УДК 342.9 (477)
DOI https://doi.org/10.32782/2408-9257-2024-3-24

Серебро М. В.,
докторант
Ужгородського національного університету

АКТУАЛЬНІ ПИТАННЯ АДМІНІСТРАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В УКРАЇНІ

CURRENT ISSUES OF ADMINISTRATIVE AND LEGAL REGULATION OF THE USE OF INFORMATION TECHNOLOGIES IN UKRAINE

Наукова публікація присвячена дослідженню актуальних питань адміністративно-правового регулювання використання інформаційних технологій в Україні.

Встановлено, що інформаційне законодавство на даний час містить близько чотирьох тисяч законів та інших нормативно-правових актів, які регулюють сучасні інформаційні відносини та створюють правові передумови для розвитку функціональних напрямів інформаційної діяльності. Проте, не зважаючи на значну кількість нормативних актів, якими врегульовано питання використання та розвитку інформаційних технологій, значна кількість актуальних питань у даній сфері суспільних відносин залишається не вирішеною.

До актуальних питань правового регулювання суспільних відносин у сфері використання інформаційних технологій слід віднести: захист персональних даних, а також інформації, яка відноситься до державної чи комерційної таємниці від хакерських атак; протидію поширенню в Інтернет культу насильства та жорстокості, дитячої порнографії та іншого забороненого законом контенту; запобігання використанню соціальних мереж, месенджерів для забезпечення діяльності злочинних організацій, включаючи терористичні та радикальні організації; використання інформаційних технологій та відповідних потужностей для майнінгу – забезпечення функціонування криптовалютних платформ, що перевантажує електричні мережі та часто призводить до нецільового використання технологічних потужностей; забезпечення збереження цінної інформації на альтернативних цифрових носіях з метою її захисту від втрати, знищення (стирання); правове регулювання електронної торгівлі, включаючи питання її обліку, визначення вартості цифрових продуктів, оподаткування тощо (адже комп'ютерна програма може коштувати набагато більше, ніж декларується її автором чи покупцем); протидію спаму (поширенню рекламних пропозиції без згоди споживача), що часто призводить до перевантаження електронних комунікаційних мереж, ускладнення або блокування роботи органів публічної адміністрації в результаті спам-атак; захист інтелектуальної власності, авторських прав в Інтернет.

Запропоновані шляхи вирішення проблемних питань у сфері адміністративно-правового регулювання використання інформаційних технологій шляхом внесення змін до чинного національного законодавства та застосування технічних засобів, зокрема використання можливостей штучного інтелекту для виявлення порушень прав виробників, постачальників та користувачів цифрового контенту та цифрових послуг.

Ключові слова: *інформаційні технології, регулювання, актуальні питання, цифрові послуги, публічна адміністрація, контроль, Інтернет, кіберзлочини, спам, відповідальність, програмне забезпечення, технічні рішення, сховища.*

The scientific publication is devoted to the study of topical issues of administrative and legal regulation of the use of information technologies in Ukraine.

It has been established that information legislation currently contains about four thousand laws and other normative legal acts that regulate modern information relations and create legal prerequisites for the development of functional areas of information activity. However, despite the significant number of normative acts regulating the use and development of information technologies, a significant number of topical issues in this area of public relations remain unresolved.

Current issues of legal regulation of public relations in the field of information technology use should include: protection of personal data, as well as information related to state or commercial secrets from so-called hacker attacks; countering the spread on the Internet of the cult of violence and cruelty, child pornography and other content prohibited by law; preventing the use of social networks and messengers to support the activities of criminal organizations, including terrorist and radical organizations; the use of information technologies and corresponding capacities for so-called mining – ensuring the functioning of cryptocurrency platforms, which overloads electrical networks and often leads to

inappropriate use of technological capacities; ensuring the preservation of valuable information on alternative digital media in order to protect it from loss, destruction (erasure); legal regulation of electronic commerce, including issues of its accounting, determination of the value of digital products, taxation, etc. (because a computer program can cost much more than declared by its author or buyer); countering spam (distribution of advertising offers without the consumer's consent), which often leads to overloading of electronic communication networks, complications or blocking of the work of public administration bodies as a result of spam attacks; protection of intellectual property, copyright on the Internet.

