ISSN 2072-8670 (Print) **НАУКА І ПРАВООХОРОНА**
NAUKA I PRAVOOKHORONA
DOI (Issue): https://doi.org/10.36486/np.2023.4(62) **Issue 4(62) 2023**

ІНФОРМАЦІЙНЕ ПРАВО. ПРАВО ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

УДК 340:004.056:316.32

Биков Олександр Миколайович,
доктор юридичних наук, професор,
професор кафедри теорії та історії держави і права
Університету економіки та права «КРОК»,
м. Київ, Україна
ORCID ID 0000-0003-4965-696X

ІНФОРМАЦІЙНА БЕЗПЕКА: ПРАВОВИЙ ТА КУЛЬТУРОЛОГІЧНИЙ ВИМІРИ

У статті подано перелік рекомендацій щодо забезпечення інформаційної безпеки. Пропонується налагодження ефективної міжнародної співпраці (підтримки необхідних договірних відносин, проведення дипломатичної роботи, налагодження співпраці на рівні окремих спеціалістів з кібербезпеки), вдосконалення роботи спеціальних підрозділів та встановлення додаткового контролю за кваліфікацією працівників кіберполіції, що дозволить збільшити ефективність карного розшуку кіберзлочинців. Наголошено на важливості боротьби з пропагандою та дезінформацією, перегляду фінансових механізмів реалізації стратегії із забезпечення інформаційної безпеки.

Ключові слова: *інформаційна безпека, IT-право, інформаційна культура, кібербезпека, цифрова грамотність, інформаційно-медійна грамотність.*

Кіберпростір ставить перед урядами нові виклики безпеці. Сучасний світ надзвичайно залежить від інформаційних технологій, і захист оцифрованих даних від кібератак постає як складне завдання. Щоразу більше людей, компаній і державних організацій по всьому світу стають жертвами кібератак, у тому числі через недосконаліть технологій стільникового зв'язку (GSM, UMTS, LTE тощо). Почастішали злочини в інформаційній сфері, які мають військові та політичні цілі.

Невисока вартість доступу до інтернет-ресурсів, анонімність, невизначеність загрозливих географічних зон, відсутність достатньої публічної прозорості в інформаційному середовищі призвели до появи численної кількості злочинців по всьому світу. Терористичні та інші організовані групи, окремі особи, постійно створюють нові загрози інформаційній безпеці, такі як кіберзлочинність, кібервійни, кібертероризм і кібершпигунство, соціальна інженерія тощо.

Важливо розглядати основи інформаційної безпеки як у правовому, так і в культурологічному сенсі через співвідношення її з інформаційною культурою суспільства,

DOI (Article): https://doi.org/10.36486/np.2023.4(62).21

інфомедійною та цифровою (дигітальною) грамотністю людини, позаяк у сучасному світі, де доступ до інформації надзвичайно широкий, важливо вміти відфільтровувати, оцінювати та використовувати інформацію з користю для себе, суспільства та держави.

З'ясування проблеми інформаційної безпеки складне та багатоаспектне, адже будь-які міжгалузеві наукові дослідження обтяжені необхідністю залучення до роботи фахівців з різних галузей наукових знань, а якість роботи залежать від якості синтезу одержаних результатів. Окремі питання, які стосуються теоретико-правових основ інформаційної безпеки досліджують такі відомі науковці, як Ю. Битяк, Н. Бортник, І. Гриценко, О. Дзьобань, О. Данильян, Л. Кисіль, О. Харитонова та інші. У юридичній літературі знаходимо праці, які торкаються як суто правових, так і аксіологічних аспектів інформаційної безпеки. У цьому сенсі є пізнавальними роботи М. Баран, М. Дмитренка, О. Золотар, К. Захаренка та О. Хитрої. Відбувається розробка так званої «інформаційної гігієни». У науковому середовищі її ідею розвивають О. Тихомиров, Ж. Денисюк та О. Яковлев. Цікавий розвиток філософського уявлення про інформаційну безпеку представлений працями П. Квіткіна, А. Романової, І. Дятлової, Л. Петрової та багатьох інших дослідників. Водночас вважаємо, що дослідження інформаційної безпеки на межі правового та культурологічного зрізів є недостатнім, що власне скеровує нас до означеної проблематики.

Метою статті є дослідження інформаційної безпеки як правового та соціокультурного явища, вказати на зв'язок інформаційної безпеки та інформаційної культури суспільства, обґрунтувати логічний взаємозв'язок між інформаційними ризиками та соціальними наслідками цифрової необізнаності громадян.

