АКТУАЛЬНІ ПИТАННЯ ЮРИДИЧНОЇ НАУКИ

УДК 343.9:094 (477)
DOI https://doi.org/10.32782/2408-9257-2025-2-27

Олійник А.,
аспірант кафедри адміністративного і кримінального права
Дніпровського національного університету імені Олеся Гончара

ФОРМУВАННЯ СТІЙКОГО ЦИФРОВОГО СУСПІЛЬСТВА: ПРЕВЕНТИВНА РОЛЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА КРИМІНАЛЬНО-ПРАВОВОЇ ПОЛІТИКИ У ЗАПОБІГАННІ ЗЛОЧИННОСТІ

BUILDING A SUSTAINABLE DIGITAL SOCIETY: THE PREVENTIVE ROLE OF INFORMATION SECURITY AND CRIMINAL LAW POLICY IN CRIME PREVENTION

Стрімка та всеосяжна цифровізація суспільства, незважаючи на беззаперечні переваги, генерує нові виклики та загрози для людини, її прав і свобод. Зростання обсягів даних, розвиток штучного інтелекту та повсюдне проникнення цифрових технологій створюють унікальне середовище для розвитку нових форм злочинності. Стрімкий розвиток технологій вимагає не лише адаптації, а й проактивного формування стійкого цифрового середовища, здатного ефективно протистояти цим викликам. Тому дослідження превентивної ролі інформаційної безпеки та кримінально-правової політики є критично важливим для забезпечення довіри та стабільності у суспільстві, що дедалі більше залежить від цифрових технологій.

У сучасному цифровому світі, де технології глибоко інтегровані в усі сфери життя, формування стійкого цифрового суспільства стає імперативом національної безпеки та добробуту. У статті було визначено, що цей процес вимагає системного підходу, де ключову превентивну роль відіграють інформаційна безпека та кримінально-правова політика у запобіганні злочинності проти людини. Досліджено офіційні статистичні дані Офісу Генерального прокурора України, які свідчать про постійне та значне зростання кількості кримінальних правопорушень у сфері інформаційних технологій, що підкреслює нагальну потребу в ефективних превентивних механізмах.

У статті досліджено такий новий вимір безпеки, як когнітивна безпека, що полягає у здатності людини критично сприймати інформацію та захищати власну свідомість від маніпуляцій. Проаналізовано роль когнітивної війни, де свідомість стає полем бою, та підкреслено, що ефективна протидія цьому вимагає розвитку критичного мислення та медіаграмотності громадян. Визначено, що когнітивна безпека є яскравим прикладом синергії між технічними рішеннями інформаційної безпеки та кримінально-правовою політикою, що забезпечує відповідальність за поширення маніпуляцій.

Підсумовуючи, зазначено, що інформаційна безпека має стати основним напрямом кримінологічної політики України, а її реалізація потребує удосконалення на законодавчому, правозастосовному та організаційному рівнях. Акцентовано увагу на транснаціональному характері кіберзлочинів та необхідності розвитку системи кібербезпеки та законодавства, що забезпечить правоохоронним органам необхідні інструменти для ефективного запобігання та розслідування цих злочинів.

Ключові слова: *національна безпека, цифрове середовище, інформаційна безпека, медіаграмотність, кіберзлочинність, інформація, політика, запобігання злочинності, кримінальне правопорушення.*

The rapid and pervasive digitalization of society, despite its undeniable advantages, generates new challenges and threats to individuals, their rights, and freedoms. The growth of data volumes, the development of artificial intelligence, and the widespread penetration of digital technologies create a unique environment for the emergence of new forms of crime. The swift advancement of technologies demands not just adaptation, but also the proactive formation of a resilient digital environment capable of effectively countering these challenges. Therefore, research into the preventive role of information security and criminal law policy is critically important for ensuring trust and stability in a society increasingly dependent on digital technologies.

In the modern digital world, where technologies are deeply integrated into all spheres of life, the formation of a resilient digital society becomes an imperative for national security and well-being. The article defined that this process requires a systemic approach, where information security and criminal law policy play a key preventive role in preventing crime against individuals. Official statistical data from the Prosecutor General's Office of Ukraine were analyzed, which indicate a constant and significant increase in the number of criminal offenses in the field of information technologies, emphasizing the urgent need for effective preventive mechanisms.

