

Ю. А. Кокарча
orcid.org/0000-0003-0874-3688
кандидат політичних наук,
доцент кафедри права
Вінницького торговельно-економічного інституту
Державного торговельно-економічного університету

ТРАНСФОРМАЦІЯ ІНФОРМАЦІЙНОГО ЗАКОНОДАВСТВА В ПРОЦЕСІ ІНТЕГРАЦІЇ ДО ЄС

Розвиток сучасних технологій та збільшення обсягів інформації створює потребу в ефективному захисті персональних даних та інформації. В світі набуває популярності застосування інформаційних технологій в різних сферах діяльності, що збільшує ризик втрати конфіденційної інформації. У зв'язку з цим, проблема захисту персональних даних та інформації стає актуальною і вимагає належного регулювання в рамках інформаційного законодавства.

Крім того, Україна веде активну політику щодо європейської та євроатлантичної інтеграції, тому необхідність у досягненні європейських стандартів інформаційного законодавства набуває важливості. Необхідність розробки та впровадження ефективних заходів з захисту інформації та персональних даних стає актуальним завданням для країни, що дозволить зберегти важливу інформацію та персональні дані від несанкціонованого доступу.

У зв'язку з цим, тема про трансформацію інформаційного законодавства в процесі інтеграції до ЄС є дуже актуальною для нашого часу, а її дослідження дозволить виявити та проаналізувати проблеми, які виникають у процесі європейської та євроатлантичної інтеграції України в галузі інформаційного законодавства.

Аналіз наукової літератури дозволяє нам стверджувати, що проблемам трансформації законодавства та інтеграції до ЄС, зокрема також в інформаційній сфері приділяли увагу в своїх наукових дослідженнях як вітчизняні, так і зарубіжні вчені, в даному дослідженні ми зверталися до праць: Батиргарєєвої В., Легкої О., Отамась І., Сverdлик З., Солодкої О., Фролової О., Хаустової М. та ін.

Метою статті є проаналізувати європейське законодавство в інформаційній сфері та з'ясувати, наскільки ефективно Україна впроваджує стандарти ЄС в галузі інформаційного законодавства та які проблеми виникають на шляху їх реалізації. Дослідження обраної теми має важливе значення для практичної роботи у сфері захисту персональних даних та інформації, а також для розробки та вдосконалення законодавчих актів в галузі інформаційного законодавства.

У наш час інформація стала однією з найважливіших цінностей суспільства завдяки величезному зростанню інтенсивності інформаційних відносин за останні півстоліття. Цифрова трансформація, яка охоплює всі сфери життєдіяльності, стала неможливою без застосування інформаційно-комп'ютерних технологій, і її головною метою є створення інформаційного простору.

Під інформаційним простором слід розуміти середовище здійснення суб'єктами інформаційної сфери діяльності, пов'язаної зі створенням, збиранням, одержанням, зберіганням, використанням, поширенням, охороною та захистом інформації, на яку поширюється юрисдикція України, а також функціонуванням національної інформаційної інфраструктури (Солодка, 2020, с. 45).

У європейському інформаційному просторі існує потужна правова основа, що регулює функціонування самого простору, використання інформаційних продуктів, захисту прав інтелектуальної власності, а також дотримання безпекових вимог. Забезпечення правової підґрунтя функціонування та відкритості державних інформаційних ресурсів є обов'язковою умовою для інтеграції єдиного інформаційного простору України з європейським та світо-

вим інформаційним простором. Організаційна основа інформаційного простору пов'язана з функціонуванням державних та недержавних органів формування інформаційної політики та забезпечення інформаційної безпеки.

Дискусія щодо необхідності спільного загальноєвропейського регулювання обробки та захисту персональних даних розпочалася 2009 р. з ініціативи Європейської комісії. Документом, який встановив таке регулювання, став Загальний регламент про захист персональних даних (англ. General Data Protection Regulation, GDPR, надалі – Регламент). Європейська комісія опублікувала його проєкт з метою обговорення в січні 2012 р., ухвалення на рівні ЄС відбулося 14 квітня 2016 р., а набрання чинності – 25 травня 2018 р. Цей документ складається з 11 розділів та 99 статей та супроводжується 173 коментарями (англ. Recitals). Серед головних особливостей юридичної дії Регламенту можна виділити такі:

- його дія поширюється на всіх громадян держав – членів ЄС, а також резидентів ЄС, незалежно від їхнього громадянства;
- територіальна дія Регламенту поширюється на територію як держав – членів ЄС, так і держав, що входять до Європейської економічної зони (Норвегія, Ісландія та Ліхтенштейн);
- Регламент – акт прямої дії, він загальнообов'язковий та застосовується державами – членами ЄС без додаткового ухвалення внутрішніх нормативних актів.

