УДК 004.056 DOI https://doi.org/10.35546/kntu2078-4481.2024.2.23

В. В. КАЛЬЧЕНКО
старший викладач кафедри кібербезпеки
Сумський державний університет,
підполковник
Управління Державної служби спеціального зв'язку
та захисту інформації України в Сумській області
ORCID: 0000-0001-6492-3806

В. К. ОБОДЯК
кандидат технічних наук, доцент,
доцент кафедри кібербезпеки
Сумський державний університет,
магістрант
Харківський національний університет радіоелектроніки
ORCID: 0000-0002-8539-1252

І. О. ПУГАЧ
асистент кафедри кібербезпеки
Сумський державний університет,
магістрант
Сумський державний університет
ORCID: 0009-0002-9644-9357

НОРМАТИВНІ ВИМОГИ УКРАЇНИ В СФЕРІ КІБЕРЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ У ПОРІВНЯННІ З ВИМОГАМИ США ТА ЄС

У сучасних реаліях, захист персональних даних є невід'ємною складовою прогресу суспільства та суттєвою впливає на його безпеку життєдіяльності. Захист персональних даних – це не лише особиста відповідальність, але й важливий аспект функціонування держави та бізнесу. В статті розглянуто актуальне питання застосування нормативних вимог у сфері кіберзахисту для збереження персональних даних, які обробляються в інформаційно-комунікаційних системах. Система захисту персональних даних в Україні потребує ретельного дослідження та вдосконалення, а отже існує необхідність вивчення нормативних документів Сполучених Штатів Америки та Європейського Союзу, які визнані лідерами у сфері захисту персональних даних. Для цього необхідно провести порівняння нормативних вимог України, США та ЄС з акцентом на кіберзахист, а не лише на організаційні аспекти захисту.

Забезпечення кібербезпеки та захисту персональних даних – є ключовим фактором розвитку цифрової економіки України. Однак маємо зазначити, що положення американських та європейських актів щодо захисту персональних даних значно ширші, ніж у Законі України «Про захист персональних даних». Виявлення прогалин та недоліків у нормативному регулюванні кіберзахисту персональних даних в Україні є основою для подальшого покращення нормативних документів.

Впровадження норм та американського та європейського законодавства у сферу безпеки персональних в Україні значно посилить кіберзахист персональних даних. Що в свою чергу значно покращить рівень довіри громадян та бізнесу до держави, стимулюватиме розвиток цифрової економіки та сприятиме інтеграції України в світовий цифровий простір.

Перспективою подальших досліджень має стати розробка методики оцінки рівня кіберзахисту персональних даних в інформаційно-комунікаційних системах, розробка рекомендацій щодо кіберзахисту на основі кращих світових норм та практик, що допоможе Україні стати лідером у цій галузі.

Ключові слова: *кіберзахист, персональні дані, захист інформації, нормативні вимоги, CCPA, GDPR.*

V. V. KALCHENKO
Senior Lecturer at the Cybersecurity Department
Sumy State University,
Lieutenant Colonel
Office of the State Service of Special Communications
and Information Protection of Ukraine in Sumy Oblast
ORCID: 0000-0001-6492-3806

V. K. OBODIAK
Candidate of Technical Science, Associate Professor,
Associate Professor at the Cybersecurity Department
Sumy State University,
Master of Science Student
Kharkiv National University of Radio Electronics
ORCID: 0000-0002-8539-1252

I. O. PUHACH
Assistant Lecturer at the Cybersecurity Department
Sumy State University,
Master of Science Student
Sumy State University
ORCID: 0009-0002-9644-9357

REGULATORY REQUIREMENTS OF UKRAINE IN THE FIELD OF CYBER PROTECTION OF PERSONAL DATA IN INFORMATION AND COMMUNICATION SYSTEMS IN COMPARISON WITH THE REQUIREMENTS OF THE USA AND THE EU

In today's realities, the protection of personal data is an integral part of the society's progress and has a significant impact on its safety. Protection of personal data is not only a personal responsibility, but also an important aspect of the functioning of the state and business. The article deals with the topical issue of the application of regulatory requirements in the field of cyber protection for the preservation of personal data processed in information and communication systems. The personal data protection system in Ukraine needs research and improvement, and therefore there is a need to study the regulatory documents of the United States of America and the European Union, which are recognized as leaders in the field of personal data protection. It is necessary to compare the regulatory requirements of Ukraine, the USA and the EU with an emphasis on cyber protection, but not just on the protection of personal data.

