



УДК 004.056.5:339.924(477)

[https://doi.org/10.52058/2786-6300-2026-2\(44\)-410-423](https://doi.org/10.52058/2786-6300-2026-2(44)-410-423)

Климчук Олександр Васильович доктор економічних наук, професор, професор кафедри публічного управління та менеджменту, Вінницький державний педагогічний університет імені Михайла Коцюбинського, м. Вінниця, <https://orcid.org/0000-0002-9427-9561>

Яременко Олександр Іванович кандидат наук з державного управління, доцент, декан факультету права, публічного управління і менеджменту, Вінницький державний педагогічний університет імені Михайла Коцюбинського, м. Вінниця, <https://orcid.org/0000-0002-3053-2257>

ГАРМОНІЗАЦІЯ ВІТЧИЗНЯНОГО ЗАКОНОДАВСТВА ДО ЄВРОПЕЙСЬКИХ СТАНДАРТІВ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ: ВИКЛИКИ ДЛЯ ПУБЛІЧНОЇ ВЛАДИ

Анотація. У статті досліджено теоретико-методологічні та концептуальні засади гармонізації вітчизняного законодавства України у сфері кібербезпеки та захисту персональних даних із європейськими стандартами в умовах цифрової трансформації публічного управління, євроінтеграційних процесів і зростання гібридних загроз.

Обґрунтовано, що кібербезпека та захист персональних даних у сучасному цифровізованому суспільстві набувають статусу ключових складових національної безпеки, демократичного врядування та довіри громадян до органів публічної влади, а ефективність державної політики у цій сфері значною мірою залежить від рівня узгодженості національного правового регулювання з нормами та стандартами ЄС.

Доведено, що процес гармонізації законодавства з положеннями Загального регламенту про захист даних (GDPR), директив NIS/NIS2 та інших актів права ЄС не може обмежуватися формальною імплементацією правових норм, а має розглядатися як комплексний багаторівневий процес у системі публічного управління та адміністрування.

Визначено, що на стратегічному рівні він пов'язаний із формуванням цілісної державної політики кібербезпеки та захисту персональних даних, на інституційному – зі зміцненням спроможності та координації органів публічної влади, на нормативно-правовому – з узгодженням національного законодавства з європейськими стандартами, а на операційному – з практичним упровадженням цих вимог у діяльність публічних інституцій.



Запропоновано науково обґрунтований підхід до розуміння гармонізації законодавства як інструменту трансформації системи публічного управління, спрямованого на досягнення балансу між безпековими інтересами держави та дотриманням прав і свобод людини у цифровому середовищі. Обґрунтовано, що реалізація такого підходу сприятиме підвищенню кіберстійкості держави, удосконаленню механізмів публічного управління, зміцненню довіри суспільства до публічної влади та наближенню України до повноцінної інтеграції у європейський правовий і цифровий простір.

Ключові слова: публічне управління, кібербезпека, захист персональних даних, євроінтеграція, гармонізація законодавства, нормативно-правове регулювання, цифрова трансформація, національна безпека.

Klymchuk Oleksandr Vasylovych Doctor of Economics, Professor, Professor of the Department of Public Administration and Management, Vinnytsia Mykhailo Kotsiubynskyi State Pedagogical University, Vinnytsia, <https://orcid.org/0000-0002-9427-9561>

Yaremenko Oleksandr Ivanovych Candidate of Sciences in Public Administration, Associate Professor, Dean of the Faculty of Law, Public Administration and Management, Vinnytsia Mykhailo Kotsiubynskyi State Pedagogical University, Vinnytsia, <https://orcid.org/0000-0002-3053-2257>

HARMONIZATION OF NATIONAL LEGISLATION WITH EUROPEAN STANDARDS OF CYBERSECURITY AND PERSONAL DATA PROTECTION: CHALLENGES FOR PUBLIC AUTHORITIES

Abstract. In the article, the theoretical, methodological, and conceptual foundations of harmonizing Ukraine's national legislation in the field of cybersecurity and personal data protection with European standards are examined in the context of the digital transformation of public administration, European integration processes, and the intensification of hybrid threats. It is substantiated that cybersecurity and personal data protection in today's digitalized society acquire the status of key components of national security, democratic governance, and public trust in public authorities, while the effectiveness of state policy in this area largely depends on the level of coherence between national legal regulation and the norms and standards of the European Union.

It is proven that the process of harmonizing legislation with the provisions of the General Data Protection Regulation (GDPR), the NIS/NIS2 Directives, and other EU legal acts cannot be limited to the formal implementation of legal norms, but should be regarded as a comprehensive multi-level process within the system of public management and administration. It is determined that at the strategic level this process



is associated with the formation of an integrated state policy on cybersecurity and personal data protection; at the institutional level, with strengthening the capacity and coordination of public authorities; at the regulatory level, with aligning national legislation with European standards; and at the operational level, with the practical implementation of these requirements in the activities of public institutions.