Регламент визначає правила гри для всіх учасників процесу захисту та обробки персональних даних – як суб'єктів, так і для володільців і розпорядників та контрольних органів у цій сфері. Зокрема, документ містить повний каталог прав суб'єктів персональних даних, які були раніше закріплені в Директиві та Хартії та розширює їхній зміст (Регламент Європейського Парламенту і Ради (ЄС) 2016/679, 2016).

Інформаційне законодавство в Європейському союзі є однією з найбільш розвинутих та ретельно вивчених галузей законодавства. Його головною метою є забезпечення захисту особистих даних громадян ЄС та забезпечення безпеки від кіберзлочинності.

Зокрема, ENISA (Агентство Європейського Союзу з кібербезпеки) є першим інструментом внутрішнього ринку, спрямованим на підвищення опірності ЄС до ризиків у сфері кібербезпеки. Його діяльність орієнтована на забезпечення безперервності послуг, що дають економіці та суспільству ЄС змогу функціонувати належним чином. Отже, функціями ENISA є надання допомоги Європейській Комісії, державам-членам ЄС та бізнесу виконувати вимоги мережевої та інформаційної безпеки, включаючи чинне та майбутнє право ЄС; ENISA є центром експертизи як для держав-членів, так й для інституцій ЄС з отримання консультацій з питань, пов'язаних із мережевою та інформаційною безпекою; Агентство вносить в розвиток свій внесок та імплементації законів та політики ЄС в різні сектори в сфері кібербезпеки тощо.

Право Європейського Союзу про кібербезпеку не розглядає окремо заходи з кібербезпеки, захист конфіденційності й захист мереж чи інформаційних систем, а має на меті узгоджені дії щодо захисту засобів, інформації та конфіденційності як частину екосистеми кібербезпеки.

Проте, варто виокремити Директиву NIS2, яка була офіційно ухвалена Парламентом, а потім Радою у листопаді 2022 року та набула чинності 16 січня 2023 року. Директива про мережеву та інформаційну безпеку (NIS) є дуже важливим загальноєвропейським законодавством про кібербезпеку, і її конкретною метою є досягнення високого спільного рівня кібербезпеки в державах-членах. Хоча даний документ збільшив можливості держав-членів щодо кібербезпеки, його впровадження виявилось складним, що призвело до фрагментації на різних рівнях внутрішнього ринку. Щоб відповісти на зростаючі загрози, пов'язані з цифровізацією та сплеском кібератак, Комісія подала пропозицію замінити Директиву NIS i, таким чином, посилити вимоги безпеки, розглянути питання безпеки ланцюгів постачання, оптимізувати зобов'язання щодо звітності та запровадити більш жорсткі вимоги, наглядові заходи та суворіші вимоги до виконання, включаючи узгоджені санкції в ЄС. Запропоноване розширення сфери застосування NIS2 шляхом фактичного зобов'язання більшої кількості організацій і секторів вживати заходів має на меті підвищити рівень кібербезпеки в Європі в довгостроковій перспективі (The NIS2 Directive, 2022).

Ще одним важливим законодавчим актом ЄС є Акт про цифрову операційну стійкість (DORA) – це законодавчий акт Європейського Союзу, який був прийнятий 16 липня 2021 року

та оновлений 29 листопада 2022 року. Цей закон має на меті забезпечити стійкість інформаційних технологій (ІТ) у ЄС, зокрема, в області критичної інфраструктури (наприклад, електромереж, транспорту, банківської системи тощо) та в державних органах (DORA, 2022).

DORA встановлює єдині вимоги до безпеки мережевих та інформаційних систем компаній і організацій, що працюють у фінансовому секторі, а також критично важливих третіх сторін, які надають їм послуги, пов'язані з ІКТ (інформаційно-комунікаційними технологіями), такі як хмарні платформи або служби аналізу даних. DORA створює нормативну базу для цифрової операційної стійкості, згідно з якою всі фірми повинні бути впевнені, що вони можуть протистояти, реагувати та відновлюватися після всіх типів збоїв і загроз, пов'язаних з ІКТ. Ці вимоги однорідні для всіх держав-членів. Основною метою є запобігання та пом'якшення кіберзагроз.

