



25 NOVEMBER, 2022
SYDNEY, AUSTRALIA

**CURRENT ISSUES OF SCIENCE,
PROSPECTS AND CHALLENGES**

III INTERNATIONAL SCIENTIFIC AND THEORETICAL CONFERENCE



**EUROPEAN
SCIENTIFIC
PLATFORM**





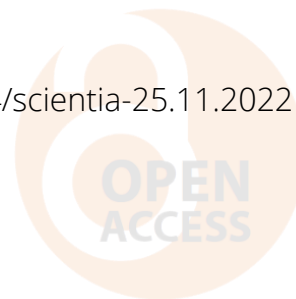
25 November, 2022

Sydney, Australia

**CURRENT ISSUES OF SCIENCE,
PROSPECTS AND CHALLENGES**

III International Scientific and Theoretical Conference

Sydney, 2022



Chairman of the Organizing Committee: Holdenblat M.

Responsible for the layout: Zrada S.

Responsible designer: Bondarenko I.

C 95 **Current issues of science, prospects and challenges:** collection of scientific papers «SCIENTIA» with Proceedings of the III International Scientific and Theoretical Conference, November 25, 2022. Sydney, Australia: European Scientific Platform.

ISBN 979-8-88831-306-0

DOI 10.36074/scientia-25.11.2022

Papers of participants of the III International Multidisciplinary Scientific and Theoretical Conference «Current issues of science, prospects and challenges», held on November 25, 2022 in Sydney are presented in the collection of scientific papers.



The conference is included in the Academic Research Index ReserchBib International catalog of scientific conferences and registered for holding on the territory of Ukraine in UKRISTEI (Certificate № 365 dated August 26th, 2022).

Conference proceedings are publicly available under terms of the Creative Commons Attribution-ShareAlike 4.0 International License (CC BY-SA 4.0).

UDC 001 (08)

© Participants of the conference, 2022

© Collection of scientific papers «SCIENTIA», 2022

© European Scientific Platform, 2022

ISBN 979-8-88831-306-0

CONTENT

SECTION 1.

ECONOMIC THEORY, MACRO- AND REGIONAL ECONOMY

SIMULATION OF ECONOMIC DYNAMICS SYSTEMS BASED ON INTEGRAL EQUATIONS

Kornichenko O., Strelchenko A.A. 10

АНАЛІЗ ВПЛИВУ ДЕРЖАВНОГО БОРГУ НА ЕКОНОМІКУ УКРАЇНИ ПРОТЯГОМ ОСТАННІХ РОКІВ

Антощук І.А...... 12

ОЦІНКА СУЧАСНОГО СТАНУ МЕТАЛУРГІЙНОЇ ПРОМИСЛОВОСТІ УКРАЇНИ

Бондаренко Н.М...... 14

ПРОБЛЕМИ ПІДПРИЄМСТВ СВІТУ В ПЕРІОД НЕСТАБІЛЬНОЇ СИТУАЦІЇ

Маркова С.В., Маказан Є.В., Сухарева К.В., Петрук В.В. 17

SECTION 2.

ENTREPRENEURSHIP, TRADE AND SERVICE SECTOR

ВЛАСТИВОСТІ, ОЗНАКИ ТА ПОКАЗНИКИ ОЦІНЮВАННЯ РІВНЯ ЕКОНОМІЧНОГО РОЗВИТКУ ПІДПРИЄМСТВ

Ємельянов О.Ю. 21

SECTION 3.

FINANCE AND BANKING; TAXATION, ACCOUNTING AND AUDITING

АУДИТОРСЬКИЙ РИЗИК. ПОМИЛКИ І ОБМАН В АУДИТОРСЬКІЙ ПРАКТИЦІ

Бобріченко В.В. 24

ДЕРЖАВНИЙ ПОДАТКОВИЙ МЕНЕДЖМЕНТ: РЕТРОСПЕКТИВА ОПОДАТКУВАННЯ ПОДАТКОМ НА ПРИБУТОК ПІДПРИЄМСТВ В УКРАЇНІ

Дем'яненко К.О...... 27

МЕДИЧНЕ СИТРАХУВАННЯ В УКРАЇНІ – СУЧАСНІ МОЖЛИВОСТІ РОЗВИТКУ

Безкровний О.В., Блискавка А.Ю., Федь В.Ю. 30

МЕТОДИКА ПРОВЕДЕННЯ АУДИТУ: ЗАКОРДОННИЙ ДОСВІД

Бобріченко В.В. 33

ПРАВОВЕ РЕГУЛЮВАННЯ ПЕРЕМІЩЕННЯ ВАЛЮТНИХ ЦІННОСТЕЙ ЧЕРЕЗ МИТНИЙ КОРДОН УКРАЇНИ

Бобріченко В.В. 36

| | |
|--|-----------|
| РОЛЬ МАЛОГО ТА СЕРЕДНЬОГО БІЗНЕСУ У РОЗВИТКУ ЕКОНОМІКИ УКРАЇНИ Скіп Р.А. | 39 |
|--|-----------|