Proposed ways of solving problematic issues in the field of administrative and legal regulation of the use of information technologies by making changes to the current national legislation and using technical means, in particular, using the capabilities of artificial intelligence to detect violations of the rights of producers, suppliers and users of digital content and digital services.

Key words: *information technologies, regulation, current issues, digital services, public administration, control, Internet, cybercrimes, spam, responsibility, software, technical solutions, storage.*

Актуальність теми. Сучасне суспільство часто називають постіндустріальним або інформаційним, зважаючи на рівень технологічного прогресу та цифровізації суспільних відносин. Комп'ютерні технології проникли майже у всі сфери суспільного життя і більшість людей є користувачами Інтернет та споживачами цифрових послуг та цифрового контенту. Програмне забезпечення, оцифровані аудіовізуальні твори давно є повноцінним товаром. Органи публічної адміністрації цивілізованих держав також все більше використовують інформаційні технології для оптимізації управлінської діяльності, надання адміністративних послуг.

Разом з тим, тотальне проникнення інформаційних технологій у всі сфери суспільного життя несе із собою цілий ряд загроз як для особистої безпеки людини, так і для національної безпеки держави. Доступність персональної інформації, яку фізичні та юридичні особи власноруч викладають в мережу, можливість підробки цифрового контенту та відсутність належного рівня захисту комп'ютерних, електронних комунікаційних мереж збільшує випадки протиправного, несанкціонованого втручання в роботу останніх, вчинення злочинів проти власності, честі та гідності користувачів Інтернет, призводить до спотворення або знищення цінної інформації.

Таким чином, процес інформатизації (цифровізації) потребує все більшого юридичного супроводу, а інформаційні технології стають окремим об'єктом адміністративно-правового регулювання.

Різні аспекти правового регулювання використання та розвитку інформаційних технологій завжди були в центрі уваги науковців. Із останніх наукових праць слід виділити роботи Д. Біленької «Адміністративно-правове регулювання інформаційних відносин в Україні», О. Берназюка «Цифрові технології у праві: сучасний погляд у майбутнє», Т. Ковальової та О. Гунбіної «Правові проблеми надання адміністративних послуг з використанням інтернет-технологій», О. Комарова «Адміністративно-правовий статус суб'єктів здійснення цифрової трансформації регіону», А. Краковської та М. Бабик «Цифровізація адміністративних послуг в Україні: проблеми та перспективи розвитку», А. Омельченка «Суспільні відносини у сфері цифровізації як предмет правового регулювання», Р. Стефанчука «Інформаційні технології та право: quo vadis?», І. Тищенкової «Адміністративні процедури надання електронних публічних послуг публічною адміністрацією в Україні».

Проте, актуальні питання адміністративно-правового регулювання використання інформаційних технологій в Україні ще не були предметом окремого наукового аналізу, що актуалізує підготовку даної публікації.

Постановка завдання. Метою наукової публікації є дослідження актуальних питань адміністративно-правового регулювання використання інформаційних технологій в Україні з метою формулювання пропозицій щодо удосконалення чинного національного законодавства та юридичної практики у даній сфері суспільних відносин.

Методологія даної публікації включає філософські (закони та прийоми діалектики), загальнонаукові (системний та структурно-функціональний методи, прийоми логічного методу: аналіз, синтез, дедукція та індукція) та спеціально-юридичні методи дослідження (формально-юридичний метод як похідний від аксіоматичного методу дослідження, а також

метод юридичного моделювання). Також в процесі дослідження використовуються такі загальновідомі наукові підходи як цивілізаційний, антропоцентричний, телеологічний та синергетичний.

Так, синергетичний підхід розглядає сферу використання інформаційних технологій як самостійну систему суспільних відносин, що прагне до самоорганізації та самовдосконалення.