Однією з найбільш важливих умов вступу України до Європейського Союзу є адаптація вітчизняного законодавства до стандартів та норм ЄС. З цієї метою було прийнято низку законів, які стосуються електронного документообігу та електронного цифрового підпису, підтримки електронного урядування та цифрової економіки в Україні, що спрямована на діджиталізацію країни.

Концептуальні засади державної політики у сфері інформатизації, розвитку інформаційного суспільства та електронного урядування визначено, насамперед, у низці таких законодавчих актів, як закони України «Про інформацію», «Про захист персональних даних», «Про адміністративні послуги», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про електронний документ та електронний документообіг», Типову інструкцію з документування управлінської інформації в електронній формі та організації роботи з електронними документами в діловодстві, електронного міжвідомчого обміну, затвердженої постановою Кабінету Міністрів України від 17.01.2018 № 55, Порядку роботи з електронними документами у діловодстві та їх підготовки до передавання на архівне зберігання, затверджений наказом Мін'юсту від 11.11.2014 № 1886/5, Вимог до форматів даних електронного документообігу в органах державної влади, затверджених наказом Державного агентства з питань електронного урядування України від 07.09.2018 № 60, Вимог у сфері електронних довірчих послуг та Порядку перевірки дотримання вимог законодавства у сфері електронних довірчих послуг, затверджених постановою Кабінету Міністрів України від 07.11.2018 № 992 тощо (Отамась, 2020).

Стосовно законодавства про захист персональних даних, на національному рівні це регламентовано: ст. 32 Конституції України: «Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини»; ч. 2 ст. 21 Закону України «Про інформацію»: «конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, установлених законом»; ч. 1 ст. 7 Закону України «Про захист персональних даних», причому норми ч. 1 цієї статті не застосовуються в разі, якщо обробка персональних даних здійснюється за умови надання суб'єктом персональних даних однозначної згоди на обробку таких даних (п. 1 ч. 2) чи необхідна в цілях охорони здоров'я (п. 6 ч. 2); та підзаконними нормативно-правовими актами (Типовий порядок обробки персональних даних; Порядок здійснення Уповноваженим ВРУ контролю за додержанням законодавства про захист персональних даних; Порядок повідомлення Уповноваженого ВРУ з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, про структурний підрозділ або відповідальну особу, що організовує роботу, пов'язану із захистом персональних даних під час їх обробки, а також оприлюднення вказаної інформації) (Легка, 2021, с. 76).

Аналізуючи законодавство ЄС про кібербезпеку, варто наголосити, що прийнята Директива NIS2 є прикладом для вдосконалення законодавства України, адже національне законодавство в сфері кібербезпеки обмежується рішенням Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України», Законом України «Про основні засади забезпечення кібербезпеки України».

Також варто наголосити, що Україна активно залучає американський та європейський досвід, міжнародні стандарти у сфері кіберзахисту. Фахівці із Держспецзв'язку, наприклад, розробили Загальні правила обміну інформацією про кіберінциденти (Протокол TLP), що відповідають рекомендації Європейської агенції з кібербезпеки (ENISA Considerations on the Traffic Light Protocol) та документу Форуму команд реагування та безпеки (FIRST Standards Definitions and Usage Guidance – версії 1.0 «Traffic Light Protocol») (Свердлик, 2022, с. 180).

Поділяємо думку О. Трофименко, про те, що з метою посилення стійкості критичної національної інфраструктури з кібербезпеки український уряд регулярно бере участь у міжнародному співробітництві з реагування на кіберінциденти, маючи доступ до передового міжнародного досвіду та сучасних алгоритмів реагування на кіберінциденти. Саме розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки, участь у заходах зі зміцнення довіри у кіберпросторі, які проводяться під егідою ОБСЄ, та поглиблення співпраці України з ЄС і НАТО посилюють спроможності нашої держави у сфері кібербезпеки і відповідають національним інтересам (Трофименко та ін., 2019, с. 153).

Важливим кроком вперед стало започаткування українськими закладами вищої освіти спеціальності 125 «Кібербезпека» (далі – «Кібербезпека»), що розвивається швидкими темпами та у кожному конкретному закладі має певну змістову градацію (Свердлик, 2022, с. 181).

Поряд із низкою законодавчих ініціатив, які вдалося вже реалізувати, варто відзначити діяльність національних агентств та комісій, координаційних центрів, що мають на меті зближення з Європейським союзом у всіх сферах державної діяльності.

