https://doi.org/10.31891/2219-9365-2025-83-3
УДК 316.776:004.58

ВОЙТОВИЧ Олеся
Вінницький національний технічний університет
https://orcid.org/0000-0001-8964-7000
voytovych.olesya@vntu.edu.ua
ВОЛИНЕЦЬ Віталій
Вінницький національний технічний університет
https://orcid.org/0009-0006-7999-1290
volynets1026@gmail.com

ОСОБЛИВОСТІ ЗАКОНОДАВСТВА ЩОДО АУДИТУ КІБЕРБЕЗПЕКИ В РІЗНИХ РЕГІОНАХ СВІТУ

Стаття присвячена порівняльному аналізу нормативних вимог з аудиту кібербезпеки в ключових регіонах світу в умовах глобальної цифрової трансформації. Дослідження систематизує та зіставляє регуляторні підходи в Європейському Союзі, Північній Америці, Азії та Африці, з особливим акцентом на вимоги до фінансового сектору. Регіональний аналіз виявив кардинальні відмінності у підходах: від жорстко регламентованого та централізованого в ЄС (GDPR, NIS2) до гнучкого, керованого ринковими практиками в США (NIST CSF, SOC 2), неоднорідного в Азії з елементами жорсткого державного контролю (китайський MLPS 2.0) та фрагментованого в Африці, де неефективні панафриканські ініціативи поступаються місцем національним законодавствам, що стикаються з викликами імплементації. Дослідженням встановлено, що головним викликом для міжнародних компаній є навігація у складному та неузгодженому регуляторному середовищі. У відповідь на це, стаття пропонує практичні "дорожні карти" для виходу фінансових компаній на ринки кожного з розглянутих регіонів. Також підкреслюється розрив між формальною відповідністю вимогам та реальною кіберстійкістю, що особливо помітно в регіонах з дефіцитом кваліфікованих кадрів та слабкими інституціями.

Ключові слова: кібербезпека, аудит кібербезпеки, регуляторні вимоги, цифрова трансформація, міжнародні стандарти з кібербезпеки.

VOITOVYCH Olesia, VOLYNETS Vitalii
Vinnytsia National Technical University

FEATURES OF LEGISLATION ON CYBER SECURITY AUDITING IN DIFFERENT REGIONS OF THE WORLD

The article is dedicated to a comparative analysis of the cyber security audit regulatory requirements in key regions of the world amidst global digital transformation. The study systematizes and compares regulatory approaches in the European Union, North America, Asia, and Africa, with a special focus on the requirements for the financial sector. The analysis covers key standards and legislative acts, including GDPR, NIS2, NIST CSF, PCI DSS, as well as leading national laws in China, such as MLPS 2.0, and in Africa, such as POPIA, NDPA, and DPA. The regional analysis revealed fundamental differences in approaches: from the strictly regulated and centralized in the EU (GDPR, NIS2) to the flexible, market-practice-driven in the USA (NIST CSF, SOC 2), heterogeneous in Asia with elements of strict state control (China's MLPS 2.0), and fragmented in Africa, where ineffective pan-African initiatives give way to national legislation facing implementation challenges. The study establishes that the main challenge for international companies is navigating this complex and inconsistent regulatory environment, which often results in significant operational overhead and the phenomenon of "compliance fatigue" due to duplicated audits across various standards. In response, the article offers practical "roadmaps" for financial companies to enter the markets of each of the considered regions, emphasizing the need for tailored, risk-based strategies. It also highlights the critical gap between formal compliance with requirements and actual cyber resilience. This disconnect is particularly noticeable in regions with a shortage of qualified personnel and weak institutional frameworks, where "paper compliance" may not translate into robust protection against sophisticated cyber threats. In conclusion, the article provides a structured overview of the global landscape of cybersecurity regulations and practical recommendations for building adaptive strategies for ensuring regulatory compliance in the context of international operations.

Keywords: Cyber security, cyber security audit, regulatory requirements, digital transformation, international standards in cyber security.

