Міністерство освіти і науки України
Західноукраїнський національний університет
Навчально-науковий інститут міжнародних відносин
ім. Б. Д. Гаврилишина
Кафедра міжнародних економічних відносин

ОЛИВКО Максим Васильович

Інформаційна безпека та кіберзагрози у міжнародному менеджменті

спеціальність 073-Менеджмент
освітньо-професійна програма Міжнародний менеджмент
кваліфікаційна робота за освітнім ступенем «бакалавр»

Виконав студент
групи МЕНМ-41
Оливко М.В.
_____
підпис

Науковий керівник:
к.е.н., доцент
Сохацький О.Ю.
_____
підпис

Кваліфікаційну роботу
Допущено до захисту
«__»_____20___р.
Завідувач кафедри
_____
підпис

Тернопіль - 2025

ЗМІСТ

ВСТУП

У сучасному глобалізованому світі кіберпростір став не лише платформою для комунікації, інновацій та економічного розвитку, але й ареною для новітніх загроз і конфліктів. В умовах цифрової трансформації та стрімкого впровадження інформаційно-комунікаційних технологій особливої актуальності набуває проблема забезпечення інформаційної безпеки. Для міжнародного менеджменту, який оперує в мультикультурному, правовому та технологічному середовищі, загрози кібербезпеки мають особливо вагомий вплив, оскільки порушення конфіденційності, цілісності чи доступності інформації може призвести до глобальних криз, фінансових втрат, порушення репутації та стратегічної нестабільності бізнесу.

Метою даної бакалаврської роботи є комплексне дослідження інформаційної безпеки як ключового елемента міжнародного менеджменту, аналіз основних кіберзагроз, з якими стикаються транснаціональні компанії, а також оцінка підходів до управління ризиками в кіберсфері на стратегічному рівні.

Об’єктом дослідження виступають процеси забезпечення кібербезпеки в діяльності міжнародних компаній. Предметом – системи менеджменту інформаційної безпеки, нормативно-правові та організаційні засади протидії кіберзагрозам у глобальному корпоративному середовищі.

Актуальність теми зумовлена зростанням інтенсивності кібератак, поширенням гібридних загроз, включаючи шкідливе програмне забезпечення, фішинг, соціальну інженерію, інсайдерські атаки, а також викликами, пов’язаними з віддаленою роботою, хмарними інфраструктурами та міжнаціональними регуляторними розбіжностями. Сучасні реалії потребують розробки гнучких, багаторівневих систем захисту, інтегрованих у загальну стратегію міжнародного управління.

Практична значущість дослідження полягає в можливості використання сформульованих висновків і рекомендацій для вдосконалення політик

інформаційної безпеки, оптимізації процедур реагування на інциденти та формування стійкої корпоративної культури безпеки.

Робота складається з трьох розділів: у першому висвітлено теоретико-методологічні засади інформаційної безпеки в міжнародному менеджменті; у другому – проаналізовано сучасні виклики, загрози й вразливості цифрового середовища в транснаціональному бізнесі; третій розділ присвячено механізмам протидії кіберризикам, стандартам, інституційним практикам і стратегічному управлінню безпекою в міжнародних компаніях.

РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В МІЖНАРОДНОМУ МЕНЕДЖМЕНТІ

1.1. Сутність та концепція інформаційної безпеки у сфері міжнародного бізнесу

У XXI столітті інформація перетворилася на ключовий ресурс для міжнародних компаній, порівняний за цінністю з фінансовими активами чи матеріальними ресурсами. З огляду на це, забезпечення інформаційної безпеки стало не лише технічною функцією IT-відділів, а стратегічним завданням керівництва. Інформаційна безпека в міжнародному менеджменті — це комплексна система захисту даних, процесів та інфраструктури компанії від внутрішніх і зовнішніх загроз у глобальному цифровому середовищі.

