УДК 338.24:004(477)
DOI https://doi.org/10.24144/2788-6018.2026.02.2.40

КОМПЛАЄНС ЯК ЕЛЕМЕНТ КОРПОРАТИВНОГО УПРАВЛІННЯ В ІТ-СЕКТОРІ УКРАЇНИ: ЄВРОІНТЕГРАЦІЙНИЙ КУРС

Теличко О.А.,
кандидатка юридичних наук, доцент,
завідувачка кафедри права,
Державний університет економіки і технологій
ORCID: 0000-0003-2536-7442

Рекун В.А.,
доцент, кандидат юридичних наук,
доцент кафедри права,
Державний університет економіки і технологій
ORCID: 0000-0002-2636-9426

Теличко О.А., Рекун В.А. Комплаєнс як елемент корпоративного управління в ІТ-секторі України: євроінтеграційний курс.

У статті досліджується комплаєнс як структурний елемент системи корпоративного управління в ІТ-секторі України в умовах євроінтеграційного курсу держави. Обґрунтовано, що в цифровому середовищі комплаєнс трансформується з інструмента формального дотримання вимог у стратегічний механізм управління ризиками, забезпечення прозорості та підвищення інвестиційної привабливості компаній. Визначено галузеву специфіку комплаєнс-систем ІТ-компаній, зумовлену транскордонністю діяльності, обробкою чутливих даних і швидким технологічним розвитком, що випереджає нормотворчі процеси.

Встановлено, що станом на початок 2026 року ЄС сформував цілісну архітектуру цифрового регулювання, яка охоплює режими, обов'язкові для українських ІТ-компаній та проаналізовано вплив ключових актів цифрового права Європейського Союзу – GDPR, Директиви NIS 2, AI Act та Cyber Resilience Act – на формування нових стандартів корпоративної відповідальності українських ІТ-компаній, з урахуванням їх екстериторіальної дії. Виявлено ключові перешкоди розвитку комплаєнсу в ІТ-секторі: нормативну фрагментарність, кадровий дефіцит DPO– та CCO-фахівців, сприйняття комплаєнсу як витратного елементу, складність адаптації до динамічного регуляторного середовища ЄС та відсутність цілісної державної політики стимулювання систем відповідності.

Окрему увагу приділено гармонізації національного законодавства з цифровим acquis ЄС, зокрема реформуванню сфери захисту персональних даних, посиленню інституційної спроможності наглядових органів та запровадженню фінансових механізмів підтримки комплаєнс-інфраструктури малого і середнього ІТ-бізнесу. Запропоновано комплекс заходів приведення комплаєнс-стандартів вітчизняного ІТ-сектору у відповідність до євроінтеграційних вимог на нормативному, фінансово-стимулюючому, інституційному та корпоративному рівнях. Зроблено висновок, що відповідність цифровому acquis ЄС є не лише юридичним обов'язком, а ключовою передумовою збереження доступу українських ІТ-компаній до ринку ЄС, а комплаєнс набуває стратегічного значення для їх конкурентоспроможності.

Ключові слова: комплаєнс, корпоративне управління, ІТ-сектор, євроінтеграція, захист персональних даних, кібербезпека, цифровий комплаєнс, управління ризиками, єдиний цифровий ринок ЄС.

Telichko O.A., Rekun V.A. Compliance as an element of corporate governance in Ukraine's IT sector: the EU integration course.

The article examines compliance as a structural element of the corporate governance system in the IT sector of Ukraine in the context of the country's European integration course. It is substantiated that in the digital environment, compliance is transformed from a tool for formal compliance into a strategic mechanism for risk management, ensuring transparency and increasing the investment attractiveness of companies. The industry-specific nature of compliance systems of IT companies is determined, due to cross-border activities, processing of sensitive data and rapid technological development that is ahead of regulatory processes. It is established that as of the beginning of 2026, the EU has formed a

holistic architecture of digital regulation, which covers regimes mandatory for Ukrainian IT companies, and the impact of key acts of digital law of the European Union – GDPR, NIS 2 Directive, AI Act and Cyber Resilience Act – on the formation of new standards of corporate responsibility of Ukrainian IT companies, taking into account their extraterritorial effect, is analyzed. Key obstacles to the development of compliance in the IT sector were identified: regulatory fragmentation, staff shortage of DPO and CCO specialists, perception of compliance as a cost element, difficulty in adapting to the dynamic EU regulatory environment and the lack of a coherent state policy to stimulate compliance systems.

