УДК 338.24:658.012.4:004.056
DOI: https://doi.org/10.32782/2413-9971/2025-57-3

Горбаньова В.О.
докторка філософії з менеджменту,
старша викладачка кафедри менеджменту
Міжнародного гуманітарного університету
ORCID: https://orcid.org/0000-0002-0022-5133
Горбаньов І.М.
кандидат юридичних наук,
старший науковий співробітник, доцент,
професор кафедри кримінально-правових дисциплін
Одеського державного університету внутрішніх справ
ORCID: https://orcid.org/0000-0002-4100-605X

Gorbanova Viktoriia
Doctor of Philosophy in Management,
Senior Lecturer, Department of Management
International Humanitarian University
Gorbanov Igor
Candidate of Legal Sciences,
Senior Research Fellow, Associate Professor,
Professor of the Department of Criminal Law Disciplines
Odesa State University of Internal Affairs

МІЖНАРОДНИЙ ДОСВІД КОРПОРАТИВНОГО УПРАВЛІННЯ ПІДПРИЄМСТВАМИ ІЗ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Анотація. Стаття присвячена трансформації корпоративного управління в умовах цифровізації та зростання кіберзагроз. Показано, що традиційний акцент на контролі фінансів і прозорості поступається місцем управлінню цифровими ризиками, захисту даних і забезпеченню стійкості бізнесу. Розглянуто зовнішні й внутрішні кіберзагрози, їх види та наслідки для корпоративного сектору. Проаналізовано міжнародний досвід США, ЄС та провідних корпорацій (Microsoft, Siemens, Samsung, IBM), що інтегрували кібербезпеку у стратегії управління. Запропоновано архітектурну модель корпоративного управління з урахуванням цифрових ризиків, яка передбачає багаторівневий підхід, інтеграцію стандартів ISO/IEC та рекомендацій NIST. Зроблено висновок, що адаптація міжнародних стандартів ISO/IEC 27001, NIST CSF, GDPR та NIS2 до національних реалій та їх впровадження у бізнес-середовище дозволить підвищити рівень захисту компаній і прискорить їх інтеграцію у глобальну економіку.

Ключові слова: стратегічне управління, корпоративне управління, інформаційна безпека, конкурентні переваги підприємств, стратегія розвитку підприємств, цифровізація підприємств, інформатизація бізнесу, корпоративна безпека, автоматизація бізнес процесів, інновації, сталий розвиток.

Вступ та постановка проблеми. У сучасних умовах цифрової трансформації бізнесу та зростання інформаційних загроз корпоративне управління набуває нового змісту. Якщо раніше воно зосереджувалося на балансі інтересів власників, менеджменту та стейкхолдерів, то нині тісно інтегрується з управлінням ризиками, насамперед у сфері кібербезпеки. Забезпечення інформаційної безпеки стає не лише інновацією, а й необхідністю, зумовленою економічними та правовими чинниками.

По-перше, цифровізація бізнес-процесів, електронний документообіг, хмарні технології, штучний інтелект і великі дані різко підвищили залежність бізнесу від IT-систем. У таких умовах навіть незначні порушення безпеки спричиняють фінансові втрати, репутаційні ризики й падіння конкурентоспроможності. Традиційні підходи корпоративного управління, орієнтовані на фінансовий контроль і планування, вже не гарантують належного захисту інтересів власників.

По-друге, нові виклики змінюють функції органів управління. Підприємства мають розробляти політики інформаційної безпеки, контролювати впровадження систем захисту даних, формувати резерви для ліквідації наслідків кіберінцидентів. Корпоративне управління перетворюється на комплексну систему забезпечення стійкості підприємства.

По-третє, в умовах гібридних загроз компанії формують нову культуру управління, що інтегрує ризик-менеджмент із кіберзахистом. Водночас брак досвіду, ресурсів і належного регулювання ускладнює цей процес.

По-четверте, проблемність полягає у відсутності усталеного підходу до поєднання корпоративного управління й кібербезпеки. У науковій літературі переважають окремі дослідження цих сфер, тоді як їхня інтеграція перебуває на стадії становлення. Це зумовлює потребу в комплексному дослідженні специфіки корпоративного управління з урахуванням кіберзагроз.

Аналіз останніх досліджень і публікацій. У контексті сучасної корпоративної практики кібербезпека поступово перетворюється на критичний елемент системи корпоративного управління, оскільки інформаційні активи набувають ключової ролі в бізнес-діяльності. Така проблематика стає предметом дослідження національних науковців, зокрема: А.С. Полторак, А.Л. Сухорукової та А.І. Бурковської «Кібербезпека в системі трансформації управління бізнес-організацією» (2021 р.); крім того, у статті О.Ю. Кузьменко, О.В. Маклюка і О.О. Чернишової «Кібербезпека бізнесу під час війни» (2022 р.); Л.В. Шостак, А.А. Федонюка і О.О. Помазун «Особливості кібербезпеки бізнесу в умовах воєнного часу» (2022 р.); В.О. Ткача «Глобальне управління у сфері кібербезпеки» (2024 р.); А.В. Ільєнко, В.А. Телющенко, О.В. Дубчак «Сучасні кіберзагрози критичної інфраструктури України та світу» (2025 р.) та інших. Однак попри значну розробленість окресленої проблематики, питання впливу кібербезпеки на корпоративне управління підприємством залишаються вельми актуальною темою.