Ensuring cyber security and protection of personal data is a key factor in the development of Ukraine's digital economy. However, it's noteworthy that the provisions of the American and European acts on the protection of personal data are much broader than mentioned in Ukraine's Law "On the Protection of Personal Data". The identification of gaps and deficiencies in the regulations of cyber protection of personal data in Ukraine is the basis for further improvement of regulatory documents.

The implementation of norms and regulatory principles of American and European legislation in the field of personal security in Ukraine will significantly strengthen the cyber protection of personal data. For example, this will significantly improve the trust level of citizens and businesses to the state, stimulate the development of the digital economy and contribute to Ukraine's integration into the global digital space.

The perspective of further research should be the development of a methodology for assessing the level of cyber protection of personal data in information and communication systems, the development of recommendations for the implementation of the best global norms and practices, which will help Ukraine become a leader in this field.

Key words: *cybersecurity, personal data, information protection, regulatory requirements, CCPA, GDPR.*

Постановка проблеми

Цифровий та інформаційний розвиток суспільства значно розширив можливості спілкування на відстані. Ведення бізнесу, фінансові операції, обмін інформацією стали швидкими та доступними завдяки мережі Інтернет. Цей стрімкий розвиток, окрім безперечних переваг, несе за собою й нові виклики, пов'язані з кібербезпекою. Підприємства стикаються з ризиком кібератак, крадіжок даних та інших загроз, а це може призвести до значних фінансових втрат та шкоді репутації. Водночас зростає проблема кіберзахисту персональних даних громадян, які обробляються в інформаційно-комунікаційних системах та вимагає посилення заходів для їх захисту від несанкціонованого доступу, використання та розкриття. Беззаперечно можна стверджувати, що темпи розвитку законодавства не завжди відповідають динаміці розвитку технологій, у свою чергу це призводить до проблем з правовим регулюванням кібервзаємовідносин, особливо в питаннях захисту персональних даних.

Аналіз останніх досліджень і публікацій

Тема захисту персональних даних набула значної популярності в наукових дослідженнях.

Деякі з них зосереджуються на аналізі викликів для конфіденційності користувачів та захисту персональних даних в контексті Інтернету речей [1]. Інші дослідження [2] розглядають необхідність регулювання конфіденційності даних та штучного інтелекту з позицій Загального європейського регламенту захисту даних (GDPR) [3]. Також існують роботи, де аналізуються проблеми особистої інформаційної безпеки та пропонуються шляхи вдосконалення кримінальної відповідальності з точки зору інформаційної безпеки громадян [4]. Також розпочато порівняння характеристик нормативних вимог України та ЄС у сфері кіберзахисту персональних даних [5].

Варто зауважити, що більшість дослідників зосереджуються на захисті персональних даних, нехтуючи кіберзахистом систем, де вони знаходяться, що може призвести до вразливості даних до кібератак. Необхідно приділяти однакову увагу обом аспектам: захисту даних та кіберзахисту систем в цілому для забезпечення сталості їх роботи.

Формулювання мети статті

Метою даного дослідження є проведення комплексного аналізу та порівняння нормативних вимог щодо кіберзахисту персональних даних в Україні, США та ЄС. Стаття має на меті виявлення прогалин та недоліків у нормативному регулюванні кіберзахисту персональних даних в Україні. Практична значущість дослідження полягає в тому, що розроблені рекомендації можуть бути використані для вдосконалення нормативного регулювання кіберзахисту не лише персональних даних в Україні, а й іншої інформації з обмеженим доступом, що не становить державної таємниці

Викладення основного матеріалу дослідження

Забезпечення інформаційної безпеки, в тому числі захист персональних даних, в США є важливим аспектом національної політики. Регуляторна база нормативних документів утворює сукупність федеральних законів, законів штатів, національних стандартів та стратегій, що створюють єдину правову систему для формування та проведення державної політики у сфері безпеки інформації, яка циркулює в інформаційних системах різних рівнів.