Particular attention was paid to the harmonization of national legislation with the EU digital acquis, in particular, to the reform of the sphere of personal data protection, strengthening the institutional capacity of supervisory authorities and introducing financial mechanisms to support the compliance infrastructure of small and medium-sized IT businesses. A set of measures was proposed to bring the compliance standards of the domestic IT sector into line with European integration requirements at the regulatory, financial-stimulating, institutional and corporate levels. It is concluded that compliance with the EU digital acquis is not only a legal obligation, but a key prerequisite for maintaining access of Ukrainian IT companies to the EU market, and compliance is of strategic importance for their competitiveness.

Key words*:* compliance, corporate governance, IT sector, European integration, personal data protection, cybersecurity, digital compliance, risk management, single EU digital market.

Постановка проблеми. Інтеграція України до Європейського Союзу формує принципово нові стандарти корпоративного управління у всіх секторах національної економіки. Особливої ваги ці трансформаційні процеси набувають для ІТ-галузі як стратегічно важливого, експортно орієнтованого та технологічно динамічного сегмента. За даними Національного банку України [1] та Львівського ІТ кластеру, у 2025 році обсяг експорту ІТ-послуг склав $6,656 млрд (+3,3% порівняно з 2024 роком). Незважаючи на виклики, спричинені воєнним станом, ІТ-сектор зберігає позицію провідного експортера послуг в Україні, а ІТ-індустрія продовжує відігравати стратегічну роль у формуванні валютних надходжень до національної економіки [2].

Водночас, ІТ-сектор функціонує в умовах посилених міжнародних вимог у сферах захисту персональних даних, кібербезпеки та фінансової прозорості, тоді як значна частина компаній, особливо МСП, не має системних комплаєнс-програм, що знижує їхню конкурентоспроможність на ринку ЄС. Також поняття «комплаєнс» залишається фрагментарно імплементованим у законодавство та часто зводиться до формального дотримання норм, що ускладнює його практичне застосування й теоретичне осмислення. У контексті євроінтеграції комплаєнс стає не лише управлінським інструментом, а необхідною передумовою інтеграції українських ІТ-компаній до єдиного цифрового ринку.

Метою статті є аналіз комплаєнсу як елемента корпоративного управління в ІТ-секторі України, дослідження відповідних вимог законодавства ЄС та визначення напрямів приведення комплаєнс-стандартів вітчизняного ІТ-сектору у відповідність до євроінтеграційних стандартів корпоративного управління.

Стан опрацювання проблематики. Проблематика комплаєнсу як елементу корпоративного управління активно досліджується у зарубіжній літературі: комплаєнс у системі ризик-менеджменту та його вплив на якість корпоративного управління (R. Burby, P. May, R. Paterson [3], I. Avianti, S. Handoyo [4], J. Koffer, D. Hemminger [7]); кібер-комплаєнс (E. Pérez Carrillo); комплаєнс в ракурсі режиму обміну даними та приватності (E. Coche, A. Kolk, M. Dekker); AI-governance як основа регуляторного комплаєнсу (F. Burns, J. Edelberg, P. Kuivanen, E. Tuomi) тощо. Серед українських авторів, які досліджують проблематику комплаєнсу та регуляторного середовища в ІТ-сфері, слід виокремити: податковий комплаєнс (О. Деменко, Є. Козлов, О. Осаволюк); регуляторний комплаєнс (В. Білошапка, Л. Калініченко, І. Охрименко); євроінтеграційний та цифровий комплаєнс (О. Маковоз, І. Маринюк, Ф. Ткачик) тощо.

Нормативну базу дослідження формують первинні акти цифрового права ЄС – GDPR [10], Директива NIS2 [11], AI Act [13], Акт про кіберстійкість [21-23] аналітичні огляди їх застосування [14; 29-30], а також національне законодавство України [18; 21-23; 28].

