

УДК 004.056.5

DOI <https://doi.org/10.32689/maup.it.2023.5.2>

Вадим КАЛЬЧЕНКО

старший викладач кафедри кібербезпеки, Сумський державний університет, вул. Харківська, 116, Суми, Україна, індекс 40007; підполковник, Управління Державної служби спеціального зв'язку та захисту інформації України в Сумській області, вул. Герасима Кондратьєва, 32/1, Суми, Україна, індекс 40000 (v.kalchenko@cto.is.sumdu.edu.ua)

ORCID: 0000-0001-6492-3806

Віктор ОБОДЯК

кандидат технічних наук, доцент, доцент кафедри кібербезпеки, Сумський державний університет, вул. Харківська, 116, Суми, Україна, індекс 40007; студент магістратури, Харківський національний університет радіоелектроніки, просп. Науки, 14, Харків, Україна, індекс 61166 (v.obodyak@cs.sumdu.edu.ua)

ORCID: 0000-0002-8539-1252

Vadym KALCHENKO

Senior Lecturer at the Cybersecurity Department, Sumy State University, 116, Kharkivska St, Sumy, Ukraine, postal code 40007; Lieutenant Colonel, Office of the State Service of Special Communications and Information Protection of Ukraine in Sumy Oblast, 32/1, Gerasyma Kondratieva St, Sumy, Ukraine, postal code 40000 (v.kalchenko@cto.is.sumdu.edu.ua)

Viktor OBODIAK

Candidate of Technical Science, Associate Professor, Associate Professor at the Cybersecurity Department, Sumy State University, 116, Kharkivska St, Sumy, Ukraine, postal code 40007; Master's Student, Kharkiv National University of Radio Electronics, 14, Nauky Ave, Kharkiv, Ukraine, postal code 61166 (v.obodyak@cs.sumdu.edu.ua)

Бібліографічний опис статті: Кальченко, В., Ободяк, В. (2023). Порівняльна характеристика нормативних вимог України та ЄС у сфері кіберзахисту персональних даних в інформаційно-комунікаційних системах. *Інформаційні технології та суспільство*, 5 (11), 14–20. DOI: <https://doi.org/10.32689/maup.it.2023.5.2>

Bibliographic description of the article: Kalchenko, V., Obodiak, V. (2023). Porivnialna kharakterystyka normatyvnykh vymoh Ukrainy ta YeS u sferi kiberzakhystu personalnykh danykh v informatsiino-komunikatsiinykh systemakh [Comparative characteristics of regulatory requirements of Ukraine and the EU in the field of personal data cyber protection in information and communication systems]. *Informatsiini tekhnologii ta suspilstvo – Information technology and society*, 5 (11), 14–20. DOI: <https://doi.org/10.32689/maup.it.2023.5.2>

ПОРІВНЯЛЬНА ХАРАКТЕРИСТИКА НОРМАТИВНИХ ВИМОГ УКРАЇНИ ТА ЄС У СФЕРІ КІБЕРЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ¹

Анотація. В статті розглянуто актуальне питання щодо застосування нормативних вимог в сфері кіберзахисту для збереження персональних даних, які обробляються в інформаційно-комунікаційних системах, адже роль глобальної мережі Інтернет стає все важливішою в житті людей незалежно від того в якій країні вони знаходяться. Можна зазначити, що проблема захисту персональних даних в жодній країні не вирішена повністю, але для досягнення більшої гарантії збереження персональних даних в своїй державі, потрібно спиратися на кращі наробки в цьому напрямку. Значних успіхів в захисті персональних даних досягли в Європейському Союзі. Відповідно, необхідно проведення досліджень, спрямованих на вивчення нормативних документів Європейського Союзу, завдяки яким досягнуті ці успіхи. Для цього, в першу чергу, потрібно порівняти нормативні вимоги України і Європейського Союзу в сфері захисту персональних даних. Особливу увагу потрібно звернути саме на кіберзахист, а не просто захист персональних даних. Адже саме в інформаційно-комунікаційних системах і відбувається основна втрата персональних даних в наш час. Результати досліджень, наведених в даній статті, показують, що нормативні документи України і основний нормативний документ Європейського Союзу, а саме «Загальний регламент про захист даних» (*General Data Protection Regulation, GDPR*), що регламентують захист персональних даних, не містять чітких і явних вимог щодо кіберзахисту персональних даних. Але вимоги GDPR, щодо захисту персональних даних більш ширші порівняно

