ISSN (Print) 2708-339X ISSN (Online) 2786-7498
Legal Bulletin № 4 (14), 2024

РОЗДІЛ 3. ТРУДОВЕ ПРАВО І ПРАВО СОЦІАЛЬНОГО ЗАБЕЗПЕЧЕННЯ; АДМІНІСТРАТИВНЕ ПРАВО І АДМІНІСТРАТИВНИЙ ПРОЦЕС; ФІНАНСОВЕ, ІНФОРМАЦІЙНЕ ПРАВО

УДК 343.3
DOI 10.31732/2708-339X-2024-14-A9

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ У СУЧАСНОМУ ЗАКОНОДАВСТВІ

Биков О.М.,
доктор юридичних наук, професор,
професор кафедри теорії та історії держави і права
Університет економіки та права «КРОК»,
м. Київ, вул. Табірна, 30-32, Україна, 03113
e-mail: oleksandrbm@krok.edu.ua,
ORCID: https://orcid.org/0000-0003-4965-696X

Савченко В.В.,
здобувачка ступеня вищої освіти «Магістр»
Університет економіки та права «КРОК»
м. Київ, вул. Табірна, 30-32, Україна, 03113,
e-mail: savchenkovv@krok.edu.ua
ORCID: https://orcid.org/0009-0008-2974-8019

PERSONAL DATA PROTECTION IN MODERN LEGISLATION

Bykov O.M.,
Doctor of Laws,
Professor of the Department of State and Legal Disciplines
of «KROK» University
Kyiv, Tabirna St., 30-32, Ukraine, 03113
e-mail: oleksandrbm@krok.edu.ua
ORCID: https://orcid.org/0000-0003-4965-696X

Savchenko V.V.,
graduate of the Master's degree
of «KROK» University
Kyiv, Tabirna St., 30-32, Ukraine, 03113
e-mail: savchenkovv@krok.edu.ua
ORCID: https://orcid.org/0009-0008-2974-8019

Анотація. *У статті розглянуто сучасні виклики захисту персональних даних, обумовлені стрімким розвитком інформаційних технологій і зростаючими кіберзагрозами. Автор досліджує проблеми, що виникають через витоки даних, соціальну інженерію та поширення фішингових атак, а також аналізує численні приклади масштабних витоків інформації, які не лише завдають фінансових збитків, але й підривають довіру громадськості до державних установ і комерційних компаній. Основну увагу приділено законодавчим аспектам захисту персональних даних в Україні, їх відповідності викликам сучасного цифрового середовища та порівнянню з міжнародними стандартами, такими як Загальний регламент про захист даних (GDPR) та стандарти ISO/IEC 27001.*

Результати аналізу свідчать про те, що чинне законодавство не завжди встигає адаптуватися до швидкого розвитку технологій, що призводить до утворення «сірих зон», які можуть використовуватися для несанкціонованого доступу до інформації. Крім того, важливими факторами зниження рівня безпеки є недоліки в організаційному управлінні, недостатня підготовка працівників і брак регулярних аудитів, а також відсутність належної координації між державними органами. У статті також запропоновано низку рекомендацій для вдосконалення законодавчої бази, включаючи введення суворіших санкцій за порушення норм, чіткі визначення ключових понять і запровадження спеціального регулювання для новітніх технологій, зокрема штучного інтелекту та блокчейну. Автор наголошує на необхідності посилення кібербезпеки в організаціях, які обробляють персональні дані, включаючи впровадження систем управління інформаційною безпекою та регулярне навчання співробітників. Підвищення обізнаності громадян також розглядається як важливий фактор, що сприятиме кращому

розумінню ризиків, пов'язаних із захистом особистої інформації. Також підкреслюється значення державної координації та міжнародного співробітництва для подолання кіберзагроз.

У результаті дослідження зроблено висновок, що лише комплексний підхід, який охоплює вдосконалення законодавства, посилення кібербезпеки, підвищення цифрової грамотності та розвиток інноваційних технологій захисту даних, здатний забезпечити належний рівень захисту персональних даних у сучасному цифровому світі.