Стаття надійшла до редакції / Received 23.07.2025
Прийнята до друку / Accepted 19.08.2025

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Цифрова трансформація та глобалізація пришвидшує запровадження різнорідних кібербезпекових стандартів і регуляцій, що суттєво різняться між різними регіонами, зокрема ЄС, Північна Америка, Азія, Африка. Підприємства, які хочуть працювати на ринках того чи іншого регіону повинні враховувати вимоги з кібербезпеки відповідних країн. Відсутність узгодженого підходу спричиняє дублювання аудитів, фрагментацію контролів, нерівномірне охоплення IT/OT і ланцюгів постачання, дублювання аудиторських вимог та перевитрати ресурсів; формальна відповідність часто не гарантує реальної стійкості. Проблема

полягає у відсутності прозорого механізму для гармонізації цих різнорідних вимог, що ускладнює розробку практичних «дорожніх карт» для виходу компаній на міжнародні ринки.

АНАЛІЗ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

Сучасна цифрова трансформація бізнесу приносить не тільки нові можливості, але й безпрецедентні кіберризики, що вимагають системних аудитів кібербезпеки. Кіберзагрози стрімко зростають: за даними звітів, кількість кібератак глобально збільшилася майже на третину у 2024 році [1]. У відповідь підприємства впроваджують міжнародні стандарти безпеки (ISO/IEC 27001, NIST CSF тощо) та проводять регулярні аудити відповідності.

Основою для побудови систем управління інформаційною безпекою у світі є міжнародні стандарти, серед яких домінують ISO/IEC 27001 та NIST Cybersecurity Framework (CSF). ISO/IEC 27001 зосереджений на відповідності вимогам системи менеджменту, тоді як NIST робить акцент на гнучкому управлінні ризиками [2].

Галузевий аналіз виявляє, що загальні фреймворки не завжди враховують унікальні ризики, особливо у сферах з операційними технологіями (OT). Кібератаки на промислові системи управління можуть мати фізичні наслідки, як продемонстрував інцидент з компанією Merck, коли атака програми-вимагача паралізувала виробничі лінії [3]. Останні дослідження підтверджують, що ризики для OT залишаються надзвичайно високими: 75% організацій з OT-інфраструктурою зазнали щонайменше одного вторгнення [4]. Проблема ускладнюється тим, що багато OT-систем є «небезпечними за задумом» (insecure-by-design), оскільки створювалися з пріоритетом надійності, а не безпеки [5]. Як наслідок, інвестиції в безпеку OT часто є реактивними і спрямовані на досягнення формальної «готовності до аудиту», а не на усунення фундаментальних архітектурних недоліків.

Складність узгодження численних вимог створює для організацій явище «втоми від відповідності» (compliance fatigue) – стан виснаження, що негативно корелює з продуктивністю та підвищує ймовірність людських помилок. Ця проблема посилюється «ефектом правового трансплантату», коли передові регуляторні моделі впроваджуються без належної інституційної та технічної бази, створюючи розрив між законодавством та його практичним виконанням [6]. У відповідь на це у наукових колах розвивається концепція Єдиного каталогу контролів (Unified Control Framework, UCF) – інтегрованої моделі, що зіставляє вимоги ключових стандартів (ISO 27001, NIST CSF, GDPR) в єдиній структурі. Такий підхід дозволяє мінімізувати дублювання аудиторських процедур за принципом «документуй один раз, відповідай багатьом», що робить розробку комплексної моделі аудиту на основі UCF актуальним завданням для подальших досліджень [7].

Незважаючи на наявні стандарти, існують невирішені проблеми: недостатня адаптація стандартів до мультигалузевих потреб та складність узгодження різних міжнародних вимог (ISO, NIST), що створює “перевтому від відповідності”. Кількісне дослідження показує, що середній показник зрілості кібераудиту складає лише ~58 зі 100 можливих балів [8]. Саме тому питання розробки адаптивної системи кібераудиту, яка здатна інтегрувати різні стандарти та вимоги, залишається актуальним і потребує подальших досліджень.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Метою роботи є: систематизація та зіставлення нормативних вимог з кібербезпеки в ключових регіонах світу – Європейському Союзі, Північній Америці, Азії та Африці і на основі проведеного аналізу надати "дорожні карти" для компаній, що планують вихід на міжнародні ринки, з урахуванням унікальних регуляторних ландшафтів кожного регіону.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