A scientifically grounded approach to understanding legislative harmonization as an instrument for transforming the system of public administration is proposed, aimed at achieving a balance between the security interests of the state and the observance of human rights and freedoms in the digital environment. It is substantiated that the implementation of this approach will contribute to enhancing the state's cyber resilience, improving public governance mechanisms, strengthening public trust in public authorities, and bringing Ukraine closer to full integration into the European legal and digital space.

Keywords: public administration, cybersecurity, personal data protection, European integration, legislative harmonization, legal and regulatory framework, digital transformation, national security.

Постановка проблеми. У сучасних умовах стрімкої цифровізації суспільних процесів кіберпростір перетворився на один із ключових вимірів функціонування держави, публічного управління та реалізації прав і свобод людини. Масове впровадження цифрових сервісів, електронного урядування, інформаційно-комунікаційних технологій, хмарних рішень і великих масивів даних істотно підвищує ефективність діяльності органів публічної влади, водночас посилюючи ризики кіберзагроз, витоків інформації, несанкціонованого доступу до персональних даних та порушення інформаційної безпеки. У цих умовах кібербезпека та захист персональних даних набувають статусу базових складових національної безпеки, демократичного врядування й довіри громадян до державних інституцій.

Для України актуальність зазначеної проблематики суттєво зростає з огляду на поєднання кількох чинників: тривалу збройну та гібридну агресію, активне використання кіберпростору як поля протистояння, а також стратегічного курсу держави на європейську інтеграцію. Кібероперації, кібератаки на критичну інфраструктуру, державні реєстри, інформаційні системи органів публічної влади та комерційного сектору, а також зловживання персональними даними громадян створюють системні виклики для функціонування держави та забезпечення прав людини.

У таких умовах гармонізація національного законо-давства у сфері кібербезпеки та захисту персональних даних з європейськими стандартами ЄС, зокрема положеннями Загального регламенту про захист даних (GDPR), Директиви NIS/NIS2 та інших актів *acquis communautaire*, стає не лише



міжнародно-правовим зобов'язанням України, а й практичною необхідністю для зміцнення державної спроможності.

Водночас процес адаптації вітчизняного законодавства до європейських стандартів супроводжується низкою складних викликів для публічної влади. Серед них необхідно відзначити такі: фрагментарність нормативно-правового регулювання, дублювання та неузгодженість наданих повноважень органів публічного управління, недостатній рівень інституційної спроможності у сфері кіберзахисту, дефіцит фахових кадрів та обмеженість практичних механізмів контролю за дотриманням вимог захисту персональних даних. Додатковою проблемою є поєднання завдань національної безпеки з необхідністю дотримання європейських стандартів прав людини, пропорційності та прозорості втручання органів державної влади у цифровий простір.

За таких умов постає об'єктивна потреба у комплексному науковому осмисленні процесів гармонізації законодавства України у сфері кібербезпеки та захисту персональних даних у контексті функціонування системи публічного управління та адміністрування. Розв'язання означеної проблеми безпосередньо пов'язане з важливими науковими та практичними завданнями, зокрема розвитком теорії публічного управління в умовах цифрової трансформації, удосконаленням механізмів державної політики кібербезпеки, підвищенням інституційної спроможності органів публічної влади, формуванням ефективної системи захисту персональних даних та забезпеченням балансу між безпековими інтересами держави й правами громадян.

Науково обґрунтований підхід до гармонізації законодавства сприятиме підвищенню довіри суспільства до публічної влади, зміцненню кіберстійкості держави та наближенню України до повноцінної інтеграції у європейський правовий і цифровий простір.

Аналіз останніх досліджень і публікацій. Опрацювання сучасних наукових досліджень і публікацій вказує на те, що проблематика гармонізації національного законодавства у сфері кібербезпеки та захисту персональних даних із європейськими стандартами перебуває у фокусі уваги як українських, так і зарубіжних науковців. Теоретико-методологічні засади державної політики у сфері кібербезпеки, інформаційної безпеки та захисту персональних даних, а також особливості правового регулювання цифрових відносин розкрито у працях таких вітчизняних дослідників: О. Буряченка, С. Глобенка, В. Горбуліна, О. Дзьобаня, І. Єфименка, Г. Красноступа, В. Ліпкана, С. Мазепи, Н. Олійник, О. Пархоменко-Куцевіл, С. Петькуна, Г. Ситника, О. Ткаченка та інших. Зазначені дослідники висвітлюють питання формування державної політики кібербезпеки, нормативно-правових механізмів захисту інформації, забезпечення прав людини у цифровому середовищі та інституційної ролі органів публічної влади у протидії кіберзагрозам.



