УДК 343.9:094 (477)
DOI https://doi.org/10.32782/2408-9257-2023-6-45

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

СУТНІСТЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЯК ПРАВОВОГО ЯВИЩА У НАЦІОНАЛЬНОМУ ТА МІЖНАРОДНОМУ ПРОСТОРІ

THE ESSENCE OF INFORMATION SECURITY AS A LEGAL PHENOMENON IN THE NATIONAL AND INTERNATIONAL SPACE

В умовах сучасних глобалізаційних загроз, у статті акцентовано увагу на необхідності адаптації національної політики інформаційної безпеки до викликів в цифровому просторі. Інформаційна безпека стає ключовою зоною для національної політики України, спрямованої на захист важливих інтересів та основоположних прав і свобод громадян. Координація між силами безпеки, владними інстанціями, місцевим самоврядуванням та громадськістю є вирішальною для протидії реальним і потенційним загрозам, що становлять виклик у сучасному глобалізованому світі. Висвітлено необхідність правильної конструкції правової системи, здатної ефективно реагувати та протидіяти злочинності у сфері цифрових технологій, на основі глибокого розуміння функціонування інформаційної безпеки.

У статті аргументовано, що створення прогресивного правового поля є основою для забезпечення інформаційної безпеки, яке включає в себе нормативну регламентацію, спрямовану на управління цифровою інформацією та захист комунікаційних систем. Реалізація стратегічних напрямів інформаційної безпеки України, розглянутих у статті, вимагає від держави здійснення комплексного підходу до боротьби з дезінформацією, розвитку медіаграмотності серед громадян, захисту особистих даних, забезпечення свободи слова, а також підтримки зв'язку з громадянами на тимчасово окупованих територіях.

Виділено важливість збалансованості між захистом інформації та захистом конституційних прав і свобод особи, в контексті вибудови ефективної системи інформаційного суспільства, яка підвищує рівень культури діалогу та протидії дезінформації. Зазначено, що для досягнення загально-попереджувальної мети стратегія інформаційної безпеки має включати інноваційні підходи до кібербезпеки, особливо у відношенні захисту критичної інфраструктури та особистих даних громадян у відповідності до міжнародних стандартів, зокрема GDPR.

Доведено що, протидія актуальним викликам у сфері інформаційної безпеки національного та глобального характеру залежить від розвитку національних та міжнародних стратегій кібербезпеки, а також від залучення до партнерства країн, які поділяють однакові цілі захисту даних та приватності в цифровому середовищі, підкреслюючи необхідність постійного технічного і технологічного вдосконалення.

Ключові слова: *національна безпека, міжнародні стандарти, цифрове середовище, стратегія інформаційної безпеки, глобалізаційні загрози, медіаграмотність, кіберзлочинність, протидія дезінформації.*

In the context of contemporary globalization threats, the article emphasizes the necessity to adapt the national policy of information security to the challenges in the digital space. Information security becomes a key area for Ukraine's national policy aimed at protecting vital interests, and the fundamental rights and freedoms of citizens. Coordination between security forces, authorities, local governance, and the public is crucial for countering actual and potential threats that challenge the modern globalized world. The article highlights the necessity of properly designing the legal system, capable of effectively responding and combating criminality in the field of digital technologies, based on a deep understanding of the function of information security.

The article argues that the creation of a progressive legal field is the basis for ensuring information security, which includes regulatory regulation aimed at managing digital information and protecting communication systems. The implementation of Ukraine's strategic directions of information security discussed in the article requires a comprehensive approach by the state to combat disinformation, develop media literacy among citizens, protect personal data, ensure freedom of speech, and maintain connection with citizens in temporarily occupied territories.

The importance of finding a balance between information protection and the protection of constitutional rights and freedoms of individuals is highlighted in the context of developing an effective information society system, which enhances the culture of dialogue and counteracts disinformation. It is noted that to achieve the general preventive goal, the strategy of information security should include innovative approaches to cybersecurity, especially regarding the protection of critical infrastructure and personal data of citizens in accordance with international standards, particularly the GDPR.