Одним із перших в світі нормативних актів, що заклав основні принципи обробки та захисту персональних даних суб'єктів став Закон США «Про приватність» (Privacy Act) [6], ухвалений у 1974 році. Законом визначено право особи на приватність, як особисте та фундаментальне, що охороняється Конституцією США й прирівнюється до основних громадянських вольностей та свобод. За суб'єктом персональних даних законом закріплено комплекс повноважень, які дозволяють здійснювати контроль за використанням своїх персональних даних федеральними відомствами та відповідними посадовими особами. До їх числа належать:

– право бути обізнаним про існування системи персональних даних;

– право бути обізнаним про цілі збору й обробки інформації;

– право на доступ до своїх персональних даних, на їхнє вивчення і отримання копії всіх даних чи їхньої частини;

– право вимагати внесення змін і доповнень у свої персональні дані.

Однак дія принципів покладених в основу цього акту значною мірою послаблюється формулюваннями, що дозволяють окремим відомствам уникати незручних вимог та значною кількістю виключень. Також варто зазначити, що з часу прийняття акту інформаційні системи значною мірою розвинулись і правове регулювання вже не відповідає сучасним умовам обробки персональних даних.

В Україні існує свій національний нормативний акт – Закон «Про захист персональних даних», який Верховна Рада України ухвалила 1 червня 2010 р. [7]. Законом утверджуються права суб'єктів персональних даних, принципи та підстави обробки персональних даних, норми щодо обробки конфіденційних категорій персональних даних, обмеження дії Закону, повноваження наглядового органу, тощо. Однак згаданий Закон не визначає вимог до комп'ютерних та інформаційних систем, в яких персональні дані циркулюють та обробляються. Закон майже цілком базується на положеннях Директиви 95/46/ЄС Європейського парламенту і Ради «Про захист фізичних осіб у зв'язку з обробкою персональних даних і вільне переміщення таких даних» від 24 жовтня 1995 року [8], яка наразі не діє і замінена Загальним регламентом із захисту персональних даних (General Data Protection Regulation – GDPR) [3].

Згідно з Планом заходів щодо імплементації Угоди про асоціацію між Україною та ЄС [9], а саме пунктом 11, Україна взяла на себе зобов'язання імплементувати норми GDPR у законодавство. У зв'язку з чим до Верховної Ради України 7 червня 2021 р. було подано проект Закону України «Про захист персональних даних» [10], який було відхилено. А 25 жовтня 2022 р. було внесено проект Закону України «Про захист персональних даних» [11], який на теперішній час перебуває на розгляді.

Усі суб'єкти, що здійснюють свою діяльність на території ЄС та обробляє персональні дані громадян ЄС на інших територіях зобов'язані дотримуватися норм Регламенту GDPR [3].

GDPR, як регламент ЄС, безпосередньо застосовується з однаковою силою в кожній з 27 держав-членів без необхідності прийняття окремих національних законів, однак він забезпечує гнучкість щодо імплементації, зміни або відступу від деяких положень в окремих країнах.

Вцілому, захист персональних даних в країнах ЄС регулюється GDPR, однак в кожній з держав існує власний галузевий нормативний акт, який імплементує чи розширює Загальний регламент.

Так, наприклад, в Австрії [12]:

– вік, за яким дитина може особисто розпоряджатися своїми персональними даними, знижено до 14 років, замість 16 в GDPR;

– регулюється система фото та відео нагляду, в частині захисту персональних даних;

– наявні стандарти обробки даних для статистичних, історичних та наукових потреб, а також у випадку невідкладної необхідності;

– не вимагається миттєве видалення даних, у випадку коли це неможливо зробити з економічних чи технічних причин.

У законодавстві Хорватії [13]:

– надано особливої уваги захисту даних неповнолітніх та прийнято відповідні регуляторні норми;

– регулюється система генетичних та біометричних даних, введено систему додаткового захисту;

– визначено особливості системи фото та відео нагляду, в частині захисту персональних даних;

– окреслені стандарти обробки даних для статистичних, історичних та наукових потреб, а також у випадку невідкладної необхідності.

Нормативні акти Чехії [14], Данії [15], Франції [16], Німеччині [17], Ірландії [18], Італії [19], Нідерланди [20], Польщі [21], Іспанія [22], Швеція [23] передбачають окремі регуляції захисту персональних даних для систем електронної комерції та маркетингу.

Акт про захист даних Фінляндії [24] встановлює:

– право громадян з 13 років розпоряджатися персональними даними на власний розсуд;

– повідомлення про витік даних має бути оголошено за 24 години, в GDPR 72 години.

