України від 05 жовт. 2017 р. № 2163-VIII. *Відомості Верховної Ради (ВВР)*. 2017. № 45. Ст. 403. URL: https://zakon.rada.gov.ua/laws/show/2163-19.

***Руснак Міла Олегівна***
студентка 102_СПРБ н.гр. ННІ права та психології НАВС

*Науковий керівник:*
***Тарасенко Володимир Петрович***
кандидат фізико-математичних наук, доцент кафедри інформаційних технологій ННІ права та психології НАВС

# ПРОБЛЕМИ ПРАВОВОГО ТА ДІЙОВОГО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ У СВІТІ ТА В УКРАЇНІ

Упродовж останніх десяти років питання регулювання кібернетичного простору перестає бути виключно «внутрішньою справою» окремих держав. Можливість використання кіберпростору організованими злочинними угрупованнями, зловмисниками-одинаками, формалізованими та неформалізованими деструктивними політичними групами, військовими і спеціальними службами держав з метою вчинення злочинів, здійснення хакерських атак за політичними мотивами, деструктивного впливу на військову й цивільну інфраструктуру (у т.ч. – критичну), збору чутливої інформації, а також прямого шпигунства в інтересах держав чи потужних корпорацій робить неможливим ігнорування цієї проблеми світовою спільнотою.

Про рівень занепокоєності провідних геополітичних гравців цим питанням свідчать численні дискусії (у т.ч. – на найвищому рівні), що пропонують визнати кібернапади «актом війни», кіберзброю прирівняти до зброї масового знищення. Проблема додатково ускладнюється двома потужними чинниками: відсутністю у ключових гравців єдиного підходу до розуміння кіберпростору і кібербезпеки загалом, а також посиленням глобальних дискусій щодо забезпечення авторських і суміжних прав у мережі Інтернет.

До останнього часу проблему кібербезпеки на міжнародному рівні було вирішено лише частково – у сфері протидії кіберзлочинності. Йдеться про прийняту Радою Європи у 2001 р. Конвенцію про кіберзлочинність, що відносить до сфери кіберзлочинів такі види правопорушень:

- правопорушення проти конфіденційності, цілісності й доступності комп’ютерних даних і систем (незаконний доступ, нелегальне перехоплення, втручання у дані чи систему, зловживання пристроями);
- правопорушення, пов’язані з комп’ютерами (підробка, шахрайство);
- правопорушення, пов’язані зі змістом (з дитячою порнографією);
- правопорушення, пов’язані з порушенням авторських та суміжних прав.

Водночас далеко не всі країни (з числа членів Ради Європи) ратифікували цей документ. Крім того, Конвенція є регіональним документом, хоча до неї приєднуються й інші країни світу. Понад те, документ не вирішує зазначених вище питань військового використання кіберпростору, формування глобальних підходів до кібербезпеки тощо. Це змушує керівництво держав формувати власну політику кібербезпеки на національному рівні в умовах глобальної невизначеності та відсутності єдиних підходів.

Більшість держав світу вже створили відповідні підрозділи (як правоохоронні, так і військові), діяльність яких спрямована на протидію кіберзагрозам і розроблення наступальних технологій. З метою вирішення цієї проблеми низка держав (США, КНР, рф) виступають із власними ініціативами щодо врегулювання питань кібербезпеки (інформаційної безпеки) на глобальному рівні, проте спостерігаються суттєві відмінності в запропонованих підходах, які не лише слабо узгоджуються між собою, а й іноді суперечать один одному. Крім того, з огляду на те, що США зберігають статус єдиної наддержави, окремі ініціативи їх національного законодавства можуть впливати на міжнародну ситуацію у цій сфері або задавати основні тенденції реформування законодавства в інших країнах. В аналітичній доповіді висвітлюються ключові міжнародні правові й політичні ініціативи (а також національні ініціативи і законопроєкти, що можуть істотно вплинути на міжнародне правове поле) у сфері кібербезпеки, визначаються можливі проблемні напрями їх реалізації та потенційна позиція України щодо них [1].

**Правове забезпечення кібербезпеки в Україні**

«Законодавче визначення кібервійни потрібне, щоб захистити українських фахівців, які виконують наступальні операції проти російських загарбників у кіберпросторі». Таку думку висловив Українському радіо інженер із кібербезпеки компанії OptiData Владислав Радецький, коментуючи ініціативу Міноборони щодо законодавчого визначення поняття «кібервійна» [2].

Якщо є кібервійна, то необхідно мати кіберзбройні сили та кіберкомандування, щоб це поняття не залишалося формальним. У нас уже є підрозділи кібероперацій у силових структурах, а також спільноти «Кіберспротив», «Кіберальянс». Тобто визначення кібервійни необхідне для захисту осіб, які виконують такі операції.

«Якщо порівняти з військовими на полі бою, то там усе зрозуміло: український захисник, який веде вогонь по противнику, діє в межах закону. Натомість особи, які здійснюють кібероперації, наразі перебувають у правовій невизначеності. Тому таке визначення необхідне також для посилення відповідальності російських угруповань та, ймовірно, вплине на посилення санкцій у сфері програмного забезпечення та послуг, які ще можуть надаватися на території рф», – зазначив Радецький [2].

Міністерство оборони України затвердило рішення щодо основних засад інформаційної безпеки та кібербезпеки в інформаційно-комунікаційних системах. Про це повідомляє пресслужба Міноборони. Відтепер усі системи, сервіси, застосунки та цифрові інструменти Міністерства оборони матимуть єдині, чітко визначені правила кібербезпеки, які враховуватимуть найкращі підходи НАТО та міжнародні стандарти.