Таким чином, попри активний розвиток суміжних напрямів, дослідження комплаєнсу як стратегічного елементу корпоративного управління в ІТ-секторі України, з урахуванням одночасного впливу євроінтеграційних зобов'язань, регуляторного перетину GDPR, NIS2, AI Act і CRA та специфіки функціонування галузі в умовах воєнного стану, залишається недостатньо розробленим як у зарубіжній так і у вітчизняній науці. Це обумовлює актуальність, теоретичну та практичну значущість пропонованого дослідження.

Виклад основного матеріалу. Термін «комплаєнс» (від англ. compliance – відповідність, дотримання) увійшов у юридичний і бізнес-дискурс у 1970-х роках у практиці федеральних регу-

ляторних органів США, де первісно означав забезпечення дотримання конкретного регуляторного режиму. Американські дослідники R. Burby, P. May, R. Paterson трактують комплаєнс «…як виконання економічними суб'єктами вимог, встановлених законодавчими органами» [3, p. 326], їхня інтерпретація акцентує увагу на важливості правової відповідності в діяльності компаній. I. Avianti та S. Handoyo істотно розширюють його зміст та підкреслюють, що «…комплаєнс – це не просто дотримання правил, він охоплює сприяння культурі етичної поведінки, дотримання правових норм та корпоративної відповідальності, що включає такі види діяльності, як розробка внутрішньої політики, навчання співробітників, аудит та звітність для запобігання неправомірним діям та сприяння прозорості» [4, p. 6], наголошуючи на тому, що комплаєнс трансформувався з механізму формальної відповідності у стратегічний елемент корпоративного управління. Відповідно до стандарту ISO 37301:2021 система управління відповідністю визначається як сукупність взаємопов'язаних елементів організації, що встановлюють і забезпечують виконання зобов'язань щодо комплаєнсу [5]. У межах доктрини корпоративного управління, заснованої на Принципах ОЕСР [5], комплаєнс розглядається як інструмент підзвітності, прозорості та управління ризиками і виступає складовою системи risk management, спрямованої на превентивне виявлення та мінімізацію правових, фінансових і репутаційних ризиків [7, p. 137].

У системі корпоративного управління ІТ-компаній комплаєнс виконує три ключові функції: превентивну (виявлення та нейтралізація регуляторних ризиків до настання порушення), захисну (мінімізація юридичної, фінансової та репутаційної відповідальності у разі інцидентів) та стратегічну (позиціонування відповідності регуляторним вимогам як конкурентної переваги на міжнародних ринках) [8].

Галузева специфіка ІТ-сектору зумовлює підвищену складність комплаєнс-систем. Діяльність ІТ-компаній має транскордонний характер і передбачає взаємодію з різними юрисдикціями та регуляторними режимами; індустрія оперує високочутливими даними, що підсилює вимоги до захисту персональної інформації та кібербезпеки; водночас темпи технологічного розвитку випереджають нормотворчі процеси, формуючи зони регуляторної невизначеності, зокрема у сфері штучного інтелекту та інших цифрових технологій. Багаторівнева регуляторна архітектура ЄС зумовлює необхідність формування в ІТ-компаніях інтегрованих систем управління відповідністю, що охоплюють усі застосовні режими цифрового регулювання.

Євроінтеграційний курс України суттєво трансформує нормативне середовище функціонування ІТ-бізнесу: станом на початок 2026 року в ЄС ухвалено понад 100 актів у сфері цифровізації [9], що формують цілісну систему цифрового регулювання. Ключове значення для українських ІТ-компаній мають:

1. Загальний регламент захисту даних (GDPR, Regulation (EU) 2016/679) [10] залишається наріжним каменем цифрового комплаєнсу. Його екстериторіальний принцип означає, що будь-яка українська ІТ-компанія, яка обробляє дані резидентів ЄС – незалежно від місця реєстрації – підпадає під дію регламенту. Регламент встановлює суворі вимоги до: отримання згоди на обробку даних; права суб'єктів даних; призначення відповідального за захист даних (DPO); повідомлення про витоки даних протягом 72 годин; транскордонної передачі даних.