Результати дослідження. Сучасний стан адміністративно-правового регулювання використання інформаційних технологій в Україні є задовільним, про що свідчить поступове зростання кількості кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Так, протягом 2018 р., згідно зі статистичними даними, обліковано 2017 вказаних кримінальних правопорушень. Їх питома вага ще незначна і становить усього 0,5 % від усіх облікованих кримінальних правопорушень у 2018 р., але за останні п'ять років зросла в 5,6 рази (у 2014 р. становила – 0,09 %) [1, с. 110].

В. Гавловський зазначає, що статистичні дані про кіберзлочини відображаються також у відомчій статистичній звітності Національної поліції України, зокрема у Звіті про результати роботи підрозділів Національної поліції України, де, крім кримінальних правопорушень, охоплених Розділом XVI КК України, зазначається ще низка кримінальних правопорушень, що вчинені з використанням електронно-обчислювальної техніки, передбачених ст. 176 КК України «Порушення авторського права і суміжних прав» і ст. 185 КК України «Крадіжка», чч. 3 і 4 ст. 190 КК України «Шахрайство», ст. 200 КК України «Незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення», ст. 229 КК України «Незаконне використання знака для товарів і послуг, фірмового найменування, кваліфікованого зазначення походження товару» і ст. 231 «Незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю», чч. 3, 4 і 5 ст. 301 КК України «Ввезення, виготовлення, збут і розповсюдження порнографічних предметів». Але цей перелік статей неповний [1, с. 109].

Т. Філіпенко, аналізуючи стан та наслідки комп'ютерної злочинності наводить наступну статистику: за підсумками 2018 року працівники Департаменту кіберполіції Національної поліції України були залучені до розслідування понад 11131 кримінальних проваджень, утому числі: 1139 – у сфері протиправного контенту, 3697 – у сфері платіжних систем, 3607 – у сфері е-комерції, 2688 – у сфері кібербезпеки. Найбільша кількість злочинів була зосереджена в місті Києві (2277), а також на території Одеської (1084), Миколаївської (903) та Львівської (729) областей. Протягом року поліцейські виявили 6 тисяч злочинів, учинених у сфері використання високих інформаційних технологій, у тому числі: 680 – у сфері протиправного контенту, 2398 – у сфері платіжних систем, 1598 – у сфері е-комерції, 1325– у сфері кібербезпеки. У 2018 році працівники кіберполіції України викрили понад 800 осіб, які були причетні до вчинення злочинів у сфері високих інформаційних технологій. Згідно зі статистикою, більша частина підозрюваних – чоловіки у віці від 25 до 40 років. У сфері кібербезпеки найбільше виявлено користувачів шкідливого програмного забезпечення, які вчиняли злочини, використовуючи придбані віруси у DarkNet. За результатами міжнародної співпраці у 2018 році було викрито 8 транснаціональних хакерських угруповань і взято участь у понад 30 міжнародних операціях [2, с. 82].

Згідно зі Звітом Національної поліції про результати роботи у 2020 році зареєстровано понад 5 тисяч кіберзлочинів, у яких вдалося оперативно затримати 106 фігурантів кримінальних проваджень, серед яких 13 педофілів. Крім того, у кіберполіції в 2020 році запрацювала сервісна служба. Вона створена для надання громадянам консультацій з питань кібербезпеки. За 9 місяців її роботи надійшло понад 100 тисяч дзвінків та більше 40 тисяч електронних звернень [3].

У Звіті Національної поліції за 2021 рік зазначено, що новітні можливості інформаційних технологій та їх стрімкий ріст у всьому світі дедалі активніше використовується людством у різних сферах діяльності. Кіберпростір створює неймовірні можливості, розширює свободу, стимулює розвиток інновацій

та збагачує суспільство. Однак, паралельно з позитивними тенденціями, набуває розвитку і кіберзлочинність, що, зрозуміло, завдає значної шкоди інтересам наших громадян та держави в цілому. З метою протидії такій кримінальній протиправності в Національній поліції функціонує підрозділ кіберполіції [4].