| | |
|---|-----------|
| РОЛЬ ОБЛІКОВОЇ ПОЛІТИКИ В УПРАВЛІННІ ПІДПРИЄМСТВОМ Ромашко О.М., Новіков В.В. | 41 |
|---|-----------|

SECTION 4.

MANAGEMENT, PUBLIC MANAGEMENT AND ADMINISTRATION

| | |
|--|-----------|
| ГАРМОНІЗАЦІЯ УПРАВЛІННЯ ЯК ПРОЦЕС ЙОГО ФІЛОСОФСЬКІ ОКРЕСЛЕНОЇ МЕТОДОЛОГІЗАЦІЇ Юшин С.О. | 43 |
|--|-----------|

| | |
|--|-----------|
| ЗАРУБІЖНИЙ ДОСВІД НАДАННЯ ПУБЛІЧНИХ ПОСЛУГ ОРГАНАМИ МІСЦЕВОГО САМОВРЯДУВАННЯ В УМОВАХ РОЗВИТКУ ЕЛЕКТРОННОГО УРЯДУВАННЯ ТА ЦИФРОВІЗАЦІЇ Голобородько Т.В., Латанська І.В. | 49 |
|--|-----------|

| | |
|---|-----------|
| ІНВЕСТУВАННЯ У РОЗВИТОК ІНТЕЛЕКТУАЛЬНОГО КАПІТАЛУ МІЖНАРОДНИХ КОРПОРАЦІЙ Гринюк Н.А., Новіков В.В. | 54 |
|---|-----------|

| | |
|--|-----------|
| ОСОБЛИВОСТІ, СУБ'ЄКТИ, ОБ'ЄКТИ ТА ІНСТРУМЕНТИ ІНВЕСТИЦІЙНОЇ ПОЛІТИКИ РЕГІОНУ Сироткіна Н.Л. | 57 |
|--|-----------|

| | |
|--|-----------|
| ХАРАКТЕРИСТИКА МЕХАНІЗМУ ЕЛЕКТРОННОГО УРЯДУВАННЯ В УМОВАХ ЦИФРОВИХ ТРАНСФОРМАЦІЙ Овчаренко І.Г. | 61 |
|--|-----------|

| | |
|---|-----------|
| ХАРАКТЕРИСТИКИ САМОДОСТАТНОСТІ ТА САМОРОЗВИТКУ ТЕРИТОРІАЛЬНИХ ГРОМАД Зайдовий О.Б. | 64 |
|---|-----------|

SECTION 5.

LAW AND INTERNATIONAL LAW

| | |
|--|-----------|
| LEGAL ASPECTS OF MAKING THE DEFENSE LEGISLATION OF UKRAINE IN ACCORDANCE WITH EURO-ATLANTIC STANDARDS Moroz Kh.V. | 67 |
|--|-----------|

| | |
|---|-----------|
| ОСОБЛИВОСТІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В СОЦІАЛЬНИХ МЕРЕЖАХ: ВПЛИВ ВОЄННОГО СТАНУ Кокарча Ю.А., Лалуєва А.О. | 70 |
|---|-----------|

| | |
|--|-----------|
| ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ПІДЗВІТНОСТІ ОРГАНІВ І ПОСАДОВИХ ОСІБ МІСЦЕВОГО САМОВРЯДУВАННЯ: ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ Голик Ю.Ю. | 75 |
|--|-----------|

Кокарча Юлія Анатоліївна

кандидат політичних наук, доцент кафедри права ВТЕІ ДТЕУ
Вінницький торговельно-економічний інститут
Державного торговельно-економічного університету, Україна

Лалуєва Анастасія Олександрівна

здобувач вищої освіти першого (бакалаврського) рівня
Вінницький торговельно-економічний інститут
Державного торговельно-економічного університету, Україна

ОСОБЛИВОСТІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В СОЦІАЛЬНИХ МЕРЕЖАХ: ВПЛИВ ВОЄННОГО СТАНУ

***Анотація.** У статті проведено аналіз актуальних питань створення, обробки та захисту персональних даних в соціальних мережах. Розглянуто соціальні мережі, як основні засоби поширення інформації в мережі Інтернет. Також здійснено аналіз переваг і недоліків різних способів захисту інформації в умовах воєнного стану, який був запроваджений внаслідок збройної агресії російської федерації проти України. Проаналізовано правове регулювання захисту персональних даних в Україні та країнах ЄС. Визначено та встановлено, що правовий режим воєнного стану допускає обмеження певних конституційних прав громадян в інтересах держави та відповідно до конституційних норм обмеження права на конфіденційність персональних даних допускається в інтересах національної безпеки.*

***Ключові слова:** інформація, соціальні мережі, захист персональних даних, конфіденційність, юридична відповідальність.*

Сучасний світ є надзвичайно технологічним. Технологізація підвищує рівень життєдіяльності людства, дозволяє ефективніше працювати в усіх сферах. Розвиток сучасних інформаційних та комунікаційних технологій (web 2.0 і web 3.0) розширюють сферу і практику соціального спілкування, обумовлюють новий чи змінюють традиційний формат зв'язків і відносин.

Одним із «продуктів» інформаційного суспільства та результатів ефективного використання, розповсюдження та збирання інформації є соціальні мережі. Їх значення в житті сучасного соціуму важко переоцінити.

Обрану проблематику досліджували як зарубіжні так і вітчизняні науковці, серед них: О. М. Чальцева, М.В. Москаленко, Тім Бернерс-Лі та Марк Фічетті, О.П. Радкевич, О.Г. Рогова, В. Д. Гавловський, М. М. Кравчук, Т.П. Попович та інші.

Метою статті є визначити поняття соціальної мережі, виокремити особливості захисту персональних даних в соціальних мережах з урахуванням воєнного стану.

Розуміючи сутність соціальних мереж, погоджуємося з думкою О. М. Чальцевою, що соціальні мережі – це «певна платформа, створена в online-просторі для організації горизонтальної взаємодії користувачів. ... У процесі масових горизонтальних комунікацій в Інтернеті може вироблятися власний інформаційний контент, який створюється самими користувачами і який важко контролювати ззовні» [1, с.143].

Соціальні мережі також є одним із найбільш відвідуваних ресурсів в глобальній мережі Інтернет. Вони мають вагомe місце в житті людей. З їх допомогою аудиторія отримує новини від традиційних до альтернативних джерел, коментує їх, тлумачить та займається поширенням з них інформації, стаючи співучасником своєрідного інформаційного процесу. Сотні мільйонів користувачів щодня витрачають чимало часу для

ознайомлення із загальнотематичними новинами в мережах на зразок Instagram чи Facebook. Люди добровільно позбавляють себе бодай частини звичної приватності (заповнюють профіль правдивими даними, завантажують свої фото), заради того, щоб дізнатись більше про інших, їх інтереси та погляди на життя. Поширення інтернету, а також оптимізація робочого та вільного часу людини стимулює до відмови від класичних форм спілкування на користь нових винаходів [2, с.143].

Дуже важко уявити сучасні комунікації між людьми, які мешкають в різних містах та країнах без активного використання соціальних мереж. Безумовно - це дуже зручно, оперативно, пізнавально й нерідко - приємно. Але, на початковому етапі, щоб майбутньому користувачеві зареєструватись в певній соціальній мережі, їх власники тим чи іншим шляхом змушують надати їм добровільну і найчастіше досить широку інформацію про користувачів (тобто - про більшість з нас). А ми, в силу певних причин, не знаємо або не розуміємо цього, внаслідок чого досить часто беззастережно, швидко, і що найцікавіше - абсолютно добровільно надаємо їм таку розширену інформацію не тільки про себе, а й навіть про своїх родичів, друзів, товаришів тощо. Іноді така інформація може суперечити основним положенням Закону України «Про захист персональних даних» [3].

