DOI: https://doi.org/10.26642/jen-2024-1(107)-207-213
УДК 004.056.5:339.924(477)

С.О. Савчук, здобувач
Державний університет «Житомирська політехніка»

Виклики гармонізації законодавства ЄС в галузі кібербезпеки для України

(Представлено: д.е.н., д.держ.упр., проф. Грицишен Д.О.)

Стаття досліджує нормативно-правову базу Європейського Союзу у сфері кібербезпеки, аналізуючи ключові регламенти та директиви, що регулюють захист цифрової інфраструктури, мереж та інформаційних систем. Особливу увагу приділено директивам NIS і NIS2, Закону про кібербезпеку (Cybersecurity Act), Загальному регламенту захисту даних (GDPR), а також Закону про цифрову операційну стійкість (DORA). У дослідженні підкреслено важливість гармонізації правових норм для забезпечення єдності цифрового ринку, зміцнення довіри користувачів та стимулювання інновацій. У статті визначено необхідність інтеграції України до європейської системи кібербезпеки, що передбачає прийняття ефективного законодавства, адаптованого до європейських стандартів, зокрема в частині управління ризиками, звітування про інциденти та захисту персональних даних. Важливою складовою цієї інтеграції є створення незалежного координаційного органу, здатного забезпечити моніторинг, реагування та міжнародну співпрацю. У статті також підкреслено значення сертифікації IT-продуктів та цифрових послуг відповідно до вимог Cybersecurity Act, що дозволить українським компаніям інтегруватися в європейський ринок. Наголошено на потребі у розвитку інституційної спроможності України, залученні кваліфікованих кадрів та підвищенні обізнаності управлінців державного і приватного секторів у питаннях кібербезпеки. Результати дослідження вказують на необхідність тісної координації між усіма зацікавленими сторонами, зокрема, державними органами, приватним сектором та міжнародними партнерами, для створення стійкої системи кібербезпеки в Україні. Запропоновані рекомендації можуть слугувати основою для подальшої гармонізації законодавства, посилення інституційної спроможності та адаптації до вимог європейського цифрового ринку.

***Ключові слова**: державне управління; інтеграція; кіберзагрози; кібербезпека; критична інфраструктура; сертифікація.*

Постановка проблеми. В Європейському Союзі діє комплексна система нормативно-правового регулювання заходів з кібербезпеки. Чинні нормативні-правові акти є відповіддю на сучасне складне та взаємопов'язане цифрове середовище. Здійснення кібератак виходить за межі національних кордонів, що робить ізольовані національні системи протидії цим загрозам недостатніми. Таким чином, порушення безпеки в одній країні, яка є членом ЄС, може мати каскадні наслідки для всіх країн партнерів. Такий транснаціональний вимір вимагає узгодженого підходу до кібербезпеки, через управління ризиками та звітуванням про інциденти порушення цифрової безпеки. Уніфіковані стандарти кібербезпеки в ЄС зменшують ризики фрагментованих нормативних актів, які можуть призвести до прогалин, збігів і різнорівневої безпеки. Єдиний цифровий ринок ЄС залежить від надійних заходів кібербезпеки для забезпечення довіри споживачів, сприяння чесній конкуренції та підтримки цифрових інновацій. Ефективне регулювання лежить в основі цієї екосистеми, створюючи безпечне середовище для цифрової трансформації.

За останнє десятиліття законодавча база Європейського Союзу щодо кібербезпеки розширилася та ускладнилася, відображаючи як мінливість загроз, так і потребу в захисті цілісності єдиного цифрового ринку. Створена структура передбачає існування декількох ключових правових інструментів. Їх синергетична дія спрямована на підвищення безпеки мережевих та інформаційних систем, встановлення загальних стандартів і роз'яснення ролей та обов'язків на національному рівні кожної країни-учасниці та в цілому ЄС. Кожен з інструментів певним чином впливає на національне законодавство, впливаючи на їхні регулятивні підходи, механізми забезпечення дотримання та розподіл ресурсів для заходів кібербезпеки.