У 2021 році задокументовано майже вдвічі більше злочинів, учинених з використанням високих інформаційних технологій. Зокрема, у майже півтора рази зросла динаміка реєстрації злочинів у банківській сфері та на третину – у сфері комп'ютерних систем. При цьому кількість розкритих кіберзлочинів збільшилася вдвічі. Періодичне обмеження соціальної активності громадян у зв'язку з посиленням карантину спровокувало збільшення на 42% шахрайств, пов'язаних з використанням електронно-обчислювальної техніки (ч. 3, 4 ст. 190 КК України). Завдяки оперативному реагуванню поліції на таку ситуацію розкрито понад 80% таких шахрайств [4].

Кіберполіцейські у 2021 році ініціювали проведення 9 міжнародних поліцейських операцій та взяли участь у 8 таких заходах на запрошення іноземних колег. Як приклад, минулого року встановлено трьох громадян України, підозрюваних у створенні вірусу «EMOTET». Через незаконні дії цих громадян потерпілим завдано збитків на суму близько 2 млрд. доларів США. Крім того, встановлено шістьох громадян України, які за допомогою шкідливого програмного забезпечення «Ransomware» завдали компаніям Республіки Корея та США збитків на загальну суму 500 млн. доларів США. Водночас кіберполіцейські продовжують тримати прямий зв'язок з громадянами. Так, у 2021 році по допомогу до кіберполіції звернулося понад 190 тис. громадян. Переважна більшість телефонувала до call-центру, водночас громадяни активно подавали звернення і через форми електронного запиту [4].

У відповідності до Звіту Національної поліції про результати роботи за 2022 рік, зросла на 49% (з 10 тис. до 14,9 тис.) кількість викритих кримінальних правопорушень у сфері високих інформаційних технологій, зокрема пов'язаних з онлайн шахрайствами – в 2,8 рази (з 2,9 тис. до 7,9 тис.) [5].

Також згідно зі Звітом Національної поліції за 2023 рік, окремими видами кримінальних правопорушень, які набули більшого поширення в умовах війни, є кіберзлочини. Виявлено в 4,1 рази більше (з 14,9 тис. до 61,4 тис.) кримінальних правопорушень у сфері високих інформаційних технологій, зокрема пов'язаних з онлайн-шахрайствами – у 5,8 рази (із 7,9 тис. до 45,7 тис.). Розкрито на 91% більше (із 7,3 тис. до 13,9 тис.) кіберзлочинів, зокрема в банківській сфері – на 12% (з 2,1 тис. до 2,4 тис.), сфері комп'ютерних систем – на 44% (з 1,3 тис. до 1,9 тис.), сфері телекомунікацій та протиправного контенту – у 3,2 рази більше (зі 101 до 323), а також онлайн-шахрайств – у 3,9 рази більше (з 1,7 тис. до 6,7 тис.) [6].

Також забезпечено ефективне відшкодування збитків, завданих кіберзлочинами. Так, у 2023 році відшкодовано 286,8 млн грн, що у 6,4 рази більше ніж у 2022 р. – 44,5 млн грн [6].

Слід відзначити, що інформаційне законодавство на даний час містить близько чотирьох тисяч законів та інших нормативно-правових актів, які регулюють сучасні інформаційні відносини та створюють правові передумови для розвитку функціональних напрямів інформаційної діяльності [7, с. 34]. Проте, не зважаючи на значну кількість нормативних актів, якими врегульовано питання використання інформаційних технологій, значна кількість актуальних питань у даній сфері суспільних відносин залишається не вирішеною.

Отже, однією з причин збільшення кількості правопорушень у сфері використання інформаційних технологій є прогалини в національному законодавстві, а саме відсутність комплексного підходу до вирішення проблемних питань у даній сфері суспільних відносин.