Виникнення нових соціальних мереж, швидке збільшення їх користувачів, популяризація використання у політичній сфері визначає також певну неузгодженість, фрагментарність науково-теоретичного висвітлення їх впливу на суспільно-політичні відносини і процеси, формування громадської думки тощо. За сучасної інформаційної доби соціальні мережі продемонстрували інструментальний і мобілізаційний потенціал самоорганізації та самоконтролю громадянського суспільства, трансформації політичної активності з віртуальної в реальну (феномен мережевих, твітерних революцій). У той же час соціальні мережі є інструментом і платформою для маніпулятивного впливу в умовах інформаційних і гібридних війн, розповсюдження неякісної інформації, розпалення протистоянь у суспільстві.

Важливо зазначити, що ще із початком впровадження в 1980-х роках, всесвітньо відомої на даний час мережі Інтернет її винахідник Тімоті Бернерс-Лі у книзі «Заснування Павутини» зазначає: «Мережа - це більш соціальне, ніж технічне явище». Задумував я її для досягнення результату - допомогти людям працювати разом, - а не як технічну іграшку. Найзагальніша мета Мережі - підтримка і поліпшення нашого існування у світі, який саме багато в чому є мережевим» [4, с.315].

Розробники Інтернету усвідомлювали, що для існування будь-якої групи ключовим є питання її цілісності, що передбачає приватність і конфіденційність. Однак, вони вважали, що «дотриманню приватності ніщо не заважає, оскільки все може здійснюватися автоматично - внесення і перевірка інформації, а також вжиття заходів забезпечення приватності» [5, с.219].

Передбачалося, що спільне використання особистої інформації при спілкуванні з іншими учасниками Мережі не заподіє жодної шкоди, а питання про конфіденційність і безпеку даних з'явилося, коли Інтернет набув світового масштабу. Розуміючи, що згода щодо приватності є «найважливішою передумовою будь-якої спільноти мережевого типу» - довірою, для забезпечення якої, розробники Всесвітньої мережі впровадили криптографію з відкритим ключем (public key cryptography - PCI), механізм шифрування інформації, завдяки якому прочитати її неможливо без ключа [6, с.470].

Однак, 12 березня 2017 р. Тімоті Бернерс-Лі однією з основних сучасних проблем Інтернету визначив втрату контролю над особистими даними. Веб - винахідник зазначив, що «значна кількість веб-сайтів пропонує безкоштовний контент в обмін на персональні дані. Багато з нас згодні з цим, хоча ми часто й приймаємо довгі та заплутані документи з умовами, але в принципі ми не заперечуємо, щоб інформація збиралася в обмін на безкоштовні послуги». Зберігаючи персональні дані особи, компанії не забезпечують можливості прямого контролю над цими даними і не дозволяють відслідковувати

інформацію про передані персональні дані третім особам [7, с.258].

Для забезпечення захисту персональних даних 14 квітня 2016 р. Європейський парламент ратифікував «Загальні положення про захист даних» (General Data Protection Regulation (GDPR), які набули чинності 25 травня 2018 р [8].

Цим актом запроваджено:

- право на забуття або право на стирання інформації;
- право на скаргу;
- право на перенесення даних та штрафи за порушення конфіденційності даних (встановлена відповідальність за порушення конфіденційності даних і в залежності від виду порушення, компанії можуть притягатися до адміністративної відповідальності у вигляді штрафу).

GDPR має екстериторіальну дію і застосовується до всіх компаній, які обробляють персональні дані резидентів і громадян ЄС, незалежно від місцезнаходження такої компанії. Зрозуміло, що філії/представництва українських організацій на території ЄС повинні будуть відповідати новим вимогам. Наприклад, компанія «А» зареєстрована на території України. Вона продає онлайн товари і надає послуги користувачам, в тому числі громадянам з країн ЄС. Послуги надаються користувачам на локальних мовах, в місцевих валютах і на національних доменах верхнього рівня країн ЄС (напр., «.de», «.nl» або «.uk»). При цьому ця організація не здійснює жодних операцій безпосередньо на території ЄС. Виникає питання чи повинна дана компанія дотримуватися положень GDPR? Так і ось чому. Компанія «А» надає послуги громадянам ЄС, оскільки: послуги оплачуються в місцевих валютах ЄС; послуги надаються на національних доменах верхнього рівня країн ЄС. Це означає, що компанія здійснює обробку персональних даних громадян ЄС на території України при наданні онлайн-послуг (наприклад, авіакомпанії, готелі, хостели тощо), що підпадає під дію GDPR, тому компанія зобов'язана дотримуватися правил ЄС у сфері обробки персональних даних [9, с.124].