2. Директива NIS 2 (Directive (EU) 2022/2555) [11] суттєво розширила коло суб'єктів, на яких поширюються вимоги кібербезпеки. Директива розрізняє «суттєві суб'єкти» (*essential entities*) та «важливі суб'єкти» (*important entities*), до яких належить широке коло постачальників хмарних послуг, керованих ІТ-послуг (*managed services*) і цифрової інфраструктури. Для українських ІТ-компаній принципово важливим є екстериторіальний ефект NIS 2: суб'єкт, що не є резидентом ЄС, підпадає під дію директиви, якщо надає послуги на території ЄС, а компанія, не зареєстрована в ЄС, зобов'язана призначити представника в одній із держав-членів, де надаються послуги; така компанія підпадає під юрисдикцію держави-члена, де перебуває її представник, а за відсутності останнього – будь-яка держава-член, на території якої надаються послуги, має право вжити правових заходів проти порушника [12]. Директива зобов'язує охоплені суб'єкти впровадити мінімальний перелік із десяти заходів управління ризиками кібербезпеки, включаючи процедури реагування на інциденти та механізми безпеки ланцюга постачання (*supply chain security*) [11]. Значні вимоги встановлено щодо управлінських органів компаній: члени правління зобов'язані затверджувати заходи кібербезпеки, проходити регулярне навчання та можуть нести особисту відповідальність за порушення вимог директиви, включно з тимчасовою забороною виконання управлінських функцій у разі грубої недбалості; поширення такого навчання на ширше коло працівників компанії є рекомендованим [12].

3. Закон ЄС про штучний інтелект (AI Act, Regulation (EU) 2024/1689) [13] – набирає чинності поетапно (2024-2027) [14]. Для українських ІТ-компаній, що розробляють або постачають рішення ШІ для ринку ЄС, AI Act формує принципово новий комплаєнс-ландшафт: обов'язкова класифіка-

ція систем ШІ за рівнем ризику, оцінки відповідності (*conformity assessment*), технічна документація, системи постринкового моніторингу та механізми людського нагляду (*human oversight*). Слід зазначити, що AI Act поширюється на будь-яку систему ШІ, розміщену на ринку ЄС або результати якої досягають користувачів в ЄС, – незалежно від юрисдикції реєстрації розробника, що робить його вимоги обов'язковими для всіх українських компаній із ЄС-клієнтами.

4. Акт про кіберстійкість (Cyber Resilience Act, Regulation (EU) 2024/2847) [15] набрав чинності 10 грудня 2024 року і має принципове значення для українських ІТ-компаній, що постачають програмні або апаратні продукти на ринок ЄС. Він застосовується до виробників, імпортерів і дистриб'юторів продуктів із цифровими елементами, незалежно від реєстрації. Вимоги: «security by design» і «security by default», повідомлення ENISA про уразливості протягом 24 годин (з 11 вересня 2026), повний обсяг обов'язків – з 11 грудня 2027. Важливі продукти включають менеджери паролів, системи управління мережами та ОС [16]. Таким чином, для українських ІТ-компаній CRA формує не лише нові комплаєнс-зобов'язання, а й конкурентну передумову для збереження доступу до ринку ЄС після грудня 2027 року.

Наведені регуляторні режими утворюють взаємопов'язану архітектуру цифрового комплаєнсу, де порушення вимог будь-якого з них може одночасно тягнути відповідальність за кількома режимами – зокрема, інцидент кібербезпеки за NIS2 може одночасно кваліфікуватися як витік персональних даних за GDPR, а вразливість у продукті з елементами ШІ – як порушення одночасно CRA та AI Act. Саме тому ізольований підхід до забезпечення відповідності кожному з режимів є недостатнім: ІТ-компанії потребують інтегрованої комплаєнс-системи, що охоплює всі чотири режими у єдиній операційній моделі.

Серед ключових перешкод розвитку комплаєнсу в ІТ-секторі можна виокремити: нормативну фрагментарність, кадровий дефіцит спеціалізованих фахівців, сприйняття комплаєнсу як витратного елементу, складність адаптації до динамічного регуляторного середовища ЄС та обмеженість державних стимулів. Останній чинник заслуговує окремої аналітичної уваги, оскільки він характеризує системну прогалину у взаємодії держави та приватного сектору в питаннях регуляторної відповідності.