Виділення невирішених раніше частин загальної проблеми. Попри зростання кількості досліджень у сфері інтеграції інформаційної безпеки в корпоративне управління, низка аспектів проблеми залишається недостатньо опрацьованою. Існуючі моделі корпоративного управління не повною мірою враховують специфіку цифрової економіки та масштаби сучасних кіберзагроз. Відсутність інтегрованих підходів призводить до зниження стійкості підприємств, обмеження їхнього інноваційного потенціалу та формування бар'єрів на шляху сталого розвитку. Тому науково-практичне завдання полягає в розробці системи корпоративного управління, яка: поєднувала б традиційні управлінські функції з інструментами управління інформаційними ризиками; забезпечувала б ефективну взаємодію органів корпоративного управління з підрозділами з кіберзахисту; відповідала б міжнародним стандартам прозорості, підзвітності та відповідальності; враховувала б національні особливості правового регулювання та економічного розвитку. Отже, дослідження міжнародного досвіду корпоративного управління підприємствами з урахуванням сучасних загроз кібербезпеки є надзвичайно актуальним і має вагоме прикладне значення для забезпечення стабільного функціонування та сталого розвитку організацій у глобалізованому та високотехнологічному середовищі.

Метою статті є дослідження та узагальнення міжнародного досвіду корпоративного управління підприємствами із забезпечення кібербезпеки.

Результати дослідження. Корпоративне управління традиційно визначається як система відносин між власниками капіталу, менеджментом підприємства та іншими зацікавленими сторонами, яка покликана забезпечувати ефективне використання ресурсів, досягнення стратегічних цілей та підвищення вартості бізнесу, у тому числі підтримувати конкурентоспроможність і довгострокову стійкість бізнесу. У науковій літературі воно розглядається як багатогранна категорія, що включає правові, економічні, організаційні та соціальні аспекти [1, с. 4-8]. Відповідно до принципів Організації економічного співробітництва та розвитку [2], корпоративне управління спрямоване на створення прозорої, підзвітної та відповідальної системи контролю, яка забезпечує баланс інтересів власників і менеджерів, а також захист прав інших стейкхолдерів.

У класичних моделях корпоративного управління основна увага приділялася фінансовим аспектам діяльності підприємств та контролю за ефективністю роботи менеджменту. Проте у XXI столітті під впливом глобалізації, цифрової трансформації економіки та зростання ролі нематеріальних активів сутність і завдання корпоративного управління зазнали значних змін.

Цифрова епоха характеризується переходом підприємств до моделей, що ґрунтуються на використанні інформаційних технологій, електронного документообігу, автоматизованих систем управління, аналітики великих даних, штучного інтелекту та хмарних сервісів. Це призводить до суттєвої трансформації функцій корпоративного управління. Якщо раніше пріоритетними завданнями були контроль і фінансова звітність, то сьогодні дедалі більшого значення набувають питання управління ризиками, забезпечення інформаційної безпеки, захисту персональних даних та побудови довіри в цифровому середовищі.

Важливим елементом трансформації є вимушена поява нових функцій корпоративного управління, серед яких можна виокремити: 1) управління інформаційними ризиками, зокрема, включення до порядку денного рад директорів питань кіберзахисту, інвестицій у системи безпеки та управління інцидентами; 2) забезпечення цифрової прозорості щодо формування механізмів відкритого інформування стейкхолдерів про стан цифрової інфраструктури підприємства; 3) інтеграція інноваційних технологій, наприклад, прийняття стратегічних рішень щодо впровадження цифрових платформ, блокчейну, автоматизації бізнес-процесів; 4) формування культури кібербезпеки як розвиток компетентностей працівників, навчання персоналу правилам безпечної поведінки у цифровому середовищі.

Отже, у цифрову епоху корпоративне управління виходить за межі класичного контролю фінансових потоків та формування стратегій. Воно стає системою комплексного управління економічних, правових, технологічних, соціальних та етичних аспектів діяльності підприємств. Трансформація його функцій обумовлює необхідність перегляду усталених

моделей та пошуку нових підходів, що дозволять забезпечити стійкість підприємств у середовищі, де інформаційні та кіберзагрози стають одним із ключових факторів впливу на бізнес.

Для пізнання сутності кіберзагроз та негативного впливу на корпоративне середовище та бізнес-структури розглянемо їх види, а також потенційні руйнівні наслідки. Отже, кіберзагрози можна умовно поділити на дві основні групи: 1) зовнішні загрози – атаки хакерських угруповань, фішингові кампанії, розповсюдження шкідливого програмного забезпечення, DDoS-атаки, кібершпигунство та атаки на інфраструктуру постачальників; 2) внутрішні загрози – несанкціоновані дії співробітників (навмисні або випадкові), витік даних через недбалість, зловживання доступом, саботаж, а також використання вразливостей у внутрішніх IT-системах. При чому внутрішні інциденти часто є більш руйнівними, оскільки пов'язані з доступом до критичних ресурсів підприємства [3, с. 7–15].