Безпека – явище соціокультурне. Вона передбачає стан захищеності людини, родини, цілого етносу, народу чи держави, разом з їхніми традиціями, звичаями, правами, укладом життя та цінностями. У сучасному глобалізованому світі, де інформація стала ключовим ресурсом, зростає значення інформаційної безпеки як засобу захисту інформації від несанкціонованого доступу, модифікації, маніпуляції чи знищення. Зростає потреба захисту кожної окремої людини, суспільства та держави від загроз, які постійно примножуються в інформаційному середовищі. За останнє десятиліття наслідки порушення інформаційної безпеки стають фінансово дорожчими і характеризуються більш руйнівними наслідками. Сьогодні більшість економічної, комерційної, культурної, соціальної та урядової діяльності та взаємодії країн на всіх рівнях, включаючи окремих осіб, неурядові організації та державні установи, здійснюються в кіберпросторі. Багато приватних компаній і державних організацій по всьому світу стикаються з проблемою кібератак і небезпекою технологій бездротового зв'язку [10, с. 1–3].

Поступово актуалізується проблематика розвитку інформаційного права, як у цілому, так і його безпекових аспектів зокрема. Питання інформаційної безпеки набувають неабиякої актуальності у світлі глобалізації та формування інформаційного суспільства, за нової інформаційної ери існування людства, і завдяки появі нового типу суспільних відносин, які пов'язані з обігом інформації. Перед наукою постає логічне питання, чому, коли суспільство досягло такого високого рівня інформаційного розвитку, який сьогодні, безумовно, характеризуємо як благо сучасної цивілізації, науковці з

усього світу б'ють на сполох через загрози, які з собою приносить оцифрований світ. Відповідь на це питання шукатимемо й ми в окремо означених аспектах нашої праці. Людина повинна мати свободу вибору інформації і вільний доступ до неї. «В інформаційній свободі, зазначають О. Дзьобань і О. Данильян, обов'язковою є така ознака, як наявність безлічі джерел інформації. Це означає, що для користування інформаційною свободою людина повинна мати доступ до кількох виробників, розповсюджувачів інформації, від яких вона може отримати різноманітну інформацію, узагальнивши яку, зробить вибір на користь певних дій, таким чином реалізуючи свою свободу [3, с. 11]. Як вірно зазначає О. Тихомиров, розвиток інформаційних технологій продовжує створювати дешеві і доступні засоби поширення інформації, через що інформаційний простір наповнюється контентом, який створює так званий шумовий ефект з небажаної і непотрібної для людини інформації. Частку корисної інформації в такому інформаційному шумі науковець характеризує як мізерну, акцентуючи на необхідності захисту людини від шкідливої інформації, вироблення спеціальних здібностей людини до інформаційної селективності, що буде одним з показників її інформаційної культури [7, с. 19].

Контроль держави за обігом інформації – це складний процес. Він має свої переваги та недоліки, які важливо враховувати в часі розробки політики інформаційної безпеки.

До переваг відносимо забезпечення безпеки даних, дотримання нормативних вимог. Насамперед йдеться про сектори, такі як фінанси, охорона здоров'я, ІТ, де є чітко прописані правила щодо обробки та зберігання інформації. Контроль, здійснюваний державою в інформаційній сфері допомагає ефективному управлінні ресурсами, зменшує ризики помилок, які можуть призвести до втрати даних або порушення їх цілісності.

Водночас здійснення належного контролю за обігом інформації затратний у часі та ресурсах, потребує постійних інвестицій в обладнання, програмне забезпечення та навчання персоналу. Суворий контроль може обмежувати швидкість доступу до інформації, а це зі свого боку уповільнює суспільні процеси. Надто жорсткий контроль за обігом інформації з боку держави посягає на основоположні права та свободи людини, такі як свобода слова, вільний доступ до інформації тощо. Враховуючи ці фактори, під час забезпечення інформаційної безпеки важливо збалансувати вплив держави на інформаційне середовище з потребами суспільства та держави, що в реальних умовах постає як надзвичайно складне завдання.