Значний внесок у дослідження європейських підходів до регулювання кіберпростору та захисту персональних даних зробили зарубіжні науковці, зокрема К. Беннетт, Л. Бикер, С. Вахтер, П. Де Герт, М. Коен, Р. Познер, Дж. Рейденберг, досліджуючи еволюцію європейського права у сфері захисту даних, імплементацію Загального регламенту про захист даних (GDPR), розвиток директив і регламентів ЄС у сфері кібербезпеки, а також баланс між безпековими інтересами держави і захистом приватності. Особливу увагу приділено інституційним моделям регулювання, механізмам державного контролю та ролі публічної влади у забезпеченні цифрових прав громадян.

Водночас, попри наявність значного масиву наукових напрацювань, низка важливих аспектів означеної проблематики залишається недостатньо дослідженою. Зокрема, бракує комплексних міждисциплінарних досліджень, спрямованих на аналіз гармонізації вітчизняного законодавства з європейськими стандартами кібербезпеки та захисту персональних даних саме з позицій публічного управління та адміністрування. Недостатньо розробленими залишаються питання інституційної спроможності органів публічної влади до імплементації вимог GDPR і директив ЄС у національну правову систему, координації між суб'єктами публічного управління із дотриманням стандартів прав людини у цифровому середовищі. Саме ці невирішені раніше складові загальної проблеми зумовлюють необхідність подальших наукових розвідок і визначають наукову спрямованість означеної статті.

Мета статті полягає у теоретико-практичному обґрунтуванні та комплексному аналізі процесів гармонізації вітчизняного законодавства України у сфері кібербезпеки та захисту персональних даних з європейськими стандартами, а також визначенні ключових викликів і напрямів удосконалення механізмів публічного управління та адміністрування в умовах цифрової трансформації, євроінтеграції та зростання кіберзагроз для підвищення інституційної спроможності органів публічної влади, забезпечення балансу між національною безпекою і захистом прав людини та формуванням стійкої системи кіберзахисту держави.

Виклад основного матеріалу. В умовах сьогодення розвиток публічного управління та адміністрування відзначається глибокою цифровою трансформацією, що істотно міняє способи взаємодії держави, суспільства та індивіда. Цифрова трансформація суспільства докорінно змінює характер функціонування системи публічного управління, розширюючи межі державного втручання у цифровий простір та водночас підвищуючи залежність держави від стабільності, безпеки й надійності інформаційно-комунікаційних систем. Кіберпростір у сучасних умовах виступає не лише технологічною платформою для надання публічних послуг, а й самостійним середовищем реалізації владних повноважень, політичної комунікації, економічної діяльності та здійснення



основоположних прав і свобод людини. У цьому контексті кібербезпека та захист персональних даних набувають системного значення як ключові елементи державної спроможності та демократичного врядування.

Внаслідок глобалізації, децентралізації влади та зростаючої конкуренції між державами на перший план виходить здатність швидко реагувати й адаптуватися до викликів цифрової епохи та захисту інформації, що визначає рівень їх національної конкурентоспроможності, стабільності, економічної та інформаційної безпеки [1]. Зокрема, нормативно-правова база Європейського Союзу щодо кібербезпеки спрямована на формування стійкої та надійної цифрової екосистеми. Постійно враховуючи нові загрози і виклики, а також розширюючи сферу діяльності, ЄС прагне до узгодження своїх принципів конфіденційності, основних прав і гармонізації ринку з нагальними вимогами цифрової трансформації. Завдяки комплексній співпраці між державами-членами, зацікавленими сторонами приватного сектору та державними інституціями ЄС запроваджуваний регуляторний підхід гарантує те, що єдиний цифровий ринок буде залишатися безпечним і надійним, надаючи користь усім громадянам і підприємствам ЄС [2].

В умовах збройної та гібридної агресії проти України кіберпростір перетворився на один із головних театрів протистояння, де поєднуються технічні, інформаційні, психологічні та правові впливи. Масштабні кібератаки на об'єкти критичної інфраструктури, державні реєстри, інформаційні системи органів публічної влади та суб'єктів господарювання супроводжуються поширенням дезінформації, маніпуляцій громадською думкою та спробами підризу довіри до державних інституцій. За таких умов ефективність державної політики у сфері кібербезпеки безпосередньо залежить не лише від технічних рішень, а й від якості нормативно-правового регулювання та інституційної спроможності системи публічного управління. Зокрема, масштабне оброблення різного роду персональних і корпоративних даних вимагає постійного оновлення правових стандартів щодо захисту отриманих даних, відповідальності поставальників та запровадження механізмів дієвого контролю, оскільки регуляторні розриви між різними юрисдикціями ускладнюють крос-кордонні розслідування й координацію реагування [3]. Необхідно відзначити, що ефективність захисту персональних даних в Україні є менш досконалою, в порівнянні із сформованою практикою в державах-членах ЄС, в яких для цього створені та функціонують окремі спеціалізовані органи з захисту персональних даних, що підтверджується офіційно оприлюдненою статистикою та накладенням встановлених санкцій на відповідних суб'єктів [4].