У контексті реформування законодавства Україна також потребує підтримки в розвитку інституційної спроможності. Прийняття нових законів чи оновлених норм саме собою не вирішить проблему, якщо на державному і приватному рівнях бракуватиме кваліфікованих кадрів або дієвих механізмів реалізації. Тому варто зосередитися на формуванні стратегії кібербезпеки, що передбачатиме підготовку спеціалістів, а також залучення необхідних фінансових та організаційних ресурсів. Окрему роль відіграє освіта для державного сектора і керівників приватних компаній, оскільки саме вони приймають стратегічні рішення щодо інформаційної безпеки та реагування на загрози.

Таким чином, запровадження принципів євроінтеграції в сфері кібербезпеки насамперед вимагає законодавчих змін, які врегулюють обов'язки операторів критичної інфраструктури, забезпечать прозорий та своєчасний інцидент-репортинг, створять незалежний і ефективний координаційний орган, узгодять систему сертифікації та гармонізують підходи до захисту персональних даних із європейськими стандартами. Усі ці кроки є першочерговими, тому що становлять основу для побудови комплексної, дієвої та прозорої системи кіберзахисту, що відповідає сучасним викликам і стандартам ЄС.

Метою статті є аналіз нормативно-правової бази Європейського Союзу у сфері кібербезпеки, визначення ключових аспектів її впровадження та адаптації в Україні, а також розробка рекомендацій для гармонізації українського законодавства з європейськими стандартами з метою забезпечення надійного захисту критичної цифрової інфраструктури та сприяння інтеграції України до єдиного цифрового ринку ЄС.

Аналіз останніх досліджень та публікацій. Серед зарубіжних дослідників варто зазначити роботи Р.Муді, Л.Стрельцова, Л.Керулуса, Е.Грінберга та інших. Муді Р. у своїх дослідженнях детально аналізує статистичні дані щодо рейтингу країн світу за рівнем кібербезпеки, враховуючи широкий спектр факторів, що впливають на цей показник [4]. Наприклад, Л.Стрельцов досліджував стан кібербезпеки України в період 2015–2017 років, акцентуючи увагу на ключових принципах, суб'єктах кібербезпеки, викликах та здобутках держави [13]. Однак варто зазначити, що через часові обмеження дослідження не охоплює більш пізніх змін у сфері кіберзахисту. У свою чергу Л.Керулус розглядає кібербезпеку в контексті російської агресії, зокрема висвітлює особливості кібернетичної та гібридної війни на території України [1]. Його дослідження демонструє вразливість України у сфері кіберзахисту та складність протидії агресивній імперській політиці кремля. Грінберг Е. детально досліджує кібервтручання російських хакерів в Україні, зокрема їхній вплив на енергетичний сектор, медіа, фінансову систему, транспорт, військові об'єкти та політичну інфраструктуру [9]. Значна увага приділяється аналізу масштабних кібератак, таких як вимкнення електропостачання та порушення роботи державних установ. Більшість зарубіжних дослідників зосереджуються на аспектах кібервійни між Україною та росією, акцентуючи увагу на кібератаках російських хакерів, що спрямовані проти цивільних і військових об'єктів України [12]. Водночас відповіді з боку української сторони, як правило, оцінюються як обмежені через недостатність ресурсів і технологій. Таким чином, існуюча література відображає багатогранний підхід до вивчення кібербезпеки, однак залишається необхідність у більш інтегрованому підході до аналізу як правових, так і технічних аспектів, зокрема з урахуванням нових викликів, які постають перед Україною в умовах інтеграції з європейською кібербезпековою системою.

Викладення основного матеріалу. Чинні нормативні акти ЄС сприяли розвитку екосистеми, у якій кібербезпека визнається спільною відповідальністю урядів держав, приватних підприємств та установ ЄС. У створеній системі встановлено офіційні процеси для звітування про інциденти, співпрацю та розробку спільних стандартів безпеки. Однак ефективність цих заходів залежить від ресурсів і можливостей, доступних окремим державам-членам, ступеня впровадження рекомендованих практик приватним сектором і глобального характеру кіберзагроз. Хоча законодавство ЄС, безсумнівно, підвищило базові заходи безпеки, залишаються значні прогалини в тому, наскільки ефективно ці заходи перетворюються на довгострокове зниження ризику, що підкреслює необхідність постійного вдосконалення як механізмів політики, так і оперативних можливостей.

