

# ЮРИДИЧНІ НАУКИ

DOI: <https://doi.org/10.32839/2304-5809/2021-5-93-59>

УДК 341.23

Данченко Т.В., Грозан В.О.  
Київський міжнародний університет

## СПІВРОБІТНИЦТВО ДЕРЖАВ ЩОДО ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ОСОБИСТИХ ДАНИХ У КІБЕРПРОСТОРИ

**Анотація.** Стаття присвячена висвітленню сутності та змісту нині дуже важливої сфери кіберзахисту персональних даних та взагалі вмінню пристосування і правильного використання інформаційно-комунікаційних технологій (далі – ІКТ). Проаналізовано підходи інших країн щодо вирішення питання кібербезпеки та кіберзахисту. Загалом, кібербезпека – це практика захисту систем, мереж та програм від цифрових атак. Ці кібератаки, як правило, спрямовані на доступ до конфіденційної інформації, її зміну або знищення, вимагання грошей у користувачів або порушення нормальних бізнес-процесів. На сьогодні реалізація ефективних заходів з кібербезпеки є особливо складним завданням, оскільки кількість різноманітних пристроїв набагато більша ніж особисто людей, крім того частина людей, до яких можна віднести зловмисників, кіберзлочинців та різного роду хакерів самі створюють кіберзлочинні прецеденти і стають в цьому більш інноваційними. Необхідно також підкреслити актуальність самої теми, що відображається в забезпеченні ефективного захисту в кіберпросторі.

**Ключові слова:** персональні дані, кіберзахист, кібербезпека, кіберпростір, інформаційно-комунікаційні технології, інформація, кіберзлочин.

Danchenko Tatiana, Grozyan Victoria  
Kyiv International University

## COOPERATION OF STATES TO ENSURE THE PROTECTION OF PERSONAL DATA IN CYBER-SPACE

**Summary.** The article is devoted to the coverage of the essence and content of the very important now area of cyber protection of personal data and in general the ability to adapt and use information and communication technologies (hereinafter – ICT). The approaches of other countries to addressing cybersecurity are analyzed. In general, cybersecurity is a practice of protecting systems, networks and programs from digital attacks. These cyberattacks are usually aimed at accessing confidential information, altering or destroying it, extorting money from users or disrupting normal business processes. Today, the implementation of effective cybersecurity measures is a particularly difficult task, as the number of different devices is much greater than people personally, in addition, some people who include criminals, cybercriminals and various hackers themselves create cybercrime precedents and become more innovative at this. It is clear that the widespread use of information and communication technologies (ICT) is a factor in growth and innovation, as well as a source of asymmetric cyber threats. About two million people worldwide have access to the Internet and ICT-supporting services, which are becoming an increasingly important part of our daily lives. With increasing reliance on ICT and the interconnected nature of critical infrastructure, we are terribly vulnerable to possible disruptions and exploitation by malicious cyberattacks. The problem of protection and dissemination of personal data throughout life accompanies a person and permeates all spheres of society and the state. Understanding the importance and necessity of creating a system of effective protection of personal data depends on the peace and well-being of both the individual and society and the state as a whole. Despite the lack of a common view on what constitutes cyberwar or cyberterrorism, governments have an obligation to ensure that infrastructure is absolutely protected from various types of cyber threats and that their legal and political boundaries allow for effective prevention, deterrence, protection and mitigation, as well as to deter possible cyberattacks. It is also necessary to emphasize the relevance of the topic, which is reflected in the provision of effective protection in cyberspace.

**Keywords:** personal data, cybersecurity, cyberspace, information and communication technologies, information, cybercrime.

**Постановка проблеми.** На сьогоднішній день сфера персональних даних являється дуже важливою частиною нашого життя. Дедалі більше, майже в кожній сучасній людині з'являються комунікації в електронному просторі і захист персональних даних став актуальною темою. Тим більше, що останнім часом персональні дані українських громадян періодично з'являються в мережі інтернет.

Персональні дані або особисті дані – це інформація про особу, яка була ідентифікована або може бути конкретно ідентифікована.

Словом, це абсолютно будь-яка інформація про людину.

Це поле включає збір, обробку та використання особистих даних різного роду, починаючи від повсякденного життя сім'ї чи оточення (наприклад та сама реклама, надіслана по телефону або електронною поштою) до комерційних і політичних сфер.