Розкриємо сутність окремих різновидів кіберзагроз для корпоративного сектору:

1. Фінансові атаки є найбільш поширеним видом загроз для корпоративних структур, які спрямовані на заволодіння фінансовими ресурсами підприємства. Це можуть бути несанкціоновані перекази коштів, шахрайські транзакції, підробка платіжних реквізитів або компрометація систем електронних платежів. За даними міжнародних досліджень, саме фінансові атаки становлять до 40 % усіх кібератак на корпоративний сектор [3, с. 7–15]. Їх особливістю є швидкість реалізації та масштабність наслідків, що ускладнює можливості підприємства щодо своєчасного реагування.

2. Крадіжка даних за розповсюдженістю знаходиться на другій позиції. Інформація виступає стратегічним активом підприємства, тому зловмисники часто спрямовують зусилля на викрадення баз даних клієнтів, комерційної інформації, результатів наукових досліджень або стратегічних планів розвитку. В умовах цифровізації бізнесу витік даних може завдати непоправної шкоди компанії, оскільки підриває довіру партнерів та клієнтів, а також створює додаткові витрати на відновлення безпеки. Окремо варто виділити ризик викрадення персональних даних працівників та клієнтів, що вимагає від корпорацій суворого дотримання міжнародних стандартів захисту інформації. Так, у 2017 році відбувся злам компанії Equifax, унаслідок якого було викрадено персональні дані понад 140 млн клієнтів. Це спричинило не лише мільярдні збитки, але й суттєві кадрові зміни в топ-менеджменті [4].

3. Промислове шпигунство є ефективним засобом ведення бізнесу у сучасних інформаційно-технологій умовах, і часто здійснюється шляхом кібератак, що спрямовані на здобуття технологічних розробок, патентованих рішень, виробничих секретів і ноу-хау. Наслідком такої діяльності є втрата конкурентних переваг, зниження інноваційного потенціалу та ускладнення процесів стратегічного планування. Сучасні тенденції свідчать, що промислове шпигунство за допомогою кіберзасобів є дешевшим і менш ризикованим для зловмисників, ніж традиційні форми нелегального отримання інформації.

4. Порушення бізнес-процесів, що за характером нагадують диверсію. Атаки на інфраструктуру підприємств, зокрема на сервери, мережеві системи та виробниче обладнання, спричиняють призупинення чи повну зупинку бізнес-процесів. До таких дій належать DDoS-атаки, блокування програмного забезпечення, втручання у системи управління виробничими процесами. Наслідки для компаній можуть бути катастрофічними: від тимчасового паралічу діяльності до зупинки виробництва, що супроводжується не лише фінансовими втратами, а й репутаційними та соціальними ризиками. Так, у 2020 році був злам SolarWinds, який показав небезпеку атаки на ланцюги постачання, що змусило компанії впроваджувати додаткові рівні перевірки контрагентів та партнерів [5].

Наслідками кібератак для корпоративного управління можуть стати: 1) фінансові збитки у формі прямих збитків (втрата коштів, виплата викупу за відновлення даних), а також у вигляді непрямих витрат – на відновлення інформаційних систем, проведення внутрішніх розслідувань, удосконалення систем захисту; 2) втрата репутації, що зачіпає довіру партнерів, інвесторів і клієнтів. Втрата репутації внаслідок витоку даних або порушення безперервності бізнесу є довготривалим наслідком, який важко подолати. Репутаційні ризики знижують ринкову капіталізацію підприємств, ускладнюють залучення інвестицій та формують недовіру серед потенційних контрагентів; 3) юридична відповідальність у вигляді значних штрафних санкцій, компенсацій постраждалим клієнтам, судових процесів або кримінальної відповідальності керівників, наприклад, як за порушення стандартів захисту персональних даних у компаніях країн ЄС.

Узагальнюючи наведену інформацію зазначимо, що кіберзагрози виступають складним і небезпечним явищем, що суттєво трансформує систему корпоративного управління. Вказані загрози охоплюють усі сфери функціонування підприємства. Усвідомлення масштабів і наслідків кібератак вимагає від корпоративних структур системний підхід до інтеграції кібербезпеки у стратегії управління, впровадження комплексних систем моніторингу та реагування на інциденти, а також формування корпоративної культури інформаційної безпеки.

Аналіз міжнародного досвіду з забезпечення інформаційної безпеки підприємств дозволяє виявити ефективні практики, які можуть бути імплементовані у вітчизняне корпоративне середовище. Так, американська модель корпоративного управління відзначається високим рівнем інтеграції питань кібербезпеки у стратегічний порядок денний ради директорів. Після низки масштабних кібератак, зокрема на компанії Target (2013 р.), Equifax (2017 р.) та Colonial Pipeline (2021 р.), стало очевидним, що проблематика кіберризиків має розглядатися на рівні найвищих управлінських

органів [4; 6; 7]. Рада директорів корпорацій у США несе фідуціарну відповідальність перед акціонерами за збереження вартості компанії та мінімізацію ризиків. Кіберзагрози у цьому контексті трактуються як ключові стратегічні ризики, здатні вплинути на фінансову стабільність і репутацію компанії. Тому дедалі більше корпорацій створюють у структурі ради директорів комітети з питань кібербезпеки або включають кіберризики до порядку денного комітетів з аудиту та управління ризиками, які оцінюють адекватність політик і процедур кіберзахисту; аналізують результати внутрішніх і зовнішніх аудитів у сфері IT-безпеки; контролюють витрати на кібербезпеку та оцінюють їх ефективність; здійснюють моніторинг інцидентів та планів реагування.