Відтак, виникає гостра необхідність створення сучасної системи інформаційно-аналітичного забезпечення законотворчої, нормотворчої та правозастосовної діяльності, яка обумовлена актуальністю вирішення проблем



розбудови нормативно-правових основ нової держави, формування її інформаційно-правової бази, зростання якісних показників та скорочення технологічного процесу законотворення з подальшим прийняттям у парламенті відповідних нормативних актів [5]. Результати проведеного аналізу європейських стандартів відображають основні тенденції розвитку інформаційної політики Європейського Союзу, ключовою серед яких є посилення ролі кібербезпеки в сфері забезпечення інформаційної безпеки, що здійснює критичний вплив не лише на економічну систему ЄС, а й на розвиток демократичних процесів, а також на безпеку та здоров'я населення [6].

Саме тому наразі особливого значення набуває проблематика гармонізації вітчизняного законодавства України у сфері кібербезпеки та захисту персональних даних з європейськими стандартами. Європейський Союз упродовж останніх десятиліть сформував комплексну модель нормативно-правового регулювання цифрового простору, яка базується на поєднанні високих стандартів захисту прав людини з ефективними механізмами забезпечення безпеки. Загальний регламент про захист даних (GDPR), Директива NIS та її оновлена редакція NIS2, Регламент про кіберстійкість, а також інші акти *acquis communautaire* формують багаторівневу систему правових норм, спрямованих на підвищення кіберстійкості держав-членів та комплексний захист цифрових прав громадян. Адаптація цих стандартів до національної правової системи України є складним і багатовимірним процесом, що виходить за межі суто юридичної імплементації норм. Вона потребує трансформації підходів до публічного управління, перегляду повноважень органів влади, удосконалення механізмів міжвідомчої координації, розвитку кадрового потенціалу та впровадження нових управлінських практик. У цьому сенсі гармонізація законодавства постає як інструмент системної модернізації державного управління в умовах цифрової трансформації.

С. Мазепа також відзначає, що процес імплементації європейських правових норм в законодавство України характеризується значною складністю та багатовекторністю, оскільки сучасна система європейського регулювання інформаційної безпеки базується на комплексному підході, який поєднує в собі захист персональних даних, кібербезпеку критичної інфраструктури та боротьбу з кіберзлочинністю. До основних принципів європейського підходу належать такі: превентивність, пропорційність, підзвітність та міжнародне співробітництво. Вони створюють надійне підґрунтя для забезпечення цифрової безпеки в умовах глобалізації інформаційного простору [7]. При цьому технологічні виклики щодо імплементації європейського законодавства пов'язані з необхідністю формування технічної інфраструктури, яка відповідатиме європейським стандартам кібербезпеки. Впровадження вимог відносно захисту персональних даних, повідомлення про порушення безпеки, проведення оцінки впливу



на захист даних потребує значних інвестицій у інформаційні системи та підготовку кваліфікованих кадрів. Відсутність достатніх технічних та фінансових ресурсів може суттєво уповільнити процес приведення національних систем у відповідність до європейських вимог [8].

До того ж, недосконалість українського законодавства проявляється у таких ключових аспектах: прийняті закони та законодавчі акти мають переважно декларативний характер [9], прослідковується недостатній рівень прозорості щодо згоди на обробку даних; застосовуються слабкі санкції за порушення кібербезпеки, які не здатні створити превентивного ефекту; відсутність в країні незалежного спеціалізованого державного органу контролю за дотриманням чинного законодавства [10].

Загалом аналіз чинного законодавства України у сфері кібербезпеки та захисту персональних даних свідчить про наявність певних досягнень, зокрема ухвалення базових законів, стратегій і концепцій, спрямованих на формування державної політики у цій сфері. Так, основним нормативно-правовим актом, який нині регулює цю сферу, є оновлений Закон України “Про захист персональних даних”, який був прийнятий ще у 2010 р. [11]. Але, поряд із цим, зберігається фрагментарність правового регулювання, що проявляється у дублюванні функцій окремих органів публічної влади, нечіткості розмежування відповідальності та відсутності єдиного підходу до управління кіберризиками. Така ситуація ускладнює імплементацію європейських стандартів та знижує ефективність практичної реалізації державної політики.

Отож необхідно відзначити, що у європейській практиці ключовим принципом регулювання кіберпростору є ризик-орієнтований підхід, який передбачає диференціацію вимог залежно від характеру діяльності суб’єкта, обсягу оброблюваних даних та потенційних наслідків кіберінцидентів.