Проте, слід пам'ятати, якщо не використовувати приватні дані в правильному напрямку і належним чином, зловмисники можуть використати інформацію про вас у своїх цілях, і зазвичай це призводить до порушення прав та сво-

бод людини, зокрема права на приватне життя. Адже сучасні бази даних, соціальні мережі та дошки оголошень дають змогу збирати інформацію майже про кожного. Ось так деякі компанії продають свої послуги (наприклад call center-и).

#### **Аналіз останніх досліджень і публікацій.**

Теоретико-методологічним підґрунтям даної статті стали наукові розробки таких вітчизняних дослідників, як: Бем М.В., Городинський І.М., Родіоненко О.М., Головченко В.В., Миронюк О.І., Пилипчук В.Г., Бобрик В.І., Дмитренко О.А., Пазюк А.В., Сопілко І.М., Романюк І.І., та ін. Окремі аспекти проблеми захисту персональних даних досліджували зарубіжні науковці: Д. Боркінг, С. Дейвіс, К. Беннетт, Л. Брендейс, В. Котші, М. Кьорбі, Р. Кларк, Г. Саттон, (D. Borking, S. Davis, K. Bennett, L. Brandeis, W. Kotshi, M. Corby, R. Clark, G. Sutton) та ін.

**Виділення не вирішених раніше частин загальної проблеми.** Актуальність даної теми підтверджується дослідженнями відомих авторів. На жаль, роботи вказаних та багатьох інших авторів не дають цілісного уявлення про єдину систему захисту персональних даних та про сучасний стан упорядкування суспільних інформаційних відносин, перспективи його комплексного розвитку в світі, та Україні зокрема. У цьому контексті актуальним залишається визначення вектору систематизації та розвитку такої теми як захист персональних даних у кіберпросторі.

**Мета статті.** Головною метою цієї роботи полягає у вивченні, систематизації та визначенні перспективи такої теми як захист персональних даних.

**Виклад основного матеріалу.** Статтею 32 Конституції України [1] гарантовано право людини на невтручання в її особисте життя. Крім того не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, окрім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

Абзацом десятим ст. 2 Закону «Про захист персональних даних» [2] визначено, що персональні дані – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. Проте у цьому Законі прямо не сказано, що вся інформація про особу – це її персональні дані.

Порівняно з Україною, досвід Європи у захисті прав та свобод людини ґрунтується на правозастосовній практиці країн Європейського Союзу, судових рішеннях Європейських співтовариств, міжнародно-правових актів щодо захисту прав і свобод людини. Інститут захисту персональних даних в ЄС базується на принципах законності, цільової визначеності, мінімізації, об'єктивності інформації, участі суб'єктів персональних даних у здійсненні контролю, обмеження розкриття персональних даних та інформаційної безпеки загалом. Ці принципи мають нормативну силу та є основою для створення нових правових норм у галузі праввідносин, і є обов'язковими для уповноважених органів у процесі здійснення правозастосовної діяльності. Європейська система законодавства про захист персональних даних включає в себе наступні визначні документи:

1. Конвенція про захист прав людини та основоположних свобод від 04.11.1950 р. [3].

2. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27.04.2016 р. «Про захист фізичних осіб при обробці персональних даних», а також про скасування Директиви 95/46/ЄС (Загальний регламент про захист персональних даних; далі – Регламент 679) [4].

3. Конвенція Ради Європи «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» від 28.01.1981 р. зі змінами у 1999 [5].

4. Додатковий протокол до конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та трансграничних потоків даних» від 08.11.2001 р. [6].

5. Директива 95/66/ЄС «Про обробку персональних даних і захист прав осіб у телекомунікаційному просторі» 1997 р. [7].

Відповідно до положень Директив ЄС, персональні дані – це будь яка інформація, пов'язана з ідентифікованою особою (суб'єктом даних), що зафіксована на будь якому носії. До цієї категорії потрапляють імена, поштові адреси, конфіденційна інформація, що зафіксована електронними та будь якими іншими носіями. Введено поняття «контролери даних». Це фізичні особи або організації, які визначають мету і способи обробки персональних даних.

Законодавчі акти ЄС про захист персональних даних зобов'язують всіх своїх держав-учасниць Європейського Союзу до прийняття законодавства з метою забезпечення ефективного захисту персональних даних від випадкового або незаконного знищення, втрати, модифікації, несанкціонованого розголошення або доступу (особливо, коли дані передаються через електронні мережі). Європейський Союз покладає на свої держави-члени розкриття правового захисту персональних даних через конституційні принципи, що містяться в основних правах людини, таких як право на самовизначення, право на таємницю листування, поштових відправлень, право на недоторканність житла.