М. Баран у власному дослідженні адміністративно-правого забезпечення інформаційної безпеки в Україні приходить до висновків, що основними правовими механізмами забезпечення інформаційної безпеки є встановлення правових заборон та інших обмежень поширення певних видів негативної інформації, встановлення спеціальних правил обороту інформаційної продукції певних видів, закріплення обов'язків суб'єктів інформаційних правовідносин щодо забезпечення інформаційної безпеки, ідентифікація особи абонентів, користувачів мережі Інтернет та цифрових сервісів, видалення чи обмеження доступу до протиправного контенту, встановлення юридичної відповідаль-

ності за правопорушення, які посягають на інформаційну безпеку, правове закріплення заходів контрпропаганди, правове стимулювання розвитку цифрової грамотності та формування культури інформаційної безпеки [1, с. 21]. Авторка порушує важливе питання необхідності балансу державного регулювання і одночасного здійснення заходів щодо підвищення рівня інформаційної культури суспільства.

Проблема інформаційної безпеки осмислюється на трьох її визначальних напрямах, вважає К. Захаренко, – у світлі трансформації українського суспільства загалом та його політичної системи, в контексті глобалізації сучасного світу і у стратегічному баченні як перспектива розвитку політичних інститутів, відносин і процесів, що забезпечують демократичні зміни та безпеку України загалом. Рівень інформаційної безпеки, на думку науковця, визначає стан розвитку й інших компонентів національної безпеки України, а відповідні деструктивні інформаційні впливи сьогодні проявляються фактично у всіх сферах життя суспільства [4, с. 71].

Забезпечення інформаційної безпеки потребує забезпечення конфіденційності (інформація доступна лише авторизованим користувачам), цілісності та доступності (не змінені та не пошкоджені дані, інформація доступна для користувачів у відповідному місці та у належний час). Перевірка ідентичності (авторизація), управління правами доступу, забезпечення стабільності та неперервності роботи інформаційних систем, аудит (постійний моніторинг подій та виявлення потенційних загроз інформаційній безпеці), фізична безпека (захист інформаційної інфраструктури, обладнання), шифрування (використання криптографічних методів для захисту даних під час передачі та зберігання) та інші дії, – кроки, які необхідно здійснювати для захисту від інформаційних загроз. Наведені заходи є взаємозалежними і утворюють комплексний підхід щодо захисту інформації.

П. Квіткін, І. Дятлова та Л. Петрова, наголосивши на практичному значенні вирішення проблем інформаційної безпеки, також прописують кілька важливих аспектів. Інформаційну безпеку науковці визначають як одну із фундаментальних проблем буття людства, яка справляє безпосередній вплив на стан національної безпеки держави, стан міжнародних відносин, зростання ролі засобів збройного насильства в реалізації геополітичних стратегій і забезпеченні національних інтересів держав, загострення глобальних і виникнення новітніх загроз існуванню цивілізації, у процесі цивілізаційної ідентифікації народів. Вчені наголошують, що людина є носієм різноманітної інформації, витік якої за умов дестабілізації функціонування свідомості і психіки особистості в результаті інформаційних та інформаційно-психологічних впливів у сучасних умовах справляє суттєвий вплив як на стан національної безпеки, так і на міжнародний авторитет держави, процеси суспільної життєдіяльності [5, с. 55]. Для нас важлива також думка, що інформаційна безпека особистості є інтегральною якістю особистості, яка формується в процесі цілеспрямованої діяльності і виявляється у здатності зберігати цілісність і сталість світоглядних позицій, системи цінностей і ціннісних орієнтацій, переконань і життєвих стратегій в умовах інформаційних та інформаційно-психологічних впливів, трансформації системи суспільних відносин і соціокультурних основ буття соціуму.

Інформація, проникаючи в усі сфери суспільного життя і розподіляючись відповідно до соціальних маркерів і матеріальних умов, вважає О. Хитра, створює умови інформаційної нерівності, яка зі свого боку є найкоротшим шляхом до порушення умов інформаційної безпеки і множення різних інформаційних ризиків, зокрема ризиків, пов'язаних із небезпечним впливом різних інформаційних ресурсів, які можуть мати маніпулятивний характер, з кіберзлочинністю, вторгненням у приватний інформаційний простір особистості і порушенням інформаційних прав людини [8, с. 152]. Інформаційна безпека можлива лише за умови постійного моніторингу з боку спеціальних органів державної влади за обігом інформації в режимі реального часу і потребує залучення найкращих фахівців та на основі новітніх ІТ-даних і програм.