У таблиці 1 наведено огляд основних нормативних актів і директив щодо кібербезпеки в ЄС. Зазначено головні сфери та ключові характеристики кожного нормативного документа, що пояснює їх значення та вплив на підвищення рівня кібербезпеки в різних секторах і забезпеченню стійкості єдиного цифрового середовища. Вказані регламенти стосуються широкого спектра питань, від безпеки мережі та інформаційних систем до захисту даних, стійкості фінансового сектора та стандартів кібербезпеки на рівні продуктів.

NIS Directive є першим нормативним документом, який запроваджує загальноєвропейські вимоги та рекомендації щодо регулювання кібербезпеки, з метою досягнення високого загального рівня безпеки мережевих та інформаційних систем. Директива безпосередньо стосується операторів основних послуг (OES) у таких секторах, як енергетика, транспорт і банківська справа, а також постачальників цифрових послуг, таких як хмарні сервіси та онлайн-ринки. Директива визначає практичні заходи з управління ризиками, звітування про інциденти кіберзагроз та механізми співпраці між національними групами реагування на комп'ютерну безпеку (CSIRT).

Відображаючи еволюцію цифрових загроз, Директива NIS2 розширює сферу регулювання за рахунок додаткових критичних секторів, таких як управління стічними водами, державне управління та космічна інфраструктура. Директива NIS2 розширює вимоги Директиви NIS щодо безпеки ланцюга постачання, запроваджує суворіші заходи управління та встановлює суворіші покарання за невиконання вимог.

Закон про кібербезпеку (Cybersecurity Act) посилює роль Агентства ЄС з кібербезпеки – ENISA [10], надавши йому постійний мандат і розширивши його операційні можливості. В законі регламентовано загальноєвропейську систему сертифікації кібербезпеки для продуктів, процесів і послуг інформаційно-

комп'ютерних технологій. Незважаючи на те, що вимоги системи у багатьох випадках є рекомендаційними, для програм із високим ризиком передбачені обов'язкові процедури.

Незважаючи на те, що GDPR в першу чергу зосереджений на захисті даних, Регламент перетинається з кібербезпекою через свої вимоги щодо сповіщень про порушення даних і впровадження технічних і організаційних заходів для захисту персональних даних. Всі суб'єкти, які не відповідають цим стандартам, загрожують значним штрафам.

Таблиця 1

Основні нормативно-правові документи в галузі кібербезпеки ЄС

Назва нормативного документа	Сфера впливу	Особливості
NIS Directive (2016) [6]	Безпека мереж та інформаційних систем	Управління ризиками, звітування про інциденти, OES і DSP
NIS2 Directive (2022) [7]	Розширений обсяг рамок кібербезпеки	Більш широкі сектори, зосередженість на ланцюзі поставок, суворіше управління
Cybersecurity Act [11]	Мандат і структура сертифікації ENISA	Загальноєвропейські сертифікати, робочі можливості ENISA
GDPR [16]	Захист даних і повідомлення про порушення	Організаційні заходи, значні штрафи за порушення
Digital Operational Resilience Act (DORA) [5]	Стійкість фінансового сектора до цифрових технологій	Комплексні стандарти для фінансових установ
Digital Services Act (DSA) [15]	Безпека та підзвітність платформи	Безпека даних для платформ, підзвітність модерації контенту
Digital Markets Act (DMA) [14]	Ринкова конкуренція та кібербезпека	Безпечні ринкові процеси, чесна конкуренція
Cyber Resilience Act [3]	Стандарти кібербезпеки на рівні продукту	Безпечний дизайн, безпека життєвого циклу для IoT і програмного забезпечення