Правила захисту персональних даних, які застосовуються в Європі, встановлені двома міжнародними інструментами. Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних бере початок з 1981 року і була першим міжнародним документом, який встановив юридично обов'язкові правила захисту персональних даних. Більшість європейських країн, включаючи Україну, є сторонами цього документу. Конвенція була доповнена в 2001 році Додатковим протоколом, який встановлює правила щодо органів нагляду та трансграничних потоків даних. Держави-члени Європейського Союзу також мають зобов'язання відповідно до Директиви ЄС 95/46/ЄС «Про захист прав приватних осіб стосовно обробки персональних даних та про вільний рух таких даних» 1995 р., яка містить у цілому схожі, але більш детальні положення, у порівнянні з Конвенцією.

З моменту прийняття цих інструментів інформаційно-комунікаційні технології досить швидко розвивалися, тому Європейська Комісія та Європейський Союз наполегливо працюють над тим, щоб адаптувати свої засоби захисту персональних даних до викликів двадцять першого століття.

Що ж стосується Українського національного права, питання захисту персональних даних регулюється Законом України «Про захист персональних даних», який набрав чинності у 2011 році.

Знаючи, що господарем найбільшої кількості персональних даних є держава, тому саме до неї висуваються найжорсткіші вимоги щодо захисту персональних даних, з метою забезпечення та уникнення розповсюдження персональних даних без наданої на те згоди особи. Очевидно, що витік інформації з національних баз даних лише посилить недовіру до держави та створить відчуття незахищеності від внутрішніх та зовнішніх загроз. Тому навіть якщо державні бази даних знаходяться під загрозою, однозначно ми не можемо говорити про захист власних персональних даних.

Традиційно, найбільш пристосованою і процвітаючою юрисдикцією вважається США. Однією з причин необхідності прийняття та розвитку такого законодавства є велика кількість порушень у сфері персональних даних. У зв'язку з цим урядом штату Каліфорнія було схвалено новий закон про захист персональних даних у 2020 році [8]. Перш за все, його важливість полягає в тому, що в Каліфорнії знаходяться такі глобальні корпорації як Facebook, Google, Apple, що мають справу з обробкою, і не тільки, персональних даних користувачів по всьому світу.

Метою цього закону є захист персональних даних, що обробляються юридичними особами приватного права, та контроль такої інформації. Ось чому Закон надає користувачам право знати, яким чином компанія обробляє їх дані, а також можливість вимагати видалення інформації про себе та зупинити її розповсюдження.

Що ж стосується штрафних санкцій за недотримання вимог даного Закону, то за ним передбачаються чималі фінансові збитки у декілька тисяч доларів, навіть у тому випадку, якщо компанія порушила законодавство через необачливість. Саме тому, внаслідок впровадження такого Закону в штаті Каліфорнія підвищився рівень дисциплінованості та відповідальності юридичних осіб в процесі роботи з персональними даними фізичних осіб.

Також варто зазначити, що у 2018 році домініюм Європейського Союзу був прийнятий Загальний регламент про захист даних (General Data Protection Regulation – GDPR) [9], яким встановлюються жорсткі вимоги до опрацювання персональних даних. Його мета полягає в тому, що персональні дані мають збиратися на законних, правомірних, прозорих умовах та відповідно до цільового обмеження. Окрім того, їх зберігання обмежується строком, необхідним для безпосередньо обробки, та повинно бути під захистом від несанкціонованого впливу. Найголовніше, що і як у випадку з наведеним вище законом штату Каліфорнії, юридичні особи несуть значну відповідальність за порушення вимог Регламенту щодо захисту персональних даних.

Статистика щодо ефективності застосування GDPR говорить сама за себе, адже за 2 роки його діяльності, за такі порушення було стягнуто майже 360 мільйонів євро. Водночас, ця статистика вказує на те, що в Європі все ще залишаються актуальними проблеми щодо захисту персональних даних. Втім, захист який запроваджує GDPR, у перспективі дуже навіть ефективний і має призвести до суттєвого скорочення кількості задоволених скарг та штрафів у цій сфері [10].