Аналогічним нормативним акт в Литві [25]:

– зменшено вік вільного розпорядження персональних даних до 14 років;

– встановлено штрафи за порушення галузевого законодавства у розмірі 1–1,5% річного обороту.

Проаналізувавши нормативні акти України у сфері захисту персональних даних можна дійти висновку, що вони є застарілим та не відповідають рівню сучасного цифрового розвитку.

В нормах проекту Закону України «Про захист персональних даних» [11] можна побачити, що зміни вносяться у положення щодо доступу до персональних даних, змінюються деякі терміни та визначення, а також вводиться посада «Відповідальної особи з питань захисту персональних даних». Додатково цим проектом закону пропонується внести зміни в деякі нормативні акти, дія яких безпосередньо стосується обробки персональних даних суб'єктів, у сферах трудових відносин, електронної комерції, охорони здоров'я та електронних комунікацій. Проектом пропонується впровадження відповідальності за порушення законодавства у сфері персональних даних у вигляді штрафів.

Як зазначалося, в США система нормативного регулювання безпеки персональних даних та інформаційної безпеки в цілому є розгалуженою та децентрацлізованою, однак існує кілька нормативних документів, які варто розглянути.

1 січня 2020 р. набрав чинності Закон Каліфорнії про захист персональних даних споживачів (California Consumer Privacy Act – CCPA) [26], яким вносяться зміни в розділ «Персональні дані» цивільного кодексу штату Каліфорнія [27]. До основних норм, які передбачає закон можна віднести:

1. Особа, дані якої збираються, має знати яка інформація збирається та цілі її збору, а також категорії інформації яку розпорядник має розкрити на вимогу споживача.

2. Розпорядник інформації має на верифікований запит споживача видалити персональні дані особи.

3. Компанії зобов'язані повідомити споживачів про факт продажу (передачі) даних третім особам. В свою чергу споживач має право відмовитись від продажу цієї інформації.

4. Підприємство не повинно дискримінувати споживача, який користується будь-якими правами споживача відповідно до CCPA. В свою чергу компанія може стягувати іншу вартість або надавати товари чи послуги іншої якості, якщо різниця обґрунтовано пов'язана з даними, які надає споживач, і може запропонувати споживачеві фінансові стимули для збору, продажу чи видалення. особистої інформації на основі попередньої згоди.

Порівнюючи GDPR та CCPA варто зазначити, що акти регулюють майже однакові відносини, однак мають деякі відмінності. Так норми CCPA поширюються на підприємства та організації, що обробляють дані для комерційних цілей виключно на території штату Каліфорнія, на противагу ж GDPR має ширшу дію та охоплює територію ЄС. Проте обидва мають спільну рису та захищають суб'єктів персональних даних розташованих поза юрисдикцією актів. Якщо розглядати суб'єкти захисту, CCPA захищає споживачів резидентів штату. У той же час GDPR захищає ідентифікованих суб'єктів персональних даних та осіб, яких ці дані стосуються. За визначеннями «персональних даних» CCPA окрім особистої інформації, що ідентифікує, стосується чи може бути конкретно або опосередковано пов'язана не лише зі споживачем, але й з домогосподарством.

Не зважаючи на значну схожість вимог нормативних актів існує деякий ряд відмінностей. Наприклад, CCPA гарантує право відмови від використання персональних даних компаніями з метою їх подальшого продажу, однак Загальний регламент [3] такої опції не включає. Відповідно до Закону Каліфорнії персональні дані осіб віком до 16-ти років не можуть використовуватися для продажу без згоди законних представників цієї особи. Загальним регламентом передбачена обов'язкова згода законних представників на будь-яку обробку персональних даних осіб до 16-ти років. Проте GDPR надає право виправляти некоректні персональні дані та доповнювати їх, що не передбачає CCPA.

В США діє стандарт NIST Privacy Framework [28], положення якого щодо безпеки персональних даних значною мірою схожі на CCPA та GDPR з точки зору практик та принципів регулювання. Стандарт функціонує на основі трьох основних принципів: ідентифікація, захист, моніторинг та оцінка. Цей стандарт впроваджується в організації як покроковий процес. Організації повинні почати з проведення оцінки ризиків конфіденційності та розробки персоналізованої програми конфіденційності. Ця програма повинна включати процеси та процедури захисту персональних даних, а також технічний контроль для їх захисту. Після того, як програму буде запущено, організації повинні контролювати та переглядати свою практику конфіденційності та вносити необхідні зміни.