Поділяємо думку Фролової О., стосовно сьогодення для України і запущену прискорену процедуру євроінтеграції. Що існує потреба у вдосконаленні нормативно-правового та організаційного забезпечення функціонування українського інформаційного простору для більш легкого входження в європейський простір. Для вдосконалення правового регулювання інформаційної сфери доцільно розглянути досвід європейських країн із забезпечення функціонування інформаційного простору. Україна потребує якнайшвидшої інтеграції до інфопростору ЄС задля безпекових, економічних, соціальних й інформаційних цілей, тому що в умовах війни з РФ та інформаційно-психологічних операцій проти українців існує потреба в достовірній і не викривленій інформації, яка функціонуватиме в спільному інфопросторі, боротьбі з маніпулятивними та замовними інфовкидами на державному й міжнародному рівнях, а також інформуванні Європи та світу про проблеми й досягнення України (Фролова, 2022, с. 76-77).

У результаті дослідження стало очевидним, що трансформація інформаційного законодавства України в процесі її інтеграції до Європейського Союзу є надзвичайно важливим кроком для забезпечення безпеки та захисту персональних даних громадян, а також розвитку електронної комерції та інших сфер інформаційної діяльності в країні.

У процесі інтеграції Україна зобов'язана адаптувати своє законодавство до європейських стандартів, що вимагає реформування інформаційного законодавства та його гармонізації з нормами та вимогами ЄС. Такі зміни вже відбулися, і ми можемо стверджувати, що Україна значно покращила своє законодавство в галузі інформаційної безпеки та захисту персональних даних.

Одним із найважливіших досягнень в цій галузі стала ратифікація Угоди про асоціацію між Україною та ЄС, яка передбачає гармонізацію українського законодавства з європейським. Україна також прийняла закон про захист персональних даних, що відповідає вимогам ЄС, Стратегію кібербезпеки України, розробили Загальні правила обміну інформацією про кіберінциденти (Протокол TLP), що відповідають рекомендації Європейської агенції з кібербезпеки (ENISA Considerations on the Traffic Light Protocol) та документу Форуму команд реагування та безпеки та ін.

Незважаючи на ці успіхи, все ще існує багато проблем та викликів, пов'язаних з інформаційною безпекою та захистом персональних даних в Україні. До них належать злочинність в галузі кібербезпеки, втручання іноземних держав у внутрішні справи України тощо. Проте, Україна активно працює над виконанням усіх вимог, щоб стати повноправним членом ЄС та отримати доступ до нових можливостей та ринків.

Література

- DORA. Цифрові фінанси: Рада ухвалила Закон про цифрову операційну стійкість, 2022. URL: <https://www.europeantimes.news/uk/2022/11> (дата звернення: 15.03.2023)
- The NIS2 Directive, 2022. URL: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI\(2021\)689333_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf) (дата звернення: 15.03.2023)
- Батиргарєва В.С. Правова платформа для забезпечення в Україні ефективного захисту цифрових трансформацій суспільства. *Інформація і право*, 2022. № 1(40). С. 21-34.
- Загальний регламент про захист даних (GDPR), 2018. URL: <https://gdpr-text.com/uk/> (дата звернення: 15.03.2023)
- Конституція України від 28 червня 1996 року. Відомості Верховної Ради України (ВВР). 1996. № 30. Ст. 141.
- Легка О.В. Актуальні питання захисту персональних даних: вітчизняний та міжнародний досвід. *Правова позиція*, 2021. № 2 (31). С. 76 (дата звернення: 16.03.2023)
- Отамась І. Діджиталізація в Україні в контексті європейських інтеграційних процесів. *Український Щорічник з Європейських Інтеграційних Студій*. 2020 Київ: APREI. Вип. IV. С. 126-138
- Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI. URL: <http://zakon.rada.gov.ua/laws/show/2297-17> (дата звернення: 16.03.2023)
- Про інформацію: Закон України від 02.10.1992 р. № 2657-XII (у редакції від 01.01.2023). Відомості Верховної Ради України (ВВР). 1992. № 48. Ст. 650. URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text> (дата звернення: 16.03.2023)
- Регламент (ЄС) 2019/881 Європейського Парламенту та Ради від 17 квітня 2019 року про ENISA (Агентство Європейського Союзу з кібербезпеки), 2019. URL: <https://eur-lex.europa.eu/eli/reg/2019/881/oj> (дата звернення: 15.03.2023)
- Регламент Європейського Парламенту і Ради (ЄС) 2016/679 про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) від 27 квітня 2016 року. URL: https://zakon.rada.gov.ua/laws/show/984_008-16%23Text#Text (дата звернення: 15.03.2023)
- Свердлик З. Кібербезпека та кіберзахист: питання порядку денного в українському суспільстві. *Український журнал з бібліотекознавства та інформаційних наук*, 2022. Випуск 10. С. 180-181.
- Солодка О.М. Інформаційний простір держави як сфера реалізації інформаційного суверенітету. *Інформація і право*, 2020. № 4(35). С. 39-46.
- Трофименко О., Прокоп Ю., Логінова Н., Задерейко О. Кібербезпека України: аналіз сучасного стану. *Захист інформації*. 2019. Т. 21, № 3. С. 150-157. DOI: <https://doi.org/10.18372/2410-7840.21.13951> (дата звернення: 17.03.2023)
- Фролова О. Інтеграція України до Європейського інформаційного простору. *Міжнародні відносини, суспільні комунікації та регіональні студії*. 2022, Луцьк. № 2 (13). С. 66-77
- Хаустова М.Г. Правова політика України в умовах інтеграції до Європейського Союзу. *Право та інновації*, 2021. № 1 (33). С. 74-82.