Підхід України до цього питання характеризується набагато меншою кількістю таких випадків,

але не через відсутність порушень, а у зв'язку з низькою правовою культурою громадян щодо власних персональних даних та неефективною системою їх захисту. Варто зазначити, що сьогодні найефективнішим способом захисту своїх персональних даних є ретельне фільтрування, кому та з якою метою ці дані передаються. На жаль, жодна держава у світі не може забезпечити абсолютний захист персональних даних, проте сама людина може обмежити обсяг тих відомостей, на обробку яких вона дає згоду. Тобто все залежить від нас самих.

Результати дослідження та узагальнення приписів правових стандартів захисту персональних даних у законодавстві держав-членів Ради Європи, Європейського Союзу та реального стану захисту персональних даних в Україні дають змогу дійти таких загальних висновків, що персональні дані, як найбільш чутлива, делікатна та важлива для людини інформація, посідають особливе місце в інформаційних відносинах.

Проблема їх захисту і поширення протягом всього життя супроводжує людину та пронизує усі сфери діяльності суспільства і держави. Від розуміння важливості й необхідності створення системи ефективного захисту персональних даних залежить спокій та благополуччя як окремої людини, так і суспільства та держави в цілому [11].

Сучасна система захисту персональних даних в Україні не гарантує захисту приватності та персональних даних людини і громадянина, не відповідає окремим положенням Конституції України та потребує приведення у відповідність до правових стандартів ЄС, що набули чинності у травні 2018 року. Узагальнення основних принципів захисту персональних даних, які відображаються у положеннях міжнародних стандартів, передбачає обов'язкове дотримання конкретних умов застосування персональних даних для будь-яких суб'єктів інформаційних відносин.

В умовах розвитку інформаційних технологій та їх нових можливостей для тотального контролю за приватним життям людини найбільш реальні правові гарантії захисту персональних даних може надати впровадження інституту права приватної власності на свої персональні дані, що потребує подальшого теоретичного і правового опрацювання. Законодавство з питань захисту персональних даних в Україні, як і в більшості країн світу, ще не досягло своєї зрілості, навіть на термінологічному рівні.

Повна відповідальність національних законодавств країн-членів ЄС щодо захисту персональних даних сучасним правовим стандартам ЄС також не досягнута. Проблема неправомірних і несанкціонованих дій у сфері персональних даних фізичних осіб залишається вкрай актуальною в юридичному і практичному відношенні.

Щодо способів захисту прав та свобод людини і громадянина України, слід відмітити найбільш відоміші, це: судовий, позасудовий та Уповноважений Верховної Ради України з прав людини.

У міжнародній практиці основним правовим інструментом захисту прав та свобод людини, зокрема право на повагу до приватного життя, ми рахуємо статтю 8 Конвенції про захист прав людини і основоположних свобод яка іменується як «право на повагу до приватного і сімейного життя».

У статті 8 Конвенції зазначається те, що кожен має право на повагу до свого приватного і сімейного життя, до свого житла і кореспонденції. І те, що органи державної влади не можуть втручатись у здійснення цього права, за винятком випадків, коли втручання здійснюється згідно із законом і є необхідним у демократичному суспільстві в інтересах національної та громадської безпеки чи економічного добробуту країни, для запобігання заворушенням чи злочинам, для захисту здоров'я чи моралі або для захисту прав і свобод інших осіб.

**Висновки та пропозиції.** Отже, зрозуміло, що широке використання інформаційно-комунікаційних технологій (ІКТ) є фактором зростання та інновацій, а також джерелом асиметричних кіберзагроз. Близько двох мільйонів людей по всьому світу мають доступ до Інтернету та послуг, що підтримують ІКТ, які стають дедалі важливішою частиною нашого повсякденного життя. Зі збіль-

шенням залежності від ІКТ та взаємопов'язаного характеру з критичною інфраструктурою ми страшно вразливими до можливих зривів та експлуатації зловмисними кібератаками.

Без огляду на відсутність єдиного погляду щодо того, що саме являють собою поняття кібервійна або кібертероризм, уряди зобов'язані забезпечити в ідеалі абсолютну захищеність інфраструктури від різних типів кіберзагроз і щоб їх правові та політичні межі дозволяли ефективно запобігати, стримувати, захищати та пом'якшувати ситуацію а також, стримувати можливі кібератаки.

На сьогодні реалізація ефективних заходів з кібербезпеки є особливо складним завданням, оскільки кількість різноманітних пристроїв набагато більша ніж особисто людей, крім того частина людей, до яких можна віднести зловмисників, кіберзлочинців та різного роду хакерів самі створюють кіберзлочинні прецеденти і стають в цьому більш інноваційними.