В Європейському Союзі (ЄС) діє одна з найсуворіших у світі нормативних баз із кібербезпеки, що встановлює високі вимоги до захисту інформації та періодичного контролю. Ключовим актом є Загальний регламент із захисту даних (GDPR), що вимагає від організацій впроваджувати технічні та організаційні заходи безпеки, регулярно оцінювати їх ефективність і звітувати про інциденти (наприклад, про витоки даних протягом 72 годин) [9]. Недотримання вимог GDPR загрожує значними штрафами – до €20 млн або 4% світового річного обороту компанії, що стимулює проведення ретельних внутрішніх аудитів..

Інша важлива директива – NIS2 (Network and Information Security Directive 2, ухвалена у 2022 році) – поширює вимоги кібербезпеки на більше коло галузей та посилює роль аудитів у критичних секторах. Директива, за допомогою зовнішніх аудиту та інспекції, зобов’язує держави-члени контролювати операторів критичної інфраструктури. Крім того, NIS2 висуває підвищені вимоги до управління ризиками, що передбачає впровадження політик безпеки, проводити навчання персоналу, моніторинг, керування вразливостями та тестування на проникнення (pentest) там, де це доречно. Ці заходи мають регулярно перевірятися та передбачати звітування про значні кіберінциденти протягом 24 годин [10].

У ЄС, також, використовуються міжнародні стандарти, зокрема ISO/IEC 27001, сертифікація за яким є де-факто вимогою для бізнесу, особливо при роботі з фінансовим або державним сектором. Практика аудиту

включає внутрішній контроль (для підтримки сертифікацій), зовнішні перевірки від акредитованих органів та додаткові незалежні тестування (наприклад, pentest) для підвищення захищеності.

Суворість законодавства підтверджується реальними випадками, як-от багатомільйонні штрафи для British Airways та Marriott за порушення GDPR, що демонструє значні фінансові та репутаційні втрати через нехтування контролями [11]. Отже, у європейському регіоні сформувалася проактивна культура кібераудиту, де нормативні вимоги, підтримані жорсткими штрафами, поєднуються з галузевими стандартами і прозорими аудитами задля підвищення кіберстійкості.

Європейський Союз відомий одними з найжорсткіших та найбільш чітко регламентованих вимог до кібербезпеки у фінансовому секторі. Особливу увагу регулятори приділяють відповідності стандартам GDPR та DORA. Фінансовим компаніям, які мають намір успішно вийти на цей ринок, потрібно ретельно підготуватись та пройти наступні критично важливі кроки (Рис. 1).

У США відсутній єдиний федеральний закон з кібербезпеки, натомість діє система галузевих норм та добровільних стандартів, де значну роль відіграє саморегуляція індустрії. NIST Cybersecurity Framework (CSF) став «золотим стандартом» для побудови систем кіберзахисту. За даними ISACA, третина американських клієнтів припинить співпрацю з компанією після значного кіберінциденту [12]. Тому великі організації регулярно проводять внутрішні аудити за NIST, CIS Controls чи ISO 27001, щоб запевнитися у належному рівні безпеки й запобігти втраті клієнтів.