На відміну від більшості держав-членів ЄС, де розвиток комплаєнс-інфраструктури малого і середнього бізнесу підтримується спеціалізованими фінансовими інструментами, в Україні відсутня комплексна та системна державна політика цільового стимулювання впровадження систем відповідності в ІТ-галузі. На рівні ЄС програма «Цифрова Європа» [17] у 2025-2026 роках передбачає співфінансування цифрових і кібербезпекових проєктів МСП (у межах 50–75% вартості залежно від напряму фінансування), включаючи ініціативи, спрямовані на підвищення відповідності вимогам NIS 2 та CRA. Україна є асоційованою учасницею програми з вересня 2022 року та має право брати участь у більшості відкритих конкурсів. Водночас частина кібербезпекових конкурсів має обмежений режим участі з огляду на міркування стратегічної безпеки, що зменшує можливості українських компаній щодо отримання фінансування за окремими напрямами, найбільш релевантними для розбудови комплаєнс-інфраструктури. На національному рівні певним винятком є спеціальний правовий режим «Дія.City», запроваджений Законом України «Про стимулювання розвитку цифрової економіки в Україні» [18]. Попри зниження податкового навантаження на ІТ-бізнес і зростання кількості резидентів (станом на початок лютого 2026 року – 3 707 компаній [19]), режим не передбачає цільових механізмів стимулювання інвестицій у комплаєнс-інфраструктуру – зокрема податкових преференцій для витрат на сертифікацію за стандартами ISO/IEC 27001 чи ISO 37301, підготовку DPO-фахівців або проведення оцінок впливу на захист даних (DPIA).

Таким чином, державна цифрова політика України залишається переважно орієнтованою на фіскальні стимули розвитку галузі без прямого пов'язання податкових інструментів із досягненням конкретних комплаєнс-показників, що зумовлює потребу у формуванні більш цілісної моделі підтримки регуляторної відповідності ІТ-сектору.

З метою приведення комплаєнс-стандартів вітчизняного ІТ-сектору у відповідність до євроінтеграційних вимог необхідним є комплекс взаємопов'язаних заходів:

1. На нормативному рівні. Відповідно до статті 15 Угоди про асоціацію між Україною та ЄС Україна взяла на себе зобов'язання забезпечити належний рівень захисту персональних даних відповідно до найвищих європейських та міжнародних стандартів [20], що на практиці означає гармонізацію з GDPR. Законопроєкт № 8153 «Про захист персональних даних», прийнятий Верховною Радою за основу в першому читанні 20 листопада 2024 року, передбачає імплементацію фундаментальних принципів GDPR – включно з обов'язковим повідомленням про порушення, оцінкою впливу на захист даних і суттєво підвищеними санкціями за невідповідність [21]. Важливим елементом реформи є створення незалежного спеціалізованого наглядового органу у сфері захисту персональних даних до 2027 року. Чинна модель, за якої відповідні функції здійснює Уповноважений Верховної

Ради України з прав людини, потребує інституційної трансформації для повної відповідності вимогам ст. 51–52 GDPR щодо функціональної та організаційної незалежності наглядового органу [10]. Паралельно триває гармонізація суміжного цифрового законодавства: Закон «Про електронні комунікації» адаптує європейські технічні та процедурні стандарти [22], Закон «Про цифровий контент та цифрові послуги» імплементує директиви ЄС щодо захисту споживачів [23]. В межах переговорів про вступ до ЄС розглядається імплементація Digital Services Act та Digital Markets Act [24]. Звіт Європейської Комісії 2025 року відзначив прогрес у сфері інтелектуальної власності та підготовці до єдиного цифрового ринку, але рекомендує ухвалити новий закон про персональні дані та створити незалежний наглядовий орган, що критично для комплаєнсу IT-компаній [25].