***Ключові слова**: персональні дані, захист персональних даних, інформаційні технології, глобалізація, законодавство, кібербезпека, приватність, витік даних, кібератаки.*

***Формул**: 0, рис.: 0, табл.: 0, бібл.: 13.*

***Abstract**. The article examines the current challenges of personal data protection caused by the rapid development of information technology and growing cyber threats The author examines the problems arising from data leaks, social engineering and the spread of phishing attacks, and analyses numerous examples of large-scale information leaks that not only cause financial losses but also undermine public trust in government agencies and commercial companies. The main focus is on the legislative aspects of personal data protection in Ukraine, its compliance with the challenges of the modern digital environment and comparison with international standards, such as the General Data Protection Regulation (GDPR) and ISO/IEC 27001 standards.*

The results of the analysis show that the current legislation does not always keep pace with the rapid development of technology, which leads to the creation of 'grey areas' that can be used for unauthorised access to information. In addition, important factors in reducing the level of security are deficiencies in organisational management, insufficient training and lack of regular audits, as well as lack of proper coordination between government agencies. The article also offers a number of recommendations for improving the legal framework, including the introduction of stricter sanctions for violations of regulations, clear definitions of key concepts, and the introduction of special regulation for new technologies, including artificial intelligence and blockchain. The author emphasises the need to strengthen cybersecurity in organisations that process personal data, including the introduction of information security management systems and regular employee training. Raising awareness of citizens is also seen as an important factor that will contribute to a better understanding of the risks associated with the protection of personal information. The importance of state coordination and international cooperation to overcome cyber threats is also emphasised.

The study concludes that only a comprehensive approach, which includes improving legislation, strengthening cybersecurity, increasing digital literacy and developing innovative data protection technologies, can ensure an adequate level of personal data protection in the modern digital world.

***Keywords**: Personal data, personal data protection, information technology, globalisation, legislation, cybersecurity, privacy, data breach, cyberattacks*

***Formulas**: 0, fig.: 0, tabl.: 0, bibl.: 13.*

Постановка проблеми. Швидкий розвиток технологій та глобалізація суттєво збільшили обсяги персональних даних, що збираються та обробляються. Однак, законодавство часто не встигає за цими змінами, створюючи ризики для приватності. Ця робота спрямована на аналіз сучасного стану законодавчого регулювання захисту персональних даних в Україні та розробку пропозицій щодо його вдосконалення для забезпечення адекватного захисту прав громадян у цифрову епоху.

Витік персональних даних у цифрову епоху став однією з найактуальніших проблем інформаційної безпеки. Зростання кількості кібератак та вдосконалення методів збору даних призвели до підвищення ризику несанкціонованого доступу до конфіденційної інформації. Наслідки таких інцидентів можуть бути різноманітними: від фінансових втрат до порушення репутації та психологічного дискомфорту постраждалих.

Аналіз останніх досліджень і публікацій. Попри те, що питання захисту персональних даних у контексті розвитку технології та глобалізації в Україні є відносно новим, окремі аспекти цієї проблеми вже стали об'єктом досліджень українських науковців, які заклали основу для подальшого вдосконалення законодавчої бази. Зокрема, Брижко В.М., Захист персональних даних: реалії та практика сучасності, Бем М. В., Городиський І. М., Саттон Г., Родіоненко О. М. – захист персональних даних: правове регулювання та практичні аспекти, Єфремова К. В. – технології цифрової економіки та фінансова безпека, Дуравкін П. М., Гафич І. І. – сучасні виклики та майбутнє правового захисту персональних даних: під впливом розвитку цифровізації.

Виділення не вирішених раніше частин загальної проблеми. Вищезазначена проблема багатогранна й комплексна, тому потребує глибокого аналізу причин і умов витоків персональних даних, оцінки їх наслідків та розробки ефективних заходів для їх усунення. Особливу увагу слід приділити вдосконаленню систем захисту даних, щоб

запобігти повторенню подібних ситуацій та забезпечити надійний рівень безпеки інформації в умовах сучасних кіберзагроз.

Головною метою статті має стати комплексне дослідження проблеми розбіжності між швидким технологічним розвитком та законодавчим регулюванням у сфері захисту персональних даних. Завдання статті полягає в аналізі сучасного стану законодавства щодо захисту персональних даних.

Виклад основного матеріалу дослідження. На нашу думку, однією з основних причин недостатньої ефективності механізмів захисту персональних даних є недосконале правове регулювання. Швидкий розвиток технологій часто призводить до того, що законодавство не встигає за змінами, створюючи «сірі зони», які можуть використовувати зловмисники.