Відповідно до міжнародного стандарту ISO/IEC 27000:2018, інформаційна безпека трактується як збереження конфіденційності, цілісності та доступності інформації. Водночас, міжнародний бізнес функціонує у різних правових системах, підпорядковується нормам різних країн та міжнародних угод, а також стикається з транснаціональними ризиками, що значно ускладнює реалізацію політик кіберзахисту [2].

Ризики в інформаційній сфері поділяються на цілеспрямовані та випадкові**,** технічні та поведінкові**,** зовнішні та внутрішні**.** Це зумовлює необхідність створення багаторівневої системи безпеки, що охоплює:

- цифрові активи (сервери, бази даних, CRM-системи);
- людський капітал (персонал, корпоративну культуру);
- правові інструменти (політики доступу, договори про конфіденційність);
- управлінські підходи (ризик-менеджмент, сценарне планування).

У сучасному глобалізованому бізнес-середовищі інформаційна безпека є одним із визначальних чинників стабільного функціонування міжнародних

компаній. Поширення цифрових технологій, інтеграція хмарних рішень, глобальні ланцюги постачання та віддалена робота зумовили новий рівень уразливості корпоративних інформаційних систем. В умовах геополітичної нестабільності та економічної турбулентності, загрози інформаційній інфраструктурі стали інструментами впливу у конкурентній та міждержавній боротьбі [1, с. 89].

Із розвитком цифрової економіки компанії дедалі частіше стикаються з асиметричними загрозами, які не мають фізичних проявів, проте можуть спричинити значні фінансові та репутаційні втрати. Наприклад, у 2023 році середній розмір збитків від кібератак, за оцінками IBM, перевищив 4,45 млн дол. США [3]. Це зумовлює необхідність системного підходу до кіберзахисту в межах стратегічного менеджменту компанії.

Загалом інформаційні загрози у міжнародному бізнесі класифікуються залежно від джерела походження (внутрішні/зовнішні), рівня технологічної складності, наміру порушника та цільового об’єкта атаки. У таблиці 1 наведено типовий поділ загроз, що найчастіше трапляються у транснаціональних корпораціях.

Таблиця 1

Типи інформаційних загроз у міжнародному менеджменті

№	Тип загрози	Опис
1	Фішинг-атаки	Обман з метою отримання логінів/паролів або фінансової інформації
2	Шкідливе ПЗ (ransomware, spyware)	Програмне забезпечення, що блокує або шпигує за системами
3	DDoS-атаки	Перевантаження серверів для виведення з ладу
4	Витік корпоративних даних	Несанкціоноване розголошення конфіденційної інформації
5	Внутрішні загрози (інсайдери)	Помилки або зловмисні дії співробітників або підрядників
6	Компрометація бізнес-комунікацій (BEC)	Шахрайство через підроблені листи, платіжні інструкції

Джерело: складено автором на основі [1–3]

У звіті *CyberEdge Group* зазначено, що 89% компаній стикалися з фішингом, 78% – зі шкідливим ПЗ, а 62% – з витоком даних. Зазначені атаки

впливають на безперервність бізнесу, змушують компанії оновлювати політики безпеки та інвестувати у хмарні технології з вбудованими механізмами самозахисту.