It is proven that countering the current challenges in the field of information security of national and global nature depends on the development of national and international cybersecurity strategies, as well as the involvement of countries that share similar data protection and privacy goals in the digital environment, underscoring the necessity for continuous technical and technological refinement.

Key words: *national security, international standards, digital environment, information security strategy, globalization threats, media literacy, cybercrime, countering disinformation.*

Постановка проблеми. Сьогодні важливим пріоритетом національної політики у галузі інформаційної безпеки та запобіганні злочинності у сфері цифрових технологій є захист важливих інтересів, прав і свобод людини і громадянина. Спільні заходи сил безпеки, інших органів влади, місцевого самоврядування та громадськості забезпечують захист національних інтересів від реальних і потенційних загроз, що виникають у глобалізаційному світі. Тому, надзвичайно актуальною в умовах глобалізації та стрімкого розвитку цифрових технологій є проблема забезпечення інформаційної безпеки у державі. Впровадження інноваційних технологій у сферу безпеки є показником рівня розвитку країни і фактором її високого економічного та політичного рівня, спрямованим на забезпечення національних інтересів. Проте технологічний прогрес має й негативні аспекти, що визначають залежність держави і особи від системи комунікативних, енергетичних, біотехнологічних, хімічних, транспортних та фінансових послуг.

Вивчення причин і факторів, які приводять до загроз і ризиків для інформаційної безпеки країни і посилюють зростання злочинності, стає пріоритетним завданням, особливо у контексті глобалізаційних ризиків та збільшенню кількості масштабних кібератак. Оскільки злочинність може призвести до серйозних соціальних, особистісних та технічних наслідків, існує нагальна потреба у розробці і впровадженні інноваційних і ефективних стратегій для запобігання злочинам і реагування на нові форми кримінальної активності. У контексті цього, представляє науковий інтерес наукове дослідження У. Ільницької, яка представила власну характеристику заходів подолання ризиків та загроз що становлять небезпеку політичного, економічного розвитку і функціонування держави у межах європейської та євроатлантичної структури [1, с. 28].

Незважаючи на існуюче законодавство та нормативні акти, які призначені для захисту інформації в цифровому середовищі, сучасне суспільство стикається зі зростанням кіберзлочинності та інших інформаційних загроз. Це викликає необхідність переоцінки ефективності інформаційної безпеки як правового явища і її впливу на протидію кримінальним проявам у сфері цифрових технологій. Основна проблема полягає у відстеженні динаміки та адаптації правової системи до постійно змінюваних методів здійснення злочинів, а також у забезпеченні дотримання балансу між захистом інформації та забезпеченням прав та свобод особистості. Розробка нових, більш прогресивних правових інструментів і механізмів для попередження та реагування на інформаційні злочини вимагає глибокого розуміння сутності інформаційної безпеки та її функціонування в цифровому просторі

Стан опрацювання проблематики. Поняттю, засадам, складовим інформаційної безпеки її впливу на рівень злочинності у сфері цифрових технологій та стану запобігання злочинності у цій сфері присвячені наукові праці багатьох вчених. Окремі аспекти вказаної сфері були об’єктом дослідження таких вітчизняних та зарубіжних вчених, як Д. Азаров, І. Березовська, Н. Бендовський, Д. Бірюков, О. Бодунов, О. Бугера, В. Дрьомін, У. Ільницька, М. Карчевський. О. Колб, В. Ліпкан, В. Мисливий, В. Новицький, М. Присяжнюк, В. Топчий, Н. Юзікова, Т. Яцика J. Lembke та ін.

Метою статті є дослідження правового регулювання забезпечення інформаційної безпеки в Україні з метою ефективної протидії злочинності, пов’язаної з цифровими технологіями. Це передбачає аналіз правових норм і положень, що регулюють захист інформації в цифровому просторі, та оцінку їхньої дієздатності в контексті превентивної боротьби з кіберзлочинністю та іншими формами злочинів у сфері цифрових технологій.

Виклад основного матеріалу. Інформаційна безпека охоплює широкий аспект захисту незалежно від форми, в якій зберігається чи обробляється інформація. Вона включає

захист даних, процесів, інформаційних систем і мереж від незаконного доступу, використання, розкриття, розголошення, модифікації чи знищення. Принципи інформаційної безпеки забезпечують конфіденційність, цілісність і доступність всієї значимої інформації – будь то друкована, усна або електронна.