The article investigated a new dimension of security: cognitive security, defined as a person's ability to critically perceive information and protect their own consciousness from manipulation. The role of cognitive warfare, where consciousness becomes the battlefield, was analyzed, and it was highlighted that effective countermeasures require the development of critical thinking and media literacy among citizens. It was determined that cognitive security is a prime example of synergy between information security's technical solutions and criminal law policy, which ensures accountability for the spread of manipulations.

In conclusion, it was noted that information security must become the primary direction of Ukraine's criminological policy, and its implementation requires improvement at the legislative, law enforcement, and organizational levels. Attention was focused on the transnational nature of cybercrimes and the need to develop a cybersecurity system and legislation that will provide law enforcement agencies with the necessary tools for effective prevention and investigation of these crimes.

Key words: *national security, digital environment, information security, media literacy, cybercrime, information, policy, crime prevention, criminal offence.*

Постановка проблеми. Цифрове суспільство – це суспільство, у якому цифрові технології глибоко інтегровані в усі сфери життя, трансформуючи спілкування, економіку, культуру, освіту, державне управління та повсякденну діяльність людини. Це не просто використання комп'ютерів чи інтернету, а якісно новий етап розвитку, де: інформація стає ключовим ресурсом, доступною в будь-який час і з будь-якого місця; цифрові комунікації (соціальні мережі, месенджери, відеозв'язок) домінують у взаємодії між людьми; економіка все більше базується на цифрових платформах, електронній комерції та інноваційних технологіях; життя людей стає все більш залежним від цифрових пристроїв та сервісів, формуючи нові звички, моделі поведінки та соціальні взаємодії.

Формування стійкого цифрового суспільства стає не просто технічною чи правовою задачею, а імперативом національної безпеки та добробуту, де ключову, превентивну роль відіграють інформаційна безпека та кримінально-правова політика у запобіганні злочинності проти людини.

Стан опрацювання проблематики. Проблемам забезпечення інформаційної безпеки, формування кримінально-правової політики, присвячені роботи багатьох учених. Це наукові праці вітчизняних та зарубіжних учених, як Д. С. Азаров, О.М. Бодунова, Я. Берзиньш, І. Р. Березовська, О. І. Бугера, М. В. Гуцалюк, Б. М. Головкін, Г. В. Дідківська, В. М. Дрьомін, М. В. Карчевський, О. Г. Колб, А. М. Коломієць, О. В. Климчук, В. А. Ліпкан, В. В. Марков, Г. Г. Почепцов, М. М. Присяжнюк, О. В. Таволжанський, Ш. Шольберг, С. Хантінгтон, О. Е. Радутний, В. В. Топчій, Т. Л. Тропіна, А. В. Тунік, Д. М. Цехан В. М. Шевчук, В. Ю. Шепітько, Н. С. Юзікова, О. М. Яхно та інших.

Вказані видатні науковці, безперечно, зробили значний внесок у теорію і практику формування та забезпечення інформаційної безпеки та ролі кримінально-правової політики у запобіганні злочинності. Втім, на сьогодні питання, що стосуються формування стійкого цифрового суспільства, заходів запобігання злочинності у сфері інформаційних технологій в умовах воєнного стану залишаються недостатньо вивченими та потребують подальшого правового врегулювання.

Метою статті є комплексний аналіз превентивної ролі інформаційної безпеки та кримінально-правової політики у запобіганні злочинності проти людини в умовах формування стійкого цифрового суспільства, а також розробка науково обґрунтованих рекомендацій щодо їх синергійної взаємодії для забезпечення захисту прав і свобод особистості у цифровому просторі.

Виклад основного матеріалу. Актуальність теми зумовлена безпрецедентним зростанням цифрових загроз та кіберзлочинності, які щоденно ставлять під загрозу права та безпеку людини у віртуальному просторі. Сучас-

на епоха характеризується безпрецедентною цифровізацією всіх сфер життя, що, поряд із значними можливостями, створює нові та зростаючі загрози для прав і свобод людини. Зростання кіберзлочинності, особливо спрямованої проти особистості (фінансові шахрайства, кібербулінг, крадіжки ідентичності та порушення приватності), ставить під сумнів саму ідею безпечного та довірливого цифрового простору. Формування стійкого цифрового суспільства вимагає не лише реактивного реагування на злочини, а й розробки ефективних превентивних механізмів. Саме тому постає нагальна потреба в комплексному дослідженні превентивної ролі інформаційної безпеки та кримінально-правової політики, які, діючи синергічно, здатні мінімізувати ці загрози та забезпечити захист людини у віртуальному світі.