¹ Публікація підготовлена у рамках проекту Модуль Жана Моне «Досвід ЄС щодо захисту персональних даних у кіберпросторі» (2023-2026 – EUEPPDC – 101125350 – ERASMUS-JMO-2023-MODULE)

з Законом України «Про захист персональних даних». Тому можливість впровадження норм GDPR в нормативні документи України по захисту персональних даних є актуальною. Таким чином, результатом подальших досліджень має стати вироблення конкретних рекомендацій по вдосконаленню нормативних документів в Україні, спрямованих на регулювання захисту персональних даних, які базуються на нормах GDPR. Також актуальним є дослідження з розробки концепції вимог до інформаційно-комунікаційних систем з точки зору кіберзахисту для збереження персональних даних.

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

COMPARATIVE CHARACTERISTICS OF THE REGULATORY REQUIREMENTS OF UKRAINE AND THE EU IN THE FIELD OF PERSONAL DATA CYBER PROTECTION IN INFORMATION AND COMMUNICATION SYSTEMS²

Abstract. The article discusses the timely issue of applying regulatory requirements in the field of cybersecurity for the preservation of personal data processed in information and communication systems. This is due to the increasing significance of the global Internet network in people's lives, regardless of their location. It is noteworthy that the challenge of personal data protection remains unresolved in any country. However, to ensure a higher guarantee of personal data preservation within one's country, it is crucial to rely on the best practices in this domain. Significant strides have been made in personal data protection within the European Union, prompting the need for research aimed at understanding the regulatory documents that led to these successes. To achieve this, it is imperative to compare the regulatory requirements of Ukraine and the European Union in the realm of personal data protection, giving particular attention to cybersecurity, not just personal data protection. Information and communication systems are the focal point for the primary loss of personal data in contemporary times. The research presented in this article reveals that the regulatory documents of Ukraine and the principal regulatory document of the European Union, the General Data Protection Regulation (GDPR), which governs the protection of personal data, lack clear and explicit requirements for the cybersecurity of personal data. However, GDPR requirements for personal data protection are more extensive compared to Ukraine's Law "On Personal Data Protection". Consequently, the relevance of incorporating GDPR norms into Ukraine's regulatory documents on personal data protection is evident. Thus, the result of further research should be the development of specific recommendations for improving regulatory documents in Ukraine aimed at regulating the protection of personal data, based on GDPR regulations. Research on developing the concept of requirements for information and communication systems from the perspective of cybersecurity for preserving personal data is also pertinent.

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

Актуальність теми дослідження і постановка проблеми. Останні десятиліття характеризуються значним зростанням ролі Інтернету в суспільному житті. Глобальна мережа дозволяє вести бізнес, спілкуватись в режимі онлайн між собою незважаючи на відстані, проводити фінансові операції, надавати консультації, вчитися тощо. Внаслідок цього виникають питання кіберзахисту як цифрових активів підприємств так і персональних даних громадян, які обробляються в інформаційно-комунікаційних системах. Варто констатувати, що розвиток суспільних взаємовідносин в мережі Інтернет та розвиток комп'ютерних технологій в цілому відбувається набагато швидше ніж розвиток законодавства. Внаслідок цього виникають питання правового регулювання таких взаємовідносин. Особливо це стосується кіберзахисту персональних даних в інформаційно-комунікаційних системах.

Аналіз останніх досліджень і публікацій. Захисту персональних даних присвячено надзвичайно багато досліджень. Вони можуть бути спрямовані, наприклад, на аналіз викликів для конфіденційності користувачів і захисту персональних даних інтернету речей [1]. В іншій статті [2] розглядається необхідність регулювання конфіденційності даних і штучного інтелекту через Загальний регламент захисту даних (GDPR) [3]. Є, наприклад, стаття [4] в якій розглядаються проблеми особистої інформаційної безпеки та вдосконалення кримінальної відповідальності з точки зору інформаційної безпеки громадян.