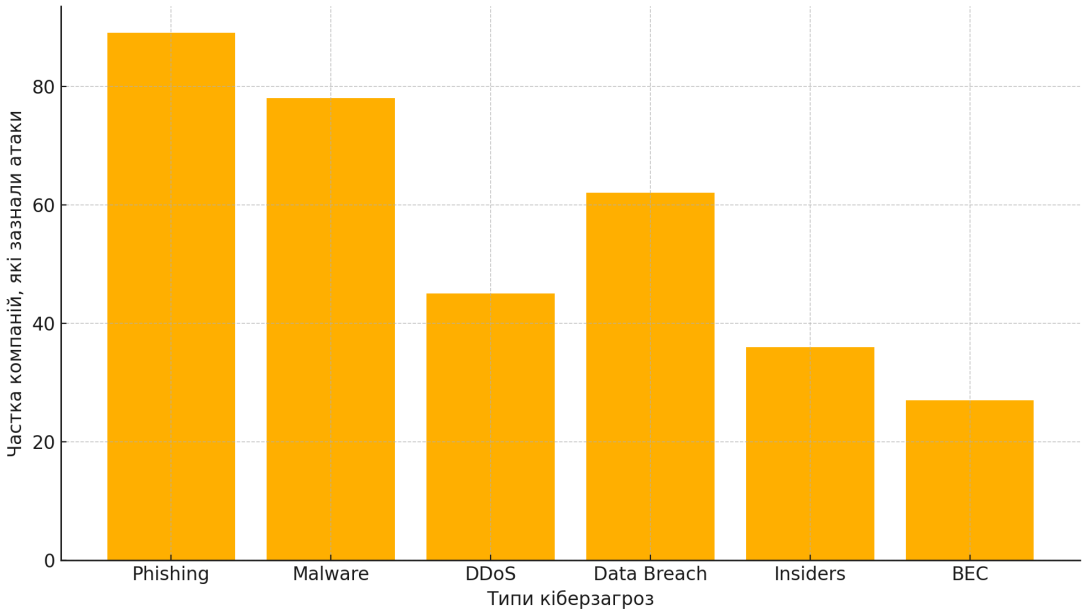

Рис 1.1 – Поширеність основних типів кіберзагроз у міжнародному менеджменті, %. *Джерело: побудовано автором за даними CyberEdge Group, 2023 [4]*

Сучасний міжнародний менеджмент зобов'язаний інтегрувати інформаційну безпеку як елемент стратегічного управління, що охоплює не лише IT-інфраструктуру, але й організаційні процеси, людський фактор, а також регуляторну відповідність до вимог GDPR, ISO/IEC, NIST тощо. Забезпечення кіберстійкості є не лише технічним, а й культурним та політичним викликом у глобальному середовищі.

З рис. 1 видно, що фішинг залишається наймасовішим типом загроз, проте DDoS-атаки, які зазвичай асоціюються з конкурентною боротьбою чи геополітичними конфліктами, мають системний характер. Наприклад, у 2022–2023 роках зросла кількість кібератак на логістичні компанії, що підтримували Україну, як частина гібридної війни (зокрема, DDoS на Maersk та A.P. Moller) [5].

Фінансові установи та хмарні платформи, зазвичай, зазнають комбінованих атак – спочатку соціальна інженерія, потім експлуатація

вразливостей у системах, далі витік та шифрування даних. Системи CRM, ERP та SCADA — найбільш вразливі точки у виробничих і логістичних міжнародних компаніях.

Компанії, що мають філії у різних країнах, часто стикаються з невідповідністю між локальними законами і глобальними політиками кібербезпеки. Це створює сірі зони відповідальності та підвищує ймовірність кіберінцидентів у разі слабкої міжфіліальної координації.

Інша загрозлива тенденція — це масова експлуатація людського чинника. Статистика показує, що понад 80% витоків даних спричинені діями працівників, через погану підготовку або навмисне порушення політик [6]. Таким чином, інвестиції лише в технічні засоби (антивіруси, фаєрволи, VPN) без належного навчання персоналу — малоефективні.

1.2. Види та джерела сучасних кіберзагроз у міжнародному бізнесі

Інформаційна безпека міжнародних компаній сьогодні перебуває під безпрецедентним тиском із боку складних, цілеспрямованих і часто добре фінансованих загроз. З огляду на активне використання цифрових технологій у менеджменті, транснаціональні компанії опинилися в середовищі, де кіберзагрози перетворилися на системні та стратегічні ризики, що впливають на стійкість бізнес-моделей, довіру клієнтів, дотримання регуляторних норм та фінансову безпеку [7].