Вітчизняне законодавство лише частково відображає цей підхід, що створює дисбаланс між рівнем формальних вимог і реальними можливостями їх виконання органами публічної влади та суб’єктами господарювання. Гармонізація з європейськими стандартами потребує запровадження більш гнучких і водночас відповідальних механізмів регулювання.

Окремої уваги заслуговує проблема захисту персональних даних у системі публічного управління, де масове впровадження електронних реєстрів, систем електронної ідентифікації, цифрових платформ надання публічних послуг істотно розширює можливості держави щодо обробки персональної інформації громадян. Водночас така ситуація підвищує ризики зловживань, несанкціонованого доступу та порушення права на приватність громадян. Європейська модель, закріплена у GDPR, виходить із презумпції пріоритету прав суб’єкта даних і покладає на органи публічної влади підвищений обсяг відповідальності за законність і безпеку обробки інформації.



Імплементація принципів GDPR у національну систему публічного управління України потребує не лише формального перенесення норм, а й зміни управлінської культури. Мова йде про перехід від традиційного виконання вимог до усвідомлення захисту персональних даних як складової публічного інтересу та елементу довіри між державою і громадянами. Важливим науковим результатом дослідження є обґрунтування того, що без інтеграції стандартів захисту персональних даних у повсякденну управлінську практику органів влади неможливо досягти стійкої цифрової трансформації.

Не менш важливим є питання інституційної спроможності органів публічної влади щодо реалізації політики кібербезпеки. Європейський досвід свідчить, що ефективна система кіберзахисту ґрунтується на чіткій координації між центральними та галузевими органами влади, наявності спеціалізованих національних центрів реагування на кіберінциденти та розвинених механізмах публічно-приватного партнерства. В Україні ці елементи перебувають у стадії становлення, що обумовлює потребу в подальшому інституційному розвитку та нормативно-правовому закріпленні відповідних повноважень.

Саме тому гармонізація вітчизняного законодавства України з європейськими стандартами кібербезпеки та захисту персональних даних має розглядатися не як одноразовий або суто юридично-технічний акт адаптації норм, а як складний багаторівневий процес трансформації системи публічного управління. Такий процес охоплює стратегічний, інституційний, нормативно-правовий та операційний рівні, кожен з яких виконує самостійну функцію, але водночас перебуває у тісному взаємозв'язку з іншими рівнями. Саме системність і узгодженість цих рівнів визначають ефективність імплементації європейських стандартів у національну практику.

На стратегічному рівні гармонізація законодавства проявляється у формуванні та узгодженні довгострокових пріоритетів державної політики у сфері кібербезпеки та захисту персональних даних із загальноєвропейськими підходами. Йдеться про інтеграцію європейських цінностей і принципів (верховенство права, пріоритет прав людини, пропорційність державного втручання та відповідальність публічної влади) у стратегічні документи України. На цьому рівні важливу роль відіграють Стратегії кібербезпеки, цифрової трансформації, національної безпеки, а також програмні документи, які напрямую пов'язані з виконанням Угоди про асоціацію між Україною та ЄС. Стратегічний рівень забезпечує концептуальну рамку гармонізації, визначаючи, що кібербезпека та захист персональних даних розглядаються не лише як технічні або силові завдання, а як елементи демократичного врядування та суспільної стійкості. Відсутність чіткої стратегічної узгодженості призводить до фрагментарності реформ, декларативності євроінтеграційних намірів і зниження довіри з боку громадян та європейських партнерів.



Інституційний рівень гармонізації пов'язаний із формуванням ефективної системи суб'єктів публічного управління, відповідальних за реалізацію політики кібербезпеки та захисту персональних даних. Європейські стандарти передбачають наявність чітко визначених повноважень, незалежних регуляторних органів, ефективних механізмів координації та підзвітності. В Україні ж інституційна модель досі характеризується розпорошеністю функцій між різними органами виконавчої влади, дублюванням повноважень і недостатньою міжвідомчою взаємодією. Гармонізація на інституційному рівні передбачає не лише створення або реформування відповідних органів, а й підвищення їх реальної спроможності діяти відповідно до європейських вимог. Це включає кадрове забезпечення, розвиток професійних компетентностей, формування культури управління ризиками та впровадження сучасних управлінських практик. Особливої ваги набуває забезпечення незалежності органів, відповідальних за захист персональних даних, що є однією з ключових вимог GDPR і важливим показником демократичності публічного управління.