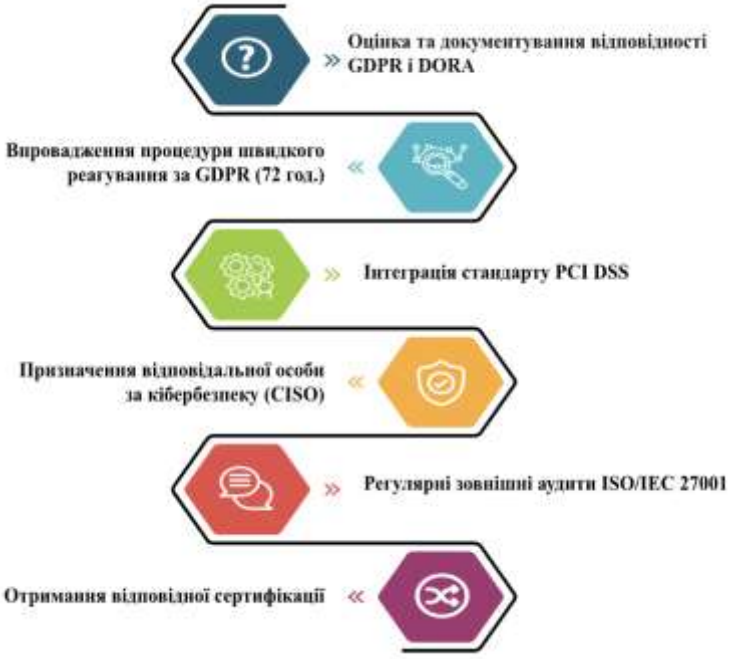

Рис. 1. Дорожня карта для виходу на ринок ЄС фінансової компанії

Також у США існують численні галузеві регламенти, які вимагають регулярних технічних аудитів або оцінок безпеки. Наприклад:

- Фінансовий сектор: Закон Гремма-Ліча-Блілі (GLBA) та рекомендації Федеральних агентств фінансового нагляду (FFIEC) зобов'язують банки та кредитні установи впроваджувати програми інформаційної безпеки, проводити щорічні оцінки ризиків і перевіряти ефективність контролів [13];
- Платіжні системи: Стандарт безпеки індустрії платіжних карт PCI DSS (розроблений консорціумом компаній Visa, MasterCard тощо) вимагає від організацій, що обробляють дані карт, щорічно проходити аудит відповідності або сканування на вразливості, а для великих продавців – зовнішній аудит акредитованим оцінювачем безпеки [14];
- Охорона здоров'я: Закон HIPAA зобов'язує медичні установи та їхніх постачальників проводити регулярні аналізи ризиків інформаційних систем, що містять медичні дані, та підтверджувати дотримання технічних стандартів захисту (шифрування, контроль доступу тощо). Порушення HIPAA може призвести до значних штрафів та приписів на усунення недоліків [14];
- Державні підрядники: Для постачальників Пентагону та інших федеральних відомств впроваджується система CMMC (Cybersecurity Maturity Model Certification), яка передбачає незалежний аудит рівня кібербезпеки організації. Без проходження CMMC-аудиту компанія не зможе отримати чи продовжити державний контракт у сфері оборони [14].

Американські технологічні компанії часто покладаються на незалежні аудити для зміцнення репутації і виконання договірних вимог партнерів. Найпоширеніший приклад – аудит за стандартом SOC 2 (System and Organization Controls 2), що фокусується на контролях безпеки, доступності, конфіденційності тощо. Окрім SOC 2, великі хмарні провайдери мають сертифікації ISO/IEC 27001, проходять регулярні тестування на проникнення із публікацією висновків, а також дотримуються фреймворку NIST CSF. Ця множинність стандартів означає, що на північноамериканському ринку ініціатива проведення аудитів часто йде від самої індустрії або замовників: бізнес, що хоче працювати з корпоративними клієнтами чи урядом, мусить мати підтвердження кіберстійкості.

Правове регулювання кібербезпеки в США має децентралізований характер, проте наглядові органи володіють дієвими механізмами для примусу до проведення аудитів. Федеральна торгова комісія (FTC) використовує повноваження щодо недобросовісної конкуренції, щоб штрафувати компанії за недостатній захист даних. Зазвичай порушення закінчуються укладенням мирової угоди, наприклад накладання на фірму багаторічних зобов'язань: протягом 20 років компанія повинна регулярно проходити сторонній аудит інформаційної безпеки і звітувати про впровадження поліпшень [15].

У Канаді нормативний ландшафт подібний до США, хоча масштаби менші. Федеральний закон PIPEDA вимагає від компаній забезпечувати належні засоби захисту персональної інформації та повідомляти регулятора (Уповноваженого з приватності) про серйозні порушення захисту даних. Організації мусять час від часу переглядати свої заходи безпеки на відповідність принципу «розумних засобів захисту». У фінансовому секторі Канади управління ризиками і кібербезпекою контролює Управління фінансових установ (OSFI), яке встановило детальні кібергігієнічні настанови для банків. OSFI вимагає від банків проводити регулярні тестування (наприклад, сканування, pentest) та щорічно звітувати про кіберінциденти і стан безпеки керівництву. Таким чином, в Канаді фактично дотримуються міжнародних стандартів і підлягають аудиту з боку регуляторів у разі інцидентів [16].