Види загроз у сфері міжнародного бізнесу класифікують не лише за технічними параметрами (тип шкідливого ПЗ, канал атаки), але й за цільовими об’єктами, тривалістю впливу, джерелами походження та юридичними наслідками. Водночас важливо враховувати контекст — міжнародна компанія зазвичай працює у декількох країнах, має сотні партнерів і філій, що створює складну й багаторівневу поверхню атаки.

Серед найпоширеніших видів кіберзагроз, які реєструють незалежні IT-центри, виділяють:

- Ransomware-атаки – шифрування даних із вимогою викупу;
- Zero-day вразливості – атаки на ще не оновлені компоненти системи;
- Фішинг і BEC – інструменти соціальної інженерії;
- DDoS-атаки – виведення з ладу серверів;
- Supply Chain Attacks – атаки через підрядників або API.

Зміна акценту з технічного порушення на цілеспрямований стратегічний вплив є показовою для останнього десятиліття. Наприклад, під час атаки на SolarWinds (2020) постраждали щонайменше 18 000 клієнтів компанії [8].

Таблиця 1.2

Основні джерела кіберзагроз у міжнародному середовищі

№	Джерело загроз	Характер впливу
1	Кіберзлочинні угруповання	Фінансове шахрайство, шифрування даних, продаж доступів
2	Державні структури (APT-групи)	Геополітична розвідка, порушення критичної інфраструктури
3	Внутрішні працівники (інсайдери)	Зумисні або випадкові витоки, саботаж, викрадення даних
4	Партнери та підрядники	Недотримання політик безпеки, випадкове зараження систем
5	Активісти (Hacktivists)	Протестні атаки, дефейс сайтів, DDoS проти урядових структур
6	Автоматизовані боти/сканери	Масове сканування вразливостей, автоматичні атаки на API

Джерело: створено автором на основі [8]

Як показано в таблиці 2, основними джерелами загроз є:

- Кіберзлочинні угруповання;
- Державні APT-групи;
- Інсайдери;
- Партнери та підрядники;
- Хактивісти та автоматизовані сканери.

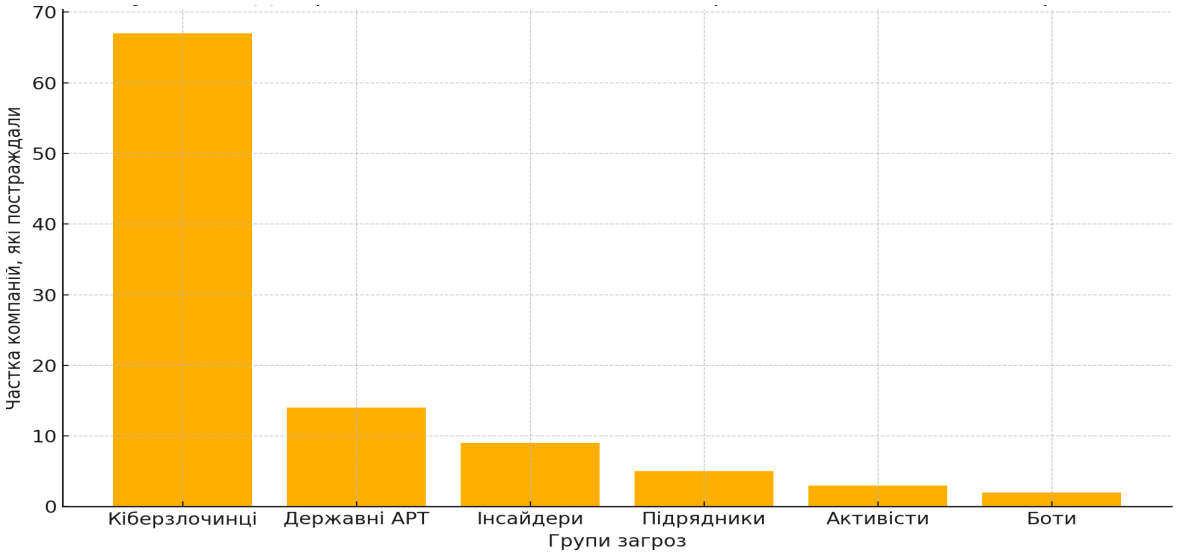

Рисунок 1.2 – Джерела найбільшої шкоди кібербезпеці за 2020–2023 роки, % *Джерело: побудовано автором за даними IBM, ENISA, Verizon [9]*