Нормативно-правовий рівень гармонізації охоплює адаптацію національного законодавства до актів права Європейського Союзу у сфері кібербезпеки та захисту персональних даних. На цьому рівні здійснюється імплементація положень GDPR, директив NIS/NIS2, а також інших європейських регламентів і рекомендацій. Важливо підкреслити, що гармонізація не зводиться до механічного копіювання норм, а потребує їх системного узгодження з національною правовою традицією, конституційними засадами та особливостями функціонування публічної влади. Проблемним аспектом нормативно-правового рівня в Україні залишається фрагментарність і несистемність правового регулювання, що ускладнює практичне застосування європейських стандартів. Гармонізація має бути спрямована на створення цілісної правової архітектури, яка забезпечує зрозумілі правила для органів публічної влади, бізнесу та громадян, а також ефективні механізми контролю й відповідальності. На цьому рівні формується правовий баланс між безпековими інтересами держави та захистом прав людини у цифровому середовищі.

Операційний рівень гармонізації є найбільш практико-орієнтованим і безпосередньо пов'язаний із повсякденною діяльністю органів публічної влади. Він охоплює впровадження європейських стандартів у конкретні управлінські процедури, адміністративні регламенти, інформаційні системи та повсякденні процеси обробки даних. Йдеться про запровадження стандартів кіберзахисту, протоколів реагування на інциденти, процедур оцінки ризиків, а також механізмів забезпечення прав суб'єктів персональних даних. На операційному рівні особливо чітко проявляється взаємозв'язок між якістю законодавства та ефективністю публічного управління. Навіть досконалі нормативні акти втрачають свою цінність за відсутності практичних інструментів реалізації,



належного ресурсного забезпечення та управлінської відповідальності. Тому гармонізація законодавства має супроводжуватися розвитком інституційної пам'яті, навчанням державних службовців і формуванням культури дотримання стандартів кібербезпеки та захисту персональних даних.

Відтак, багаторівневий підхід до гармонізації законодавства дозволяє розглядати цей процес як комплексну трансформацію системи публічного управління, а не як ізольовану правову реформу. Узгоджене функціонування стратегічного, інституційного, нормативно-правового та операційного рівнів створює передумови для формування в Україні стійкої, ефективної та орієнтованої на права людини системи кібербезпеки, що відповідає європейським стандартам і викликам сучасного цифрового середовища.

Отже, гармонізація вітчизняного законодавства у сфері кібербезпеки та захисту персональних даних є не лише вимогою євроінтеграційного курсу України, а й ключовим інструментом підвищення ефективності публічного управління. Вона сприяє формуванню стійкої, прозорої та орієнтованої на громадянина системи державного управління, здатної адекватно реагувати на сучасні цифрові та безпекові виклики. Комплексний підхід до гармонізації законодавства, що поєднує правові, інституційні та управлінські аспекти, створює передумови для зміцнення кіберстійкості держави, підвищення довіри громадян до органів публічної влади та наближення України до повноцінної інтеграції у європейський правовий і цифровий простір.

Висновки. Проведений комплексний аналіз проблематики гармонізації вітчизняного законодавства України у сфері кібербезпеки та захисту персональних даних із європейськими стандартами в контексті функціонування системи публічного управління та адміністрування виявив, що в умовах стрімкої цифровізації публічного простору, зростання кіберзагроз і триваючої гібридної агресії кібербезпека та захист персональних даних набувають статусу ключових елементів національної безпеки, демократичного врядування й довіри громадян до інститутів публічної влади. Встановлено, що ефективність державної політики у цій сфері безпосередньо залежить від рівня узгодженості національного законодавства з європейськими нормами та стандартами.

Гармонізація законодавства з європейськими стандартами кібербезпеки та захисту персональних даних має розглядатися як багаторівневий процес, який охоплює стратегічний, інституційний, нормативно-правовий та операційний рівні публічного управління та адміністрування. Формальна імплементація європейських норм без належного інституційного та управлінського забезпечення не забезпечує реального підвищення рівня кіберстійкості держави. Встановлено, що розглянутий процес гармонізації є не лише правовим або технічним завданням, а комплексним аспектом трансформації системи публічного управління, спрямованим на забезпечення балансу між безпековими



інтересами держави та дотриманням прав і свобод людини у цифровому середовищі. Реалізація такого підходу створює передумови для підвищення довіри громадян до публічної влади, зміцнення кіберстійкості держави та поглиблення європейської інтеграції України.

Перспективи подальших наукових досліджень у цьому напрямі пов'язані з необхідністю проведення поглибленого аналізу інституційних моделей реалізації європейських стандартів кібербезпеки та захисту персональних даних у державах-членах ЄС і можливостей їх адаптації до українських реалій. Особливої уваги потребують питання оцінювання ефективності імплементації GDPR і директив ЄС у практиці діяльності органів публічного управління та адміністрування, розроблення індикаторів інституційної спроможності та механізмів міжвідомчої координації у сфері кіберзахисту, що сприятиме удосконаленню теорії та практики публічного управління в умовах цифрової трансформації та підвищенню стійкості держави до сучасних кіберзагроз.