Соціальна інженерія також залишається одним з найпоширеніших методів отримання конфіденційної інформації. Багато користувачів не усвідомлюють ризики, пов'язані з передачею персональних даних через Інтернет, і не вживають належних заходів безпеки.

Окрім цього, організаційні недоліки, такі як відсутність чіткої політики інформаційної безпеки у багатьох компаніях, недостатня підготовка персоналу до кіберзагроз, брак регулярних аудитів і слабка координація дій між державними органами, також негативно впливають на загальний рівень захисту даних.

Приклади неефективності захисту даних добре ілюструють ці проблеми. Постійні витоки великих обсягів даних у таких компаніях, як Facebook (50 мільйонів паролів користувачів Facebook):

«Facebook, який вже зіткнувся з перевіркою того, як він обробляє приватну інформацію своїх користувачів, заявив у п'ятницю, що атака на його комп'ютерну мережу призвела до витоку особистої інформації майже 50 мільйонів користувачів» [11, с. 1] і LinkedIn, (700 мільйонів облікових записів):

«Публікація з'явилася на горезвісному хакерському форумі о 8:57 ранку за Лондоном.

«Привіт, у мене є 700 мільйонів записів LinkedIn за 2021 рік», – написав він.

У дописі було посилання на зразок із мільйоном записів та запрошення до інших хакерів зв'язатися з ним приватно та зробити пропозиції щодо бази даних» [12 с. 1], а також поширення фішингових атак і вірусів-вимагачів (ransomware) свідчать про вразливість існуючих механізмів безпеки. Ці інциденти підкреслюють необхідність посилення як технічних рішень, так і нормативної бази.

Правові аспекти відповідальності за витік даних регулюються національним законодавством кожної країни та міжнародними договорами і стандартами, такими як Загальний регламент про захист даних (GDPR) і стандарти ISO/IEC 27001, які встановлюють вимоги до систем управління інформаційною безпекою [6].

В Україні питання відповідальності за витік інформації регулюється Законом України «Про захист персональних даних» [5, с. 5], що визначає права суб'єктів персональних даних, обов'язки операторів і відповідальність за порушення законодавства, а також нормами Цивільного, Кримінального та Адміністративного кодексів України та Конституції України.

Для порівняння ми можемо визначити основні риси цих двох документів:

• Спільні принципи. Обидва документи базуються на загальних принципах захисту персональних даних, таких як законність, добросовісність, прозорість, обмеження цілей, мінімізація даних, точність, доступність, цілісність та конфіденційність.

• Можуть бути і відмінності у формулюванні та акцентах на певних принципах. Наприклад, GDPR надає більше уваги праву на забуття.

Для прикладу, я ще пропоную розглянути наступний популярний месенджер Telegram. Правове регулювання діяльності Telegram є складним і неоднозначним питанням, яке викликає жваві дискусії серед юристів, фахівців з кібербезпеки та представників правоохоронних органів. З одного боку, Telegram позиціонує себе як захисник приватності користувачів, використовуючи передові технології шифрування. З іншого боку, розподілена структура мережі серверів і відсутність централізованого управління ускладнюють контроль за діяльністю месенджера та забезпечення виконання вимог національного законодавства.

Ключовими проблемами правового регулювання Telegram є:

• юрисдикція, тобто встановлення юрисдикції над компанією, яка має розподілену структуру і не має офіційного представництва в багатьох країнах.

• захист персональних даних, оскільки суміщення вимог до захисту персональних даних з необхідністю боротьби з незаконною діяльністю, такою як поширення екстремістських матеріалів або дитячої порнографії.

• цензура, так як збалансування права на свободу слова з необхідністю запобігання поширенню ненависті, насильства та дезінформації.

У квітні 2023 року Європейська Комісія оприлюднила список VLOP. До списку потрапити такі платформи, як Facebook, Instagram, LinkedIn, Tik Tok, Twitter та інші. Але поріг у 45 мільйонів повинен постійно оновлюватися. Тому Європейська Комісія уповноважена доповнювати положення Регламенту. Наприклад, знизити поріг, якщо дійде висновку, що платформа має великий соціальний вплив.