Актуальність дослідження також підтверджується офіційними статистичними даними. Так, кількість кримінальних правопорушень у сфері інформаційних технологій постійно зростає. Відповідно до офіційних статистичних даних Офісу Генерального прокурора, у 2024 році обліковано 4 055 кримінальних правопорушень у сфері інформаційних технологій, шо на 214 кримінальних правопорушень більше ніж у 2023 році (цей показник становив 3 841 кримінальних правопорушень); на 640 більше ніж у 2022 році (цей показник становив 3 415 кримінальних правопорушень); на 745 у 2021 році (цей показник становив 3 310 кримінальних правопорушень); на 1557 у 2020 (цей показник становив 2 498 кримінальних правопорушень) [1]. Така тенденція свідчить про суттєве зростання, а саме на 38,4% порявняно із 2020 роком та на 5,3% порівняно із 2023 роком, кількості зареєстрованих кримінальних правопорушень

Особливої загрози кримінальні правопорушення у сфері інформаційних технологій набувають в умовах воєнного стану, оскільки поряд із бойовими діями триває масштабна інформаційна агресія з боку російської федерації проти України. Кіберзлочинці активно використовуються для зламу державних інформаційних систем, поширення дезінформації серед населення, створення фальшивих акаунтів у соціальних мережах тощо. Значного поширення набуло й кібершахрайство, коли зловмисники, видаючи себе за представників офіційних структур, намагаються незаконно отримати доступ до банківських даних громадян для заволодіння їхніми грошовими коштами.

Таким чином, інформаційна війна завдає суспільству не меншої шкоди, ніж бойові дії. З огляду на це, в Україні розпочато реформування кримінального та кримінального процесуального законодавства з метою підвищення ефективності протидії таким правопорушенням. Водночас нині рівень запобігання кіберзлочинам залишається недостатнім, зважаючи на постійне вдосконалення злочинцями методів здійснення таких дій.

Додатковою складністю у протидії кіберзлочинності є транснаціональний характер цих правопорушень, що дозволяє вчиняти їх з будь-якої точки світу, уникаючи юрисдикції національних правоохоронних органів. У зв'язку з цим особливої актуальності набуває розвиток системи кібербезпеки, а також удосконалення законодавства, яке надасть правоохоронним органам необхідні інструменти для ефективного виявлення, розслідування і запобігання таким злочинам.

У сучасному цифровому світі загрози для людини виходять далеко за межі традиційного викрадення даних чи фінансового шахрайства. Дедалі більшої актуальності набуває поняття когнітивної безпеки – здатності людини критично сприймати та опрацьовувати інформацію, захищаючи власну свідомість від маніпуляцій, дезінформації та цілеспрямованого психологічного впливу. Це безпосередньо стосується превенції злочинності проти людини, оскільки маніпуляції свідомістю часто є першим кроком до вчинення шахрайства, вимагання, або навіть вербування у злочинні угруповання.

Професор Г. Г. Почепцов вказує на важливість когнітивної безпеки, особливо в умовах сучасного інформаційного суспільства. Когнітивна безпека охоплює заходи, спрямовані на захист розумових процесів та розвиток навичок критичного мислення в суспільстві. Пропаганда та маніпуляція інформацією можуть серйозно впливати на сприйняття реальності та призводити до негативних наслідків [2]. Зміна сприйняття та ментальних операцій може мати серйозні наслідки для індивіда та суспільства в цілому.

В умовах гібридної війни та поширення інформації, безпека людини охоплює не лише її фізичну цілісність чи фінансове благополуччя, а й ментальну стійкість та здатність до об'єктивного мислення. Злочинність проти людини в цифровому просторі тепер включає також психологічний тиск, кібербулінг, створення фейкових новин для дезорієнтації та інші форми впливу на її когнітивні процеси. При цьому, стійке цифрове суспільство не може бути таким без когнітивно стійких громадян. Суспільство, яке легко піддається маніпуляціям, є вразливим до дезінформації, що може призвести до соціальної дестабілізації, паніки та навіть прямого вчинення злочинів під впливом неправдивої інформації. Тому формування критичного мислення та медіаграмотності є невід'ємною частиною цифрової стійкості.