NIST Privacy Framework надає організаціям набір передових практик і технічних вказівок щодо захисту особистої інформації. Стандарт розроблений бути гнучким для організацій, аби вони могли пристосувати власні методи конфіденційності відповідно до своїх конкретних потреб. Використовуючи структуру, організації можуть гарантувати, що їхні методи захисту конфіденційності даних відповідають галузевим стандартам і нормам.

Варто звернути увагу на національну стратегію кібербезпеки США [29] від березня 2023 року та стратегію кібербезпеки України [30], яка затверджена указом Президента 26 серпня 2021 року.

В українській стратегії кібербезпеки захист персональних даних згадується виключно у вигляді стратегічного завдання для виконання цілі К.3 Безпечні цифрові послуги – «підвищення ефективності системи захисту персональних даних громадян шляхом гармонізації законодавства України з відповідним законодавством ЄС та посилення відповідальності за порушення встановлених вимог».

В національній стратегії кібербезпеки США безпека персональних даних розглядається як комплекс критичної інформації, що потребує захисту на державному рівні. Так, в частині третій стратегії, однією з цілей визначено «захист персональних даних – фундаментальний аспект захисту приватності споживачів у цифровому майбутньому».

Технології, що ґрунтуються на даних, суттєво змінили економіку та пропонують безліч зручностей для споживачів. Проте, стрімке поширення особистої інформації розширює поле загроз і робить витоки даних більш руйнівними для людей. Коли організації, які володіють даними про людей, нехтують відповідальністю за їх обробку, вони перекладають тягар витрат на звичайних громадян. Найбільш вразливими є незахищені верстви населення, які ризикують зазнати непропорційної шкоди через витік даних.

Адміністрація президента США підтримує законодавчі зусилля, що спрямовані на:

1. Встановлення жорстких та чітких обмежень на збір, використання, передачу та зберігання особистих даних.
2. Забезпечення надійного захисту конфіденційної інформації, такої як дані про геолокацію та стан здоров'я.
3. Розробку національних стандартів захисту персональних даних, що відповідають нормам NIST.

Забезпечуючи еволюцію норм конфіденційності відповідно до нових загроз, США можуть прокласти шлях до безпечнішого майбутнього, де люди зможуть використовувати технології без ризику для своєї особистої інформації.

Висновки

Провівши дослідження та аналіз основних нормативних документів України, США і ЄС в сфері безпеки персональних даних, можна дійти висновку, що в жодному з наведених актів не визначено явних та однозначних вимог щодо кіберзахисту персональних даних. При цьому вимоги щодо безпеки персональних даних CCPA та GDPR значно ширші порівняно з нинішнім законодавством України. У разі ухвалення проекту закону від 25 жовтня 2022 р. [11] значно покращиться та осучасниться система нормативно-правового регулювання охорони персональних даних України. Прийняття закону є необхідним та дозволить привести нормативну базу до актуального стану. Проте відсутність системи регулювання обробки персональних даних неповнолітніх можна визначити як один з недоліків проекту. Ще одним з недоліків проекту є відсутність однозначного регулювання вимог до інформаційно-комунікаційних систем, в яких обробляються та циркулюють критичні особисті дані. Перспективою для подальших досліджень має стати вироблення явних та однозначних рекомендацій по вдосконаленню нормативних документів в Україні, спрямованих на регулювання системи захисту персональних даних, норм щодо інформаційно-комунікаційних систем, в яких обробляється і зберігається особиста інформація.

Публікація підготовлена у рамках проєкту Модуль Жана Моне «Досвід ЄС щодо захисту персональних даних у кіберпросторі» (2023–2026 – EUEPPDC – 101125350 – ERASMUS-JMO-2023-MODULE).

Список використаної літератури

1. Romansky, Radi. (2023). Internet of Things and User Privacy Protection. 37th International Conference on Information Technologies, InfoTech 2023 – Proceedings. URL: http://infotech-bg.com/proceedings.