«Під час постійних кібератак ворога ми маємо приділяти особливу увагу кібербезпеці. Заходи у цій сфері повинні бути системними та постійно вдосконалюватися. Саме тому нова політика передбачає регулярний перегляд і оновлення вимог Міністерства щодо кібербезпеки», – підкреслила Катерина Черногоренко, заступниця Міністра оборони з питань цифровізації, цифрових трансформацій та цифрового розвитку [3].

***Отже***, кіберпростір сьогодні виступає важливою сферою правоохоронної діяльності, що характеризується новими викликами та загрозами глобального масштабу. Відсутність єдиного міжнародного підходу до регулювання кібербезпеки, активне використання кіберпростору у військових і політичних цілях, а також зростання кіберзлочинності зумовлюють необхідність посилення як міжнародної, так і національної правової бази.

Для України особливо актуальним є формування чіткої державної політики у сфері кібербезпеки, зокрема законодавче визначення понять, створення відповідних структур та забезпечення правового захисту фахівців. Комплексний підхід до розвитку кібербезпеки сприятиме підвищенню ефективності протидії кіберзагрозам та зміцненню національної безпеки держави.

**Список використаних джерел:**

1. Дубов Д. В., Ожеван М. А. Майбутнє кіберпростору та національні інтереси України: нові міжнародні ініціативи провідних геополітичних гравців : аналіт. доп. Київ : НІСД, 2012. 32с. URL: https://niss.gov.ua/sites/default/files/2013-02/Kyberprostyr-17541.pdf.

2. Радецький В. Законодавче визначення кібервійни допоможе українському кібернаступу – експерт. *УКРІНФОРМ* : [сайт]. URL: https://www.ukrinform.ua/rubric-technology/3847725-zakonodavce-viznacennakibervijni-dopomoze-ukrainskomu-kibernastupu-ekspert.html.

3. Довгань О., Литвинова Л., Дорогих С. Кібербезпека в інформаційному суспільстві: інформаційно-аналітичний дайджест. Національна бібліотека України ім. В. І. Вернадського. Київ, 2024. № . 320 с. URL: https://ippi.org.ua/sites/default/files/2024-4.pdf.

***Кобилинська Кристіна Василівна***
студентка 101_СПРБ н.гр. ННІ права та психології НАВС

*Науковий керівник**:***
***Корнейко Олександр Васильович***
кандидат технічних наук, професор, професор кафедри інформаційних технологій ННІ права та психології НАВС

## КІБЕРБЕЗПЕКА В ДІЯЛЬНОСТІ ПРАВНИКА: СУЧАСНІ ЗАГРОЗИ ТА МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ

Рівень розвитку інформаційно-комунікаційних технологій істотно трансформує юридичну практику. Використання комп'ютерної техніки та мобільних пристроїв (ноутбуків, планшетів, смартфонів) стало невід'ємною складовою професійної діяльності правника. Водночас цифровізація породжує нові ризики для забезпечення цілісності, конфіденційності та доступності інформації, зокрема персональних даних та службової (корпоративної) таємниці, оскільки юристи систематично здійснюють збір, обробку, зберігання та поширення даних, тобто виникає потреба у комплексному їх захисті за допомогою організаційно-технічних та правових механізмів. Без належного рівня інформаційної безпеки ефективна юридична діяльність є неможливою.

У сучасних умовах правники стають об'єктами атак не лише у фізичному середовищі, але й у кіберпросторі. Зловмисники та недобросовісні конкуренти активно застосовують цифрові інструменти, включно з методами соціальної інженерії, для отримання несанкціонованого доступу до професійної інформації. Попри це, значна частина юридичної спільноти досі недооцінює актуальність проблеми кібербезпеки, вважаючи її віддаленою від власної практики. Така позиція створює передумови для серйозних порушень: приклади використання елементарних паролів або відсутність базових налаштувань безпеки підтверджуються емпіричними дослідженнями у сфері інформаційної безпеки [1].

Електронні кабінети, онлайн-реєстри, електронна пошта та месенджери (Gmail, Telegram тощо) забезпечують зручність комунікації, проте водночас виступають потенційними точками входу для атак. Часто для компрометації даних достатньо одного фішингового повідомлення, яке спонукає користувача самостійно передати конфіденційну інформацію [2]. Дослідження Modic та Anderson засвідчили, що рівень освіти не є визначальним чинником уразливості до шахрайських схем; набагато вагомішими є психологічні фактори – втома, поспіх чи перебування під тиском [2].

Особливого значення набуває правовий аспект захисту даних. Відповідно до статті 22 Закону України «Про адвокатуру та адвокатську діяльність» адвокат зобов'язаний забезпечувати збереження адвокатської таємниці незалежно від форми її існування – паперової чи цифрової [3]. Таким чином, відповідальність за витік інформації покладається саме на правника, а не на зловмисника.

Дослідження [4] також виявляють гендерні особливості у сприйнятті кіберзагроз: чоловіки-юристи частіше демонструють надмірну впевненість у власних технічних знаннях, що призводить до ігнорування базових правил безпеки, тоді як жінки-правниці більш схильні реагувати на повідомлення з емоційним чи персоналізованим змістом. Обидва сценарії створюють різні, але однаково небезпечні вектори атак.

Ефективний захист інформації передбачає впровадження низки базових заходів: використання двофакторної автентифікації, застосування різних паролів для різних сервісів із залученням менеджерів паролів, шифрування документів під час передачі клієнтам, створення резервних копій на незалежних носіях, а також ретельну перевірку електронних повідомлень перед відкриттям посилань [5].