Після набрання чинності «Загальних положень про захист даних» чимало компаній зіткнулися з проблемою адаптації політики приватності до нових вимог у сфері захисту персональних даних. Основні вимоги до змісту політики приватності містяться в ст.13 і ст.14 GDPR. Основна помилка при складенні політики приватності - це розпорошення інформації про окрему обробку персональних даних серед різних розділів, коли укладачі описують категорії оброблюваних даних окремо від цілей, а цілі - окремо від правових підстав обробки (згода, інтерес, вимога закону тощо). Це не слід робити, тому що суб'єкту даних (людині) не зрозуміло, з якою метою персональні дані обробляються. Наприклад, на початку 2019 р. Національна комісія з питань інформатизації і свободи Франції оштрафувала компанію «Google» на 50 мільйонів євро. Одним з порушення було те, що важлива інформація про цілі обробки, терміни зберігання категорій персональних даних, що підлягають обробці була розміщена у різних документах. Французький регулятор зазначив, що корпорація «Google» не надає споживачам чіткої та доступної інформації про те, як саме збираються та зберігаються їхні персональні дані [8].

Найбільш зацікавленими у захисті персональних даних у соціальних мережах є користувачі, а також власники ресурсу. Перші бажають зберегти у таємниці приватне життя, а другі - отримати якомога більше користувачів. Незважаючи на існування у соціальних мережах політики конфіденційності, виключно від користувачів залежить наповнення контенту персональною інформацією. На серверах соціальних мереж створюються «централізовані сховища» персональної інформації, обсяги якої з кожним днем зростають у міру того, як користувачі її наповнюють [10, с.42].

Із запровадженням в Україні воєнного стану, відповідно до Указу Президента від 24.02.2022 року «Про запровадження воєнного стану в Україні» затвердженого Законом України, в засобах масової інформації почали з'являлись повідомлення про певні випадки незаконного збирання персональних даних, не лише з метою шахрайства, а й для стеження

за волонтерами, публічними службовцями та цивільним населенням.

В умовах воєнного стану виникли нові та ускладнилися існуючі види правопорушень у досліджуваній сфері. Яскравими прикладами таких порушень є: умисне надання правоохоронним органам персональних даних особи і недостовірної інформації щодо співпраці такої особи з державою-агресором; «злиття» персональних даних військовослужбовців Збройних Сил України, журналістів, громадських активістів, членів їхніх родин з метою їх ідентифікації та подальшого переслідування пособниками держави-агресора; створення веб-сайтів з недостовірною інформацією щодо надання громадянам України матеріальної допомоги від держави або міжнародних організацій після заповнення ними анкет персональних даних з метою подальшого їх розповсюдження тощо [11].

Найбільшою кількістю персональних даних володіє держава, яка повинна дотримуватися суворих правил щодо збереження, обробки інформації, поводження з нею. Глобальною проблемою, яка не оминула навіть найбільш розвинені країни світу, залишається відсутність дієвих універсальних заходів з протидії кібератакам на державні бази даних. Слід наголосити, що кібератаки є небезпечним інструментом ведення війни, який доводить свою ефективність і потребує залучення невеликої кількості ресурсів. У відповідь на вказаний виклик Україна активно залучає до оборони національної безпеки ІТ-фахівців, що слід визнати позитивним кроком на шляху до забезпечення захисту персональних даних в умовах воєнного стану [12, с.53].

Необхідність захисту прав суб'єктів персональних даних в умовах дії правового режиму воєнного стану вкрай висока. Навіть в умовах бойових дій право на життя, право на повагу до гідності, право на свободу та особисту недоторканність, визначені в Конституції України, мають бути дотримані. Україна, яка поступово інтегрується до Європейського Союзу, має відповідне законодавство, спрямоване на створення якісної системи правового захисту персональних даних, відповідно до стандартів ЄС [13].

Зважаючи на розглянуте попередньо, варто зазначити, що користувачі сучасних інформаційних технологій повинні:

- розуміти, що їх персональні дані мають цінність та мають бути повідомлені, що компанії, особливо ті, які пропонують безкоштовні послуги, використовують їх персональні дані в управлінні своїм бізнесом та можуть надавати їх третім особам;
- ознайомитися з політикою конфіденційності компанії та продуктів, які вона пропонує споживачам;
- вміти реалізовувати і захищати свої права в умовах воєнного стану та в умовах гібридної війни, а також вимагати, щоб був дозвіл переглядати, редагувати і видаляти персональні дані, тому що, персональні дані належать виключно користувачам.