Література:

1. Климчук О. В. Цифрова трансформація в системі управління економічною безпекою держави. *Цифровізація як чинник економічної трансформації та соціально-економічної безпеки України: теорія, практика, перспективи: колективна монографія*. Рига, Латвія: Baltija Publishing, 2025. С. 128–178.
2. Савчук С. О. Виклики гармонізації законодавства ЄС в галузі кібербезпеки для України. *Економіка, управління та адміністрування*. 2024. № 1 (107). С. 207–213. DOI: [https://doi.org/10.26642/ema-2024-1\(107\)-207-213](https://doi.org/10.26642/ema-2024-1(107)-207-213).
3. Пархоменко-Куцевіл О. Концептуальні засади впровадження цифровізації як виклику для формування інформаційної безпеки. *Успіхи і досягнення у науці*. 2025. № 8 (18). С. 599–608. DOI: [https://doi.org/10.52058/3041-1254-2025-8\(18\)-599-608](https://doi.org/10.52058/3041-1254-2025-8(18)-599-608).
4. Пристай Р.А. Національні органи захисту даних в Європейському Союзі: роль і практика в сфері захисту персональних даних в соціальних мережах. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2024. Т. 2. № 82. С. 245–252. DOI: <https://doi.org/10.24144/2307-3322.2024.82.2.39>.
5. Климчук О. В. Інформаційні системи і технології в управлінні. Конспект лекцій. Вінниця: ДонНУ ім. Василя Стуса. 2021. 160 с.
6. Олійник Н., Петрос І. Еволюція європейських нормативно-правових стандартів та механізмів управління інформаційною безпекою в органах публічної влади в умовах цифрових трансформацій. *Вісник післядипломної освіти: збірник наукових праць. Серія «Соціальні та поведінкові науки; Управління та адміністрування»*. 2025. Вип. 32 (61). С. 328–346. DOI: <https://doi.org/10.58442/3041-1858-2025-32>.
7. Мазепа С. Міжнародний досвід захисту інформаційної безпеки: імплементація європейських правових норм в законодавство України. *Науковий вісник Ужгородського Національного Університету. Серія: Право*. 2025. Вип. 90: частина 3. С. 289–296. DOI: <https://doi.org/10.24144/2307-3322.2025.90.3.42>.
8. Мазепа С.О. Імплементація європейських стандартів інформаційної безпеки в національне законодавство: проблеми та перспективи. *Держава та регіони. Серія: Право*. 2025. № 3 (88). С. 44–49. DOI: <https://doi.org/10.32782/1813-338X-2025.3.6>.



9. Климчук О.В. Нормативно-правове регулювання виробництва біопалива: світовий досвід та проблемні аспекти в Україні. *Глобальні та національні проблеми економіки*. 2015. Вип. № 3. С. 107–110. URL: <http://global-national.in.ua/archive/3-2015/22.pdf>.

10. Кирик А. Гармонізація законодавства України із загальним регламентом ЄС про захист даних (GDPR): виклики та перспективи. *Успіхи і досягнення у науці*. 2025. № 11 (21). С. 156–169. DOI: [https://doi.org/10.52058/3041-1254-2025-11\(21\)-156-169](https://doi.org/10.52058/3041-1254-2025-11(21)-156-169).

11. Про захист персональних даних: Закон України від 1 червня 2010 року № 2297-VI. *Верховна Рада України. Законодавство України*. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>.

References:

1. Klymchuk, O. V. (2025). Tsifrova transformatsiia v systemi upravlinnia ekonomichnoi bezpekoii derzhavy [Digital transformation in the system of state economic security management]. In *Tsifrovizatsiia yak chynnyk ekonomichnoi transformatsii ta sotsialno-ekonomichnoi bezpeky Ukrainy: teoriia, praktyka, perspektyvy: kolektyvna monografiia [Digitalization as a factor of economic transformation and socio-economic security of Ukraine: theory, practice, prospects: collective monograph]* (pp. 128–178). Riga, Latvia: Baltija Publishing [in Ukrainian].

2. Savchuk, S. O. (2024). Vyklyky harmonizatsii zakonodavstva YeS v haluzi kiberbezpeky dlia Ukrainy [Challenges of harmonizing EU legislation in the field of cybersecurity for Ukraine]. *Ekonomika, upravlinnia ta administruvannia – Economics, Management and Administration*, 1 (107), 207–213. Retrieved from DOI: [https://doi.org/10.26642/ema-2024-1\(107\)-207-213](https://doi.org/10.26642/ema-2024-1(107)-207-213) [in Ukrainian].