Виділення недосліджених частин загальної проблем. Основна увага дослідників звертається на проблему захисту персональних даних як таких, а не на те, що потрібно зробити в інформаційно-комунікаційних системах для захисту цих даних.

Формулювання мети статті. Метою даної статті є аналіз та порівняння наявних нормативних вимог у сфері кіберзахисту персональних даних в Україні та Європейському союзу. Також стаття має на меті виробити рекомендації щодо покращення нормативного регулювання кіберзахисту персональних даних, що обробляються в інформаційно-комунікаційних системах українських органів державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях незалежно від їх форми власності.

Виклад основного матеріалу. Вперше основні принципи обробки персональних даних, права осіб персональні дані яких обробляються, та норми щодо транскордонної передачі даних були викладені в Конвенції Ради Європи № 108 «Про захист осіб у зв'язку з автоматизованою обробкою персональних

²The publication is prepared within the Jean Monnet Module project "EU Experience in Personal Data Protection in Cyberspace" (2023-2026 – EUEPPDC – 101125350 – ERASMUS-JMO-2023-MODULE)

даних», ухваленій ще 28 січня 1981 р. [5]. З метою впровадження положень європейського нормативного акту до законодавства України, Верховна Рада України 1 червня 2010 р. ухвалила Закон «Про захист персональних даних» [6]. В ньому було закріплено принципи обробки персональних даних, права суб'єктів персональних даних, основні підстави для обробки персональних даних, підстави для обробки чутливих категорій персональних даних, положення щодо обмеження дії Закону, повноваження наглядового органу, тощо. Проте даний Закон не визначає технічних вимог до комп'ютерних систем, в яких ці персональні дані обробляються. Цей Закон фактично повністю базувався 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 [7], яка наразі скасована і замінена Загальним регламентом із захисту персональних даних (General Data Protection Regulation – GDPR) [3].

Зазначений документ обов'язковий до виконання всіма суб'єктами господарювання, які знаходяться на території ЄС. Проте його особливістю є те, що даному регламенту повинен відповідати і будь-який інший суб'єкт господарювання, який обробляє персональні дані громадян ЄС, навіть якщо він знаходиться поза його межами (в іншій країні). Наразі варто констатувати, що існуюче законодавство України в сфері захисту персональних даних застаріло і не відповідає сучасним вимогам та рівню технологічного розвитку.

Відповідно до пункту 11 Плану заходів щодо імплементації Угоди про асоціацію між Україною та ЄС [8] Україна взяла зобов'язання щодо вдосконалення законодавства про захист персональних даних та приведення його у відповідність до GDPR. До Верховної Ради України 7 червня 2021 р. було подано проєкт Закону України «Про захист персональних даних», проте даний законопроєкт не було прийнято [9].

У відповідності до статті 8 Закону України «Про захист інформації в інформаційно-комунікаційних системах» [10] інформація, вимога щодо захисту якої встановлена законом, повинна оброблятися в системі із застосуванням комплексної системи захисту інформації (КСЗІ) з підтверженою відповідністю. Підтвердження відповідності здійснюється за результатами державної експертизи в порядку, встановленому законодавством. Також варто зазначити, що в нашій країні існує низка нормативних документів системи технічного захисту інформації (НД ТЗІ), в яких висуваються вимоги як до самої комплексної системи захисту інформації, так і до порядку складання, наповнення та оформлення документів на таку систему. Аналізуючи увесь перелік українських нормативних документів та вимог, які в них містяться – комплексну систему захисту інформації можна представити у вигляді двох великих складових. Перша складова – це безпосередньо програмні, апаратні та програмно-апаратні компоненти, які дозволяють технічними засобами досягти захищеності інформації (забезпечення конфіденційності, цілісності та доступності інформації). Друга складова – це перелік нормативних, розпорядчих, експлуатаційних документів, що регламентують порядок обробки інформації, що захищається та порядок роботи на комп'ютерній системі зі створеною КСЗІ. Варто констатувати, що на даний момент не існує НД ТЗІ або інших нормативних документів, в яких чітко висуваються технічні вимоги щодо захисту персональних даних. Наразі в Україні прийнято Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури [11], в яких містяться вимоги щодо кіберзахисту. Проте даний нормативний документ регламентує тільки порядок кіберзахисту об'єктів критичної інформаційної інфраструктури України, що внесені до відповідного переліку.