Закон про цифрову операційну стійкість (Digital Operational Resilience Act – DORA) відповідає потребам фінансового сектора в кібербезпеці, встановлюючи стандарти цифрової стійкості для таких суб'єктів ринку, як банки та постачальники платіжних послуг [5]. Натомість Закон про цифрові послуги (DSA) і Закон про цифрові ринки (DMA) регулюють онлайн-платформи, зосереджуючись на безпечній обробці даних і підзвітності платформи, опосередковано впливаючи на кібербезпеку. Однією з останніх ініціатив ЄС щодо підвищення рівня кібербезпеки країн-учасниць є Cyber Resilience Act [3]. Ініційований закон спрямований на те, щоб цифрові продукти, разом з пристроями Інтернету речей, були безпечними за своєю конструкцією та підтримували безпеку протягом усього життєвого циклу.

Аналіз чинних нормативно-правових актів щодо кібербезпеки, які прийняті в ЄС, та напрям законодавчих ініціатив вказують, що пріоритетними секторами є енергетика, транспорт, банківська справа, охорона здоров'я та водопостачання. Оскільки ці сектори є невід'ємною частиною соціальної та економічної стабільності, то кіберзагрози в цих областях можуть мати серйозні транскордонні наслідки, що вимагає суворого регуляторного нагляду. Регламентація кібербезпеки сервісів хмарних обчислень, онлайн-ринків та пошукових систем перебувають під постійними змінами та уточненнями зі сторони законодавчих ініціатив. Також варто зазначити про постійне розширення зобов'язань, зокрема згідно з NIS2, що відображає критичну роль вказаних галузей на цифровому ринку ЄС. Усвідомлюючи ризики, пов'язані з кібератаками на державні установи, NIS2 включає національні, регіональні та місцеві органи влади в свою сферу дії. Запропонований Закон про стійкість до кібербезпеки підкреслює необхідність кібербезпеки на рівні продукту, виступаючи за стандарти «безпеки проєктів» для захисту спільного європейського ринку.

Такі нормативні акти, як GDPR [16] і Закон про кібербезпеку [11], безпосередньо застосовуються в країнах-членах, тоді як такі директиви, як NIS2, вимагають імплементації визначених норм у національному законодавстві. Незважаючи на зусилля щодо гармонізації, зберігаються відмінності у застосуванні та тлумаченні регламентних норм серед країн-учасниць. Закони ЄС про кібербезпеку часто мають екстратериторіальні наслідки, як видно з результатів застосування GDPR до суб'єктів, які мають доступ та користуються даними резидентів ЄС. Подібні принципи поширюються на правила кібербезпеки, що стосуються компаній за межами ЄС, які працюють на єдиному ринку.

Правила ЄС щодо кібербезпеки зобов'язують компанії застосовувати надійні методи управління ризиками та повідомляти про значні інциденти, щоб пом'якшити їхній вплив. Встановлюючи базові вимоги безпеки для критичної інфраструктури та цифрових послуг, ЄС прагне зміцнити свій колективний

кіберзахист. Такі ініціативи, як схеми сертифікації Закону про кібербезпеку, спрямовані на підвищення довіри споживачів і бізнесу до цифрових технологій, стимулюючи інновації та зростання. ЄС сприяє співпраці через мережі національних CSIRT [2], галузевих центрів обміну інформацією та аналізу (ISAC) і Організаційної мережі зв'язку з кіберзагроз (CyCLONe) [8], прискорюючи обмін розвідувальною інформацією про загрози та скоординоване реагування на безпекові інциденти.

Заходи кібербезпеки відповідають зобов'язанням ЄС щодо конфіденційності та захисту даних, захищаючи права громадян у цифровому суспільстві. Нові технології, такі як штучний інтелект, квантові обчислення та 5G, вимагають постійної адаптації нормативно-правової бази для усунення нових вразливостей. Відмінності в ресурсах і правових традиціях держав-членів призводять до непослідовного застосування стандартів кібербезпеки. Забезпечення наскрізної безпеки в усіх ланцюгах постачання створює додаткові труднощі для компаній. Міжнародний характер кіберзагроз вимагає узгодження з глобальними стандартами та співпраці з партнерами за межами ЄС для усунення нормативної асиметрії інформації. Встановлення балансу між суворими вимогами безпеки та сприянням інноваціям залишається ключовим регуляторним завданням.