***Узагальнюючи***, слід зазначити, що сучасний стан кібербезпеки у правничій сфері не є критичним, проте характеризується недостатнім рівнем усвідомлення проблеми серед професійної спільноти. Наявні інструменти захисту та законодавчі вимоги [6] створюють основу для належного функціонування, однак ключовим залишається формування культури кібербезпеки як невід'ємної складової юридичної діяльності. Забезпечення кібербезпеки має розглядатися не як факультативний елемент, а як системний та постійний процес, що гарантує захист інтересів клієнтів і професійну відповідальність правника.

**Список використаних джерел:**

1. Діордіца І. В. Кібербезпека адвокатської діяльності в Україні та світі. *Нове українське право*. 2021. Вип. 5. С. 105–111.

2. Modic, D., Anderson, R. Reading this may harm your computer: The psychology of scams. *Journal of Cybersecurity*. 2015. Vol. 1(1). P. 87–97.

3. Про адвокатуру та адвокатську діяльність : Закон України від 05 лип. 2012 р. № 5076-VI. *Відомості Верховної Ради (ВВР)*. 2013, № 27, ст.282. URL: https://zakon.rada.gov.ua/laws/show/5076-17#Text.

4. Василець Н. М. Соціально-психологічні чинники довіри громадян в умовах цифровізації: дис. канд. психол. наук. Київ: ІПЗД НАПН України, 2021. 201 с.

5. Understanding the Role of Demographic and Psychological Factors in Users' Susceptibility to Phishing Emails: A Review. *MDPI*. 2022. Vol. 15(4). P. 2236.

6. Про основні засади забезпечення кібербезпеки України : Закон України від 05 жовт. 2017 р. № 2163-VIII. *Відомості Верховної Ради (ВВР)*. 2017. № 45. Ст. 403. URL: https://zakon.rada.gov.ua/laws/show/2163-19.

***Убога Сніжана Сергіївна***
студентка 117_СПД н.гр. ННІ права та психології НАВС

*Науковий керівник:*
***Тарасенко Володимир Петрович***
кандидат фізико-математичних наук, доцент кафедри інформаційних технологій ННІ права та психології НАВС

# НОВІ ВИКЛИКИ ТА ВИДИ КІБЕРЗЛОЧИНІВ: ПРАВОВИЙ АНАЛІЗ ТА МЕТОДИ РЕАГУВАННЯ КРІЗЬ ПРИЗМУ КОНСТИТУЦІЇ УКРАЇНИ

У сучасну епоху цифрової трансформації кіберпростір став не просто середовищем обміну інформацією, а стратегічною сферою, де перетинаються права людини, національна безпека та інтереси бізнесу. Конституція України, як закон найвищої юридичної сили, визначає, що людина, її життя, здоров'я, честь і гідність, недоторканність і безпека є найвищою соціальною цінністю (стаття 3). Захист цих цінностей у цифровому світі є прямим обов'язком держави [1].

## Штучний інтелект у руках злочинців: Deepfakes та дезінформація

Використання нейромереж для створення фальшивого аудіо- та відеоконтенту (діпфейків) створює загрозу фундаментальним правам громадян [8]:

- *Конституційний аспект*: стаття 32 Конституції гарантує кожному захист від втручання в його особисте і сімейне життя. Створення діпфейків порушує право на честь і гідність людини. Крім того, маніпуляція інформацією через ШІ суперечить статті 34, яка, гарантуючи право на свободу думки і слова, передбачає обмеження в інтересах національної безпеки та для захисту репутації інших людей.
- *Загроза*: використання ШІ для імітації голосу родичів або керівників у шахрайських схемах («ваш родич у біді») або для дестабілізації суспільства через фейкові звернення державних лідерів.

## Криптовалюти та даркнет: відмивання коштів та анонімні ринки.

Анонімність віртуальних активів створює виклики для економічної безпеки держави [3]:

- *Конституційний аспект*: згідно зі статтею 17, забезпечення економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу. Незаконний обіг коштів через даркнет підриває фінансову систему та можливість держави захищати право власності, гарантоване статтею 41.

- *Загроза*: використання криптовалют для виплати викупів після хакерських атак (Ransomware), фінансування тероризму та торгівлі забороненими товарами (наркотиками, зброєю), що відбувається поза межами державного контролю.

**Кібертероризм та кібердиверсії: захист критичної інфраструктури**

В умовах гібридної війни атаки на енергетику, банківський сектор та логістику прирівнюються до збройної агресії [4]:

- *Конституційний аспект*: стаття 17 проголошує, що захист суверенітету і територіальної цілісності України є найважливішою функцією держави. Кібердиверсії проти електромереж чи систем водопостачання загрожують життю громадян, що є порушенням конституційного права на життя (стаття 27) та безпечне довкілля (стаття 50).
- *Загроза*: дистанційне виведення з ладу систем управління АЕС, ТЕС або зупинка платіжних систем країни, що може призвести до гуманітарної катастрофи та хаосу.

**Соціальна інженерія 2.0: еволюція фішингу в месенджерах**

Злочинці переходять від масових розсилок до індивідуалізованого психологічного маніпулювання:

- *Конституційний аспект*: стаття 31 Конституції гарантує кожному таємницю листування, телефонних розмов та іншої кореспонденції. Соціальна інженерія (злам акаунтів, фішинг) є прямим посяганням на цю таємницю. Крім того, стаття 68 зобов'язує кожного не посягати на права і свободи, честь і гідність інших людей.
- *Загроза*: масштабні крадіжки персональних даних через підробні посилання у Telegram/WhatsApp, що використовуються для крадіжки коштів або доступу до конфіденційної службової інформації.