Як показує аналіз законодавства Європейського Союзу в сфері захисту інформації [12], можна виділити такі нормативні документи, дія яких розповсюджується на всі країни-учасники ЄС: General Data Protection Regulation (GDPR) [3], Payment Services Directive (PSD2) [13], The eIDAS Regulation [14], NIS2 Directive [15].

General Data Protection Regulation (GDPR) – це основний регуляторний документ ЄС, який встановлює правила обробки персональних даних. Він надає всім зацікавленим сторонам більше контролю над їхніми даними та вимагає від організацій дотримуватися строгих процедур захисту даних.

Payment Services Directive (PSD2) – це директива ЄС, яка регулює платіжні послуги та платіжних посередників з метою збільшення конкуренції та підвищення безпеки платежів у ЄС.

The eIDAS Regulation – це регламент встановлює правила для електронних ідентифікацій та довірчих послуг для електронних транзакцій в ЄС.

NIS2 Directive: NIS2 – це директива ЄС, яка спрямована на забезпечення вищого рівня кібербезпеки в усіх країнах-членах, розширюючи обов'язки та вимоги до різних секторів та послуг.

Як зазначалось вище, основним нормативним документом ЄС в сфері захисту персональних даних є General Data Protection Regulation (GDPR). Даний документ регламентує порядок обробки персональних даних та встановлює вимоги до систем захисту в тих інформаційно-комунікаційних

системах, в яких будуть оброблятися персональні дані. Проте даний документ більше фокусується на порядку та процедурах обробки персональних даних, питання кіберзахисту в чистому вигляді не розглядаються. Але можна виділити деякі його положення, які так чи інакше стосуються даного питання, а саме:

1. Необхідність забезпечення конфіденційності, цілісності та доступності інформації, що обробляється в системі (стаття 32).
2. Необхідність проведення тестування і оцінки тих заходів, які були вжиті для захисту персональних даних (стаття 32).
3. Використання шифрування (стаття 32).
4. Контроль доступу до персональних даних (стаття 32).
5. Здатність відновлювати доступність персональних даних у випадку виникнення фізичного або технічного інциденту (стаття 32).
6. Впровадження «псевдонімізації» (стаття 32).
7. Необхідність впровадження концепції “privacy by design” та “privacy by default” (стаття 25).
8. Необхідність мінімізації терміну зберігання даних (стаття 5).

Зазначені положення зазвичай є стандартними для будь-яких систем кіберзахисту, окрім «псевдонімізації» та концепції “privacy by design” та “privacy by default”. В GDPR «псевдонімізація», або «використання псевдонімів» – це опрацювання персональних даних у спосіб, який не дозволяє віднести персональні дані до конкретного суб'єкта без використання додаткової інформації.

Концепція “privacy by design” означає, що такі поняття, як «конфіденційність» та «безпека», повинні впроваджуватись в товари і послуги на самих ранніх етапах їх розробки та протягом всього життєвого циклу продукту. В свою чергу “privacy by default” означає, що в усіх продуктах і послугах повинні бути встановлені найвищі налаштування конфіденційності. Наприклад, якщо якась послуга вимагає реєстрації чи збирання даних, за замовчуванням повинно збиратися мінімально можлива кількість даних, необхідних для надання послуги [16]. Той факт, що необхідність застосування даних концепцій надається в нормативному документі, вимагає від установ та організацій бути більш відповідальними в виборі підходів до обробки персональних даних.

Нормативні документи України [6, 17] не містять чітких і явних вимог щодо кіберзахисту персональних даних. Аналізуючи ці нормативні документи, можна виділити наступні вимоги для побудови системи кіберзахисту на підприємстві:

1. Необхідність забезпечення конфіденційності, цілісності та доступності персональних даних (стаття 24 [6], пункти 3.3, 3.13, 3.14 [17]).
2. Необхідність забезпечення резервного копіювання персональних даних (стаття 24 [6], пункт 3.3 [17]).

При цьому вищезазначені вимоги в нормативних документах явно не прописані, а виходять з тексту статей.