У компаніях активно застосовується принцип «кіберекспертизи у раді директорів», що передбачає залучення до складу ради незалежних директорів із досвідом у сфері інформаційних технологій і кібербезпеки, що забезпечує кваліфікований контроль та зменшує інформаційну асиметрію між технічними фахівцями та управлінським рівнем. Додатковим механізмом регулювання є зобов'язання щодо розкриття інформації про кіберризики у звітності публічних компаній, які встановлює Комісія з цінних паперів та бірж США (SEC) [8]. Ці правила зобов'язують компанії інформувати інвесторів про кіберінциденти та розкривати інформацію про корпоративні політики управління кіберризиками. Це формує прозорість і дисциплінує корпорації у питаннях безпеки.

Не менш важливим інструментом є NIST Cybersecurity Framework, розроблений Національним інститутом стандартів і технологій США. Він ґрунтується на п'яти ключових функціях – ідентифікація, захист, виявлення, реагування та відновлення – і слугує універсальною моделлю для побудови комплексних систем кіберзахисту [9].

У Європейському Союзі інтеграція кібербезпеки у корпоративне управління здійснюється переважно через нормативно-правові акти та міжнародні стандарти.

Одним із ключових елементів є Загальний регламент про захист даних (далі – GDPR), що набув чинності у 2018 р. GDPR зобов'язує компанії впроваджувати належні технічні та організаційні заходи для захисту персональних даних, а також негайно повідомляти регуляторів та суб'єктів даних про витоки інформації. Для корпорацій це означає не лише технічний обов'язок забезпечити безпеку даних, а й управлінську відповідальність. Недотримання вимог GDPR загрожує штрафами до 20 млн євро або до 4 % річного обороту компанії, що спонукає ради директорів приділяти особливу увагу питанням захисту даних [10, с. 1–88].

Ще одним інструментом є міжнародні стандарти, зокрема ISO/IEC 27001, що встановлює вимоги до систем управління інформаційною безпекою (далі – СУІБ), і визначає її як процес забезпечення конфіденційності, цілісності та доступності інформації, а також таких властивостей, як автентичність і достовірність. Сертифікація за цим стандартом стала своєрідним «золотим стандартом» для транснаціональних компаній, оскільки дозволяє продемонструвати партнерам та інвесторам відповідність високим вимогам у сфері кіберзахисту. Стандарт акцентує увагу на процесному підході, управлінні ризиками та безперервному циклі вдосконалення. Для корпоративного управління це означає включення процесів управління ризиками інформаційної безпеки до системи загального менеджменту компанії, інтеграцію політик IT-безпеки з фінансовими та стратегічними планами [11].

Окреме місце у розвитку світової практики посідає Британський стандарт BS 7799, який став основою для створення ISO/IEC 27001 та визначив базові підходи до побудови ефективної СУІБ. Цей стандарт передбачає комплекс заходів, що охоплюють як організаційні, так і технічні аспекти захисту даних. Він акцентує на необхідності формування чіткої політики інформаційної безпеки, яка встановлює стратегічні цілі та принципи захисту активів, а також передбачає розподіл обов'язків між підрозділами і посадовими особами. Значну увагу приділено навчанню персоналу, підвищенню рівня обізнаності про ризики та запровадженню механізмів звітності щодо інцидентів. Ключовим елементом BS 7799 є визначення переліку критично важливих інформаційних активів, до яких належать конфіденційні ресурси в електронній, паперовій, магнітній чи оптичній формі, бази даних, програмне забезпечення, акустична інформація, відомості, отримані співробітниками у процесі виконання службових обов'язків, а також автоматизовані системи, мережеве обладнання, канали зв'язку та технічні засоби захисту. Доступ до таких активів має бути чітко регламентований та документально зафіксований, із застосуванням процедур ідентифікації, автентифікації та авторизації. Ефективна стратегія передбачає класифікацію даних за рівнем важливості, побудову архітектури безпеки та визначення заходів захисту для кожної категорії, враховуючи тип даних, їх зміст, коло користувачів та необхідний рівень перевірки автентичності. Такий підхід забезпечує системність і гнучкість управління інформаційною безпекою та повністю узгоджується із сучасними принципами корпоративного управління [12].

Європейський Союз у 2022 році також запровадив Директиву NIS2, яка поширює обов'язки у сфері кібербезпеки на широкий спектр підприємств критичної інфраструктури та великий бізнес. Цей документ зобов'язує ради директорів забезпечувати належне управління кіберризиками, що закріплює відповідальність топменеджменту за безпеку цифрових активів [13].

Таким чином, європейський підхід базується на поєднанні жорсткого правового регулювання та впровадження міжнародних стандартів управління, що створює системну основу для інтеграції кібербезпеки у корпоративне управління.

Інтеграція кібербезпеки у корпоративне управління проявляється також у практиках провідних

транснаціональних корпорацій, які формують глобальні стандарти у цій сфері. Так, компанія Microsoft послідовно позиціонує кібербезпеку як стратегічний пріоритет корпоративного управління. У структурі ради директорів діє комітет з аудиту та управління ризиками, який здійснює нагляд за політиками безпеки. Microsoft щорічно публікує Cybersecurity Report, що містить дані про інциденти, нові загрози та ефективність заходів захисту. Окрім того, компанія інвестує мільярди доларів у розробку рішень для кіберзахисту, що поєднує бізнес-інтереси та корпоративну відповідальність [14].