Telegram до цього списку поки що не потрапив, адже він має менше 45 мільйонів активних користувачів на місяць в ЄС. Втім, відсутність Telegram серед VLOP не означає, що платформа випадає з поля зору Європейської Комісії і національних регуляторів. Європейська Комісія повинна наглядати за VLOP. А національні органи (Digital Services Coordinators) будуть відповідати за нагляд за меншими платформами. Ці органи повинні бути створені державами-членами ЄС до 17 лютого 2024 року [13, с 1].

Які наслідки мають порушення законодавства про захист персональних даних?

Порушення законодавства про захист персональних даних можуть мати серйозні наслідки як для осіб, чиї дані були скомпрометовані, так і для компаній або організацій, відповідальних за їх обробку.

Одним з основних наслідків є фінансові санкції. Органи регулювання можуть накладати значні штрафи на компанії за порушення законодавства. Наприклад, відповідно до Загального регламенту про захист даних (GDPR) в ЄС [3], штрафи можуть досягати 4% від річного обсягу бізнесу або 20 мільйонів євро, залежно від того, що більше. В Україні, відповідно до статті 188-39 Кодексу України про адміністративні правопорушення, за порушення [2] законодавства у сфері захисту персональних даних можуть накладатися адміністративні штрафи.

Крім того, відшкодування збитків також є важливим аспектом. Постраждалі особи можуть подати позови на відшкодування збитків, завданих витоком або неналежним обробленням їхніх даних. Це може включати як матеріальні, так і нематеріальні збитки, відповідно до статті 1166 Цивільного кодексу України [3].

Згідно зі статтею 182 Кримінального кодексу [4], незаконні дії щодо збору, зберігання, використання, знищення, поширення або зміни конфіденційної інформації про особу, якщо це не підпадає під регулювання інших статей Кодексу, тягнуть за собою покарання у вигляді штрафу від п’ятисот до тисячі НМДГ, виправних робіт до двох років, арешту до шести місяців або обмеження волі до трьох років.

Зауважу, що розповсюдження неправдивої інформації, яка завдає шкоди репутації особи, є порушенням права на захист честі і гідності (стаття 29 Конституції України) [1].

Також, особливо актуальним питання захисту персональних даних стало в умовах повномасштабної війни в Україні. Масова мобілізація, переміщення населення та посилення кібератак створюють додаткові ризики для витоку персональних даних

Як ми можемо запобігти витоку персональних даних? Щоб забезпечити безпеку особистої інформації, необхідні комплексні заходи, які охоплюють як удосконалення законодавчої бази, так і підвищення рівня кібербезпеки організацій та обізнаності громадян.

Удосконалення законодавчої бази є одним з ключових напрямків у забезпеченні захисту персональних даних. Це передбачає регулярний перегляд та оновлення законодавства з урахуванням нових технологій та викликів. Посилення відповідальності за порушення законодавства шляхом збільшення штрафних санкцій та введення кримінальної відповідальності за найсерйозніші правопорушення також є важливим кроком. Крім того, необхідно створити чіткі та зрозумілі визначення ключових понять, щоб уникну-

ти неоднозначностей у застосуванні закону. Окрему увагу слід приділити регулюванню нових технологій, таких як штучний інтелект та блокчейн, які відкривають нові можливості для обробки персональних даних, але водночас створюють нові ризики.

Підвищення рівня кібербезпеки організацій є не менш важливим завданням. Організації, що обробляють персональні дані, повинні обов'язково впроваджувати та сертифікувати системи управління інформаційною безпекою. Регулярні аудити безпеки дозволять виявляти та усувати вразливості в системах захисту. Навчання персоналу також є важливим елементом, оскільки саме люди часто стають причиною кібератак. Захист від кібератак шляхом впровадження ефективних систем захисту є невід'ємною частиною забезпечення безпеки даних.

Підвищення обізнаності громадян є ключовим фактором у забезпеченні захисту персональних даних. Проведення широких інформаційних кампаній допоможе людям зрозуміти ризики, пов'язані з розголошенням персональних даних, та навчитися захищати свою інформацію. Включення тем кібербезпеки та захисту персональних даних до шкільних та університетських програм сприятиме формуванню цифрової грамотності у молодіжного покоління.