Відповідно до Стратегії інформаційної безпеки до 2025 року, інформаційна безпека України – це невід'ємна частина загальної національної безпеки, яка визначається захищеністю державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших ключових інтересів людини, суспільства і держави. Це також гарантує права та свободи громадян щодо збирання, зберігання, використання та поширення інформації, а також доступ до достовірної та об'єктивної інформації. Забезпечується ефективна система захисту від негативних інформаційних впливів, таких як координоване поширення недостовірної інформації, деструктивна пропаганда та інші інформаційні операції, а також запобігання несанкціонованому розповсюдженню, використанню та порушенню інтегритету обмеженої інформації [2].

Інформаційна безпека є правовим явищем, оскільки вона має чітке законодавче підґрунтя та регулюється низкою правових актів на національному та міжнародному рівнях. Основи інформаційної безпеки як правового явища включають відповідне правове регулювання, засади, зобов'язання та відповідальність, інституційні механізми та міжнародні стандарти.

Правову основу інформаційної безпеки становлять норми що стосуються цифрового середовища, які вказують на форми і методи захисту даних, управління цифровою інформацією та комунікаційними системами. Так, у ст. 17 Конституції України проголошено, що забезпечення інформаційної безпеки України є однією з найважливіших функцій держави справою всього Українського народу» [3]. Продовженням є визначення поточних та прогнозованих загроз національній безпеці та національним інтересам України з урахуванням зовнішньополітичних та внутрішніх умов, визначених у Стратегії національної безпеки України [4]. Детально питання основ національної безпеки України було розглянуто у дослідженні професора О.Г. Колба [5]

Наступним кроком нормативного закріплення сутності, мети, завдань, загроз заходів захисту інформаційної безпеки було Рішення Ради національної безпеки і оборони України від 29 грудня 2016 року, де було схвалено Доктрину інформаційної безпеки України (далі – Доктрина), яка стала стратегічним документом щодо окреслення концептуальних засад державної політики у сфері інформаційної безпеки [6]. Основні положення Доктрини включали головну мету та стратегічні завдання державної інформаційної політики; основні принципи інформаційної безпеки, серед яких цілісність, автономія, суверенітет у інформаційному просторі, врахування демократичних цінностей і прав людини; характеристику потенційних внутрішніх та зовнішніх загроз національній інформаційній безпеці, включаючи дезінформацію, кібератаки та втручання в інформаційний простір; зазначення кроків та механізмів реагування на виклики і загрози інформаційній безпеці, у тому числі, наголос зроблено на необхідності співпраці з іноземними державами та міжнародними організаціями у сфері інформаційної безпеки; визначені ролі та обов'язки різних органів державної влади, об'єднань громадян та бізнесу у реалізації інформаційної політики.

Після втрати чинності Доктрини, рішенням Ради національної безпеки і оборони України від 15 жовтня 2021 року приймається Стратегія інформаційної безпеки до 2025 року (далі – Стратегія). Стратегія містить визначення загроз, засобів захисту, механізмів виявлення та запобігання злочинам у сфері інформаційної безпеки [2]. Основними напрямами реалізації Стратегії є протидія дезінформації, розвиток медіакультури та медіаграмотності. Важливими аспектами також є захист особистих даних та культури вільного вираження поглядів, підтримка зв'язку з громадянами на тимчасово окупованих територіях та розвиток стратегічних комунікацій. Крім цього, стратегія передбачає створення ефективної системи інформаційного суспільства та підвищення рівня культури діалогу. Також, вона охоплює положення про кібербезпеку, захист від дезінформації, захист критичної інфраструктури та інші аспекти, спрямовані на міцний захист національних інтересів України. Як і в Доктрині,

у Стратегії визначено сутність, засади, механізми інформаційної безпеки, наголошено на доцільності міжнародної співпраці та імплементації міжнародних угод та директив, таких як Конвенція про кіберзлочинність, GDPR (General Data Protection Regulation), що формують міжнародно-правову основу інформаційної безпеки. Поряд з цим, у Стратегії більш чітко ніж у Доктрині визначені глобальні та національні виклики та загрози, з урахуванням яких сформовані напрями забезпечення інформаційної безпеки України у стійкісті та взаємодії, для досягнення яких необхідним є виконання семи стратегічних цілей та завдань. Визначено механізми захисту інформаційної безпеки України, які включають координацію діяльності різних органів виконавчої влади, нормативно-правове регулювання, моніторинг і прогнозування загроз, популяризацію та захист інтересів країни.