**Висновки та пропозиції щодо реагування**

Спираючись на норми Конституції України, правоохоронна діяльність у кіберпросторі повинна базуватися на таких принципах:

*Пріоритетність прав людини:* будь-які методи розслідування кіберзлочинів (перехоплення трафіку, доступ до даних) мають відповідати принципу законності та здійснюватися за рішенням суду, як того вимагають статті 30 та 31 Конституції.

*Державна підтримка кіберзахисту:* необхідно посилити відповідальність за кібердиверсії проти критичної інфраструктури, розглядаючи їх як замах на національну безпеку (ст. 17) [4].

*Міжнародне співробітництво:* оскільки кіберзлочинність не має кордонів, Україна, керуючись курсом на європейську інтеграцію, має гармонізувати законодавство про ШІ та криптовалюти з міжнародними стандартами (Budapest Convention on Cybercrime) [6, 7].

*Просвітницька роль:* держава має забезпечити реалізацію права громадян на інформацію про кіберзагрози, формуючи цифрову культуру суспільства [2, 5].

## Підсумок

Конституція України надає правоохоронним органам необхідний ціннісний орієнтир: технології мають служити людині, а не бути інструментом її пригноблення чи пограбування. Захист кіберпростору – це сучасна форма захисту державного суверенітету та конституційного ладу України.

## Список використаних джерел:


1. Конституція України : Закон України від 28 черв. 1996 р. № 254к/96-ВР. *Відомості Верховної Ради України (ВВР)*. 1996. № 30. Ст. 141. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text.
2. Про основні засади забезпечення кібербезпеки України : Закон України від 05 жовт. 2017 р. № 2163-VIII. *Відомості Верховної Ради (ВВР)*. 2017. № 45. Ст. 403. URL: https://zakon.rada.gov.ua/laws/show/2163-19.
3. Про національну безпеку України : Закон України від 21 черв. 2018 р. № 2469-VIII. *Відомості Верховної Ради (ВВР)*. 2018. № 31. Ст. 241. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text.
4. Про критичну інфраструктуру : Закон України від 16 листоп. 2021 р. № 1882-IX. *Відомості Верховної Ради (ВВР)*. 2023. № 5. Ст. 13. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text.
5. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26 серп. 2021 р.№ 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013?utm_source=chatgpt.com.
6. Конвенція про кіберзлочинність : ратифіковано із застереженнями і заявами Законом України від 07 верес. 2005 р. № 2824-IV. *Відомості Верховної Ради (ВВР)*. 2006. № 5-6. Ст. 71. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text.
7. Директива європейського парламенту і ради (ЄС) 2022/2555 від 14 грудня 2022 року про заходи для високого спільного рівня кібербезпеки на всій території Союзу, внесення змін до Регламенту (ЄС) № 910/2014 та Директиви (ЄС) 2018/1972 та скасування Директиви (ЄС) 2016/1148 (Директива NIS 2). URL: https://zakon.rada.gov.ua/laws/show/9a3_001-22#Text.
8. Регламент (ЄС) 2024/1689 (EU AI Act) щодо гармонізованих правил у сфері штучного інтелекту. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689.

***Гой Катерина Володимирівна***
студентка 202_СПС н.гр. ННІ права та психології НАВС

*Науковий керівник:*
***Пакриш Олександр Євгенійович***
кандидат технічних наук, доцент, доцент кафедри інформаційних технологій ННІ права та психології НАВС

# ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ АВТОМАТИЗАЦІЇ КІБЕРАТАК ТА СТВОРЕННЯ ДІПФЕЙКІВ

У сучасному світі стрімкий розвиток технологій суттєво змінює всі сфери людської діяльності. Особливе місце серед інновацій займає штучний інтелект (ШІ), який відкриває нові можливості для науки, медицини, освіти та бізнесу. Проте разом із перевагами виникають і нові ризики. Однією з найсерйозніших проблем є використання ШІ в кіберзлочинності, зокрема для автоматизації кібератак та створення діпфейків [1].

Актуальність цієї теми зумовлена тим, що кіберзагрози стають дедалі складнішими, а їх наслідки – масштабнішими. Зловмисники активно використовують сучасні технології для досягнення своїх цілей, що створює серйозну небезпеку для окремих осіб, організацій і навіть держав.

***Штучний інтелект*** – це галузь комп'ютерних наук, яка займається створенням систем, здатних виконувати завдання, що зазвичай потребують людського інтелекту. До таких завдань належать навчання, аналіз інформації, прийняття рішень та розпізнавання образів.

Основними технологіями ШІ є: машинне навчання, нейронні мережі та обробка природної мови. Завдяки цим інструментам ШІ може аналізувати великі обсяги даних, знаходити приховані закономірності та адаптуватися до нових умов. Саме ці властивості роблять його потужним інструментом як для захисту інформації, так і для її порушення [2].

Однією з найбільш небезпечних сфер застосування штучного інтелекту є кіберзлочинність [3]. ШІ дозволяє автоматизувати багато процесів, які раніше потребували значних зусиль з боку людини.

*По-перше*, штучний інтелект здатний самостійно знаходити вразливості в комп'ютерних системах. Він аналізує програмний код і мережеву активність, виявляючи слабкі місця, які можуть бути використані для атак.

*По-друге*, ШІ використовується для створення шкідливого програмного забезпечення. Сучасні віруси можуть змінювати свою структуру, щоб уникати виявлення антивірусами. Такі програми здатні навчатися і адаптуватися до нових умов.