Нормативна база ЄС щодо кібербезпеки спрямована на створення стійкої та надійної цифрової екосистеми. Звертаючи увагу на нові загрози та розширюючи сферу дії, ЄС прагне узгодити свої принципи конфіденційності, основних прав і гармонізації ринку з вимогами цифрової трансформації. Завдяки співпраці між державами-членами, зацікавленими сторонами приватного сектору та інституціями ЄС регуляторний підхід гарантує, що єдиний цифровий ринок залишається безпечним і надійним, приносячи користь усім громадянам і підприємствам ЄС.

Основоположним елементом цієї сукупності є оригінальна Директива про безпеку мережевих та інформаційних систем (Директива NIS), прийнята в 2016 році [6]. Будучи першим загальноєвропейським законом, присвяченим кібербезпеці, Директива NIS створила загальну основу для забезпечення безпеки основних соціальних послуг (енергетика, транспорт і охорона здоров'я) та для постачальників цифрових послуг. Директива передбачала низку обов'язкових змін у національному законодавстві країн-учасниць ЄС, що неминуче призвело до різної реалізації залежно від існуючої правової інфраструктури, адміністративних можливостей і стратегічних пріоритетів кожної країни. Директива вимагала створення груп реагування на інциденти комп'ютерної безпеки (CSIRT) і компетентних органів у кожній державі. Головною метою було підвищення рівня транскордонної співпраці та звітності про здійснені та потенційні кіберзагрози. Тим не менш, виникли розбіжності, зокрема щодо визначення «основних послуг» і порогів для повідомлення про інциденти безпеки. У результаті, незважаючи на основоположні досягнення Директиви, країни зіткнулися з нерівномірним навантаженням щодо дотримання та стандартами забезпечення виконання передбачених вимог.

Усвідомлюючи ці складнощі та швидку еволюцію кіберзагроз, у 2022 році ЄС запровадив вдосконалені підходи до кібербезпеки через Директиву NIS2. NIS2 розширює сферу дії, щоб охопити ширший спектр секторів, посилює вимоги до управління та встановлює більш суворі режими покарань для тих, хто не відповідний. З точки зору національного законодавства, розширення норм Директиви – охоплення державного управління та критичної цифрової інфраструктури на додаток до початкових основних послуг – посилило як адміністративну, так і фінансову відповідальність національних органів влади. Впровадження NIS2 зобов'язує держави-члени оновити або замінити своє існуюче законодавство, уточнити повноваження національних CSIRT та розширити канали співпраці для реагування на інциденти. Ініціативи в сторону більшої підзвітності та чітких зобов'язань щодо управління ризиками в ланцюзі постачання цифрових послуг демонструє спробу ЄС досягти вищого рівня гармонізації законодавства, хоча її кінцева ефективність залежить від узгодженості та чіткості національного впровадження.

Паралельно з Директивами NIS і NIS2 Закон про кібербезпеку 2019 року додав ще один рівень до регуляторної архітектури ЄС [11]. Будучи нормативним актом, Закон негайно набув чинності в усіх державах-членах, тим самим зменшуючи правову фрагментацію, яка зазвичай виникає, коли директиви передбачають лише рекомендації до законодавчих змін. Закон про кібербезпеку посилив роль Агентства Європейського Союзу з кібербезпеки (ENISA), надавши йому постійний мандат і розширивши обов'язки. Прийняття закону передбачало створення загальноєвропейської системи сертифікації кібербезпеки для продуктів, процесів і послуг ІКТ. Прямий вплив ENISA на держави-члени полягав у тому, щоб заохотити, а в деяких випадках і примусити національні органи з кібербезпеки активніше співпрацювати з Агентством у встановленні та підтримці стандартів сертифікації. Незважаючи на те, що сертифікація залишається добровільною для багатьох секторів, існує ймовірність того, що вимоги до сертифікації стануть обов'язковими в сферах високого ризику, що посилить обов'язковість відповідності як для національних регуляторів, так і для приватних організацій.