References

- DORA. Tsyfrovi finansy: Rada ukhvalyla Zakon pro tsyfrovu operatsiynu stiikist, 2022. URL: <https://www.europeantimes.news/uk/2022/11> [in Ukrainian].
- The NIS2 Directive, 2022. URL: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI\(2021\)689333_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf) [in EU].
- Batyrhareieva, V.S. (2022) Pravova platforma dlia zabezpechennia v Ukraini efektyvnoho zakhystu tsyfrovyykh transformatsii suspilstva. *Informatsiia i pravo*, № 1(40), s. 21-34 [in Ukrainian].
- Zahalnyi rehlament pro zakhyst danykh (GDPR), 2018. URL: <https://gdpr-text.com/uk/> [in Ukrainian].
- Konstytutsiia Ukrainy vid 28 chervnia 1996 roku. Vidomosti Verkhovnoi Rady Ukrainy (VVR). 1996. № 30. St. 141 [in Ukrainian].
- Lehka, O.V. (2021) Aktualni pytannia zakhystu personalnykh danykh: vitchyzniani ta mizhnarodni dosvid. *Pravova pozytsiia*, № 2 (31). s.76 [in Ukrainian].
- Otamas, I. (2020) Didzhytalizatsiia v Ukraini v konteksti yevropeiskykh intehratsiinykh protsesiv. *Ukrainskyi Shchorichnyk z Yevropeiskykh Intehratsiinykh Studii*, Vyp. IV, s. 126-138 [in Ukrainian].
- Pro zakhyst personalnykh danykh : Zakon Ukrainy vid 01.06.2010 r. № 2297-VI. (u redaktsii vid 27.10.2022) <https://zakon.rada.gov.ua/laws/main/2297-17#Text> [in Ukrainian].
- Pro informatsiiu: Zakon Ukrainy vid 02.10.1992 r. № 2657-XII (u redaktsii vid 01.01.2023). Vidomosti Verkhovnoi Rady Ukrainy (VVR). 1992. № 48. St. 650. URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text>

[in Ukrainian].

Rehlement (IeS) 2019/881 Yevropeiskoho Parlamentu ta Rady vid 17 kvitnia 2019 roku pro ENISA (Ahentstvo Yevropeiskoho Soiuzu z kiberbezpeky), 2019. URL: <https://eur-lex.europa.eu/eli/reg/2019/881/oj> [in EU].

Rehlement Yevropeiskoho Parlamentu i Rady (IeS) 2016/679 pro zakhyst fizychnykh osib u zviazku z opratsiuvanniam personalnykh danykh i pro vilnyi rukh takykh danykh, ta pro skasuvannia Dyrektyvy 95/46/IeS (Zahalnyi rehlement pro zakhyst danykh) vid 27 kvitnia 2016 roku. URL: https://zakon.rada.gov.ua/laws/show/984_008-16%23Text#Text [in EU].

Sverdlyk, Z. (2022) Kiberbezpeka ta kiberzakhyst: pytannia poriadku dennoho v ukrainskomu suspilstvi. *Ukrainskyi zhurnal z bibliotekoznavstva ta informatsiinykh nauk*, Vypusk 10. s.180-181[in Ukrainian].