Пунктом 3.2 [17] вимагається у розпорядника персональних даних самостійно визначити перелік і склад заходів, спрямованих на безпеку обробки персональних даних з урахуванням вимог законодавства в сфері інформаційної безпеки. Таким чином, в Україні кіберзахист персональних даних вимагається іншими нормативними актами.

Так, згідно зі ст. 11 Закону України «Про інформацію» [18], до конфіденційної інформації про фізичну особу належать, зокрема, дані про її національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, а також адреса, дата і місце народження. Враховуючи даний факт, чітка вимога щодо захисту такого роду інформації міститься в Законі України «Про захист інформації в інформаційно-комунікаційних системах» [10] та в «Правилах забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах» [19].

В цих документах можна зазначити наявність вимог з кіберзахисту:

1. Забезпечення конфіденційності, цілісності та доступності інформації (п.п. 5, 6 [19]).
2. Забезпечення криптографічного захисту інформації (шифрування) конфіденційної інформації в органах державної влади, органах місцевого самоврядування, на підприємствах, в установах та організаціях, які належать до сфери їх управління, військових формуваннях, які створені відповідно до закону (пункти 9, 13 [19]).
3. Забезпечення аудиту подій (пункт 11 [19]).
4. Розмежування повноважень привілейованого та звичайного користувача (пункт 11 [19]).
5. Забезпечення ідентифікації та автентифікації користувачів (пункт 13 [19]).
6. Забезпечення цілісності засобів захисту інформації в системі (пункт 15 [19]).
7. Забезпечення антивірусного захисту (пункт 16 [19]).

Можна зробити висновок, що в Україні не існує нормативного документу, який би чітко формулював вимоги до кіберзахисту інформаційно-комунікаційних систем, в яких обробляються персональні дані. Внаслідок цього виникає проблема реалізації дієвого захисту такого роду чутливої інформації.

Висновки та перспективи подальших досліджень. Нормативні документи України і основний нормативний документ Європейського Союзу, а саме «Загальний регламент про захист даних» (General Data Protection Regulation, GDPR), що регламентують захист персональних даних, не містять чітких і явних вимог щодо кіберзахисту персональних даних. Але вимоги GDPR щодо захисту персональних даних більш ширші порівняно з Законом України «Про захист персональних даних». Тому можливість впровадження норм GDPR в нормативні документи України по захисту персональних даних є актуальною. Таким чином, результатом подальших досліджень має стати вироблення конкретних рекомендацій по вдосконаленню нормативних документів в Україні, спрямованих на регулювання захисту персональних даних, які базуються на нормах GDPR. Також актуальним є дослідження з розробки концепції вимог до інформаційно-комунікаційних систем з точки зору кіберзахисту для збереження персональних даних.

Список використаних джерел:

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. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Amendment to Convention ETS. No. 108 allowing the European Communities to accede. URL: <https://rm.coe.int/1680078b37>.
6. Закон України «Про захист персональних даних». URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>.
7. 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.
8. 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>.
9. Проект Закону України «Про захист персональних даних». URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=72160.
10. Закон України «Про захист інформації в інформаційно-комунікаційних системах». URL: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text>.
11. Загальні вимоги до кіберзахисту об'єктів критичної інфраструктур. Затверджено постановою Кабінету Міністрів України від 29 червня 2019 р. № 518. URL: <https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text>.
12. [Лит. Стаття по законодавству ЕС] Mantelero, A., Vaciago, G., Esposito, M. S., Monte N. The common EU approach to personal data and cybersecurity regulation. *International Journal of Law and Information Technology*, 2020, 28, 297–328 doi: 10.1093/ijlit/eaad021. URL: <https://academic.oup.com/ijlit/article/28/4/297/6120059?login=false>.
13. Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance). URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L2366>.
14. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG.
15. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance). URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555&qid=1704742816799>.
16. Guidelines 4/2019 on Article 25 Data Protection by Design and by Default. Version 2.0. Adopted on 20 October 2020. URL: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en.
17. Типовий порядок обробки персональних даних. Затверджено наказом Уповноваженого Верховної Ради України з прав людини 08.01.2014 № 1/02-14. URL: https://zakon.rada.gov.ua/laws/show/v1_02715-14#Text.