Співпраця державних органів є необхідною умовою для ефективного протистояння кіберзагрозам. Створення єдиного координаційного центру з кібербезпеки дозволить оперативно реагувати на кіберінциденти. Обмін інформацією між різними державними органами сприятиме підвищенню ефективності боротьби з кіберзлочинністю. Розширення міжнародного співробітництва в галузі кібербезпеки дозволить обмінюватися досвідом та розробляти спільні підходи до боротьби з кіберзлочинністю.

Розвиток технологій захисту даних є одним з найперспективніших напрямків у забезпеченні кібербезпеки. Підтримка наукових досліджень у сфері кібербезпеки та розробка нових технологій захисту даних дозволить створити більш ефективні системи захисту. Створення інноваційних екосистем сприятиме розвитку стартапів та малих підприємств, які займаються розробкою рішень у сфері кібербезпеки.

Також, необхідно, для захисту персональних даний у воєнний час слід встановити чіткі правила і процедури збору, обробки та зберігання персональних даних, особливо тих, що стосуються військовозобов'язаних та внутрішньо переміщених осіб.

Висновки. Проведене дослідження виявило, що проблема захисту персональних даних є надзвичайно актуальною в сучасному цифровому світі. Недостатня ефективність механізмів захисту даних зумовлена комплексом взаємопов'язаних факторів.

По-перше, застаріле законодавство не встигає за швидкими темпами розвитку технологій, створюючи «сірі зони», які активно експлуатуються зловмисниками. По-друге, низький рівень кібергігієни користувачів та організаційні недоліки в компаніях роблять їх вразливими до кібератак. По-третє, відсутність ефективної координації між державними органами ускладнює боротьбу з кіберзлочинністю.

Витоки персональних даних у великих компаній, таких як Facebook та LinkedIn, наочно демонструють масштаби проблеми. Воєнний стан в Україні додатково ускладнює ситуацію, оскільки створює нові ризики для витоку даних, пов'язані з мобілізацією, переміщенням населення та посиленням кібератак.

Для вирішення цієї проблеми необхідний комплексний підхід. Захист персональних даних є одним з найважливіших викликів сучасності. Лише за умови спільних зусиль держави, бізнесу та громадянського суспільства можна забезпечити ефективний захист персональних даних та створити безпечне цифрове середовище.

Література:

1.Конституція України, Документ 254к/96-ВР, чинний, поточна редакція Редакція від 01.01.2020, підстава - 27-IX, URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text. (дата звернення: 25.10.2024р.)

2.Кодекс України про адміністративні правопорушення. Документ 80731-X, чинний, поточна редакція. Редакція від 09.08.2024, підстава 3886-IX. URL: https://zakon.rada.gov.ua/laws/show/80731-10#Text. (дата звернення: 25.10.2024р.)

3.Цивільний кодекс України. Документ 435-IV, чинний, поточна редакція. Редакція від 28.04.2023, підстава 2989-IX, 2970-IX URL: https://zakon.rada.gov.ua/laws/show/435-15#Text (дата звернення: 26.10.2024р).

4.Кримінальний кодекс України, Документ 2341-III, чинний, поточна редакція. Редакція від 07.09.2024, підстава 3902-IX. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text. (дата звернення: 26.10.2024 р.)

5.ЗАКОН УКРАЇНИ «Про захист персональних даних», Документ 2297-VI, чинний, поточна редакція. Редакція від 27.04.2024, підстава - 3585-IX. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text. (дата звернення: 27.10.2024р.)

6.РЕГЛАМЕНТ ЄВРОПЕЙСЬКОГО ПАРЛАМЕНТУ І РАДИ (ЄС) 2016/679, Документ 984_008-16, чинний, поточна редакція. Прийняття від 27.04.2016. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text. (дата звернення: 27.10.2024р.)

7.Брижко В.М. Захист персональних даних: реалії та практика сучасності. Державна наукова установа «Інститут інформації, безпеки і права Національна академія правових наук України. Журнал «Інформація і право», № 3(9) / 2013. (дата звернення: 27.10.2024 р.)

8.Бем М. В., Городиський І. М., Саттон Г., Родіоненко О. М. Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник. К.: К.І.С., 2015. 220 с. URL: https://rm.coe.int/168059920c. (дата звернення: 27.10.2024 р.)