Solodka, O.M. (2020) Informatsiinyi prostir derzhavy yak sfera realizatsii informatsiinoho suverenitetu. *Informatsiia i pravo*, № 4(35), s. 39-46.

Trofymenko, O., Prokop, Yu., Lohinova, N., & Zadereiko, O. (2019). Kiberbezpeka Ukrainy: analiz suchasnoho stanu [Cybersecurity of Ukraine: Analysis of the current situation]. *Ukrainian Information Security Research Journal*, 21(3), 150–157. <https://doi.org/10.18372/2410-7840.21.13951> [in Ukrainian].

Frolova, O. (2022) Intehratsiia Ukrainy do Yevropeiskoho informatsiinoho prostoru. *Mizhnarodni vidnosyny, suspilni komunikatsii ta rehionalni studii*, № 2 (13), s. 66-77 [in Ukrainian].

Khaustova, M.H. (2021) Pravova polityka Ukrainy v umovakh intehratsii do Yevropeiskoho Soiuzu. *Pravo ta innovatsii*, № 1 (33), s. 74-82 [in Ukrainian].

Анотація

Кокарча Ю. А. Трансформація інформаційного законодавства України в процесі інтеграції до ЄС. – Стаття.

У статті розглядається важливість адаптації національного законодавства до вимог європейського правового простору, зокрема у сфері інформаційної безпеки. В контексті процесу інтеграції до ЄС, Україна змушена ставити перед собою низку завдань, пов'язаних із забезпеченням інформаційної безпеки та захистом прав громадян. У цьому відношенні важливим є визначення чіткої політики, що спрямована на забезпечення інформаційної безпеки та формування правильної свідомості громадськості про ризики інформаційної війни. Стаття присвячена процесу гармонізації інформаційного законодавства України з європейськими стандартами та вимогами, який є важливим елементом інтеграції України до Європейського Союзу. Автори зазначають, що інформаційне законодавство є важливим компонентом для розвитку електронної комерції, кібербезпеки та захисту персональних даних.

Також, у статті описано основні аспекти європейського інформаційного законодавства, зокрема, Регламент про захист персональних даних (GDPR), який є одним з найважливіших законодавчих актів у сфері захисту персональних даних в світі, Директиву NIS2, DORA. Описано роботу і функції ENISA. Автори статті також аналізують та порівнюють законодавчі акти України та Європейського Союзу, що стосуються захисту персональних даних та кібербезпеки. Досліджують зміни, які Україна внесла в своє інформаційне законодавство в рамках інтеграції до ЄС.

У заключенні, автори узагальнюють, що Україна зробила значний прогрес у гармонізації свого інформаційного законодавства з європейськими стандартами, але водночас вказують на необхідність подальших зусиль для подальшої гармонізації та вдосконалення інформаційного законодавства в Україні.

Ключові слова: інформаційне законодавство, інтеграція до ЄС, інформаційна безпека, кібербезпека, персональні дані, політика.

Summary

Kokarcha Yu. A. Transformation of information legislation of Ukraine in the process of integration into the EU. – Article.

The article examines the importance of adapting national legislation to the requirements of the European legal space, in particular in the field of information security. In the context of the EU integration process, Ukraine is forced to face a number of tasks related to information security and protection of citizens' rights. In this regard, it is important to define a clear policy aimed at ensuring information security and forming the correct awareness of the public about the risks of information warfare. The article is devoted to the process of harmonization of information legislation of Ukraine with European standards and requirements, which is an important element of Ukraine's integration into the European Union. The authors note that information legislation is an important component for the development of e-commerce, cyber security and personal data protection.

Also, the article describes the main aspects of European information legislation, in particular, the Personal Data Protection Regulation (GDPR), which is one of the most important pieces of legislation in the field of

personal data protection in the world, the NIS2 Directive, DORA. The work and functions of ENISA are described. The authors of the article also analyze and compare the legislative acts of Ukraine and the European Union related to the protection of personal data and cyber security. Changes that Ukraine made to its information legislation as part of EU integration are being studied.

In conclusion, the authors summarize that Ukraine has made significant progress in harmonizing its information legislation with European standards, but at the same time point to the need for further efforts to further harmonize and improve information legislation in Ukraine.

Key words: information legislation, EU integration, information security, cyber security, personal data, policy.