Когнітивна безпека реалізується через просвітницькі кампанії з медіаграмотності, розвитку критичного мислення, навчання розпізнаванню маніпулятивних технік та фейків. Це включає не лише захист даних, а й захист свідомості користувача від шкідливого інформаційного контенту. Технічні засоби можуть допомагати у виявленні ботів та тролів, але кінцеве рішення про довіру інформації приймає людина.

Пропаганда та маніпулювання інформацією застосовуються з метою впливу на когнітивні процеси людини шляхом формування спеціально сконструйованих інформаційних повідомлень, здатних активізувати певні шаблони та упередження. Такий вплив може спотворювати сприйняття дійсності та формувати хибні переконання й небажані уявлення. Щоб протистояти подібному впливу, необхідно розвивати критичне мислення, перевіряти інформацію через різноманітні джерела та здійснювати її самостійний аналіз. Окрім цього, важливим є підвищення рівня медіаграмотності, що дозволяє відрізняти достовірні джерела від маніпулятивних і споживати інформацію більш усвідомлено та обережно.

У сучасних умовах, особливо зважаючи на агресивну гібридну війну, людська свідомість перетворилася на основне поле бою. Метою ведення так званої когнітивної війни є не просто зміна поглядів людини, а й фундаментальна трансформація її способу мислення та подальших дій. Це підкреслює критичну важливість концепції когнітивної безпеки (COGSEC).

COGSEC виходить за рамки традиційної інформаційної безпеки, акцентуючи увагу на усвідомленні того, як інформація може бути цілеспрямовано використана для маніпуляції думками, переконаннями та поведінкою людей у сучасному перенасиченому інформаційному середовищі. Когнітивна війна — це, по суті, форма конфлікту, де психологічний та інформаційний вплив застосовується для досягнення стратегічних цілей. Основною метою COGSEC є збереження когнітивної системи забезпечення об'єктивності, незалежності при прийнятті рішень [3].

У публікації 2014 р. латвійський дослідник Янис Берзиньш (Jānis Bērziņš) наголошував, що «російський погляд на сучасну війну ґрунтується на ідеї, що основним полем бою є погляди, і, як наслідок, у війнах нового покоління має домінувати інформаційно-психологічна війна з метою змусити військове та цивільне населення супротивника підтримати нападника на шкоду власному уряду та країні» [4, с. 5–13].

У сучасних реаліях маніпуляції інформацією, дезінформація та пропаганда через соцмережі становлять критичну загрозу для стабільності як окремих держав, так і всієї міжнародної спільноти. Ці форми інформаційної війни підривають довіру до демократичних інститутів, руйнують суспільну згуртованість та загрожують національній безпеці.

Згідно зі Стратегією інформаційної безпеки України, затвердженою Указом Президента від 15 жовтня 2021 року, інформаційна політика Російської Федерації визнана прямою загрозою не лише для України, а й для інших демократичних країн. Російські спецслужби цілеспрямовано здійснюють спеціальні інформаційні операції, спрямовані на ключові демократичні процеси, зокрема вибори, та прагнуть посилити внутрішні розбіжності як в Україні, так і за її межами. Технології гібридної війни, які Росія застосовує проти України, швидко адаптуються та поширюються на інші держави. Відповіддю на таку дезінформаційну агресію є запровадження обмежувальних заходів (санкцій) та створення ефективного механізму моніторингу й притягнення до відповідальності за їх порушення [5].

Указом Президента України «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» визначено актуальні питання щодо взаємодії уповноважених державних органів стосовно забезпечення інформаційної безпеки, системи їх повноважень щодо захисту інтересів українців і країни в цілому в інформаційній сфері [6].

Кримінально-правова політика має адаптуватися до нових викликів. Це може стосуватися криміналізації дезінформації, маніпуляцій громадською думкою, що мають злочинні наслідки, а також розробки механізмів відповідальності за психологічний тиск та домагання в цифровому просторі, які призводять до шкоди психічному здоров'ю. Крім того, важливою є правова просвіта громадян щодо їхніх прав у інформаційному просторі та механізмів захисту від психологічного впливу.

Так, когнітивна безпека є яскравим прикладом синергії між інформаційною безпекою та кримінально-правовою політикою. Технічні рішення інформаційної безпеки можуть виявляти джерела маніпуляцій, а кримінально-правовою політикою – забезпечувати правову відповідальність за їх поширення. Водночас, освіта та підвищення свідомості громадян є спільним завданням обох сфер, що безпосередньо впливає на здатність людини захистити себе від цифрових загроз на когнітивному рівні.