Німецька корпорація Siemens інтегрувала кібербезпеку у всі бізнес-процеси, включно з виробництвом та постачальницькими ланцюгами. Компанія розробила Програму корпоративної кібербезпеки (Siemens Cybersecurity Program), яка передбачає багаторівневий підхід до управління ризиками. Особливістю є орієнтація на промислову безпеку, що актуально для виробничих підприємств [15].

Схожим чином діє південнокорейська корпорація Samsung, яка застосовує модель "Security by Design", сутністю якої є інтеграція безпекових вимог на всіх етапах життєвого циклу продуктів. У корпоративному управлінні компанія реалізує політику багаторівневого контролю: від наглядової ради до спеціалізованих комітетів, відповідальних за аудит інформаційної безпеки, через впровадження глобальних стандартів ISO/IEC 27001 та ISO/IEC 27701 [16].

Компанія IBM запровадила модель "Cybersecurity Risk Heat Map", що дозволяє ранжувати ризики за ймовірністю та впливом на бізнес, з відповідною прив'язкою фінансування заходів безпеки [17].

Приклади цих корпорацій свідчать, що успішна інтеграція кібербезпеки у корпоративне управління можлива лише за умови стратегічного підходу з боку найвищих органів управління та поєднання технічних, організаційних і правових інструментів.

Аналіз практики провідних міжнародних корпорацій підводить до формування ефективної моделі корпоративного управління з урахуванням сучасних загроз кібербезпеки. Якщо у традиційних моделях управління головний акцент робився на прозорості, підзвітності та збалансованості інтересів акціонерів і менеджменту, то нині одним із ключових пріоритетів стає безпека даних і цифрових інфраструктур. У цьому контексті постає завдання інтеграції корпоративного управління та системи кіберзахисту в єдину управлінську концепцію.

Основними концептуальними підходами до інтеграції корпоративного управління та системи кіберзахисту виступають:

– інституціональний підхід, що передбачає створення формальних структур і органів (комітетів з кібербезпеки, служб ризик-менеджменту) для забезпечення належного рівня контролю за цифровими ризиками;

– процесний підхід, який розглядає кіберзахист як невід'ємну складову бізнес-процесів і включає безпекові аспекти в етапи стратегічного, операційного та інноваційного управління;

– культурний підхід, що акцентує увагу на формуванні ціннісних орієнтирів і поведінкових моделей співробітників, орієнтованих на підтримання високих стандартів кібергігієни;

– системний підхід, який поєднує технічні, організаційні, правові та соціальні інструменти, забезпечуючи комплексність управління кіберризиками.

Таким чином, інтеграція корпоративного управління та системи кіберзахисту повинна розглядатися як багаторівневий комплексний процес.

Архітектура моделі корпоративного управління з урахуванням цифрових ризиків та кіберзагроз вимагає забезпечення взаємозв'язку між ключовими суб'єктами управління, бізнес-процесами та інструментами контролю.

На нашу думку, архітектурна модель, з урахуванням розміру суб'єкта господарської діяльності, має включати такі елементи:

– наглядовий рівень – рада директорів та спеціалізовані комітети, що визначають політику у сфері кібербезпеки, контролюють її виконання та інтегрують у загальну стратегію компанії;

– стратегічний рівень – топ-менеджмент, який відповідає за розробку планів кіберзахисту, розподіл ресурсів та управління ризиками;

– операційний рівень – служби інформаційної безпеки, IT-відділи та підрозділи ризик-менеджменту, що реалізують політику кіберзахисту на практиці;

– поведінковий рівень – співробітники всіх підрозділів, які беруть участь у формуванні культури кібербезпеки та дотриманні стандартів корпоративної безпеки;

– зовнішнє середовище – державні регулятори, партнери, постачальники та клієнти, що взаємодіють із компанією і впливають на формування її цифрових ризиків

Така архітектура моделі передбачає постійну циркуляцію інформації між рівнями – від наглядової ради до працівників і навпаки, що дозволяє оперативно реагувати на нові виклики та формувати адаптивну систему управління.

Формування ефективної моделі корпоративного управління для забезпечення інформаційної безпеки неможливе без опори на міжнародні стандарти та кращі практики. Стандарти ISO/IEC 27001, рекомендації NIST Cybersecurity Framework, директиви GDPR і NIS2 у ЄС створюють уніфіковані рамки для організації процесів кіберзахисту на рівні корпорацій. Їх імплементація дозволяє підприємствам не лише захистити власні ресурси, але й забезпечити відповідність вимогам інвесторів і міжнародних партнерів.

Водночас, у національному контексті важливим є гармонізування українського законодавства у сфері корпоративного управління та кібербезпеки з європейськими практиками. Це передбачає оновлення нормативно-правової бази, розвиток інституційної спроможності регуляторів та стимулювання бізнесу до впровадження систем управління кіберризиками.