18. Закон України «Про інформацію». URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text>.

19. Правила забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах. Затверджено постановою Кабінету Міністрів України від 29 березня 2006 р. № 373. URL: <https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text>.

References:

1. Romansky, R. (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. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Amendment to Convention ETS. No. 108 allowing the European Communities to accede. (1981). <https://rm.coe.int>. Retrieved from <https://rm.coe.int/1680078b37>.

6. 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].

7. Dyrektyva 95/46/leS 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].

8. Plan zakhodiv z vykonannia Uhody pro asotsiatsiiu mizh Ukrainoiu, z odnii storony, ta Yevropeiskym Soiuzom, Yevropeiskym ta Yevropeiskym Soiuzom, Yevropeiskym spivtovarystvom z atomnoi enerhii i yikhnyimi 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].

9. Proekt Zakonu Ukrainy "Pro zakhyst personalnykh danykh". [The Draft Law of Ukraine "On Personal Data Protection"]. (n.d.). <https://w1.c1.rada.gov.ua>. Retrieved from https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=72160 [in Ukrainian].

10. Zakon Ukrainy "Pro zakhyst informatsii v informatsiino-komunikatsiinykh systemakh". [Law of Ukraine "On Protection of Information in Information and Communication Systems"]. <https://zakon.rada.gov.ua>. Retrieved from <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text> [in Ukrainian].

11. Zahalni vymohy do kiberzakhystu ob'iektiv krytychnoi infrastruktur. Zatverdzheno postanovoiu Kabinetu Ministriv Ukrainy vid 29 chervnia 2019 r. № 518. [General requirements for cyber protection of critical infrastructure facilities. Approved by the Resolution of the Cabinet of Ministers of Ukraine of June 29, 2019 No. 518]. (2019). <https://zakon.rada.gov.ua>. Retrieved from <https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text> [in Ukrainian].

12. Mantelero, A., Vaciago, G., Esposito, M. S., Monte N. (2020) The common EU approach to personal data and cybersecurity regulation. *International Journal of Law and Information Technology*, 2020, 28, 297–328 doi: 10.1093/ijlit/aaa021. Retrieved from <https://academic.oup.com/ijlit/article/28/4/297/6120059?login=false>.

13. Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance). (2015). <https://eur-lex.europa.eu>. Retrieved from <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L2366>.

14. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. (2014). <https://eur-lex.europa.eu>. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG.

15. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance). (2022). <https://eur-lex.europa.eu>. Retrieved from <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555&qid=1704742816799>.

16. Guidelines 4/2019 on Article 25 Data Protection by Design and by Default. (2019). <https://edpb.europa.eu>. Retrieved from https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en.

17. Typovyi poriadok obrobky personalnykh danykh. Zatverdzheno nakazom Upovnovazhenoho Verkhovnoi Rady Ukrainy z prav liudyny 08.01.2014 № 1/02-14. [Typical procedure for processing personal data. Approved by the order of the Commissioner for Human Rights of the Verkhovna Rada of Ukraine on January 8, 2014 No. 1/02-14]. (2014). <https://zakon.rada.gov.ua>. Retrieved from https://zakon.rada.gov.ua/laws/show/v1_02715-14#Text [in Ukrainian].

18. Zakon Ukrainy "Pro informatsiiu". [Law of Ukraine "On Information"]. (n.d.). <https://zakon.rada.gov.ua>. Retrieved from <https://zakon.rada.gov.ua/laws/show/2657-12#Text> [in Ukrainian].

19. Pravyła zabezpechennia zakhystu informatsii v informatsiinykh, elektronnykh komunikatsiinykh ta informatsiino-komunikatsiinykh systemakh. Zatverdzheno postanovoiu Kabinetu Ministriv Ukrainy vid 29 bereznia 2006 r. № 373. [Rules for information protection in information, electronic communication and information and communication systems. Approved by the Resolution of the Cabinet of Ministers of Ukraine dated March 29, 2006 No. 373]. (2006). <https://zakon.rada.gov.ua>. Retrieved from <https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text> [in Ukrainian].