## Список літератури:

1. Конституція України : Відомості Верховної Ради України (ВВР). 1996. № 30. С. 141. URL: <https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text>
2. Закон України «Про захист персональних даних» : Відомості Верховної Ради України (ВВР). 2010. № 34. Ст. 481. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>
3. Конвенція про захист прав людини і основоположних свобод від 4 листопада 1950 року. URL: [https://zakon.rada.gov.ua/laws/show/995\\_004#Text](https://zakon.rada.gov.ua/laws/show/995_004#Text)
4. Загальний Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (GDPR – General Data Protection Regulation). URL: [https://zakon.rada.gov.ua/laws/show/984\\_008-16#Text](https://zakon.rada.gov.ua/laws/show/984_008-16#Text)
5. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28 січня 1981 року. URL: [https://zakon.rada.gov.ua/laws/show/994\\_326#Text](https://zakon.rada.gov.ua/laws/show/994_326#Text)
6. Додатковий протокол до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних від 8 листопада 2001 року. URL: [https://zakon.rada.gov.ua/laws/show/994\\_363#Text](https://zakon.rada.gov.ua/laws/show/994_363#Text)
7. Директива 95/66/ЄС від 14 грудня 1995 року. URL: [https://www.legislation.gov.uk/eudr/1995/66/pdfs/eudr\\_19950066\\_adapted\\_en.pdf](https://www.legislation.gov.uk/eudr/1995/66/pdfs/eudr_19950066_adapted_en.pdf)
8. Закон Сполучених Штатів Америки про конфіденційність споживачів у Каліфорнії від 1 січня 2020 року (California Consumer Privacy Act (CCPA)). URL: <https://oag.ca.gov/privacy/ccpa>
9. Загальний Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (GDPR – General Data Protection Regulation). URL: [https://zakon.rada.gov.ua/laws/show/984\\_008-16#Text](https://zakon.rada.gov.ua/laws/show/984_008-16#Text)
10. Відслідковування дотримання вимог GDPR. Статистика накладання штрафів. URL: <https://www.enforcementtracker.com/?insights>
11. Bem M.V., Gorodisky I.M., Sutton G., Rodionenko O.M. Захист персональних даних: правове регулювання та практичні аспекти. Київ : К.І.С., Видано Радою Європи. F-67075 Strasbourg Cedex, 2015. 2020 с.

## References:

1. Constitution of Ukraine: Information of the Verkhovna Rada of Ukraine (VVR), 1996, № 30, art. 141. URL: <https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text>
2. Law of Ukraine "On Personal Data Protection": Information of the Verkhovna Rada of Ukraine (VVR), 2010, № 34, art. 481. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>
3. Convention for the Protection of Human Rights and Fundamental Freedoms of November 4, 1950. URL: [https://zakon.rada.gov.ua/laws/show/995\\_004#Text](https://zakon.rada.gov.ua/laws/show/995_004#Text)
4. General Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EU (GDPR – General Data Protection Regulation). URL: [https://zakon.rada.gov.ua/laws/show/984\\_008-16#Text](https://zakon.rada.gov.ua/laws/show/984_008-16#Text)
5. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981. URL: [https://zakon.rada.gov.ua/laws/show/994\\_326#Text](https://zakon.rada.gov.ua/laws/show/994_326#Text)
6. Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data concerning Supervisors and Cross-Border Data Flows of 8 November 2001. URL: [https://zakon.rada.gov.ua/laws/show/994\\_363#Text](https://zakon.rada.gov.ua/laws/show/994_363#Text)
7. Directive 95/66/EU of 14 December 1995. URL: [https://www.legislation.gov.uk/eudr/1995/66/pdfs/eudr\\_19950066\\_adapted\\_en.pdf](https://www.legislation.gov.uk/eudr/1995/66/pdfs/eudr_19950066_adapted_en.pdf)
8. The United States California Consumer Privacy Act (CCPA) of January 1, 2020. URL: <https://oag.ca.gov/privacy/ccpa>
9. General Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EU. URL: [https://zakon.rada.gov.ua/laws/show/984\\_008-16#Text](https://zakon.rada.gov.ua/laws/show/984_008-16#Text)
10. GDPR Enforcement Tracker. Fines statistics. URL: <https://www.enforcementtracker.com/?insights>
11. Bem M.V., Gorodisky I.M., Sutton G., Rodionenko O.M. (2015) Protection of personal data: legal regulation and practical aspects. Kyiv: KIS, Published by the Council of Europe. F-67075 Strasbourg Cedex, 2020 p.