Так, до актуальних проблем правового регулювання суспільних відносин у сфері використання інформаційних технологій слід віднести:

– захист персональних даних, а також інформації, яка відноситься до державної чи комерційної таємниці від так званих хакерських атак (як правило правопорушники отримують доступ до захищених інформаційних систем маючи спільників, які безпосередньо працюють у певній організації, що використовує захищену інформаційну систему);

– протидію поширенню в Інтернет культу насильства та жорстокості, дитячої порнографії та іншого забороненого законом контенту (стрімке поширення соціальних мереж, їх

закритих каналів створює суттєву загрозу національному інформаційному простору, адже перевірка віку користувача як правило має формальний характер і доступ до забороненого контенту легко отримують діти та підлітки);

– запобігання використанню соціальних мереж, месенджерів для забезпечення діяльності злочинних організацій, включаючи терористичні та радикальні організації (значна кількість соціальних месенджерів має наскрізне шифрування, тому органам публічної адміністрації, зокрема спецслужбам важко відслідковувати потенційно небезпечний цифровий контент, який поширюється у соціальних мережах та їх месенджерах);

– протидію поширенню спаму – інформації, яка забруднює цифровий простір та ускладнює роботу інформаційних систем, органів публічної адміністрації (ст. 363-1 КК України передбачає кримінальну відповідальність за поширення спаму, якщо вказані дії призвели до порушення або припинення роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку [8]. Проте актуальним залишається питання встановлення адміністративної відповідальності за систематичне поширення спаму без настання вказаних наслідків);

– використання інформаційних технологій та відповідних потужностей для так званого майнінгу – забезпечення функціонування криптовалютних платформ, що перевантажує електричні мережі та часто призводить до нецільового використання технологічних потужностей (використання наявних потужностей комп'ютерних мереж для майнінгу, особливо в умовах воєнного стану, становить загрозу національній економічній та енергетичній безпеці, тим більше, що майнінг може здійснюватись із використанням бюджетних комп'ютерів, комунікаційних мереж органів публічної адміністрації; до прикладу – у 2019 році слідчі територіального управління Державного бюро розслідувань, розташованого у місті Києві, повідомили про підозру двом особам Державної судової адміністрації України, які незаконно використовували мережеве та комп'ютерне обладнання ДСА для налагодження роботи інтернет-магазинів та видобутку криптовалюти);

– забезпечення збереження цінної інформації на альтернативних цифрових носіях з метою її захисту від втрати, знищення, стирання (особливої актуальності в умовах воєнного стану набуває питання збереження національного фонду цифрової інформації, адже сервери, на яких зберігається ключова інформація, можуть стати об'єктом ракетних атак або опинитися на окупованій території. Тому актуальною є правова регламентація використання для розміщення цінних інформаційних ресурсів (дублікатів державних реєстрів, баз даних органів публічної адміністрації) матеріальних носіїв інформації, які розташовані в Європейському Союзі, США, Японії та інших дружніх для України державах);

– правове регулювання електронної торгівлі, включаючи питання її обліку, визначення вартості цифрових товарів, оподаткування тощо (комп'ютерна програма може коштувати набагато більше, ніж декларується її автором чи покупцем, ще складніше відслідковувати надання приватними особами цифрових послуг – від написання текстів до адміністрування веб-сайтів);

– захист прав і свобод учасників інформаційних відносин від протиправних посягань: кіберзлочинності, булінгу тощо (як справедливо зазначає В. Гавловський зважаючи на високий рівень латентності кіберзлочинності (наразі обліковується тільки 10–20 % вчинених злочинів, а решту становить латентна злочинність), а також низький рівень звітно-реєстраційної дисципліни, сьогодні говорити про будь-яку офіційну статистику, яка повно й достовірно відображає стан і структуру кіберзлочинності, проблематично. Можливо проаналізувати тільки динаміку цього виду злочинності, структуру злочинності, стан криміногенної ситуації у цій сфері на основі облікованих злочинів [1, с. 109-110]);

– захист інтелектуальної власності, авторських прав в Інтернет (належний рівень захисту інтелектуальної власності в національному сегменті Інтернет є однією з головних умов набуття Україною повноправного членства в Європейському Союзі).

