

4. Звіт про кінцеве дослідження щодо інформованості цільових аудиторій про основні аспекти кібербезпеки: підготовлено для Представництва Фонду цивільних досліджень та розвитку США в Україні. URL: [info_sapiens_crdf_report_ua_2024.pdf](https://info.sapiens.crdf_report_ua_2024.pdf)

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

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

Старовойт Аліна Олексіївна,

здобувач ступеня вищої освіти бакалавра
навчально-наукового інституту права та
психології Національної академії
внутрішніх справ

Науковий керівник:

Смаглюк О. В., доцент кафедри
кримінального права та кримінології
навчально-наукового інституту права та
психології Національної академії
внутрішніх справ, кандидат юридичних
наук, доцент

ВПЛИВ ЦИФРОВИХ ТЕХНОЛОГІЙ НА ПРАВОВЕ РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

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

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

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

Кримінальний кодекс України передбачає відповідальність за злочини у сфері комп'ютерної інформації. Зокрема, статті 361–363¹ встановлюють покарання за несанкціоноване втручання в роботу комп'ютерних систем, створення чи розповсюдження шкідливих програм, незаконне копіювання або використання інформації з обмеженим доступом [4, с. 210–212]. Закон України «Про інформацію» [3, с. 12–14] визначає основні принципи інформаційної діяльності, права та обов'язки суб'єктів інформаційних відносин, а також механізми захисту інформації.

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

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

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

Список використаних джерел

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

Ступак Діана Русланівна,

здобувач ступеня вищої освіти бакалавра
навчально-наукового інституту права та
психології Національної академії
внутрішніх справ

Науковий керівник:

Козачина А. М., старший викладач
кафедри кримінального права та
кримінології навчально-наукового
інституту права та психології
Національної академії внутрішніх справ,
доктор філософії

КОГНІТИВНА ВІЙНА: НОВЕ ПОЛЕ БОЮ, ЩО ВИКОРИСТОВУЄ НАШ МОЗОК

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