Іншим законодавчим заходом зі значними наслідками для кібербезпеки, хоча й не зосередженим виключно на цій сфері, є Загальний регламент захисту даних (GDPR). Встановлюючи жорсткі зобов'язання щодо безпеки даних, сповіщення про порушення та штрафні санкції за невідповідність, GDPR суттєво вплинув на те, як організації та регулятори реагують на ризики кібербезпеки. Держави-члени через свої

національні органи із захисту даних забезпечують виконання вимог GDPR у поєднанні з національними законами, що випливають із NIS або NIS2. Такий подвійний нагляд потенційно створює складнощі, оскільки суб'єктам ринку може знадобитися час, щоб орієнтуватися у зобов'язаннях щодо звітності, що збігаються та, відповідно, забезпечити заходи безпеки як захисту даних, так і цілям безпеки мережі. Незважаючи на це, розроблений та прийнятий графік сповіщення про порушення GDPR сприяв проактивному підходу в секторі кібербезпеки, підвищенню якості практик безпеки даних, а також послідовному звітуванню про кіберзагрози національним органам влади та органам ЄС.

Останнім доповненням до нормативно-правової системи ЄС щодо кібербезпеки є Закон про цифрову операційну стійкість (DORA) [5], який адаптований до фінансового сектору. Галузь фінансових послуг стала центром уваги для ЄС, враховуючи її системну важливість і вразливість до цілеспрямованих кібератак. DORA передбачає комплекс заходів для забезпечення безперервності фінансової діяльності у разі кіберзагроз, враховуючи оцінку ризиків, стрес-тестування та суворий нагляд за сторонніми постачальниками. Фінансові регулятори держав-членів, як наслідок, отримують розширені повноваження щодо нагляду як за місцевими, так і закордонними фінансовими установами. Негативним наслідком для суб'єктів є підвищення витрат, які виникають у зв'язку з законодавчими ініціативами. Така динаміка змін демонструє рух ЄС у бік більш детального та секторального регулювання, визнаючи, що загрози кібербезпеці для критично важливих економічних секторів потребують спеціалізованих регламентів, інструкцій та регулятивних механізмів.

Україна, прагнучи інтегруватися до європейського правового та політичного простору, стикається з низкою викликів у сфері кібербезпеки. Відповідно до вимог ЄС та практик його держав-членів, українське законодавство потребує наближення як у технічних аспектах (встановлення чітких стандартів безпеки, процедури інцидент-репортингу), так і в організаційній структурі (удосконалення координаційних органів, розподілу повноважень та відповідальності). Серед першочергових змін, які необхідні для гармонізації з європейською системою, можна виокремити кілька напрямів.

Перш за все вкрай важливо ухвалити чи оновити законодавчу базу, яка встановлює вимоги до операторів критичної інфраструктури, а також до компаній, що надають цифрові послуги. Директива ЄС щодо безпеки мереж і інформаційних систем (NIS/NIS2) передбачає обов'язкове визначення «операторів основних послуг» і «важливих суб'єктів». Для України це означає потребу внести зміни до вже існуючих законодавчих актів або підготувати нові, що чітко формалізують критерії, за якими обираються критичні об'єкти, та встановити для них вимоги з управління ризиками й реагування на інциденти. Без формалізації цих вимог у національному праві важко досягти єдиного підходу в масштабах усієї держави. Крім того, необхідно запровадити системи обов'язкового звітування про кіберінциденти. У країнах ЄС оператори essential services і digital service providers мають визначені строки та процедури інформування національних компетентних органів про інциденти, що можуть негативно впливати на безпеку надаваних послуг або на нормальну роботу критичної інфраструктури. Для України актуально розробити чіткий механізм, де буде вказано, хто й протягом якого часу зобов'язаний повідомляти про інциденти, як відбуватиметься їхня класифікація та які санкції застосовуватимуться в разі недотримання вимог. Такий підхід дасть змогу підвищити рівень прозорості та оперативності, з якими компанії і державні структури реагують на кібератаки.