2. На рівні державних фінансових стимулів. Враховуючи наявну прогалину у вітчизняній цифровій політиці, доцільним є запровадження цілеспрямованих механізмів підтримки витрат IT-компаній на впровадження комплаєнс-систем. Зокрема, в межах інструментів підтримки малого і середнього підприємництва у цифровому секторі доцільно розробити програму часткового відшкодування витрат МСП на: первинне впровадження систем управління відповідністю (ISO 37301) та інформаційної безпеки (ISO/IEC 27001); проведення незалежних комплаєнс-аудитів; підготовку DPO-фахівців; здійснення оцінок впливу на захист даних (DPIA). Фінансування таких програм може здійснюватися через поєднання національного бюджету та доступних інструментів ЄС – зокрема, грантів програми «Цифрова Європа» за напрямами, відкритими для України як асоційованого учасника, а також у рамках механізму TAIEX [26], який доцільно використовувати для підвищення інституційної спроможності державних органів та наглядових структур у сфері захисту персональних даних і кібербезпеки, оскільки його мандат спрямований на підтримку гармонізації законодавства та професійної підготовки регуляторів, а не на пряме фінансування бізнесу. Додатковим інструментом стимулювання може стати запровадження податкових преференцій для витрат підприємств на сертифікацію та аудит комплаєнсу – за аналогією з механізмами податкового стимулювання витрат на науково-дослідні та дослідно-конструкторські роботи (НДДКР), які широко застосовуються в державах-членах ЄС [27]. Такий підхід дозволив би поєднати фіскальну політику з досягненням конкретних регуляторних результатів у сфері цифрової безпеки та комплаєнсу.

Критично важливим є формування координаційної платформи між Міністерством цифрової трансформації України, Уповноваженим Верховної Ради України з прав людини, Асоціацією IT Ukraine та провідними IT-підприємствами з метою: розробки єдиної методології оцінки комплаєнс-зрілості; стандартизації вимог до корпоративних комплаєнс-систем у контексті євроінтеграції; підготовки типових внутрішніх політик і процедур для МСП IT-сектору, адаптованих до вимог GDPR, NIS 2 та AI Act. Інституційні передумови для такої взаємодії поступово формуються. Зокрема, Стратегія цифрового розвитку інноваційної діяльності України до 2030 року, розроблена з ініціативи Міністерства цифрової трансформації у співпраці з Міністерством освіти і науки та Офісом ефективного регулювання (BRDO) за підтримки Проєкту USAID «Кібербезпека критично важливої інфраструктури України», визначає розвиток безпечного кіберпростору одним із пріоритетних напрямів та передбачає міжвідомчу координацію як ключовий інструмент реалізації цифрових реформ [28]. Водночас участь України як асоційованого члена у програмі «Цифрова Європа» створює інституційні можливості для розвитку моделей публічно-приватної взаємодії між державними органами, галузевими асоціаціями та бізнесом на рівні ЄС [17]. Аналогічна модель узгодженої координації доцільно має бути поширена на сферу комплаєнс-підтримки IT-сектору, де наразі відсутні системні механізми стратегічного узгодження регуляторної політики та практики її імплементації.

3. На корпоративному рівні ефективна комплаєнс-система IT-компанії має включати: призначення DPO (для компаній, що обробляють дані резидентів ЄС у великому масштабі або спеціальні категорії даних, ст. 37 GDPR та законопроєкт № 8153) [10; 21] та офіцера з комплаєнсу (CCO); розробку та оновлення внутрішніх політик і процедур; навчання персоналу; технічні та організаційні заходи захисту даних за принципами privacy by design та privacy by default; регулярні комплаєнс-аудити та оцінку ризиків; ефективні канали повідомлення про порушення (whistleblowing).

Системна відповідь на кадровий дефіцит у сфері комплаєнсу передбачає формування спеціалізованих освітніх програм для підготовки DPO-, CCO– та compliance-фахівців у профільних закладах вищої освіти та на базі галузевих асоціацій. Важливим є включення до навчальних планів з юриспруденції, кібербезпеки та менеджменту дисциплін із цифрового права ЄС, управління відповідністю та корпоративної етики, а також розвиток механізмів визнання міжнародних сертифікацій (CIPP/E, CIPM, CIPT від IAPP; CCEP від SCCE) на національному рівні [29].