Інформаційна безпека в правовому контексті охороняє також основоположні права людини, зокрема право на приватність та конфіденційність, які є важливою частиною прав людини. Тому правові аспекти інформаційної безпеки є значущим компонентом в структурі сучасного права і державної політики.

При розробці та впровадженні стратегії інформаційної безпеки, важливо враховувати міжнародні стандарти та вимоги GDPR. Це дозволить забезпечити відповідність з вимогами захисту персональних даних та конфіденційності, що є ключовими компонентами ефективної стратегії інформаційної безпеки. Загальний регламент з охорони даних (GDPR) стандартизує та посилює захист персональних даних у Європейському Союзі (ЄС) та Європейському Економічному Просторі (ЄЕП). GDPR набрав чинності 25 травня 2018 року і має на меті забезпечення більш високого рівня захисту особистих даних громадян ЄС, а також спрощення регулювання обробки та передачі цих даних. Важливі аспекти GDPR включають у себе права осіб на доступ до власних даних, право на забуття (право вимагати видалення своїх персональних даних), обмеження обробки даних, право на перенос даних та обов'язки стосовно захисту даних для суб'єктів обробки даних. GDPR також накладає обов'язки на організації, які збирають та обробляють дані громадян ЄС, що включають у себе вимоги до забезпечення безпеки даних, повідомлення про порушення безпеки даних та виконання аудитів щодо відповідності. Загальний регламент з охорони даних (GDPR) становить ключовий компонент законодавства у сфері захисту особистих даних та вимагає відповідності від організацій, які операційно займаються обробкою даних громадян ЄС. Імплементація Загального регламенту з охорони даних GDPR в Україні не тільки підвищить рівень захисту даних, але й позитивно вплине на міжнародну торгівлю та довіру до українських компаній, що співпрацюють з європейським ринком. GDPR сприяє підвищенню міжнародного співробітництва з Україною при розслідуванні та переслідуванні кіберзлочинів, оскільки вимагає від компаній співпрацювати з наглядовими органами. Основні положення Загального регламенту з охорони даних, які можна запровадити до національної правової платформи, сприятимуть підвищенню відповідальності онлайн-сервісів та цифрових платформ, зміцненню захисту персональних даних їх користувачів і забезпеченню системної основи для боротьби з кіберзлочинністю.

Стратегія інформаційної безпеки України передбачає активне залучення до міжнародного співробітництва в сфері кібербезпеки та обміну досвідом з іншими країнами. Україна прагне підтримувати спільні стандарти та процедури для захисту інформації, а також взаємно надавати допомогу в разі кібератак чи інших загроз, які можуть виникнути. Міжнародне співробітництво у сфері захисту цифрового середовища відіграє ключову роль у зміцненні національної та глобальної інформаційної безпеки.

Актуальні виклики сьогодення та глобалізаційні ризики обумовлюють необхідність всебічного захисту цифрового середовища від протиправних, злочинних посягань. Слушно зазначає професор Н.С. Юзікова, що незадовільний стан інформаційної безпеки, розміщення у цифровому середовищі спотвореної, провокаційної інформації або дезінформації про політичні, економічні, соціальні процеси, що відбуваються в Україні, негативно впливає на суспільну свідомість громадян України; детермінує зміни у поведінці та комунікації особистості; сприяє формуванню деформованих моральних установок, девіантної пове-

дінки та асоціального способу життя; продукує віктимну, суїцидальну поведінку [7; 8]. А враховуючи швидкі темпи цифровізації та постійну трансформацію глобальний ризиків, питання розробки ефективних заходів у протидії злочинності і забезпеченні інформаційної безпеки є доцільними і актуальними.