2. Brown, R., Truby J., Imad Antoine Ibrahim. Mending Lacunas in the EU's GDPR and Proposed Artificial Intelligence Regulation. European Studies. Volume 9 (2022): Issue 1. (August 2022). URL: https://sciendo.com/issue/EUSTU/9/1/.

3. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN.

4. Yu Zhang, Haoyun Dong. Criminal law regulation of cyber fraud crimes—from the perspective of citizens' personal information protection in the era of edge computing. Journal of Cloud Computing volume 12, Article number: 64 (2023). URL: https://journalofcloudcomputing.springeropen.com/articles/10.1186/s13677-023-00437-3#citeas.

5. Кальченко, В., Ободяк, В. (2024). Порівняльна характеристика нормативних вимог України та ЄС у сфері кіберзахисту персональних даних в інформаційно-комунікаційних системах. Інформаційні технології та суспільство, (5 (11), 14-20. https://doi.org/10.32689/maup.it.2023.5.2.

6. Privacy Act of 1974. U.S. Government Information. URL: https://www.govinfo.gov/content/pkg/STATUTE-88/pdf/STATUTE-88-Pg1896.pdf.

7. Закон України "Про захист персональних даних". URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text.

8. Директива 95/46/ЄС Європейського парламенту і Ради «Про захист фізичних осіб у зв'язку з обробкою персональних даних і вільне переміщення таких даних» від 24 жовтня 1995 року. URL: https://zakon.rada.gov.ua/laws/show/994_242#Text.

9. План заходів з виконання Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони. Затверджено постановою Кабінету Міністрів України від 25 жовтня 2017 р. № 1106. URL: https://zakon.rada.gov.ua/laws/show/1106-2017-%D0%BF#Text.

10. Проект Закону України "Про захист персональних даних" від 07.06.2021 р. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/26873.

11. Проект Закону України "Про захист персональних даних" від 25.10.2022. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/40707.

12. Federal Act concerning the Protection of Personal Data (DSG). URL: https://www.ris.bka.gv.at/Dokumente/Erv/ERV_1999_1_165/ERV_1999_1_165.html.

13. Act on the implementation of the general data protection regulation. URL: https://azop.hr/national-legislation/.

14. Act of 12 March 2019 about the processing of personal data. URL: https://www.zakonyprolidi.cz/translation/cs/2019-110?langid=1033&srcid=1029.

15. Lov nr 502 af 23/05/2018 om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven). URL: https://www.retsinformation.dk/eli/lta/2018/502.

16. La loi Informatique et Libertés. URL: https://www.cnil.fr/fr/la-loi-informatique-et-libertes.

17. Federal Data Protection Act (BDSG). URL: https://www.gesetze-im-internet.de/englisch_bdsg/index.html.

18. Data protection act 2018. Number 7 of 2018. URL: https://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/html.

19. Personal data protection code. Containing provisions to adapt the national legislation to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. URL: https://www.garanteprivacy.it/codice.

20. Uitvoeringswet Algemene verordening gegevensbescherming. URL: https://wetten.overheid.nl/BWBR0040940/2021-07-01.

21. The Act of 10 May 2018 on the Protection of Personal Data. URL: https://uodo.gov.pl/en/660/1464.

22. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. URL: https://www.boe.es/eli/es/lo/2018/12/05/3.

23. Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning. URL: https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/lag-2018218-med-kompletterande-bestammelser_sfs-2018-218/.

24. Data Protection Act (1050/2018, amendments up to 239/2023 included) Translation from Finnish. URL: https://www.finlex.fi/en/laki/kaannokset/2018/en20181050.pdf.

25. Republic of Lithuania Law on legal protection of personal data, 11 June 1996 No I-1374 (As last amended on 3 November 2016 – No XII-2709). URL: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/ef70b5d2f14811e78f3dc265493430ae.

26. California Consumer Privacy Act of 2018. URL: https://cppa.ca.gov/regulations/pdf/cppa_act.pdf.

27. The Civil Code of California. URL: https://leginfo.legislature.ca.gov/faces/codesTOCSelected.xhtml?tocCode=CIV&tocTitle=+Civil+Code+-+CIV.

28. NIST Privacy Framework: a tool for improving privacy through enterprise risk management, version 1.0. URL: https://doi.org/10.6028/NIST.CSWP.01162020.

29. National Cybersecurity Strategy, March 1, 2023. URL: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf .

30. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України". URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text.