Наступним важливим моментом є створення або посилення незалежного координаційного органу, відповідального за кібербезпеку на державному рівні. У контексті європейської інтеграції України потрібно забезпечити, аби цей орган мав чітко прописані функції щодо моніторингу, контролю, методичної підтримки й міжнародної взаємодії. У низці країн ЄС такими органами є національні CERT або спеціалізовані агентства, що підтримують зв'язок із ENISA (Агентство Європейського Союзу з кібербезпеки), а також беруть участь у спільних вправах і кризових координаційних ініціативах (наприклад, EU-CyCLONe). Участь України в подібних тренуваннях і обмін досвідом з європейськими інституціями допомагають інтегрувати національну систему кіберзахисту в загальноєвропейський механізм реагування.

Окремо варто наголосити на важливості запровадження системи сертифікації та стандартів кібербезпеки, сумісних з EU Cybersecurity Act. На рівні ЄС поступово формується підхід до добровільної чи обов'язкової сертифікації IT-продуктів і цифрових послуг. Для України доречно передбачити механізм, який у перспективі дозволить вітчизняним виробникам та постачальникам послуг отримувати європейські сертифікати і виходити на європейський ринок без додаткових бар'єрів. Водночас це підвищить конкурентоспроможність українських компаній та стимулюватиме їх покращувати рівень безпеки власної продукції.

Не менш суттєвою є сфера захисту персональних даних. Загальний регламент ЄС із захисту даних (GDPR), хоч і не є виключно кібербезпековим, однак вимагає дотримання високих стандартів захисту інформації. Україна вже робить кроки до наближення свого законодавства про персональні дані до європейських стандартів, але задля повноцінної інтеграції потрібно вдосконалити підходи до контролю, інцидент-менеджменту та штрафних санкцій за порушення. Це дасть змогу уникнути суперечностей між різними аспектами регулювання (наприклад, інцидент-репортинг у межах кібербезпеки та повідомлення про витік даних за нормами GDPR) і зробить систему більш цілісною.

Висновки та перспективи подальших досліджень. Підходи щодо інтеграції політики в галузі кібербезпеки, зокрема через Закон про цифрову операційну стійкість для фінансових послуг і Закон про цифрові послуги для онлайн-платформ, висвітлюють тенденцію до більш детального регулювання практики кібербезпеки. Вказані заходи можуть краще реагувати на унікальні профілі загроз, з якими стикаються різні галузі. Вони також відображають розуміння того, що фінансові ринки, системи охорони здоров'я та цифрові платформи мають особливу вразливість для потенційних загроз у цифровому середовищі. Незважаючи на те, що різні кола стейкхолдерів у галузі позитивно ставляться до таких законодавчих ініціатив, швидке поширення нових нормативно-правових актів – деяких у формі директив, а інших – у вигляді нормативних актів, викликає занепокоєння щодо дублювання або конфлікту вимог до звітності, особливо в ситуацій, коли кілька органів влади беруть участь у моніторингу відповідності. Нормативно-правова база ЄС у сфері кібербезпеки демонструє високий рівень комплексності, який є результатом синхронізації законодавчих ініціатив держав-членів з метою захисту єдиного цифрового ринку. Впровадження таких інструментів, як NIS2 та Cybersecurity Act, забезпечує підвищення рівня кібербезпеки, стимулюючи тісну співпрацю між урядами, приватним сектором та інституціями ЄС. Для України інтеграція в європейський правовий простір у цій сфері передбачає гармонізацію національного законодавства із європейськими стандартами. Пріоритетними завданнями є формування законодавчих вимог до операторів критичної інфраструктури, запровадження системи інцидент-репортингу, створення незалежного органу координації та впровадження сертифікаційних стандартів. Особливу увагу необхідно приділити розвитку професійної підготовки кадрів і зміцненню інституційної спроможності, що є основою для забезпечення ефективного функціонування системи кібербезпеки в умовах зростаючих цифрових викликів.