*По-третє*, значно вдосконалилися фішингові атаки. Завдяки ШІ зловмисники можуть створювати персоналізовані повідомлення, які виглядають максимально правдоподібно. Вони враховують інтереси, стиль спілкування та поведінку жертви, що значно підвищує ефективність атак.

Крім того, ШІ використовується в соціальній інженерії – методі психологічного впливу на людину з метою отримання конфіденційної інформації. Наприклад, зловмисник може імітувати стиль листування керівника компанії або знайомої особи.

Також варто згадати про автоматизовані DDoS-атаки, які за допомогою ШІ можуть змінювати свою тактику в режимі реального часу, ускладнюючи захист від них.

Окрему загрозу становлять діпфейки – штучно створені відео, аудіо або зображення, які виглядають як справжні. Вони створюються за допомогою складних алгоритмів, зокрема генеративних нейронних мереж. Діпфейки дозволяють підробляти обличчя людей у відео, змінювати голос або створювати повністю вигадані сцени. Сучасні технології настільки вдосконалені, що відрізнити підробку від реальності стає дуже складно [4].

Існують різні види діпфейків:

- відео (підміна обличчя);
- аудіо (імітація голосу);
- зображення;
- текстові фальсифікації.

Діпфейки становлять серйозну небезпеку для суспільства. Однією з головних загроз є політичні маніпуляції. За допомогою підроблених відео можна поширювати неправдиву інформацію про політичних діячів, впливаючи на громадську думку.

Ще однією проблемою є шахрайство. Наприклад, зловмисники можуть імітувати голос керівника компанії та віддавати фальшиві розпорядження про переказ коштів.

Діпфейки також використовуються для дискредитації людей, що може завдати значної шкоди їхній репутації. Крім того, вони сприяють поширенню дезінформації, викликаючи паніку та недовіру до медіа.

Не менш важливим є питання порушення приватності, оскільки зображення людини можуть використовуватися без її дозволу.

Сучасні кіберзлочинці часто поєднують різні технології для досягнення максимального ефекту. Наприклад, діпфейк може використовуватися разом із фішингом або соціальною інженерією.

Уявімо ситуацію, коли працівник компанії отримує відеозвернення від «керівника» з проханням терміново виконати певну дію. Якщо це відео є діпфейком, то ймовірність того, що працівник повірить і виконає вказівку, значно зростає.

Такі комбіновані атаки є особливо небезпечними, оскільки вони впливають не лише на технічні системи, а й на людську психологію.

Для боротьби з використанням ШІ у кіберзлочинності необхідно застосовувати комплексний підхід.

*По-перше*, важливо розвивати технології виявлення діпфейків. Це можуть бути спеціальні алгоритми, які аналізують відео та аудіо на наявність ознак підробки.

*По-друге*, необхідно підвищувати рівень кіберграмотності населення. Люди повинні вміти розпізнавати фішингові атаки та критично оцінювати інформацію.

*По-третє*, важливу роль відіграє законодавче регулювання. Необхідно розробляти закони, які обмежують незаконне використання ШІ.

Також слід використовувати сам штучний інтелект для захисту – наприклад, для виявлення аномалій у мережі та запобігання атакам.

***Отже***, штучний інтелект є потужним інструментом, який може використовуватися як на благо людства, так і на шкоду. Його застосування у сфері кіберзлочинності відкриває нові можливості для зловмисників, роблячи атаки більш складними, масштабними та небезпечними.

Особливу загрозу становлять діпфейки, які здатні впливати на свідомість людей, поширювати дезінформацію та підривати довіру до інформаційних джерел.

У зв’язку з цим надзвичайно важливо розвивати засоби захисту, підвищувати обізнаність суспільства та вдосконалювати законодавство. Лише комплексний підхід дозволить мінімізувати ризики та забезпечити безпечне використання штучного інтелекту.

**Список використаних джерел:**


1. Kietzmann J., Lee L. Deepfakes: Trick or treat? Understanding the rise of synthetic media. *Business Horizons*. 2020. Vol. 63(2). P. 135–146.
2. Goodfellow I., Pouget-Abadie J., Mirza M. Generative Adversarial Networks. *Communications of the ACM*. 2014. Vol. 63(1). P. 139–144.
3. Brundage M., Avin S., Clark J. The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. *arXiv preprint*. 2018.
4. Tolosana R., Vera-Rodriguez R., Fierrez J. Deepfakes and Beyond: A Survey of Face Manipulation and Fake Detection. *Information Fusion*. 2020. Vol. 64. P. 131–148.

***Козіна Олена Вікторівна***
студентка 204_СПД н.гр. ННІ права та психології НАВС

*Науковий керівник:*
***Кудінов Вадим Анатолійович***
кандидат фізико-математичних наук, доцент, завідувач кафедри інформаційних технологій ННІ права та психології НАВС

# ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У ЗЛОЧИННИХ ЦІЛЯХ: СУЧАСНІ ВИКЛИКИ ТА МЕХАНІЗМИ ПРОТИДІЇ

Інформації технології не стоять на місці, а постійно розвиваються. На сьогоднішній день ми живемо в світі, де йде стрімкий техногенний розвиток, включно з розвитком систем штучного інтелекту (далі – ШІ) [1].

Системи ШІ в теорії є гарним інструментом – нині не потрібно користувачу витрачати багато часу на пошук потрібної інформації в Google, адже є такі зручні інструменти як ChatGPT або GeminiAI, які не лише знайдуть бажану інформацію за секунди, але й зможуть пояснити цю саму інформацію зрозумілою людині мовою та стилем мовлення. ШІ може згенерувати текст, презентацію, зображення, чи, навіть пісню. Ми навіть не помітили, як ШІ оточив нас: згенеровані відео та картинки, вбудований ШІ в телефон, ШІ в Google. Часом виникає питання: де ж закінчується людина і де починається Штучний Інтелект?