Серед актуальних ризиків у сфері інформаційної безпеки можна виокремити кібератаки, які включають фішинг, віруси, програми-вимагачі та інші загрози, які можуть порушити інформаційну безпеку; шпигунське програмне забезпечення, що включає програми, які збирають інформацію без відома користувача; витоки даних: несанкціонована публікація або розкриття конфіденційної інформації.

У науковій роботі «Стратегічні засади забезпечення інформаційної безпеки в сучасних умовах» В.Я. Новицький при дослідженні інформаційної сфери виділив сучасні загрози безпеки України. Вчений до актуальних загроз інформаційній безпеці України відносить: повноформатну експансивну інформаційну політику РФ; низький рівень медійної грамотності населення; збільшення кількості глобальних дезінформаційних кампаній; інформаційне домінування РФ на тимчасово окупованих територіях; використання технологій маніпулювання свідомістю пересічних громадян щодо наслідків вступу України в НАТО та ЄС тощо [9, с. 112]. Характеризуючи національну безпеку України М.Т. Гаврильців представила характеристику факторів, які обумовлюють загрози у сфері інформаційної безпеки, що мають системний характер, і впливають на різні сфери суспільного життя людини і нормальний розвиток держави [10, с. 200]. Ці праці становлять наукове підґрунтя для захисту інформаційної безпеки як правового явища.

Таким чином, актуальні виклики в сфері інформаційної безпеки національного та глобального характеру включають кіберзагрози, дезінформацію, крадіжку даних та порушення приватності, кібертероризм і технологічні атаки. Для протидії цим викликам необхідно розвивати міжнародні та національні стратегії кібербезпеки, підвищувати кіберзахист, зміцнювати правову базу для захисту даних, розвивати міжнародне співробітництво та вдосконалювати технічні та технологічні засоби для виявлення та протидії кіберзагрозам.

Проаналізувавши різні аспекти сутності, засад, загроз інформаційної безпеки, можна сформувати прозору картину того, як правове регулювання інформаційної безпеки впливає на запобігання злочинності у сфері цифрових технологій, та визначити, які правові інструменти є найбільш ефективними в цьому контексті та окреслити очікувані результати у цій сфері. Серед них можна визначити:

• Захищений інформаційний простір України, що включає в себе запобігання кіберзагрозам, захист критичної інфраструктури та ефективну боротьбу з кіберзлочинністю.

• Ефективне функціонування системи стратегічних комунікацій, спрямоване на підвищення рівня інформованості громадян, підтримку позитивного іміджу держави у світі та забезпечення внутрішньої стабільності.

• Ефективну протидію поширенню незаконного контенту, включаючи механізми фільтрації та контролю електронних медіа.

• Забезпечення сталого процесу інформаційної реінтеграції громадян України на тимчасово окупованих територіях, включаючи розширення доступу до українського телерадіомовлення та інформаційних ресурсів.

• Суттєве підвищення рівня медіакультури та медіаграмотності населення, сприяючи критичному осмисленню інформації та уникненню впливу дезінформації.

• Дотримання конституційних прав особи на вільне вираження своїх поглядів і переконань, а також захист приватного життя, що сприятиме збереженню свободи слова та приватності.

• Захист прав журналістів та створення умов для незалежної журналістики, що відіграє ключову роль у підтримці інформаційної свободи та прозорості.

• Формування української громадянської ідентичності, що сприятиме утвердженню загальнонаціональної єдності та патріотизму.

Правове регулювання інформаційної безпеки впливає на запобігання злочинності у сфері цифрових технологій шляхом встановлення правил, вимог та відповідальності за порушення цих правил. Ефективне правове регулювання може включати законодавчі акти, що стосуються захисту особистих даних, кібербезпеки, кіберзлочинності, електронних підписів та інших аспектів цифрових технологій.

Найбільш ефективні правові інструменти в цьому контексті можуть включати в себе чіткі норми щодо захисту особистих даних, визначення кіберзлочинності та визначення відповідальності за її скоєння, удосконалення процедур електронного підпису та надання повноважень для уповноваженим структурам для боротьби з кіберзлочинністю та забезпечення інформаційної безпеки. Ці інструменти становлять важливу основу для регулювання сфери цифрових технологій та сприяють запобіганню злочинності в цьому контексті.