References

1. Romansky, Radi. (2023). Internet of Things and User Privacy Protection. *37th International Conference on Information Technologies, InfoTech 2023 – Proceedings. http://infotech-bg.com.* Retrieved from http://infotech-bg.com/proceedings.

2. Brown, R., Truby J., Imad Antoine Ibrahim. Mending Lacunas in the EU's GDPR and Proposed Artificial Intelligence Regulation. *European Studies. Volume 9 (2022): Issue 1. (August 2022). https://sciendo.com.* Retrieved from https://sciendo.com/issue/EUSTU/9/1/.

3. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). (2016). *https://eur-lex.europa.eu.* Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN.

4. Yu Zhang, Haoyun Dong. Criminal law regulation of cyber fraud crimes—from the perspective of citizens' personal information protection in the era of edge computing. *Journal of Cloud Computing volume 12, Article number: 64 (2023). https://journalofcloudcomputing.springeropen.com.* Retrieved from https://journalofcloudcomputing.springeropen.com/articles/10.1186/s13677-023-00437-3#citeas.

5. Kalchenko, V., Obodiak, V. (2024). Porivnialna kharakterystyka normatyvnykh vymoh Ukrainy ta YeS u sferi kiberzakhystu personalnykh danykh v informatsiino-komunikatsiinykh systemakh. *Informatsiini tekhnolohii ta suspilstvo, (5 (11)), 14-20.* [Kalchenko, V., Obodiak, V. (2024). Comparative characteristics of the regulatory requirements of Ukraine and the EU in the field of personal data cyber protection in information and communication systems. I*nformation Technology and Society(5 (11)), 14-20.*] *https://journals.maup.com.ua/.* Retrieved from https://doi.org/10.32689/maup.it.2023.5.2 [in Ukrainian].

6. Privacy Act of 1974. U.S. Government Information. *https://www.govinfo.gov* Retrieved from https://www.govinfo.gov/content/pkg/STATUTE-88/pdf/STATUTE-88-Pg1896.pdf.

7. Zakon Ukrainy "Pro zakhyst personalnykh danykh". [Law of Ukraine "On Personal Data Protection"]. (n.d.). https://zakon.rada.gov.ua. Retrieved from https://zakon.rada.gov.ua/laws/show/2297-17#Text [in Ukrainian].

8. Dyrektyva 95/46/IeS Yevropeiskoho parlamentu i Rady «Pro zakhyst fizychnykh osib u zv'iazku z obrobkoiu personalnykh danykh i vilne peremishchennia takykh danykh». [Directive 95/46/EU of the European Parliament and the Council "On the protection of natural persons in connection with the processing of personal data and the free movement of such data"]. (1995). *https://zakon.rada.gov.ua*. Retrieved from https://zakon.rada.gov.ua/laws/show/994_242#Text [in Ukrainian].

9. Plan zakhodiv z vykonannia Uhody pro asotsiatsiiu mizh Ukrainoiu, z odniiei storony, ta Yevropeiskym Soiuzom, Yevropeiskym ta Yevropeiskym Soiuzom, Yevropeiskym spivtovarystvom z atomnoi enerhii i yikhnimy derzhavamy-chlenamy, z inshoi storony. Zatverdzheno postanovoiu Kabinetu Ministriv Ukrainy vid 25 zhovtnia 2017 r. № 1106. [Action plan for the implementation of the Association Agreement between Ukraine, on the one hand, and the European Union, the European and European Union, the European Atomic Energy Community and their member states, on the other hand. Approved by the Resolution of the Cabinet of Ministers of Ukraine dated October 25, 2017 No. 1106]. (2017) *https://zakon.rada.gov.ua*. Retrieved from https://zakon.rada.gov.ua/laws/show/1106-2017-%D0%BF#Text [in Ukrainian].

10. Proekt Zakonu Ukrainy "Pro zakhyst personalnykh danykh" vid 07 chervnia 2021 r.. [The Draft Law of Ukraine "On Personal Data Protection" dated June 07, 2021]. (n.d.). *https://itd.rada.gov.ua.* Retrieved from https://itd.rada.gov.ua/billInfo/Bills/Card/26873 [in Ukrainian].