**Теорія мертвого Інтернету** – це конспірологічна теорія, поширена з кінця 2010-тих років, яка стверджує, що починаючи з 2016 року, Інтернет «вимер», і більша частина його користувачів це не люди, а боти, а увесь контент, що міститься в ньому є згенерованим штучним інтелектом.

Звісно, наявність людей виключає той факт, що Інтернет є мертвим на всі 100%, але важко посперечатись, що більшість користувачів не становлять боти. Тікток та Інстаграм сповнені акаунтів, увесь контент яких є повністю згенерований штучним інтелектом. Це та крихка межа між розвагою і загрозою, яка дуже легко стирається. Згенеровані ШІ зображення можуть стати легким способом маніпуляцій, шахрайства та пропаганди [2]. Сьогодні це широко використовується в пропаганді ворога – фейкова інформація просувається через чат-боти, згенеровані ШІ відео українських військових та звернення посадових осіб становлять особливу загрозу [3]. За 2025 рік Центр протидії дезінформації зафіксував понад 70 операцій, які пов’язані зі штучним інтелектом, що були проведені російською федерацію. Вони зібрали понад 7 мільйонів переглядів, охопивши значну аудиторію.

**Порушення авторських прав** є ще одною загрозою, яку несе штучний інтелект. Для того, аби генерувати картинки, фотографії, музику, анімації та відео штучний інтелект тренується, використовуючи фотографії та відео реальних людей, діджитал арти, музику та анімації реальних художників, що відбувається часто без згоди людей, яким належить дані матеріали. Таким чином, після навчання на наданих в Інтернеті матеріалах, штучний інтелект генеруватиме власні, майже ідентичні до тих, що належать реальним людям [1].

**Досвід Південної Кореї** може стати для нас прикладом того, як же можна боротися з вищезазначеними загрозами. Ця країна є першою в світі, яка реально взялась за регулювання штучного інтелекту та сфер його використання. За новим законодавством, в Південній Кореї запроваджено людський нагляд за автоматизованими системами. Було створено спеціальний орган – Національний комітет зі штучного інтелекту, функціями якого є регулювання індустрії ШІ, встановлювати напрямки її розвитку та контролювати її вплив на суспільство.

Введено обов'язкове правило позначати контент, згенерований ШІ, якщо його складно відрізнити від реального. Україна може перейняти цей досвід, прийнявши подібний закон, що визначатиме точний курс розвитку ШІ та створить відповідний орган, який регулюватиме цей розвиток [4]. Необхідно запровадити обов'язкову позначку контенту, що був згенерований штучним інтелектом, якщо його не можна відрізнити від реального, впроваджувати санкції щодо використання генеративного ШІ з умислом завдати шкоди іншим людям.

***Отже***, розвиток інформаційних технологій здійснюється здебільшого на благо функціонування суспільства, але існує вірогідність того, що нові досягнення в цій сфері можуть використовуватися в злочинних цілях. Як приклад, це стосується систем штучного інтелекту. Тому, на наш погляд, необхідно своєчасно запровадити низку заходів, які б суттєво зменшили вірогідність використання систем штучного інтелеккту в злочинних цілях.

**Список використаних джерел:**

1. Trystan S. Goetze. AI Art is Theft: Labour, Extraction, and Exploitation. FAccT'24, June 03–06, 2024, Rio de Janeiro, Brazil. P. 186–196. URL: https://dl.acm.org/doi/epdf/10.1145/3630106.3658898.

2. Dan Hendrycks, Mantas Mazeika, Thomas Woodside. An Overview of Catastrophic AI Risks. *Cornell University* : [site]. URL: https://arxiv.org/pdf/2306.12001.

3. Інформаційні операції рф з використанням ШІ у соцмережах. *Центр протидії дезінформації* : [сайт]. URL: https://cpd.gov.ua/international-direction/yevropa/informaczijni-operacziyi-rf-z-vykorystannyam-shi-u-soczmerezhah/.

4. Framework Act on the Development of Artificial Intelligence and Establishment of Trust. *CSET* : [site]. URL: https://cset.georgetown.edu/wp-content/uploads/t0625_south_korea_ai_law_EN.pdf.

***Фертіль Анастасія Ігорівна***
студентка 201_СПС н.гр. ННІ права та психології НАВС

*Науковий керівник:*
***Тарасенко Володимир Петрович***
кандидат фізико-математичних наук, доцент кафедри інформаційних технологій ННІ права та психології НАВС

# ЛЮДСЬКИЙ ФАКТОР У СИСТЕМІ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ: ПСИХОЛОГІЯ ЗЛОЧИНЦЯ, ЖЕРТВИ ТА ПРАВООХОРОНЦЯ ЯК ВЗАЄМОПОВ'ЯЗАНІ ЕЛЕМЕНТИ

Кіберзлочинність традиційно сприймається як сфера високих технологій, де головними дійовими особами виступають програмні коди, шкідливе програмне забезпечення та технічні вразливості. Однак, як слушно зауважує Тарнвір Сінгх, дослідження кібербезпеки неможливе без розуміння психології – як кібератак, так і кіберзахисту [1]. За своєю суттю кіберзлочин – це завжди міжлюдська взаємодія, лише опосередкована цифровими технологіями. Людина залишається центральним елементом цієї системи: вона ухвалює рішення про вчинення злочину, вона стає жертвою через власні психологічні особливості і вона ж протидіє злочинності, зазнаючи при цьому специфічних професійних навантажень.