Висновки. Розгляд сутності інформаційної безпеки як правового явища у запобіганні злочинності у сфері цифрових технологій дає підстави для наступних висновків. Правові норми є фундаментальними у забезпеченні інформаційної безпеки. Належне законодавство формує основу для протидії кіберзагрозам, забезпечення конфіденційності, цілісності та доступності інформації. Національне законодавство часто не в змозі встигати за стрімкими змінами в технологічному секторі, що вимагає постійного оновлення та доповнення правових механізмів запобігання і реагування на протиправні, злочинні дії.

Важливо наголосити, що гармонізація національного законодавства з міжнародними стандартами інформаційної безпеки сприяє подоланню трансграничної кіберзлочинності. При цьому, доцільно забезпечити баланс між інформаційною безпекою та захистом громадянських свобод, особливо в питаннях приватності і доступу до інформації у контексті дотримання Загального регламенту з охорони даних (GDPR). Тому розробка і впровадження інноваційних технологічних та програмних рішень може значно підвищити рівень інформаційної безпеки та спроможність правової системи адаптуватися до нових викликів. Цьому безперечно буде сприяти крос-дисциплінарний підхід, що полягає у необхідності залучення експертів різних галузей для створення ефективних правових, технічних і освітніх стратегій забезпечення інформаційної безпеки в Україні.

Аналіз правового регулювання інформаційної безпеки в Україні становить підґрунтя для висновку, що законодавство є критичним для захисту цифрового простору від кіберзагроз та забезпечення конфіденційності та доступності інформації. Гармонізація національних норм до міжнародних стандартаів, особливо GDPR, зможе зміцнити транскордонну кібербезпеку і водночас забезпечити права і свободи громадян. Розробка та імплементація інноваційних рішень разом із кросдисциплінарною співпрацею експертів зможе значно підвищити рівень захисту інформаційної безпеки та відповіді на новітні виклики. Очікувані результати охоплюють забезпечення інформаційної свободи, приватності та підтримання сталого доступу до інформаційних ресурсів, що стане основою для формування суспільної єдності та сприятиме ефективній боротьбі з дезінформацією та кіберзлочинністю на національному та міжнародному рівні.

ЛІТЕРАТУРА:

1. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози. *Humanitarian vision*. 2016. Vol. 2, Num. 1. С. 27–32.

2. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» : Указ Президента України від 28 грудня 2021 р. № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#n7

3. Конституція України. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text

4. Про рішення Ради національної безпеки і оборони України «Про Стратегію національної безпеки України» : Указ Президента України від 14 вересня 2020 року. URL: https://www.president.gov.ua/documents/3922020-35037

5. Колб О. Г., Бендовський Н. Г. Про деякі напрями діяльності, що стосується національної безпеки України. *Держава та регіони* : науково-виробничий журнал. *Серія: Право.* 2021. № 2 (72). С. 82–87.

6. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» : Указ Президента України від 25 лютого 2017 р.№ 47/2017 https://zakon.rada.gov.ua/laws/show/47/2017#Text

7. Юзікова Н.С. Інформаційна безпека у системі заходів запобігання кримінальним правопорушенням у сфері інформаційних технологій: досвід країн ЄС та США. *Аналітично-порівняльне правознавство.* 2023. № 5. С. 506–512. https://app-journal.in.ua/wp-content/uploads/2023/11/93.pdf

8. Yuzikova N., Khomiachenko S., Korniakova T., Chasova. T. (2021). Moral and psychological features of the motivational sphere of juveniles who commit crimes: risk assessment of determining communication. *European Journal of Sustainable Development.* Vol. 10, N 1, P. 123–135. Doi 10.14207 /ejsd. 2021.v10n1p123/URL: https://ecsdev.org/ojs/index.php/ejsd/issue/view/42

9. Новицький В.Я. Стратегічні засади забезпечення інформаційної безпеки в сучасних умовах. *Інформація і право*. 2022. Вип. 1 (40). С. 111–118.

10. Гаврильців М.Т. Інформаційна безпека держави в системі національної безпеки України. *Юридичний науковий електронний журнал.* 2020. № 2. С. 200–203.