11. Proekt Zakonu Ukrainy "Pro zakhyst personalnykh danykh" vid 25 zhovtnia 2022 r.. [The Draft Law of Ukraine "On Personal Data Protection" dated October 25, 2022]. (n.d.). *https://itd.rada.gov.ua.* Retrieved from https://itd.rada.gov.ua/billInfo/Bills/Card/40707 [in Ukrainian].

12. Federal Act concerning the Protection of Personal Data (DSG). *https://www.ris.bka.gv.at* Retrieved from https://www.ris.bka.gv.at/Dokumente/Erv/ERV_1999_1_165/ERV_1999_1_165.html.

13. Act on the implementation of the general data protection regulation. *https://azop.hr* Retrieved from https://azop.hr/national-legislation/.

14. Act of 12 March 2019 about the processing of personal data. *https://www.zakonyprolidi.cz* Retrieved from https://www.zakonyprolidi.cz/translation/cs/2019-110?langid=1033&srcid=1029.

15. Lov nr 502 af 23/05/2018 om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven). [Act no. 502 of 23/05/2018 on supplementary provisions to the regulation on the protection of natural persons in connection with the processing of personal data and on the free exchange of such information (Data Protection Act).] *https://www.retsinformation.dk* Retrieved from https://www.retsinformation.dk/eli/lta/2018/502 [in Danish].

16. La loi Informatique et Libertés.[The Data Protection Act] Retrieved from https://www.cnil.fr/fr/la-loi-informatique-et-libertes [in French].

17. Federal Data Protection Act (BDSG). *https://www.gesetze-im-internet.de* Retrieved from https://www.gesetze-im-internet.de/englisch_bdsg/index.html.

18. Data protection act 2018. Number 7 of 2018. *https://www.irishstatutebook.ie* Retrieved from https://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/html.

19. Personal data protection code. Containing provisions to adapt the national legislation to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. https://www.garanteprivacy.it Retrieved from https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9740796.

20. Uitvoeringswet Algemene verordening gegevensbescherming. [Implementation Act of the General Data Protection Regulation]. *https://wetten.overheid.nl* Retrieved from https://wetten.overheid.nl/BWBR0040940/2021-07-01 [in Dutch].

21. The Act of 10 May 2018 on the Protection of Personal Data. *https://uodo.gov.pl* Retrieved from https://uodo.gov.pl/en/660/1464.

22. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. [Organic Law 3/2018, of December 5, on the Protection of Personal Data and guarantee of digital rights] *https://www.boe.es* Retrieved from https://www.boe.es/eli/es/lo/2018/12/05/3 [in Spanish].

23. Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning. [Act (2018:218) with supplementary provisions to the EU's data protection regulation]. *https://www.riksdagen.se* Retrieved from https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/lag-2018218-med-kompletterande-bestammelser_sfs-2018-218/ [in Swedish].

24. Data Protection Act (1050/2018, amendments up to 239/2023 included) Translation from Finnish. *https://www.finlex.fi* Retrieved from https://www.finlex.fi/en/laki/kaannokset/2018/en20181050.pdf.

25. Republic of Lithuania Law on legal protection of personal data, 11 June 1996 No I-1374 (As last amended on 3 November 2016 – No XII-2709). *https://e-seimas.lrs.lt* Retrieved from https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/ef70b5d2f14811e78f3dc265493430ae

26. California Consumer Privacy Act of 2018. *https://cppa.ca.gov* Retrieved from https://cppa.ca.gov/regulations/pdf/cppa_act.pdf .

27. The Civil Code of California. *https://leginfo.legislature.ca.gov* Retrieved from https://leginfo.legislature.ca.gov/faces/codesTOCSelected.xhtml?tocCode=CIV&tocTitle=+Civil+Code+-+CIV.

28. NIST Privacy Framework: a tool for improving privacy through enterprise risk management, version 1.0. *https://nvlpubs.nist.gov* Retrieved from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf.

29. National Cybersecurity Strategy, March 1, 2023. *https://www.whitehouse.gov* Retrieved from https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf .

30. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 travnia 2021 roku "Pro Stratehiiu kiberbezpeky Ukrainy". [On the decision of the National Security and Defense Council of Ukraine dated May 14, 2021 "On the Cybersecurity Strategy of Ukraine"]. *https://zakon.rada.gov.ua* Retrieved from https://zakon.rada.gov.ua/laws/show/447/2021#Text [in Ukrainian].