3. Parkhomenko-Kutsevil, O. (2025). Kontseptualni zasady vprovadzhennia tsyfrovizatsii yak vyklyku dlia formuvannia informatsiinoi bezpeky [Conceptual foundations of digitalization implementation as a challenge for information security formation]. *Uspikhy i dosiahnennia u nauks – Successes and Achievements in Science*, 8 (18), 599–608. Retrieved from DOI: [https://doi.org/10.52058/3041-1254-2025-8\(18\)-599-608](https://doi.org/10.52058/3041-1254-2025-8(18)-599-608) [in Ukrainian].

4. Prystai, R. A. (2024). Natsionalni orhany zakhystu danykh v Yevropeiskomu Soiuzi: rol i praktyka v sferi zakhystu personalnykh danykh v sotsialnykh merezhakh [National data protection authorities in the European Union: Role and practice in the field of personal data protection in social networks]. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Serii: Pravo – Scientific Bulletin of Uzhhorod National University. Series: Law*, Vol. 2, No. 82, 245–252. Retrieved from DOI: <https://doi.org/10.24144/2307-3322.2024.82.2.39> [in Ukrainian].

5. Klymchuk, O. V. (2021). Informatsiini systemy i tekhnolohii v upravlinni [Information systems and technologies in management]. *Konspekt lektsii [Lecture notes]*. Vinnytsia: DonNU im. Vasylya Stusa. [in Ukrainian].

6. Oliynyk, N., & Petroie, I. (2025). Evoliutsiia yevropeiskyykh normatyvno-pravovykh standartiv ta mekhanizmv upravlinnia informatsiinoiu bezpekoii v orhanakh publichnoi vlady v umovakh tsyfrovyykh transformatsii [Evolution of European legal standards and mechanisms of information security management in public authorities under digital transformations]. *Visnyk pislyadypolnoi osvity: zbirnyk naukovykh prats. Serii «Sotsialni ta povedinkovi nauky; upravlinnia ta administruvannia» – Bulletin of Postgraduate Education: Collection of Scientific Works. Series “Social and Behavioral Sciences; Management and Administration”*, 32 (61), 328–346. Retrieved from DOI: <https://doi.org/10.58442/3041-1858-2025-32> [in Ukrainian].

7. Mazepa, S. (2025). Mizhnarodnyi dosvid zakhystu informatsiinoi bezpeky: implemientatsiia yevropeiskyykh pravovykh norm v zakonodavstvo Ukrainy [International experience of information security protection: implementation of European legal norms in the legislation of



Ukraine]. *Naukovyi visnyk Uzhhorodskoho Natsionalnoho Universytetu. Serii: Pravo – Scientific Bulletin of Uzhhorod National University. Series: Law*, 90 (3), 289–296. Retrieved from DOI: <https://doi.org/10.24144/2307-3322.2025.90.3.42> [in Ukrainian].

8. Mazepa, S. O. (2025). Implementatsiia yevropeiskykh standartiv informatsiinoi bezpeky v natsionalne zakonodavstvo: problemy ta perspektyvy [Implementation of European information security standards into national legislation: problems and prospects]. *Derzhava ta rehiony. Serii: Pravo – State and Regions. Series: Law*, 3 (88), 44–49. Retrieved from DOI: <https://doi.org/10.32782/1813-338X-2025.3.6> [in Ukrainian].

9. Klymchuk, O. V. (2015). Normatyvno-pravove rehuliuвання vyrobnytstva biopaliva: svitovyi dosvid ta problemni aspekty v Ukraini [Legal regulation of biofuel production: global experience and problematic aspects in Ukraine]. *Hlobalni ta natsionalni problemy ekonomiky – Global and National Problems of Economics*, 3, 107–110. Retrieved from URL: <http://global-national.in.ua/archive/3-2015/22.pdf> [in Ukrainian].

10. Kirik, A. (2025). Harmonizatsiia zakonodavstva Ukrainy iz zahalnym rehlamentom YeS pro zakhyst danykh (GDPR): vyklyky ta perspektyvy [Harmonization of Ukrainian legislation with the EU General Data Protection Regulation (GDPR): challenges and prospects]. *Uspikhy i dosiahnennia u nautsi – Successes and Achievements in Science*, 11 (21), 156–169. Retrieved from DOI: [https://doi.org/10.52058/3041-1254-2025-11\(21\)-156-169](https://doi.org/10.52058/3041-1254-2025-11(21)-156-169) [in Ukrainian].

11. Pro zakhyst personalnykh danykh: Zakon Ukrainy vid 1 chervnia 2010 roku № 2297-VI [On Personal Data Protection: Law of Ukraine of June 1, 2010, No. 2297-VI]. *Verkhovna Rada Ukrainy – Legislation of Ukraine*. Retrieved from URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text> [in Ukrainian].

Дата першого надходження статті до видання: 23.01.2026

Дата прийняття статті до друку після рецензування: 10.02.2026