Міжнародний досвід корпоративного управління підприємствами із забезпечення інформаційної безпеки свідчить про наявність певної специфіки, зокрема, урахування необхідності інтеграції управління ризиками у корпоративні стратегії. Вказане є реакцією на специфічну природу кіберзагроз, які не обмежуються технічним аспектом є комплексними, динамічними та здатними спричиняти системні руйнівні наслідки для бізнесу [18]. Цей процес передбачає формування цілісної системи оцінювання та моніторингу ризиків, які пов'язані з використанням цифрових технологій, обробкою великих масивів даних, впровадженням хмарних рішень та взаємодією з цифровими екосистемами. Стратегічне бачення ризиків має бути включене у загальні бізнес-цілі компанії [2]. Це означає, що питання кібербезпеки повинні розглядатися на етапі розробки корпоративної стратегії поряд із фінансовими, маркетинговими та інноваційними аспектами. Зокрема, інтеграція управління кіберризиками вимагає: 1) розробки політик і процедур щодо ідентифікації та реагування на загрози; 2) визначення стратегічних пріоритетів у сфері інформаційної безпеки; 3) залучення ресурсів для реалізації проєктів цифрової безпеки; 4) створення системи регулярного звітування на рівні ради директорів щодо стану захищеності підприємства.

У такий спосіб корпоративні стратегії мають перетворюватися на комплексні документи, які враховують як економічні, так і технологічні виклики, а також забезпечують баланс між розвитком та безпекою.

Означена нами раніше практика провідних міжнародних корпорацій свідчить про ефективність створення у складі наглядових рад спеціалізованих комітетів, що відповідають за управління питаннями кібербезпеки. Така інституціоналізація функцій контролю за кіберризиками дає можливість забезпечити системний та незалежний нагляд за впровадженням політик безпеки, а також підвищує рівень прозорості управлінських рішень [19]. Комітети з кібербезпеки зазвичай мають такі завдання: 1) оцінка ризиків і розробка рекомендацій щодо пріоритетних напрямів інвестування у безпеку для ради директорів; 2) моніторинг відповідності діяльності компанії міжнародним стандартам; 3) контроль ефективності внутрішніх процедур кіберзахисту та реагування на інциденти; 4) аналіз інцидентів та розробка планів зниження вразливостей. Важливим аспектом є формування таких комітетів на принципах професійної компетентності. До їхнього складу мають входити незалежні експерти з кібербезпеки, IT-аудитори та представники служби безпеки компанії [20]. Це забезпечить багатопрофільний підхід до аналізу загроз та визначення управлінських рішень.

Традиційно ефективність корпоративного управління оцінювалася через фінансові показники. Проте у цифрову епоху виникає потреба у розширенні системи оцінювання результативності, зокрема у сфері управління кіберризиками. Запровадження ключових показників ефективності (далі – KPI) у сфері кібербезпеки дозволяє перевести питання безпеки з площини технічних характеристик у площину стратегічного управління [21]. Серед можливих KPI у сфері кібербезпеки можна виділити: час реагування на кіберінциденти та їх динаміка, кількість успішно відбитих атак, відсоток персоналу, що пройшов навчання з кібергігієни, рівень відповідності міжнародним стандартам (ISO/IEC 27001), а також обсяг інвестицій у кіберзахист [9]. Запровадження KPI дозволяє наглядовим радам та акціонерам мати об'єктивні інструменти для оцінювання ефективності управлінських рішень у сфері кіберзахисту.

Одним з ключових елементів специфіки корпоративного управління у контексті сучасних кіберзагроз є формування корпоративної культури кібербезпеки. Жодні технічні рішення не здатні забезпечити повного захисту без активної участі людського фактора. Міжнародна корпоративна практика показує, що значна частина інцидентів у сфері кібербезпеки відбувається через недбалість або низький рівень обізнаності співробітників. Формування культури кібербезпеки передбачає: 1) навчання та підвищення кваліфікації персоналу щодо основ інформаційної безпеки; 2) створення системи корпоративних цінностей, що підкреслюють важливість безпечного поводження з даними; 3) розробку програм мотивації для співробітників, які дотримуються правил кібергігієни; 4) комунікацію з боку топ-менеджменту, що демонструє пріоритетність безпеки як частини корпоративної культури [22].

Інституціоналізація практик кібербезпеки у стандарти підприємства підвищує довіру інвесторів і партнерів, що особливо актуально для компаній, інтегрованих у глобальні ланцюги постачання [23].

Висновки. Міжнародний досвід корпоративного управління підприємствами підтверджує, що кібербезпека стає невід'ємною складовою корпоративного управління. Встановлено, що кіберзагрози мають комплексний вплив на підприємства, зачіпаючи їх операційну діяльність, фінансову стабільність та репутацію.

Формування ефективної моделі корпоративного управління з урахуванням сучасних кіберзагроз є комплексним завданням, яке передбачає інтеграцію системи кіберзахисту у всі рівні управління підприємством. Концептуальні підходи до інтеграції корпоративного управління та безпеки передбачають використання інституціональних, процесних, культурних та системних інструментів. Архітектура моделі має багаторівневу структуру, що охоплює наглядовий, стратегічний, операційний і поведінковий рівні. У свою чергу, стратегічне планування та ризик-менеджмент стають ключовими механізмами забезпечення кіберстійкості підприємств.