Північноамериканський ринок (особливо США) вирізняється більш гнучким та менш централізованим підходом до регулювання кібербезпеки. Однак саме ця гнучкість створює необхідність ретельного аналізу локальних вимог, зокрема стандартів окремих штатів та рекомендацій NIST Cybersecurity Framework. Нижче наведені критичні кроки, без яких повноцінний вихід фінансових компаній на американський ринок буде ускладнений (Рис. 2).

Рис. 2. Дорожня карта для виходу на ринок Північної Америки фінансової компанії

Сінгапур відомий як технологічний хаб з прогресивним кіберзаконодавством. Закон про кібербезпеку (Cybersecurity Act) 2018 р. встановив жорсткі вимоги для операторів критично важливої інформаційної інфраструктури, зобов'язуючи їх проводити регулярні аудити безпеки (щонайменше раз на 2 роки) та щорічні оцінки ризиків, звітуючи перед Агентством кібербезпеки. Невиконання цих вимог тягне значні покарання, включно зі штрафами та/або ув'язненням [17]. Підхід Сінгапуру до кібербезпеки є інституціоналізованим та проактивним, що було підкреслено після масштабного кіберінциденту з витоком медичних даних SingHealth у 2018 р., після якого було проведено ретельне розслідування, а на винних накладено штрафи [18].

Китайська Народна Республіка має одну з найбільш всеосяжних систем кіберрегулювання, тісно пов'язану з державним контролем. Основою є Закон «Про кібербезпеку» 2017 р., що ввів багаторівневу схему захисту (MLPS 2.0). Згідно з нею, всі інформаційні системи класифікуються за 5 рівнями критичності, і

компанії з системами високих рівнів зобов'язані залучати сторонніх аудиторів для регулярного оцінювання. Окремо для операторів критичної інформаційної інфраструктури встановлено вимогу щонайменше раз на рік проводити перевірку та оцінку безпеки і подавати звіт державному регулятору. Невиконання вимог несе серйозні наслідки, аж до відкликання ліцензій [19].

В Індії регулювання кібербезпеки активно розвивається. У 2023 р. прийнято Закон про цифровий захист даних (DPDP), який накладає на компанії вимоги, подібні до GDPR, зокрема щодо реалізації заходів безпеки та проведення аудитів для захисту персональних даних [20]. Національний центр реагування (CERT-In) з 2022 р. зобов'язує великі сервіси зберігати журнали подій щонайменше 180 днів та повідомляти про кіберінциденти не пізніше 6 годин після виявлення, що стимулює компанії до регулярного моніторингу та оцінки стану захищеності.

Ринок Китаю характеризується особливо жорстким державним контролем за дотриманням норм кібербезпеки. Для фінансових компаній принципово важливим є дотримання місцевого законодавства, особливо стандарту MLPS 2.0 та вимог локалізації даних. Щоб успішно почати діяльність у Китаї, компанії повинні пройти наступні важливі етапи підготовки (Рис. 3).

Рис. 3. Дорожня карта для виходу на ринок Китаю фінансової компанії

У підсумку, азійський регіон неоднорідний: Сінгапур демонструє режим, схожий на західний, з чіткими правилами та штрафами. У Китаї діє режим жорсткого державного нагляду й примусу, де аудити є частиною загального кіберконтролю. Країни на кшталт Індії перебувають на шляху до всеохоплюючої системи, поступово впроваджуючи аудити на практиці. Індійські IT-компанії проходять сертифікацію ISO 27001 та SOC 2 для роботи з міжнародними клієнтами, а в Сінгапурі після запровадження обов'язкових аудитів рівень підготовленості операторів критичної інфраструктури значно зріс.