References:

1. Cerulus, L., «How Ukraine became a test bed for cyberweaponry», *POLITICO*, [Online], available at: https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/
2. *CSIRTs Network*, official website, [Online], available at : https://csirtsnetwork.eu/
3. «Cyber Resilience Act», *European Commission*, [Online], available at: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act
4. Bishoff, P., «Cybersecurity rankings by country: Worst & Best Countries Ranked. Comparitech», [Online], available at: https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/?fbclid=IwAR2vUYEilDvxl-ktT0WiZ0hRygCw-q0q19IGSnKay-UbVbRbprB5P7jSfDg
5. «Digital Operational Resilience Act "DORA"», [Online], available at: https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en
6. European Parliament And Of The Council (2016), *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*, [Online], available at : http://data.europa.eu/eli/dir/2016/1148/oj
7. European Parliament And Of The Council (2022), *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*, [Online], available at: http://data.europa.eu/eli/dir/2022/2555/2022-12-27
8. *EU CyCLONe. ENISA*, official website, [Online], available at: https://www.enisa.europa.eu/topics/eu-cyber-crisis-and-incident-management/eu-cyclone
9. Greenberg, A., «How an Entire Nation Became Russia's Test Lab for Cyberwar», *WIRED*, [Online], available at: https://www.wired.com/story/russian-hackers-attack-ukraine/
10. ENISA, «Policy Observatory», [Online], available at: https://www.enisa.europa.eu/topics/state-of-cybersecurity-in-the-eu/cybersecurity-policies/policy-observatory
11. European Parliament And Of The Council (2019), *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No. 526/2013 (Cybersecurity Act)*, [Online], available at: http://data.europa.eu/eli/reg/2019/881/oj
12. Semeniy, J., Glushchenko, S. and Makarevich, O. (2018), «Getting the Deal Through», *Cybersecurity*, [Online], available at: https://www.asterslaw.com/press_center/publications/getting_the_deal_through_cybersecurity_2018_ukraine/
13. Streltsov, L. (2017), «The System of Cybersecurity in Ukraine: Principles, Actors, Challenges, Accomplishments», *Eur. J. Secur. Res.*, No. 2, pp. 147–184, doi: 10.1007/s41125-017-0020-x.
14. *The Digital Markets Act*, official website, [Online], available at: https://digital-markets-act.ec.europa.eu/index_en
15. *The Digital Services Act*, official website, [Online], available at: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en
16. «Zahalnyi rehlament pro zakhyst danykh», *GDPR*, [Online], available at : https://gdpr-text.com/uk/

Савчук Сергій Олександрович – здобувач кафедри національної безпеки, публічного управління та адміністрування Державного університету «Житомирська політехніка».

https://orcid.org/0009-0007-7436-0702.

Наукові інтереси:

– державна політика протидії кіберзлочинності.

E-mail: savcukserij4@gmail.com.

Savchuk S.O.

Challenges of EU legislation harmonization in the field of cyber security for Ukraine

The article examines the European Union's regulatory framework in the cyber security field, analyzing the key regulations and directives governing the protection of digital infrastructure, networks, and information systems. Particular attention is paid to the NIS and NIS2 directives, the Cybersecurity Act, the General Data Protection Regulation (GDPR), and the Digital Operational Resilience Act (DORA). The study highlights the importance of legal harmonization to ensure the unity of the digital market, strengthen user trust, and stimulate innovation. The article defines the need for Ukraine's integration into the European cyber security system, which involves the adoption of adequate legislation adapted to European standards, particularly regarding risk management, incident reporting, and personal data protection. An important integration component is creating an independent coordinating body that ensures monitoring, response, and international cooperation. The article also emphasizes the importance of certification of IT products and digital services following the requirements of the Cybersecurity Act, which will allow Ukrainian companies to integrate into the European market. The need to develop Ukraine's institutional capacity, attract qualified personnel, and increase the awareness of public and private sector managers in cyber security issues was emphasized. The study results indicate the need for close coordination between all stakeholders, including government agencies, the private sector, and international partners, to create a sustainable cybersecurity system in Ukraine. The proposed recommendations can serve as a basis for further harmonization of legislation, strengthening institutional capacity, and adaptation to the requirements of the European digital market.

Keywords: public administration; integration; cyber threats; cyber security; critical infrastructure; certification.

Стаття надійшла до редакції 31.01.2024.