Процес забезпечення інформаційної безпеки фінансово затратний, адже вимагає роботи великої кількості людей. Індійська дослідниця Г. Діптібен вважає, що у науковій та практичній літературі є велика кількість вказівок щодо забезпечення інформаційної безпеки. Авторка наголошує на тому, що хоча можливі й інші цікаві тактики, як-от стримування, обман, виявлення та своєчасна реакція, більшість досліджень зосереджено на тому, як запобігти загрозам безпеці за допомогою саме технологічних засобів протидії [9, с. 1–2]. Пояснити такий стан речей можна лише недостатньою розробкою механізму соціальної протидії кіберзлочинам та іншим порушенням в інформаційній сфері.

У сучасному світі реальність може бути представлена за допомогою теоретично необмеженої кількості просторів, що описують відповідні сфери об'єктивної реальності. Одним із них є інформаційний простір, а виявлення його специфіки нині – одна з найактуальніших проблем соціально-культурного значення, яка породжує питання формування інформаційної культури суспільства. Ж. Денисюк та О. Яковлев наголошують на тому, що вже не можна говорити про культуру як про щось, що є відірване від сучасних засобів комунікації, цифрових засобів та способів збирання, обробки, створення інформації. Технічна складова стала невід'ємною складовою інформаційної культури і оволодіння нею є задачею для тих, хто прагне до високого рівня розвитку особистості. Інформаційна ж культура стає до певної міри маркером, мірою розвиненості навичок індивіда в інформаційній сфері [2, с. 19].

Для того, щоб захиститися від загроз, користувачам Інтернету важливо бути достатньо обізнаними, не відкривати підозрілі посилання або вкладення у електронних листах, перевіряти адреси вебсайтів перед введенням будь-яких особистих даних, використовувати надійне антивірусне програмне забезпечення та регулярно слідувати правилам кібербезпеки.

Урядам країн необхідно організовувати та постійно проводити з громадянами різних вікових груп навчання з кібербезпеки та «інформаційної гігієни», що дозволить значно зменшити ризики інформаційної безпеки і, відповідно, кількість постраждалих осіб.

Про інфомедійну грамотність людини сьогодні найчастіше йдеться в контексті налагодження ефективності навчального процесу, в аспекті боротьби з пропагандою, різного роду фейками та дезінформацією. Інформаційно-медійна грамотність потребує наявності психологічного елемента – критичного мислення людини під час пошуку,

відбору та використання тієї чи іншої інформації. Безумовно, така грамотність є нічим іншим як компонентою індивідуальної культури людини у XXI столітті.

Цифрова грамотність (також відома як цифрова компетентність або дигітальна грамотність) – це набір знань, навичок і умінь, необхідних для ефективного використання цифрових технологій і ресурсів у сучасному інформаційному суспільстві. Основні аспекти цифрової (дигітальної) грамотності включають розуміння базових принципів роботи комп'ютера, операційних систем, програмного забезпечення, вміння роботи з файлами і папками, шукати інформацію в мережі Інтернет, використовувати пошукові системи, оцінювати достовірність інформації з онлайн-джерел, розуміння основних загроз в інтернеті (вірусів, методів шахраювання, кібербулінгу тощо), вміння захищати свої особисті дані, створювати надійні паролі, користуватися антивірусними програмами тощо. Цифрова грамотність включає уміння особи використовувати цифрові інструменти для комунікації, такі як електронна пошта та соціальні мережі, працювати з документами у Microsoft Office та на Google Disk, обробляти зображення та відеофайли тощо.

Цифрова грамотність, на нашу думку, є важливим і невідмінним технічним елементом інформаційної культури людини. Її значення зростає у світі сучасних інформаційних технологій, адже такі технології є необхідними для багатьох аспектів життя сучасної людини, включаючи освіту, роботу, комунікації чи розваги. Набуття цифрових умінь та навичок допомагає людям бути успішними і ефективними.

Інформаційну культуру як чинник, який впливає на забезпечення інформаційної безпеки, маємо розглядати в таких аспектах. По-перше, інформаційна культура може розглядатися як складова загальної культури індивіда. Таке вузьке розуміння дає нам уявлення про інформаційну культуру як про спосіб сучасної людини мислити внаслідок оволодіння нею певними навичками, розвитку спеціальних умінь у процесі здійснення інформаційно-інтелектуальної діяльності. Інформаційна культура особи є комплексом знань, навичок та умінь, цінностей, які дозволяють людині ефективно використовувати інформаційні ресурси, розуміти й аналізувати інформацію, а також свідомо та критично оцінювати її достовірність та значення.