Інформаційна безпека у сучасних умовах має стати основним напрямом кримінологічної політики України та удосконалення у зв’язку з цим форм її реалізації на законодавчому, правозастосовному, організаційному та інших рівнях.

Під час військових конфліктів і в умовах воєнного стану інформаційний простір часто використовується як інструмент впливу на громадську свідомість, дестабілізацію суспільства та втручання у внутрішню й зовнішню політику держави. Інформаційні загрози можуть проявлятися у вигляді дезінформації, пропагандистських кампаній, кібератак, обмеження доступу до інформації та інших форм втручання в інформаційні ресурси й інфраструктуру. Забезпечення інформаційної безпеки передбачає створення ефективної системи протидії таким загрозам, розвиток кіберзахисту, моніторинг і нейтралізацію дезінформації, зміцнення інформаційної інфраструктури держави, а також удосконалення механізмів інформаційної протидії та контрпропаганди [7].

Отже, державна політика щодо забезпечення інформаційної безпеки є важливою складовою національної безпеки. В її основі повинна бути системна превентивна діяльність органів державного управління щодо надання гарантій інформаційної безпеки особистості, соціальним групам, суспільству і державі в цілому. Аналіз свідчить про існування реальних загроз інформаційній безпеці України [8, с. 158].

Висновки. Підсумовуючи необхідно зазначити, що взаємозв'язок інформаційної безпеки та кримінально-правової політики розкриває багатогранну проблему, тісно пов'язану з національною безпекою та захистом інтересів як окремих громадян, так і держави в цілому. В умовах тривалого конфлікту та воєнного стану, інформаційна безпека перестає бути лише технічним питанням; вона стає ключовим елементом загальної системи оборони країни та запорукою її життєво важливих інтересів.

Отже, інформаційна безпека відіграє вирішальну превентивну роль у запобіганні шкоді, що завдається людині через упереджене інформування, маніпуляції та інші форми впливу на свідомість і поведінку громадян. Вона активно сприяє зміцненню стійкості суспільства до інформаційних атак, допомагаючи вчасно виявляти та ефективно боротися з дезінформацією й іншими інформаційними загрозами. Зрештою, надійний підхід до інформаційної безпеки, доповнений проактивною кримінально-правовою політикою, є незамінним для формування стійкого цифрового суспільства, яке ефективно запобігає злочинності проти людини та оберігає її права в дедалі складнішому та взаємопов'язаному світі. Тому формування стійкого цифрового суспільства – це комплексний процес, який вимагає постійної адаптації та вдосконалення. Провідна превентивна роль інформаційної безпеки та кримінально-правової політики полягає у створенні багатошарової системи захисту, яка не лише реагує на кримінальні правопорушення, але й активно запобігає їм, знижуючи вразливості людини та підвищуючи її безпеку в дедалі більш цифровізованому світі. Це вимагає міждисциплінарного підходу, постійного моніторингу кіберзагроз та тісної співпраці всіх зацікавлених сторін.

ЛІТЕРАТУРА:

1. Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування: офіційний сайт Офісу Генерального прокурора. URL: https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2

2. Почепцов Г. Г. Теория комунікації. Київ : Ваклер, 2001. 656 с.

3. Протидія когнітивній війні: інформованість і стійкість. НАТО Ревю. 20.05.2021. URL: https://www.nato.int/docu/review/uk/articles/2021/05/20/ protid ya-kogntivnj-vjn- nformovanst-stjkst/index.html

4. Jānis Bērziņš. Russia's New Generation Warfare in Ukraine: *Implications for Latvian Defense Policy. Policy Paper*. April 2014. № 02. P. 5–13.

5. Про рішення ради національної безпеки і оборони України від 15 жовтня 2021 року «Про стратегію інформаційної безпеки»: Указ Президента України від 28 грудня 2022 року № 685/2021 / Офіційний веб-портал Президента України. URL: https://zakon.rada.gov.ua/laws/show/685/2021#n33

6. Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації: Рішення РНБО від 29 грудня 2016 року. Офіційний сайт Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/n0015525-16#Text

7. Бондаренко В. О. Інформаційна безпека сучасної держави: концептуальні роздуми. URL: http://www.crime-research.iatp.org.ua/library/strateg.htm

8. Данільян О. Г., Дзьобань О. П., Панов М. І. Національна безпека України: структура та напрямки реалізації : навч. посіб. Х. : Фоліо, 2002. 285 с.