Наведені актуальні питання регулювання інформаційних відносин потребують особливої уваги органів публічної адміністрації та

цілком можуть бути вирішені засобами адміністративного та кримінального права.

Висновки. Проведене дослідження актуальних питань адміністративно-правового регулювання використання інформаційних технологій в Україні дає підстави сформулювати висновок про те, що положення національного законодавства, яким врегульовані вищевказані суспільні відносини, потребує удосконалення та приведення у відповідність до стандартів Європейського Союзу.

З метою удосконалення захисту персональних даних, а також інформації, яка відноситься до державної чи комерційної таємниці від хакерських атак пропонується розміщення відповідної інформації на серверах, які розташовані виключно на території держав-членів ЄС та США, належать корпораціям, які гарантують високий ступінь захисту інформаційних ресурсів (розміщення державних реєстрів та баз даних на декількох альтернативних серверах в країнах ЄС та США повинно бути регламентовано на рівні закону – в національному законодавстві вже є відповідний позитивний приклад [9]).

З метою протидії поширенню в Інтернеті культу насильства та жорстокості, дитячої порнографії та іншого забороненого законом контенту пропонується на рівні закону зобов'язати інтернет-провайдерів встановлювати інтернет-фільтри для блокування забороненого контенту. Також для виявлення та блокування відповідного контенту варто використовувати можливості штучного інтелекту (відповідний порядок використання штучного інтелекту та блокування забороненого контенту доцільно затвердити на рівні відомчих нормативно-правових актів).

З метою запобігання використанню соціальних мереж, месенджерів для забезпечення діяльності злочинних організацій, включаючи терористичні та радикальні організації, пропонується заборонити (блокувати) використання в Україні месенджерів, які не надають доступ до переписки абонентів спецслужбам, використовують зашифровані закриті канали. Як приклад, загрозу національній безпеці становить інтернет-месенджер (застосунок для обміну повідомленнями) «Telegram».

З метою протидії поширенню спаму – інформації, яка забруднює цифровий простір та ускладнює роботу інформаційних систем, органів публічної адміністрації пропонується встановити адміністративну відповідальність за поширення спаму, тобто умисне систематичне масове розповсюдження повідомлень електрозв'язку, здійснене без попередньої згоди адресатів, що не призвело до порушення або припинення роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

З метою запобігання невпорядкованому використанню інформаційних технологій та відповідних потужностей для майнінгу (забезпечення функціонування криптовалютних платформ) пропонується в найкоротші строки внести зміни до Податкового кодексу України щодо особливостей оподаткування операцій з віртуальними активами з метою забезпечення набуття чинності Законом України «Про віртуальні активи». В останньому має бути чітко передбачена заборона суб'єктам владних повноважень та працівникам органів публічної адміністрації здійснювати майнінг із використанням технологічних потужностей державних підприємств, установ чи організацій. Крім того, відповідальність за вказані дії доцільно передбачити в окремій статті Кримінального кодексу України.

З метою правового врегулювання електронної торгівлі, включаючи питання її обліку, визначення вартості цифрових товарів, оподаткування тощо пропонується використовувати можливості штучного інтелекту для визначення реальної вартості цифрових товарів та обліку торгових операцій, пов'язаних з їх обігом (Концепцію розвитку штучного інтелекту в Україні схвалено розпорядженням КМУ від 2 грудня 2020 р. № 1556-р [10]). Технологія штучного інтелекту дозволяє оперативно моніторити маркетингові пропозиції, прайс-листи, торгові майданчики всіх учасників ринку та надавати користувачу об'єктивну статистичну інформацію.

Як зазначено в самій Концепції розвитку штучного інтелекту в Україні, впровадження інформаційних технологій, частиною яких є технології штучного інтелекту, є невід'ємною складовою розвитку соціально-економічної, науково-технічної, оборонної, правової та іншої діяльності у сферах загальнодержавного значення [10].