9.Єфремова К. В. Технології цифрової економіки та фінансова безпека. Право та інновації. 2023. № 2 (42). С. 7-11. URL: https://doi.org/10.37772/2518-1718-2023-2(42)-1 (дата звернення: 27.10.2024 р.)

10.Дуравкін П. М., Гафич І. І. Сучасні виклики та майбутнє правового захисту персональних даних: під впливом розвитку цифровізації. Право та інновації. 2023. № 3 (43). С. 89-100. (дата звернення: 27.10.2024 р.)

11.Журнал The New York Times. Стаття «Порушення безпеки Facebook викрило акаунти 50 мільйонів користувачів», дата публікації: 28 вересня 2018р. Електронна стаття, URL: https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html (дата звернення: 28.10.2024 р.).

12.Джо Тайді . BBC News Україна. Стаття: «Я викрав дані 700 млн користувачів LinkedIn задля розваги», дата публікації: 18 липня 2021р. Електронна стаття: URL: https://www.bbc.com/ukrainian/features-57833124 (дата звернення: 28.10.2024 р.)

13.Спесивцева О. Центр демократії та верховенства права за фінансової підтримки International Media Support. Стаття: «Неприступна фортеця Telegram: чи в силах держави регулювати платформу?», дата публікації: 28 вересня 2023 р. URL: https://cedem.org.ua/analytics/telegram-regulyuvaty-platformu/ (дата звернення: 30.10.2024 р.)

References:

1.Constitution of Ukraine, Document 254к/96-BP, current, current edition - Edition of 01.01.2020, grounds - 27-IX, URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text(Accessed October 25, 2024).

2.Code of Ukraine on Administrative Offences. Document 80731-X, current, current edition - Edition of 09.08.2024, basis - 3886-IX. URL: https://zakon.rada.gov.ua/laws/show/80731-10#Text(Accessed October 25, 2024).

3.Civil Code of Ukraine. Document 435-IV, current, current edition - Edition of 28.04.2023, basis - 2989-IX, 2970-IX URL: https://zakon.rada.gov.ua/laws/show/435-15#Text (Accessed October 26, 2024).

4.Criminal Code of Ukraine, Document 2341-III, current, current edition - Edition of 07.09.2024, basis - 3902-IX. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text(Accessed October 26, 2024).

5.LAW OF UKRAINE 'On Personal Data Protection', Document 2297-VI, current, current edition - Edition of 27.04.2024, grounds. 3585-IX URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text(Accessed October 27, 2024).

6.REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (EU) 2016/679, Document 984_008-16, current, current version - Adoption of 27.04.2016 URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text(Accessed October 27, 2024).

7.Bryzhko V.M. Protection of personal data: realities and practice of the present. State Scientific Institution 'Institute of Information, Security and Law of the National Academy of Legal Sciences of Ukraine'. Journal 'Information and Law', No. 3 (9) / 2013 (Accessed October 27, 2024).

8.Bem MV, Gorodissky IM, Sutton G, Rodionenko O. Protection of personal data: Legal regulation and practical aspects: a scientific and practical manual. K.: K.I.S., 2015. 220 p. URL: https://rm.coe.int/168059920c. (Accessed October 27, 2024).

9.Digital economy technologies and financial security. Law and Innovation. 2023. № 2 (42). C. 7-11. URL: https://doi.org/10.37772/2518-1718-2023-2(42)-1 (Accessed October 27,2024).

10.REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (EU) 2016/679, Document 984_008-16, current version - Adoption of 27.04.2016. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text(Accessed October 27,2024).

11.Mike Isaac and Sheera Frenkel. The New York Times «Facebook Security Breach Exposes Accounts of 50 Million Users», Electronic article, URL: https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html (Accessed October 28, 2024).

12.Joe Tidy. BBC News Ukraine. Article: 'I stole the data of 700 million LinkedIn users for fun', date of publication: 18 July 2021. URL: https://www.bbc.com/ukrainian/features-57833124 (Accessed October 28,2024).

13.Spesivtseva O. Centre for Democracy and Rule of Law with the financial support of International Media Support. Article: 'The Impregnable Fortress of Telegram: Is the State Able to Regulate the Platform?', published: 28 September 2023. URL: https://cedem.org.ua/analytics/telegram-regulyuvaty-platformu/(Accessed October 30, 2024).

Стаття надійшла до друку 01 листопада 2024 року