До основних аспектів інформаційної культури особистості відносимо: знання про інформаційні технології (розуміння основних принципів роботи комп'ютерів, мережі Інтернет, програмного забезпечення, цифрових пристроїв тощо); навички з пошуку та обробки інформації: (уміння швидко знаходити важливу інформацію в мережі, використовуючи різні пошукові системи, ефективно фільтрувати та опрацьовувати знайдену інформацію); критичне мислення як здатність людини аналізувати інформацію з різних джерел, розрізняти конкретні факти від домислів, виявляти випадковість та підозрілість у джерелах інформації; етика інформаційного спілкування (включає розуміння правил поведінки в мережі Інтернет, захист персональних даних, уникнення кібербулінгу та інших негативних явищ в онлайн-середовищі, повагу до прав інших користувачів мережі); творчий підхід до використання інформації – вміння використовувати відібрану інформацію для розв'язання проблем у реальному житті, створення нових ідей, розвитку особистого та професійного потенціалу).

Особливої значущості набуває формування навичок протидії інформаційним загрозам, тим більше в умовах інформаційної війни, коли вони набувають агресивних форм. У цьому контексті важливим є розвиток критичного мислення особистості, що передбачає вміння аналізувати та оцінювати інформацію, робити самостійні висновки, протидіяти маніпуляціям, яким вона піддається дедалі більше. Критичність мислення є вагомою складовою технічних, політичних, правових заходів щодо забезпечення інформаційної безпеки [6, с. 8].

З правового погляду, для реалізації стратегій з інформаційної безпеки необхідні такі дії: вдосконалення на найвищому державному рівні стратегії з інформаційної безпеки та проведення жорсткого контролю за її дотриманням; налагодження ефективної міжнародної співпраці щодо забезпечення інформаційної безпеки (включає договірну, дипломатичну роботу, співпрацю спеціалістів з кібербезпеки тощо); ефективний карний розшук на території України та притягнення до юридичної відповідальності кіберзлочинців, відповідно до національного законодавства та укладених міжнародних договорів; вдосконалення роботи спеціальних підрозділів, як-от кіберполіція, проведення перевірки відповідності її штату займаним посадам, доукомплектування відповідних міжрегіональних підрозділів, де виникатиме така необхідність спеціалістами найвищої категорії; законодавче закріплення додаткового фінансування можливості залучення до боротьби із загрозами інформаційній безпеці необхідної кількості найкращих ІТ-спеціалістів приватного сектору, що дозволить створити паритетні умови у перехопленні кіберзлочинців на етапах підготовки та втручання в кібербезпеку.

Сучасний інформаційний світ є водночас великим досягненням і небезпекою. Держава має здійснювати постійний моніторинг інформаційного середовища, своєчасно виявляти та притягати до відповідальності осіб, які за допомогою інформаційних технологій, використовуючи медіа- та інтернет-ресурси, свідомо вчиняють протиправні дії, наприклад поширюють неправдиву інформацію, діють з метою розповсюдження ворожої пропаганди, фейків, здійснюють іншу діяльність, спрямовану проти прав та свобод людини і громадянина.

Інформаційна безпека особистості включає захист психіки і свідомості людини від небезпечних інформаційних впливів (маніпулювання свідомістю, дезінформування, спонукання до конфліктів з іншими особами, соціальними групами та державою). Необхідно підвищувати рівень теоретичної та практичної підготовки людини, за якого досягається захищеність її життєво важливих інтересів від інформаційних загроз.

Особливо важливою, на нашу думку, є: розробка відповідних навчальних програм з цифрової та інфомедійної грамотності, і відповідно, проведення навчань серед населення різних вікових груп; дотримання етики інформаційного спілкування; дотримання інформаційної гігієни та основних правил безпечної роботи з інформацією в мережі Інтернет. Насамперед це стосується нерозповсюдження неперевіреної інформації, нерозголошення своїх персональних даних, інформації про своє приватне життя тощо.

Потрібні дієві механізми заохочення населення до співпраці з державою щодо виявлення можливих загроз інформаційній безпеці, як-от створення гарячих ліній та окремих відділів на базі правоохоронних органів, які перевірятимуть одержану інформацію.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Баран М. В.* Адміністративно-правове забезпечення інформаційної безпеки в Україні: дис. … д-ра філософії за спеціальністю 081 «Право». Львів. держ. ун-т внутр. справ. Львів. 2022. 242 с. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/5076/1/baran_d.pdf. (дата звернення: 16.10.2023).