Аналіз міжнародних стандартів, зокрема ISO/IEC 27001, NIST CSF, GDPR та NIS2, показав, що їх адаптація до національних реалій та впровадження у бізнес-середовище дозволить підвищити рівень

захисту компаній і прискорить їх інтеграцію у глобальну економіку.

Ключовими напрямами виступають інтеграція управління ризиками у корпоративні стратегії, створення спеціалізованих комітетів з інформаційної безпеки (кібербезпеки), використання KPI для оцінки ефективності та розвиток корпоративної культури безпеки. Синергія цих елементів формує нову якість корпоративного управління, здатного забезпечити стійкість бізнесу в умовах зростання кіберзагроз.

Список використаних джерел:

1. Мартинюк В. П., Литвиненко І. В. Корпоративне управління: теорія і практика : навч. посіб. Київ : КНЕУ, 2020. 312 с.
2. Сайт Організації економічного співробітництва та розвитку. URL: https://www.oecd.org/ (дата звернення: 10.09.2025).
3. Грабовський П. Д., Коваленко М. О. Інформаційна безпека та захист інформації : підручник. Харків : Фактор, 2019. 456 с.
4. Компанія Equifax зазнала збитків на суму $87,5 млн. в третьому кварталі 2017 року. URL: https://amica.ua/kompaniya-equifax-zaznala-zbytkiv-na-sumu-87-5-mln-v-tretomu-kvartali (дата звернення: 10.09.2025).
5. Злом SolarWinds: як уникнути вразливостей кіберзахисту. URL: https://techexpert.ua/solarwinds-attack-security (дата звернення: 10.09.2025).
6. Компанія Target підтвердила факт кібератак. URL: https://www.golosameriki.com/a/1829390.html (дата звернення: 10.09.2025).
7. Компанія Colonial Pipeline заплатила хакерам мільйонний викуп. URL: https://www.ukrinform.ua/rubric-world/3245081-amerikanska-colonial-pipeline-zaplatila-hakeram-miljonnij-vikup-bloomberg.html (дата звернення: 10.09.2025).
8. Комісії з цінних паперів і бірж США. URL: https://uk.wikipedia.org/wiki/Комісія_з_цінних_паперів_і_бірж_США (дата звернення: 10.09.2025).
9. National Institute of Standards and Technology (NIST). Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. Gaithersburg. MD : NIST, 2018. 55 p.
10. General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. *Official Journal of the European Union*. 2016. L 119. p. 1–88.
11. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection. *Information security management systems – Requirements*. Geneva : International Organization for Standardization, 2022. 38 p.
12. British Standards Institution. BS 7799-1:1999. *Information security management. Code of practice for information security management.* London: BSI, 1999. 58 p.
13. Measures for a high common level of cybersecurity across the Union : Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 (NIS2 Directive). *Official Journal of the European Union*. 2022. L 333. p. 80–152.
14. Звіт про цифровий захист Microsoft за 2023 рік. URL: https://www.microsoft.com/uk-ua/security/business/security-intelligence-report (дата звернення: 10.09.2025).
15. Cybersecurity – protecting what we value URL: https://www.siemens-energy.com/global/en/home/company/cybersecurity.html (дата звернення: 10.09.2025).
16. Secure by Design: від концепції до необхідності у 2025. URL: https://10guards.com/ua/blog/2025/04/18/secure-by-design-from-concept-to-cybersecurity-imperative-in-2025 (дата звернення: 10.09.2025).
17. IBM Corporation. IBM Security: Cybersecurity Risk Heat Map Methodology. Armonk, NY: IBM Security, 2023. 25 p.
18. PwC. Global Digital Trust Insights 2022. URL: https://www.pwc.com (дата звернення: 10.09.2025).
19. KPMG. Boards and Cybersecurity: A Practical Guide. URL: https://home.kpmg (дата звернення: 10.09.2025).
20. EY. Global Board Risk Survey. URL: https://www.ey.com (дата звернення: 10.09.2025).
21. ISACA. Measuring Cybersecurity Performance: Metrics and Key Performance Indicators. URL: https://www.isaca.org (дата звернення: 10.09.2025).
22. ENISA. Cybersecurity Culture in Organisations. European Union Agency for Cybersecurity. URL: https://www.enisa.europa.eu (дата звернення: 10.09.2025).
23. Accenture. State of Cybersecurity Resilience 2021. URL: https://www.accenture.com (дата звернення: 10.09.2025).

References:

1. Martyniuk V. P., Lytvynenko I. V. (2020) *Korporatyvne upravlinnia: teoriia i praktyka* [Corporate governance: theory and practice] : navch. posib. Kyiv : KNEU, 312 p. (in Ukrainian)
2. Website of the Organization for Economic Cooperation and Development. Available at: https://www.oecd.org/ (accessed 09.10.2025).
3. Hrabovskyi P. D., Kovalenko M. O. (2019) *Informatsiina bezpeka ta zakhyst informatsii* [Information security and information protection]: pidruchnyk. Kharkiv : Faktor, 456 p.
4. Kompaniia Equifax zaznala zbytkiv na sumu $87,5 mln. v tretomu kvartali 2017 roku [Equifax suffered losses of $87.5 million in the third quarter of 2017]. Available at: https://amica.ua/kompaniya-equifax-zaznala-zbytkiv-na-sumu-87-5-mln-v-tretomu-kvartali (accessed 09.10.2025).
5. Zlom SolarWinds: yak unyknuty vrazlyvostei kiberzakhystu [SolarWinds Hack: How to Avoid Cybersecurity Vulnerabilities]. Available at: https://techexpert.ua/solarwinds-attack-security (accessed 09.10.2025).