З метою захисту прав і свобод учасників інформаційних відносин від протиправних посягань: кіберзлочинності, булінгу тощо пропонується посилити кримінальну відповідальність за вчинення злочинів з використанням електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Зокрема, санкції всіх частин перших статей Розділу XVI КК України повинні передбачати можливість застосування до порушника покарання у вигляді позбавлення на певний строк. Така пропозиція обумовлена підвищеним ступенем суспільної небезпеки кримінальних правопорушень, які вчиняються з використанням інформаційних технологій, адже як правило шкода завдається як публічним, так і приватним інтересам, причому, в більшості випадків, інтересам багатьох користувачів.

З метою захисту інтелектуальної власності, авторських прав в Інтернет також пропонується використовувати можливості штучного інтелекту, інструменти якого дозволяють виявляти порушення авторських прав в мережі та блокувати доступ до відповідних інформаційних ресурсів. Порядок використання можливостей штучного інтелекту для зазначених цілей також доцільно регламентувати на рівні відомчих нормативно-правових актів.

Підсумовуючи слід зазначити, що наведений перелік пропозицій щодо удосконалення чинного національного законодавства у сфері використання інформаційних технологій не є вичерпним, що актуалізує проведення подальших наукових пошуків у даному напряму.

ЛІТЕРАТУРА:

1. Гавловський В.Д. Аналіз стану кіберзлочинності в Україні. *Інформація і право.* 2019. № 1 (28). С. 108–117.

2. Філіпенко Т. Стан та наслідки комп'ютерної злочинності. *Цифрова платформа: інформаційні технології в соціокультурній сфері.* 2020. Том 3 № 1. С. 79–86.

3. Звіт Національної поліції України про результати роботи у 2020 році. Національна поліція України. *Офіційний вебпортал. Річні звіти.* URL: https://media-www.npu.gov.ua/npu-pre-prod/sites/1/Docs/Dialnist/Richni_zvity/zvit-npu-za-2020-rik_com.pdf

4. Звіт Національної поліції України про результати роботи у 2021 році. Національна поліція України. *Офіційний вебпортал. Річні звіти*. URL: https://media-www.npu.gov.ua/npu-pre-prod/sites/1/Docs/Dialnist/Richni_zvity/Zvit_NPU_2021_.pdf

5. Звіт Національної поліції України про результати роботи у 2022 році. Національна поліція України. *Офіційний вебпортал. Річні звіти.* URL: https://media-www.npu.gov.ua/npu-pre-prod/sites/1/ НПУ за 2022 рік_.pdf

6. Звіт Національної поліції України про результати роботи у 2023 році. Національна поліція України. *Офіційний вебпортал. Річні звіти*. URL: https://media-www.npu.gov.ua/npu-pre-prod/sites/1/Docs/Dialnist/Richni_zvity/zvit_NPU_2023.pdf

7. Пилипчук В.Г., Цимбалюк В.С. Історико-правові проблеми становлення і розвитку інформаційної сфери та інформаційного права в Україні (кінець XX – початок XXI століття). *Вісник Національної академії правових наук України.* 2016. № 4 (87). С. 29-44.

8. Кримінальний кодекс України від 5 квітня 2001 року № 2341-III. Дата оновлення: 19.05.2024. URL: https://zakon.rada.gov.ua/laws/show/2341-14/ed20240519#Text (дата звернення: 01.06.2024).

9. Верховна Рада ухвалила закон про зберігання персональних даних українців на закордонних серверах, який є частиною мобілізаційного законодавства. *Судово-юридична газета. Публікації. Законодавство.* 16.01.2024. URL: https://sud.ua/uk/news/publication/290726-verkhovnaya-rada-prinyala-zakon-o-khranenii-personalnykh-dannykh-ukraintsev-na-zarubezhnykh-serverakh-yavlyayuschiysya-chastyu-mobilizatsionnogo-zakonodatelstva (дата звернення: 01.06.2024).

10. Про схвалення Концепції розвитку штучного інтелекту в Україні: розпорядження КМУ від 2 грудня 2020 р. № 1556-р. Дата оновлення: 29.12.2021. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text (дата звернення: 01.06.2024).