2. *Денисюк Ж. З., Яковлєв О. В.* Формування інформаційної культури суспільства в умовах цифровізації. Вісник Національної академії керівних кадрів культури і мистецтв. 2021. № 2. С. 18–22.

3. *Дзьобань О., Данильян О.* Права і свободи людини: інформаційний вимір. Вісник Національного юридичного університету імені Ярослава Мудрого. 2023. № 3 (58). Серія: філософія, філософія права, політологія, соціологія. С. 6–22.

4. З*ахаренко К. В.* Інституційний вимір інформаційної безпеки України: трансформаційні виклики, глобальні контексти, стратегічні орієнтири: дис. … д-ра політичних наук за спеціальністю 23.00.02 «Політичні інститути та процеси». Нац. пед. ун-т імені М. Драгоманова, Львів. нац. ун-т імені Івана Франка. Львів. 2021. 423 с. URL: https://lnu.edu.ua/wp-content/uploads/2021/04/dis_zakharenko.pdf (дата звернення: 16.10.2023).

5. *Квіткін П. В., Дятлова І. В., Петрова Л. О.* Інформаційна безпека особистості: теоретико-методологічний аналіз. Вісник Національного юридичного університету імені Ярослава Мудрого. 2021. № 4 (51). Серія: філософія, філософія права, політологія, соціологія. С. 46–62.

6. *Мельничук В. Горохова Л.* Критичне мислення як складова інформаційної безпеки. Вісник Львівського університету. 2022. Вип. 29. Серія: філософські науки. С. 7–13.

7. *Тихомиров О.* Ідея інформаційної гігієни в контексті інформаційної безпеки і захисту інформаційних прав людини. Науковий юридичний журнал «Правові новели». 2023. № 20. С. 59–65. URL: http://legalnovels.in.ua/journal/20_2023/8.pdf . (дата звернення: 16.10.2023).

8. *Хитра О. Л.* Інформаційна безпека людини як базова аксіологічна константа. Modern information technologies and their implementation in the processes of social and technical project management. Abstracts of IV International Scientific and Practical Conference. Boston. USA. 17–18 February 2020. P. 150–153. URL: https://isg-konf.com/wp-content/uploads/2020/02/IV-Conference-BostonUSA.pdf#page=151. (дата звернення: 16.10.2023).

9. Diptiben Ghelani. Cyber Security, Cyber Threats, Implications and Future Perspectives: A Review. American Journal of Science, Engineering and Technology. 2022. P. 1–7.

10. *Yuchong Li, Qinghui Liu.* A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Reports. 7. 2021. P. 1–11.

REFERENCES

1. *Baran, M.V.* (2022). Administratyvno-pravove zabezpechennia informatsiinoi bezpeky v Ukraini: dysertatsiia na zdobuttia stupenia doktora filosofii za spetsialnistiu 081 «Pravo». “Administrative and legal provision of information security in Ukraine”: dissertation. ... Doctor of Philosophy, specialty 081 «Law». Lviv State University of Internal Affairs. Lviv. 242 p. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/5076/1/baran_d.pdf. (Date of Application: 16.10.2023) [in Ukrainian].

2. *Denysiuk, Zh.Z., Yakovliev, O.V.* (2021). Formuvannia informatsiinoi kultury suspilstva v umovakh tsyfrovizatsii. Visnyk Natsionalnoi akademii kerivnykh kadriv kultury i mystetstv. No. 2. P. 18-22 [Ukrainian].

3. *Dzoban, O., Danylian, O.* (2023). Prava i svobody liudyny: informatsiinyi vymir. “Human rights and freedoms: information dimension”. Bulletin of the Yaroslav the Wise National University of Law. No. 3 (58). Series: philosophy, philosophy of law, political science, sociology. No. 3 (58). Seriia: filosofiia, filosofiia prava, politolohiia, sotsiolohiia. P. 6-22 [in Ukraininan].