Цифрова трансформація Африки відбувається стрімкими темпами, розширюючи поверхню для кібератак, однак регуляторний ландшафт залишається глибоко фрагментованим. Найбільш амбітна спроба гармонізації, Малабоська конвенція (Malabo Convention), виявилася малоефективною. Ухвалена ще у 2014 році, вона набула чинності лише у 2023-му, проте досі не ратифікована ключовими економіками континенту, такими як ПАР, Нігерія та Кенія. Конвенцію критикують за застарілі положення та відсутність дієвих механізмів правозастосування, що створило регуляторний вакуум [21]. Цей вакуум заповнюється національними законодавствами, де країни-лідери розробляють власні комплексні закони, часто орієнтуючись на GDPR. У ПАР діє зрілий Закон про захист персональної інформації (POPIA), що встановлює жорсткі вимоги до обробки даних та підкріплений активним регулятором зі значними повноваженнями щодо накладення штрафів [22]. Нігерія у 2023 році ухвалила Закон про захист даних (NDPA), створивши незалежну комісію та запровадивши ризик-орієнтований підхід до регулювання з суворими санкціями, що стимулювало швидкий розвиток ринку послуг із забезпечення відповідності [23]. Кенія також має GDPR-подібний Закон про захист даних (DPA), що вимагає обов'язкової реєстрації контролерів даних та встановлює 72-годинний термін для повідомлення про витоки.

Окрім цих загальних законів про захист даних, фінансові сектори в цих ключових економіках підлягають дедалі суворішим стандартам кібербезпеки, які часто встановлюються центральними банками. У ПАР Резервний банк (SARB) видав "Спільний стандарт вимог до кібербезпеки та кіберстійкості" (Joint Standard 2 of 2024), який вимагає від фінансових установ впровадження комплексних фреймворків, проведення регулярних тестів на проникнення та наявності планів реагування на інциденти. Директива SARB

прямо рекомендує узгодження з такими міжнародними стандартами, як ISO 27001 та NIST Cybersecurity Framework [24].

Центральний банк Нігерії (CBN) запровадив "Рамкову програму та керівні принципи кібербезпеки на основі ризиків", яка вимагає від банків призначати головного офіцера з інформаційної безпеки (CISO) та подавати щорічні звіти про самооцінку. Крім того, "Операційні настанови для відкритого банкінгу" вимагають впровадження політики інформаційної безпеки, оцінки загроз та багатофакторної автентифікації [25].

Своєю чергою, Центральний банк Кенії (CBK) видав "Керівництво з кібербезпеки для банківського сектору", яке зобов'язує проводити щорічні незалежні тестування, а для постачальників платіжних послуг – щоквартальні сканування вразливостей та звітувати про інциденти протягом 24 годин. Поряд із цими національними правилами, міжнародні стандарти, такі як Payment Card Industry Data Security Standard (PCI DSS), стають все більш важливими, хоча їх впровадження є складним через високу вартість та складність. Тим не менш, великі фінансові установи, такі як United Bank for Africa (UBA), вже отримали сертифікацію ISO 27001, що свідчить про поступове впровадження глобальних найкращих практик [26].

Аналіз фрагментованого регуляторного ландшафту та системних викликів дозволяє сформулювати практичні рекомендації для міжнародної фінансової компанії, що планує вихід на ринок Африки. Оскільки єдиної "африканської стратегії" не існує, необхідний диференційований підхід, заснований на найкращих практиках провідних юрисдикцій (Рис. 4).

Рис. 4. Дорожня карта для виходу на ринок Африки фінансової компанії

Незважаючи на прогресивне законодавство, існує значний розрив між нормами та їх практичною реалізацією через системні проблеми. Головною перешкодою є критичний дефіцит кваліфікованих кадрів: у ПАР, наприклад, до 63% посад у сфері кібербезпеки залишаються незаповненими. Це робить дотримання вимог надзвичайно складним і дорогим. Окрім того, органи із захисту даних часто не мають достатньої фінансової та політичної незалежності, а широкі винятки для цілей нацбезпеки підривають їхні повноваження [21]. В результаті правозастосування є непослідованим, що створює середовище "паперової відповідності", де формальне дотримання закону не гарантує реальної кіберстійкості.