*Мета* цієї роботи – проаналізувати психологічні характеристики трьох ключових фігур кіберзлочинності (правопорушника, потерпілого, правоохоронця) у їхньому взаємозв'язку та обґрунтувати необхідність інтеграції психологічних знань у систему протидії кіберзлочинності.

Розуміння того, чому люди скоюють кіберзлочини, є фундаментальним для ефективної профілактики та розслідування. Сучасні дослідження демонструють, що ***кіберзлочинці*** не є однорідною групою – їхні психологічні профілі варіюються залежно від типу злочину, віку, культурного контексту та рівня технічної підготовки [2]. Систематичний огляд 45 досліджень, проведений Trinh D.T. з колегами, виявив, що кіберзлочинцям часто притаманні нарцисизм, імпульсивність та високий рівень технічної компетентності [2]. Дослідники також пов'язують онлайн-злочинну поведінку з психопатією та іншими антисоціальними рисами [3]. Особливу увагу привертає зв'язок із макіавеллізмом (однією з рис «Темної тріади»): особи з високими показниками за цією шкалою демонструють більшу схильність до злочинної поведінки в цифровому середовищі [4].

Цікаво, що деякі дослідження вказують на кореляцію між кіберзлочинними діями та розладами аутистичного спектра, хоча цей зв'язок потребує подальшого вивчення [5]. Важливо підкреслити, що створення єдиного уніфікованого профілю кіберзлочинця в сучасних умовах є неможливим – спектр надто широкий: від ідеологічно вмотивованих підлітків-хакерів до індустрії Cybercrime-as-a-Service (CaaS) [6].

Також аналіз мотивації кіберзлочинців демонструє складну картину. Дослідження випадків реальних кіберправопорушників виявляють різноманітні спонукальні чинники:

- *Фінансова вигода* – домінує у випадках шахрайства, програм-вимагачів, крадіжки даних.
- *Ідеологічні мотиви* – характерні для хактивістів (наприклад, Anonymous), які прагнуть привернути увагу до певних проблем.
- *Визнання та самоствердження* – особливо серед молодих хакерів, які прагнуть довести свою перевагу.
- *Когнітивні викривлення* – кіберзлочинці часто використовують механізми нейтралізації, такі як заперечення відповідальності («це не я, це програма») або заперечення шкоди («це ж просто віртуальні дані, ніхто не постраждав») [7].

Василе-Кетелін Голоп та Наталія Сеулеску у своєму дослідженні підкреслюють, що вибір злочинної діяльності в кіберпросторі часто зумовлений соціальними впливами та можливостями, які відкриває онлайн-середовище [4].

Для розуміння поведінки кіберзлочинців дослідники застосовують різноманітні теоретичні моделі. Європейська комісія запропонувала міждисциплінарний підхід до профілювання, який інтегрує психологію, нейронауку, кримінологію та кіберпсихологію [8]. Важливу роль відіграє теорія онлайн-розгальмування (online disinhibition effect), яка пояснює, чому люди вчиняють в онлайн-середовищі дії, які ніколи б не вчинили в реальному житті [9].

Друга частина тріади – ***жертва*** – часто розглядається крізь призму технічної необізнаності, однак психологічні механізми віктимізації значно складніші. Авішкар Нікум наголошує, що атакувальники активно експлуатують психологічні риси людей для отримання несанкціонованого доступу, а такі техніки, як «претекстинг», стають дедалі витонченішими [5]. Денніс Тан Цзя Цзюнь з колегами детально аналізують людські фактори, що роблять можливими атаки соціальної інженерії [9]. До них належать:

- *Когнітивні здібності* – рівень інтелекту, здатність до вербального та абстрактного мислення впливають на стійкість до маніпуляцій. Когнітивне навантаження може призводити до неуважності, коли людина пропускає важливі сигнали небезпеки, зосередившись на основному завданні [9].

- *Культурні аспекти* – організаційна культура суттєво впливає на безпекову поведінку працівників. Культура безпеки в організації формує те, як люди реагують на кіберзагрози [10].
- *Особистісні риси* – дослідження виявляють зв'язок між рисами «Великої п'ятірки» (Big Five) та вразливістю до різних типів кіберзагроз. Зокрема, імпульсивність та низький рівень сумлінності (conscientiousness) можуть знижувати ефективність безпекових практик [9].
- *Психологічні фактори* – страх, альтруїзм, довіра – саме ці емоції стають мішенню для маніпуляцій. Інцидент зі зломом акаунтів у Twitter (X) 2020 року наочно продемонстрував, як маніпуляція довірою низькорівневих працівників призвела до масштабного зламу [5].

В свою чергу Аманда Віддоусон наголошує, що розуміння причин, чому одні люди стають жертвами кіберзлочинів, а інші – ні, є необхідним для забезпечення інформованого кіберзахисту [3]. Особливо вразливими є групи з підвищеною довірливістю, низьким рівнем цифрової грамотності, а також особи, які перебувають у стані стресу або емоційної нестабільності. Пандемія COVID-19, яка супроводжувалася стресом та невизначеністю, спричинила 600% зростання кіберзлочинності, оскільки злочинці активно експлуатували вразливий емоційний стан населення [10].