6. Kompaniia Target pidtverdyla fakt kiberatak [Target confirms cyberattack]. Available at: https://www.golosameriki.com/a/1829390.html (accessed 09.10.2025).
7. Kompaniia Colonial Pipeline zaplatyla khakeram milionnyi vykup [Colonial Pipeline paid hackers a million-dollar ransom]. Available at: https://www.ukrinform.ua/rubric-world/3245081-amerikanska-colonial-pipeline-zaplatila-hakeram-miljonnij-vikup-bloomberg.html (accessed 09.10.2025).
8. Komisiia z tsinnykh paperiv i birzh SShA [U.S. Securities and Exchange Commission]. Available at: https://uk.wikipedia.org/wiki/Комісія_з_цінних_паперів_і_бірж_США (accessed 09.10.2025).
9. National Institute of Standards and Technology (NIST) (2021). Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. Gaithersburg. MD : NIST, 2018. 55 p.
10. General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council (2016). *Official Journal of the European Union*. L 119. p. 1–88.
11. ISO/IEC 27001:2022 (2022). Information security, cybersecurity and privacy protection. *Information security management systems – Requirements*. Geneva : International Organization for Standardization, 38 p.
12. British Standards Institution. BS 7799-1:1999 (1999). *Information security management. Code of practice for information security management.* London: BSI, 58 p.
13. Measures for a high common level of cybersecurity across the Union : Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 (NIS2 Directive). (2022). *Official Journal of the European Union*. L 333. p. 80–152.
14. Zvit pro tsyfrovyi zakhyst Microsoft za 2023 rik [Microsoft Digital Security Report 2023]. Available at: https://www.microsoft.com/uk-ua/security/business/security-intelligence-report (accessed 09.10.2025).
15. Cybersecurity – protecting what we value (2025). Available at: https://www.siemens-energy.com/global/en/home/company/cybersecurity.html (accessed 09.10.2025).
16. Secure by Design (2025). Available at: https://10guards.com/ua/blog/2025/04/18/secure-by-design-from-concept-to-cybersecurity-imperative-in-2025 (accessed 09.10.2025).
17. IBM Corporation (2023). IBM Security: Cybersecurity Risk Heat Map Methodology. Armonk, NY: IBM Security, 25 p.
18. PwC (2022). Global Digital Trust Insights. Available at: https://www.pwc.com (accessed 09.10.2025)
19. KPMG (2021). Boards and Cybersecurity: A Practical Guide. Available at: https://home.kpmg (accessed: 09.10.2025)
20. EY (2022). Global Board Risk Survey. Available at: https://www.ey.com (accessed: 09.10.2025)
21. ISACA (2020). Measuring Cybersecurity Performance: Metrics and Key Performance Indicators. Available at: https://www.isaca.org (accessed 09.10.2025).
22. ENISA (2022). Cybersecurity Culture in Organisations. European Union Agency for Cybersecurity. Available at: https://www.enisa.europa.eu (accessed 09.10.2025).
23. Accenture (2021). State of Cybersecurity Resilience. Available at: https://www.accenture.com (accessed 09.10.2025).

INTERNATIONAL EXPERIENCE IN CORPORATE MANAGEMENT OF CYBERSECURITY ENTERPRISES

Summary. The article explores the essence of corporate governance transformation in the digital age and the impact of cyber threats on modern business models. Traditional approaches focused on financial control and transparency no longer meet the requirements of the globalized information environment. Currently, the key tasks of corporate governance are digital risk management, information asset protection, ensuring cyber resilience and building stakeholder trust. The classification of cyber threats is revealed: external and internal. The most dangerous forms are described in detail – financial attacks, data theft, industrial espionage and disruption of business processes. The consequences of cyber threats are outlined: direct financial losses, reputational losses, legal liability of management. The international experience of integrating cybersecurity into corporate governance is analyzed. The principle of "cyber expertise in the board of directors" and mandatory disclosure of information about cyber risks of US companies are studied. It is indicated that information security standards play a key role in EU companies. An analysis of the practice of leading international corporations led to the conclusion that cybersecurity is considered a strategic priority integrated into all levels of management. An architectural model of corporate governance taking into account digital risks is proposed, which covers the supervisory, strategic, operational and behavioral levels, as well as interaction with the external environment. It is based on institutional, process, cultural and systemic approaches. It is concluded that an effective corporate governance model in the digital age is impossible without the integration of international standards, the development of a corporate cybersecurity culture and the harmonization of national legislation with European practices. It was concluded that adapting the international standards ISO/IEC 27001, NIST CSF, GDPR, and NIS2 to national realities and their implementation in the business environment will increase the level of protection of companies and accelerate their integration into the global economy.

Keywords: strategic management, corporate governance, information security, competitive advantages of enterprises, enterprise development strategy, enterprise digitalization, business informatization, corporate security, business process automation, innovation, sustainable development.

Стаття надійшла: 06.08.2025
Стаття прийнята: 11.09.2025
Стаття опублікована: 30.09.2025