Одночасна дія кількох регуляторних режимів (GDPR, NIS 2, AI Act, CRA) потребує єдиної системи комплаєнс-моніторингу. Доцільно запровадити реєстр комплаєнс-зобов'язань, який консолідує вимоги, строки, відповідальних та статус виконання. У цьому контексті обговорювана на рівні Європейської Комісії ініціатива Digital Omnibus (2025 р.) спрямована на можливу гармонізацію

процедур звітування про інциденти в межах різних цифрових регламентів, зокрема через координаційні механізми за участю ENISA, а також розглядає питання оптимізації строків повідомлення про порушення [30], що вже вимагає стратегічного перегляду внутрішніх процедур реагування на інциденти в ІТ-компаніях.

Висновки. Проведене дослідження дозволяє сформулювати такі висновки.

По-перше, комплаєнс виступає системним елементом корпоративного управління ІТ-компаній, що забезпечує їх правову відповідність, мінімізує регуляторні ризики та сприяє формуванню довіри з боку клієнтів, інвесторів і партнерів. В умовах цифрової трансформації та євроінтеграції комплаєнс набуває стратегічного значення як фактор довгострокової конкурентоспроможності вітчизняних технологічних підприємств.

По-друге, євроінтеграційний курс України формує нову регуляторну архітектуру вимог до діяльності ІТ-компаній. Положення GDPR підлягають застосуванню до українських компаній у випадках, передбачених ст. 3 цього Регламенту, зокрема якщо вони пропонують товари або послуги особам, які перебувають на території ЄС, або здійснюють моніторинг їхньої поведінки. Директива NIS 2 та Регламент про штучний інтелект (AI Act) встановлюють додаткові стандарти кібербезпеки та ризик-орієнтованого регулювання технологічних рішень. Невідповідність цим вимогам може призвести не лише до юридичних санкцій, але й до обмеження доступу до внутрішнього ринку ЄС.

По-третє, аналіз свідчить про наявність структурних викликів у формуванні комплаєнс-культури в українському ІТ-секторі: для значної частини малих і середніх компаній характерною залишається відсутність формалізованих систем управління відповідністю. Подолання цього розриву потребує комплексного підходу, що поєднує нормативний рівень (гармонізація з acquis ЄС), інституційний рівень (посилення спроможності наглядових органів) та корпоративний рівень (інтеграція комплаєнсу у стратегічне управління компанією).

СПИСОК ВИКРИСТАНИХ ДЖЕРЕЛ:

1. Зовнішня торгівля товарами (відповідно до КПБ6). *Національний Банк України*. URL: https://bank.gov.ua/files/ES/Trade_m.pdf.
2. Поступова стабілізація ринку: яким був експорт ІТ-послуг у 2025 році. *Lviv IT Cluster*. URL: https://itcluster.lviv.ua/postupova-stabilizacziya-rynku-yakym-buv-eksport-it-poslug-u-2025-roczi/.
3. Burby R., May P., Paterson R. Improving Compliance with Regulations: Choices and Outcomes for Local Government. Journal of The American Planning Association. 1998. Volume 64. Issue 3. Pp. 324-334. DOI:10.1080/01944369808975989.
4. Avianti I., Handoyo S. A bibliometric analysis of governance, risk, and compliance (GRC): trends, themes, and future directions. *Humanities and Social Sciences Communications.* 2025. № 1945. Pp. 1-17. DOI; https://doi.org/10.1057/s41599-025-06194-9.
5. ISO 37301:2021. Compliance management systems – Requirements with guidance for use. Geneva: International Organization for Standardization, 2021. 48 с.
6. OECD Principles of Corporate Governance. Paris: OECD Publishing, 2023. URL: https://www.oecd.org/corporate/principles-corporate-governance.htm.
7. Koffer J., Hemminger D. Corporate Compliance Management: Legal and Organizational Frameworks. New York: Wolters Kluwer, 2020. 412 с.
8. 130+ Compliance Statistics & Trends to Know for 2026. *SecureFrame*. 2025. URL: https://secureframe.com/blog/compliance-statistics.
9. EU Digital Laws Report 2025. *IAPP*. 25 Sept. 2025. URL: https://iapp.org/resources/article/eu-digital-laws-report.
10. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). *EUR-Lex*. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng.
11. 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) № 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance). *EUR-Lex*. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27/eng.
12. Bensinger V., Kociok C. 5 Trends to Watch: 2025 EU Data Privacy & Cybersecurity. *The National Law Review*. 2025. Vol. 16. № 57. URL: https://natlawreview.com/article/5-trends-watch-2025-eu-data-privacy-cybersecurity.
13. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) № 300/2008,