Компанії, які обробляють персональні дані в електронному вигляді, а тепер це практично кожна компанія в світі, повинні навчитися краще поєднувати ризики для конфіденційності із засобами контролю конфіденційності. Чим більший ризик використання даних, тим більше призначених для користувача елементів керування доступом до персональних даних повинно бути. Елементи керування повинні включати згоду на обробку персональних даних, зручні для читання і видимі повідомлення про конфіденційність, а також доступні налаштування конфіденційності за замовчуванням.

Впровадження GDPR - це важливий крок у підвищенні рівня захисту персональних даних в ЄС і за його межами. Європейська реформа захисту персональних даних спрямована на відновлення довіри онлайн-користувачів у сфері збору, аналізу та переміщення персональних даних. Однак, захисником персональних даних повинен бути сам користувач. Завжди потрібно ретельно стежити за тим, які персональні дані надає користувач при використанні інформаційних технологій.

Розглянувши особливості захисту персональних даних в соціальних мережах, можна зробити висновки, що захист персональних даних набуває особливої актуальності із появою цифрових технологій, поряд з цим відбувається ігнорування правил безпеки

безпосередніми користувачами. Правове регулювання захисту інформаційних даних, яке вдосконалюється, орієнтуючись на європейське законодавство, потребує подальших наукових досліджень. Також, в умовах воєнного стану нових шляхів вирішення потребують протиріччя між відкритістю та конфіденційністю інформації, також між приватними та публічними інтересами. Отже, захист персональних даних вимагає подальших наукових досліджень та вдосконалення як в теоретичному полі так і практичному, оскільки загостреність суспільних протиріч породжує нові види злочинів та правопорушень у цій сфері. Хоча важливу роль у захисті персональних даних відіграє держава, проте не менш важливим є суспільне усвідомлення значення інформації та вміння розпоряджатися нею.

Список використаних джерел:

1. Чальцева О. М. Публічна політика: теоретичний вимір і сучасна практика: монографія. Вінниця: ФОП Барановська Т. П., 2017. 336 с.
2. Москаленко М.В. Захист інформації в соціальних мережах: матеріали Всеукраїнської науково-практичної конференції. Кропивницький. 2016. 143 с.
3. Про захист персональних даних: Закон України від 01.06.2010 року №2297-VI. Дата оновлення від 27.10.2022, підстава - 2438-IX. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text> (дата звернення: 17.11.2022).
4. Тім Бернерс-Лі Марк Фічетті. Заснування павутини: з чого починалась і до чого призведе соціальна мережа: книга. Київ. 2007. С.308-329.
5. Радкевич О.П. Конфіденційність персональної інформації в соціальних мережах: вісник Вищої ради юстиції. Київ. 2012. С. 215-224.
6. Рогова О.Г. Захист персональних даних у законодавстві Європейського Союзу та України: теорія та практика державного управління. 2011. Київ. С. 464-471.
7. Гавловський В. Д. До питання захисту персональних даних у соціальних мережах. Боротьба з організованою злочинністю і корупцією: теорія і практика. Київ. 2011. С. 252-262.
8. Про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних): Регламент Європейського парламенту і ради (ЄС) 2016/679 від 27.04.2016 року. Дата оновлення від 27.04.2016. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення: 16.11.2022).
9. Кравчук М. М. Міжнародний досвід правового регулювання захисту персональних даних в мережі Інтернет: наукові записки Інституту законодавства Верховної Ради України. Київ. 2013. С. 123-126.
10. Брижко В.М. Захист персональних даних: реалії та практика сучасності: інформація і право. Київ. 2013. С. 31-49.
11. Злив персональних даних українців: що сталося і як захиститися. Радіо Свобода. 2021. URL: <https://www.radiosvoboda.org/a/zlyvdanyx-i-diya/30610626.html> (дата звернення: 18.11.2022).
12. Попович Т.П. Право особи на захист персональних даних в Інтернеті: теоретико-правові аспекти: аналітично-порівняльне правознавство. 2021. Львів. С. 51-54.
13. Конституція України: 28.06.1996 року, документ 254к/96-ВР. Дата оновлення від 01.01.2020, підстава - 27-IX. URL: <https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text> (дата звернення: 17.11.2022).