ВИСНОВКИ З ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК

Проведене дослідження підтверджує, що, незважаючи на глобалізацію кіберзагроз, регуляторні підходи до кібербезпеки залишаються глибоко залежними від регіональних особливостей. Дослідження виявило критичний розрив між формальною відповідністю ("паперовою безпекою") та реальною кіберстійкістю, що загострюється через "втому від забезпечення відповідності" та дефіцит кваліфікованих кадрів, особливо в регіонах зі слабкими інституціями. Автори дійшли висновку, що в різних регіонах світу використовуються кардинально різні моделі регулювання: від жорстко централізованої в ЄС (GDPR, NIS2) до гнучкої, керованої ринковими практиками в США (NIST CSF, SOC 2), неоднорідної в Азії з елементами жорсткого державного контролю (китайський MLPS 2.0), та фрагментованої в Африці, де національні законодавства розвиваються на тлі системних викликів. Для міжнародних компаній це вимагає побудови

адаптивних систем управління, що враховують специфіку кожної юрисдикції, як демонструють розроблені "дорожні карти".

Перспективи подальших розвідок полягають у розробці інтегрованих моделей для гармонізації численних регуляторних вимог, зокрема через створення єдиного каталогу контролів (Unified Control Framework). Це дозволить перейти від формальних, дублюючих аудитів до гнучкої оцінки реальної зрілості кібербезпеки та готовності організацій до сучасних загроз.