(EU) № 167/2013, (EU) № 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance). *EUR-Lex*. URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng.
14. Hickman T., Hoffmann E., Teetzmann C., Helle K., Kirch F. EU Digital Omnibus: What changes lie ahead for the Data Act, GDPR and AI Act. *White & Case*. 05 December 2025. URL: https://www.whitecase.com/insight-alert/eu-digital-omnibus-what-changes-lie-ahead-data-act-gdpr-and-ai-act.
15. Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (Text with EEA relevance). *EUR-Lex*. URL: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng.
16. Commission Implementing Regulation (EU) 2025/2392 of 28 November 2025 on the technical description of the categories of important and critical products with digital elements pursuant to Regulation (EU) 2024/2847 of the European Parliament and of the Council. *EUR-Lex*. URL: https://eur-lex.europa.eu/eli/reg_impl/2025/2392/oj/eng.
17. The Digital Europe Programme. *Shaping Europe's digital future*. URL: https://digital-strategy.ec.europa.eu/en/activities/digital-programme.
18. Про стимулювання розвитку цифрової економіки в Україні Закон України від 15.07.2021 № 1667-IX. URL: https://zakon.rada.gov.ua/laws/show/1667-20.
19. Дія.City – офіційний сайт. URL: https://city.diia.gov.ua.
20. Draft Law of Ukraine on Personal Data Protection. *Secure Privacy*. 2022. URL: https://secureprivacy.ai/blog/draft-law-of-ukraine-on-data-protection.
21. Про прийняття за основу проекту Закону України про захист персональних даних: Постанова Верховної Ради України від 20.11.2024 № 4065-IX. *Верховна Рада України*. URL: https://zakon.rada.gov.ua/laws/show/4065-20#Text.
22. Про електронні комунікації: Закон України від 16.12.2020 року № 1089-IX. *Верховна Рада України*. URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text.
23. Про цифровий контент та цифрові послуги : Закон України від 10.08.2023 року № 3321-IX. *Верховна Рада України*. URL: https://zakon.rada.gov.ua/laws/show/3321-20#Text.
24. Україна пройшла черговий етап скринінгу відповідності законодавства нормам ЄС за розділом 10 «Цифрова трансформація та медіа». *Комітет з питань гуманітарної та інформаційної політики*. 02 квітня 2025. URL: https://kompkd.rada.gov.ua/print/76666.html? utm_source.
25. Ukraine 2025 Report. 2025 Communication on EU enlargement policy. *European Commission*. Brussels. 04.11.2025. URL: https://enlargement.ec.europa.eu/document /download/17115494-8122-4d10-8a06-2cf275eecde7_en?filename=ukraine-report-2025.pdf.
26. European Commission. TAIEX – Technical Assistance and Information Exchange instrument. URL: https://neighbourhood-enlargement.ec.europa.eu/taiex_en.
27. OECD. R&D Tax Incentives: Design, Scope and Evaluation. OECD Publishing, 2024. URL: https://www.oecd.org/en/topics/sub-issues/rd-tax-incentives.html.
28. Про схвалення Стратегії цифрового розвитку інноваційної діяльності України на період до 2030 року та затвердження операційного плану заходів з її реалізації у 2025-2027 роках: Розпорядження КМУ від 31 грудня 2024 р. № 1351-р. *Кабінет Міністрів України*. URL: https://zakon.rada.gov.ua/laws/show/1351-2024-%D1%80#Text.
29. Privacy Certification Programs. *IAPP*. URL: https://iapp.org/certify.
30. EU Digital Omnibus: How EU Data, Cyber, and AI Rules Will Shift. *Jones Day*. December 2025. URL: https://www.jonesday.com/en/insights/2025/12/eu-digital-omnibus-how-eu-data-cyber-and-ai-rules-will-shift.

Дата першого надходження рукопису до видання: 1.03.2026
Дата прийняття до друку рукопису після рецензування: 20.03.2026
Дата публікації: 3.04.2026