Третя, часто ігнорована фігура в цій системі – ***працівник правоохоронних органів***, який протидіє кіберзлочинності. Його психологічний профіль та стан безпосередньо впливають на ефективність усієї системи. Робота з кіберзлочинністю висуває специфічні вимоги до психіки працівника:

- ✓ *Високий рівень стресостійкості* – необхідність працювати з великими обсягами інформації, часто травматичного змісту.
- ✓ *Аналітичне мислення та здатність до тривалої концентрації*.
- ✓ *Комунікативна компетентність* – вміння встановлювати психологічний контакт як із жертвами (часто травмованими), так і з підозрюваними (схиляти до співпраці).
- ✓ *Емоційний інтелект та критичне мислення* – ключові навички для протидії атакам соціальної інженерії, які мають бути розвинені не лише у пересічних громадян, а й у самих правоохоронців [8].

Специфіка роботи в кіберпросторі створює додаткові фактори ризику для професійного вигорання:

- Високе інформаційне навантаження.
- Постійна взаємодія з протиправним контентом.
- Необхідність швидко адаптуватися до нових загроз.
- Конфлікт між вимогами безпеки та зручності використання технологій [7].

Олівія Гвідетті та Стефан Мазер у дослідженні, присвяченому профілюванню кіберзлочинців, наголошують, що людська динаміка, яка стоїть за кібератаками, створює унікальні виклики для правоохоронних органів, вимагаючи поєднання традиційних методів розслідування з інсайтами з поведінкових наук [10]. До того ж дослідження Джузеппе Дезольди з колегами пропонує комплексну рамку MORPHEUS для моделювання, вимірювання та пом'якшення людських факторів у кібербезпеці [7]. Ця модель, заснована на підході Cognition-Affect-Behavior (Cognition-Emotion-Behavior) та теорії атрибуції, може бути застосована і для психологічного супроводу діяльності правоохоронців, включаючи діагностику ризиків, навчання та профілактику вигорання.

**Висновки.**

Проведений аналіз демонструє, що кіберзлочинність є не лише технологічним, але й глибоко психологічним феноменом. Три ключові фігури – злочинець, жертва, правоохоронець – утворюють нерозривну систему, де кожен елемент впливає на інші.

Кіберзлочинці демонструють специфічні особистісні риси (нарцисизм, імпульсивність, схильність до маніпуляцій) та використовують когнітивні викривлення для нейтралізації моральних обмежень. Жертви стають вразливими через комплекс психологічних факторів: когнітивні обмеження, емоційні стани, особистісні риси та культурний контекст. Правоохоронці, своєю чергою, потребують не лише технічної, але й ґрунтовної психологічної підготовки, а також системи психологічного супроводу для запобігання професійному вигоранню.

Інтеграція психологічних знань у правоохоронну діяльність у кіберпросторі має відбуватися за кількома напрямами:

1. *Профілактичний* – використання психологічних знань для прогнозування та попередження злочинів.
2. *Комунікативний* – підвищення ефективності взаємодії з учасниками кримінального процесу.
3. *Реабілітаційний* – психологічна допомога жертвам кіберзлочинів.
4. *Кадровий* – психологічний супровід працівників кіберполіції.

Таким чином, психологічна компетентність стає не додатковою, а базовою вимогою для ефективної протидії кіберзлочинності в сучасних умовах.

**Список використаних джерел:**

1. Singh T. Cybersecurity, psychology and people hacking. Cham: Palgrave Macmillan; 2025. (Palgrave studies in cyberpsychology).
2. Trinh DT, Dinh TCH, Tran TNK. Exploring the psychological profile of cybercriminals: A comprehensive review for improved cybercrime prevention. *International Journal of Cyber Criminology*. 2025.
3. Widdowson A. Motivation and behaviour. In: Humans and cyber security. Taylor & Francis; 2025.

4. Golop VC, Săvulescu N. Profile of persons who act in the field of computer criminality. In: Asociația Română pentru Asigurarea Securității Informatice; 2024. P. 90-95.

5. Nikum A. Examining the human factors in cybersecurity practices: Psychological, technical, and organisational perspectives. *Asian Journal of Research in Computer Science*. 2025;18(6):292-300.

6. Lane T. Personality profiles of cyber criminals: An integration of existing research. In: Taylor & Francis; 2025.

7. Desolda G, Greco F, Lanzilotti R. MORPHEUS: A multidimensional framework for modeling, measuring, and mitigating human factors in cybersecurity. arXiv:2512.18303. 2025.

8. Bada M, Nurse JRC. Exploring cybercriminal activities, behaviors and profiles. arXiv:2308.15948. 2023.

9. Tan Jun DJ, Rafsanjani AS, Aslam S, Behjati M. Human factors in information security: A quantitative study with technical solutions to prevent social engineering attacks. *Digital Threats: Research and Practice*. 2025.

10. Guidetti O, Mather S. Malicious minds: Psychological profiling of ransomware attackers and policing challenges. In: Ransomware evolution. Taylor & Francis; 2024. P. 175-191.

*Для нотаток*

**Наукове видання**

КУДІНОВ Вадим Анатолійович

**КІБЕРПРОСТІР ЯК СФЕРА ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ: НОВІ ЗАГРОЗИ ТА МЕТОДИ РЕАГУВАННЯ**

Матеріали науково-практичного семінару

(м. Київ, 26 березня 2026 року)

Комп’ютерна верстка: *В.А. Кудінова*

---

Підписано до друку 21.03.2026. Формат 60х84/16. Папір офсетний.
Обл.-вид. арк. 4,5. Ум. друк. арк. 4,18.
Тираж 50 прим.

---

Редакційно-видавниче відділення
Національної академії внутрішніх справ
03035, Київ, пл. Солом’янська, 1

Друк: ФОП Поліщук О.В.
Свідоцтво суб’єкта видавничої справи ДК № 2142 від 31.03.2015
07400, м. Бровари, вул. Незалежності, 2, кв. 148
тел. (044) 592-13-49