References

1. Kuzior, A., Tiutiunyk, I., Zielińska, A., & Kelemen, R. (2024). Cybersecurity and cybercrime: Current trends and threats. *Journal of International Studies*, *17*(2), 220–239. https://doi.org/10.14254/2071-8330.2024/17-2/12
2. Gordon, L. A., Loeb, M. P., & Zhou, L. (2020). Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model. *Journal of Cybersecurity*, *6*(1), tyaa005. https://doi.org/10.1093/cybsec/tyaa005
3. Pircalaboiu, A., Cazoni, C., Ceausescu, C. E., Petre, B., & Dobrea, C. R. (2024). Cyber risk assessment in the pharmaceutical industry: Vulnerabilities, threats, and global response strategies. *Annals - Economy Series*, *5*, 307–319. https://ideas.repec.org/a/cbu/jrnlec/y2024v5p307-319.html
4. World Economic Forum. (2024, January). *Global cybersecurity outlook 2024*. https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf
5. Wetzels, J., Dos Santos, D. W., & Ghafari, M. (2023, May). *Insecure by design in the backbone of critical infrastructure* [Conference paper]. CPS-IoT Week '23: Cyber-Physical Systems and Internet of Things Week 2023. https://doi.org/10.1145/3576914.3587485
6. Mizrak, F., Demirel, H. G., Yaşar, O., & Karakaya, T. (2025). Digital detox: Exploring the impact of cybersecurity fatigue on employee productivity and mental health. *Discover Mental Health*, *5*(1), Article 25. https://doi.org/10.1007/s44192-025-00149-x
7. Eisenberg, I. W., Gamboa, L., & Sherman, E. (2025). *The Unified Control Framework: Establishing a common foundation for enterprise AI governance, risk management and regulatory compliance*. arXiv. https://doi.org/10.48550/arXiv.2503.05937
8. Zhylin A., Holych A., Khudyncev M (2019). Functional model of soc maturity assessment based on a maturity model. *Ukrainian Information Security Research Journal, 21*(3). https://doi.org/10.18372/2410-7840.21.13954
9. Riou, C., Azzouzi, M., Hespel, A., Guillou, E., Cuggia, M., & Jézéquel, J.-M. (2024). Ensuring GDPR compliance and security in a clinical data warehouse: Challenges and insights from a university hospital. *JMIR Medical Informatics*, *13*(1), e63754. https://doi.org/10.2196/63754
10. van 't Schip, M. (2024). The Regulation of Supply Chain Cybersecurity in the NIS2 Directive in the Context of the Internet of Things. *European Journal of Law Technology*, *15*(1). https://doi.org/10.2139/ssrn.4848048
11. Farmer, N., & Chon, L. K. (2020, December 17). *UK ICO data breach fines – What can we learn from British Airways and Marriott?*. Cleary Cybersecurity and Privacy Watch. https://www.clearycyberwatch.com/2020/12/uk-ico-data-breach-fines-what-can-we-learn-from-british-airways-and-marriott/
12. Davtyan, T. (2024). *The U.S. approach to AI regulation: Federal laws, policies, and strategies explained*. SSRN. https://doi.org/10.2139/ssrn.4954290
13. Onyekweluje, T. P., Tetteh-Kpah, C., Pinful, B., Apaflo, B. N., & Donkor, A. A. (2025). The role of IT compliance in enhancing cybersecurity measures for U.S financial institutions. *International Journal of Research Publication and Reviews*, *6*(1), 2000–2009. https://ijrpr.com/uploads/V6ISSUE1/IJRPR37874.pdf
14. Ursillo, S. J., Jr., Manske, K., & Kirk, B. (2025, January 24). *CMMC programmatic final rule status: What it means for defense contractors*. Cherry Bekaert. https://www.cbh.com/insights/articles/cmmc-compliance-and-its-implications-for-defense-contractors/
15. Gray, M. (2018). *Understanding and improving privacy 'audits' under FTC orders*. SSRN. https://doi.org/10.2139/ssrn.3165143
16. Nitin. (2025). *Cybersecurity and data privacy laws in Canada: Legal framework, challenges, and future directions*. SSRN. https://doi.org/10.2139/ssrn.5202450
17. Ang, B. (2021). Cybersecurity and legislation: The case study of Singapore. In G. Siboni & L. Ezioni (Eds.), *Cybersecurity and legal-regulatory aspects* (pp. 89–102). World Scientific Publishing.
18. Tham, I. (2018, July 20). *Personal info of 1.5m SingHealth patients, including PM Lee, stolen in Singapore's worst cyber attack*. The Straits Times. https://www.straitstimes.com/singapore/personal-info-of-15m-singhealth-patients-including-pm-lee-stolen-in-singapores-most
19. Creemers, R. (2022). China's emerging data protection framework. *Journal of Cybersecurity*, *8*(1), tyac011. https://doi.org/10.1093/cybsec/tyac011
20. Malhotra, C., & Malhotra, U. (2024). Putting interests of Digital Nagriks first: Digital Personal Data Protection (DPDP) Act 2023 of India. *Indian Journal of Public Administration*, *70*(3), 516–531. https://doi.org/10.1177/00195561241271575
21. Daigle, B. (2021, February). Data protection laws in Africa: A pan-African survey and noted trends. *Journal of International Commerce and Economics*, 1–26. https://www.usitc.gov/publications/332/journals/jice_africa_data_protection_laws.pdf&ved=2ahUKEwie4sS04qOPAxXmJxAIHaS4BRcQFnoECBwQAQ&usg=AOvVaw0NYny1R8h7e3P1ex7s_KLB
22. Chimboza, T., & Smith, E. (2024, September 12). *How does compliance with the Protection of Personal Information Act (POPI Act) affect organisations in South Africa?* [Paper presentation]. 10th Annual African Conference on Information Systems and Technology, Kennesaw, GA, United States. https://digitalcommons.kennesaw.edu/acist/2024/presentations/19
23. Victor, S. (2025). *Data protection and compliance in Nigeria: Challenges and opportunities*. SSRN. https://doi.org/10.2139/ssrn.5236705
24. Prudential Authority & Financial Sector Conduct Authority. (2024). *Joint Standard 2 of 2024: Cybersecurity and cyber resilience requirements*. Juta | Complinews. https://jutacomplinews.co.za/media/filestore/2024/07/Joint_Standard_2_of_2024__Cybersecurity__Cyber_resilience_Requirements_1.pdf
25. Nkwor, L., & Adeyemo, I. (2024, June 11). *Overview of the CBN risk-based cybersecurity framework and guidelines for deposit money banks and payment service banks*. Mondaq. https://www.mondaq.com/nigeria/security/1518574/overview-of-the-cbn-risk-based-cybersecurity-framework-and-guidelines-for-deposit-money-banks-and-payment-service-banks
26. Ministry of Information, Communications and the Digital Economy. (2025, May). *National Cybersecurity Strategy, 2025-2029 (Draft)*. https://ipi.media/wp-content/uploads/2025/05/National-Cybersecurity-Strategy-2025-2029-Draft-upload.pdf