4. *Zakharenko, K.V.* (2021). Instytutsiinyi vymir informatsiinoi bezpeky Ukrainy: transformatsiini vyklyky, hlobalni konteksty, stratehichni oriientyry: dysertatsiia na zdobuttia naukovoho stupenia doktora politychnykh nauk za spetsialnistiu 23.00.02 «Politychni instytuty ta protsesy». "Institutional dimension of information security of Ukraine: transformational challenges, global contexts, strategic orientations: dissertation ... Doctor of Political Sciences, specialty 23.00.02 'Political institutions and processes'". M. Drahomanov National Pedagogical University, Ivan Franko National University of Lviv. Lviv. 423 p. URL: https://lnu.edu.ua/wp-content/uploads/2021/04/dis_zakharenko.pdf. (Date of Application:16.10.2023) [in Ukrainian].

5. *Kvitkin, P.V., Diatlova, I.V. and Petrova, L.O.* (2021). Informatsiina bezpeka osobystosti: teoretyko-metodolohichnyi analiz. "Information security of the individual: theoretical and methodological analysis". Bulletin of the Yaroslav the Wise National University of Law. No. 4 (51). Series: philosophy, philosophy of law, political science, sociology. P. 46-62 [in Ukrainian].

6. *Melnychuk, V. Horokhova, L.* (2022). Krytychne myslennia yak skladova informatsiinoi bezpeky. "Critical thinking as a component of information security". Bulletin of Lviv University. Series: philosophical sciences. Iss. 29. P. 7-13 [in Ukrainian].

7. T*ykhomyrov, O.* (2023). Ideia informatsiinoi hihiieny v konteksti informatsiinoi bezpeky i zakhystu informatsiinykh prav liudyny. "The idea of information hygiene in the context of information security and protection of human information rights". Scientific legal journal «Legal Novels». No. 20. P. 59-65. URL: http://legalnovels.in.ua/journal/20_2023/8.pdf. (Date of Application: 16.10.2023) [in Ukrainian].

8. *Khytra, O.L.* (2020). Informatsiina bezpeka liudyny yak bazova aksiolohichna konstanta. "Human information security as a basic axiological constant". Modern information technologies and their implementation in the processes of social and technical project management. Abstracts of IV International Scientific and Practical Conference. Boston. USA. 17-18 February, 2020. P. 150-153. URL: https://isg-konf.com/wp-content/uploads/2020/02/IV-Conference-BostonUSA.pdf#page=151. (Date of Application: 16.10.2023) [in Ukrainian].

9. Diptiben, Ghelani (2022). Cyber Security, Cyber Threats, Implications and Future Perspectives: A Review. American Journal of Science, Engineering and Technology. P. 1-7 [in English].

10. *Yuchong, Li, Qinghui, Liu* (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Reports. 7. P. 1-11 [in English].

UDC 340:004.056:316.32

Bykov Oleksandr,
Doctor of Juridical Sciences,
Full Professor, Professor of the Department of State and
Legal Disciplines of «KROK» University,
Kyiv, Ukraine,
ORCID ID 0000-0003-4965-696X

INFORMATION SECURITY: LEGAL AND CULTURAL DIMENSIONS

The issue of information security in Ukraine is becoming extremely important for Ukrainian society, which, in the conditions of the russian-Ukrainian war, has become the target of direct informational-propaganda and informational-psychological operations by russia. Within the framework of theoretical jurisprudence, it is important to invigorate the development of effective information security strategies and ensure their practical implementation at both the national and international levels.

DOI (Article): https://doi.org/10.36486/np.2023.4(62).21

Our research is conditionally divided into two parts. It is important for us to provide a characteristic of information security as a legal phenomenon and to determine its essential characteristics. For this purpose, we consider information security in its broad sense, as a sociocultural phenomenon, with a characteristic set of measures aimed at protecting the integrity, confidentiality, and availability of information, and the protection of human rights, society, and the state in the information sphere. In the second part of the research, we separately consider information security at the level of the individual. We explore its connection with information culture, media literacy, and digital literacy.

The article presents a list of recommendations for ensuring information security. It suggests establishing effective international cooperation (supporting necessary contractual relationships, conducting diplomatic work, and establishing cooperation at the level of individual cybersecurity specialists), improving the work of special units of the Ukrainian internal affairs bodies, and implementing additional controls over the qualifications of cyber police officers, which will increase the effectiveness of criminal search for cybercriminals. The importance of combating propaganda and misinformation, reviewing the financial mechanisms for implementing the information security strategy, is emphasized. Legal and cultural aspects in our research also include a look at information security at the individual level, where the development of special skills and abilities in citizens that will minimize the risks of violating their rights in the information sphere is addressed.

Keywords: information security, IT-law, information culture, cybersecurity, digital literacy, information-media literacy.

Отримано 22.11.2023