Рисунок 1.2 демонструє, що основна частина руйнівних атак походить саме від кримінальних структур (67%). APT-групи використовуються як інструмент гібридної війни — приклади атак на урядові сайти України, Польщі, енергетичні системи США, Німеччини, Ізраїлю тощо [10].

Інсайдери, хоча й менш чисельні, залишаються однією з найнебезпечніших категорій. За даними Verizon DBIR (2023), 20% усіх витоків персональних даних були спричинені діями працівників [11].

Також небезпечними є «ланцюгові» атаки, в яких хакери спочатку проникають до підрядників або партнерів компанії, а звідти – до основної IT-інфраструктури. Наприклад, атака на сервіс Kaseya (2021) вразила понад 1500 клієнтів [12].

Міжнародні компанії стикаються не з одиничними кібератаками, а з мультирівневими загрозами, які змінюються залежно від сфери діяльності, регіону та політичної ситуації. Успішне управління інформаційною безпекою вимагає не лише технічної підготовки, а й глибокого розуміння геополітики, регуляторних вимог і здатності швидко адаптуватися до нових викликів.

1.3. Кібербезпека як складова стратегії корпоративного управління

У сучасному міжнародному менеджменті кібербезпека набуває системного значення не як окремий технічний елемент, а як інтегрована частина стратегічного управління. Вона впливає не лише на IT-інфраструктуру, а й на корпоративну репутацію, відповідність правовим нормам, доступ до міжнародних ринків капіталу, готовність до форс-мажорів і кризової стійкості. Компанії, які не мають чітко вибудуваної стратегії інформаційної безпеки, фактично перебувають у стані постійної вразливості до зовнішніх і внутрішніх загроз [13].

Кіберстратегія – це сукупність процедур, регламентів і інструментів, що вбудовані в загальну структуру управління ризиками компанії. Вона охоплює: ідентифікацію загроз, оцінку ймовірності інцидентів, розробку плану реагування, постійне тестування слабких місць, інвестиції в сучасні системи захисту, розробку планів з безперервності діяльності (BCP) та регулярне навчання персоналу. Відомі міжнародні фреймворки, що підтримують розробку кіберстратегії:

- NIST Cybersecurity Framework (США) – 5 функцій: Identify, Protect, Detect, Respond, Recover;
- ISO/IEC 27001:2022 – міжнародна система управління інформаційною безпекою (ISMS);
- CIS Controls – набір рекомендацій для малих і середніх підприємств;
- GDPR, NIS2 – регуляторні норми ЄС [14].

Таблиця 1.3

Ключові компоненти стратегії кібербезпеки в міжнародному менеджменті

№	Компонент стратегії	Короткий опис
1	Інвентаризація цифрових активів	Формування реєстру критичних систем, даних, платформ і хмарних сервісів
2	Оцінка ризиків та зон вразливості	Використання фреймворків NIST, ISO для аналізу слабких місць та пріоритетів

3	Регламентація політик доступу	Створення ролей доступу, аутентифікації, моніторинг сесій
4	Реагування на інциденти (CSIRT)	Створення внутрішньої групи реагування на кібератаки та аналіз логів
5	Навчання персоналу та симуляції	Регулярні тренінги, атаки-симуляції (red team), валідація політик
6	Регуляторна відповідність	Впровадження вимог міжнародного та локального законодавства

Джерело: виконано автором на основі [11]

Як свідчить практика, ефективна стратегія кібербезпеки має охоплювати не лише технологічні аспекти (firewall, IDS/IPS, шифрування), але й управлінські. Згідно з результатами глобального опитування серед CIO/CISO, основними пріоритетами виявилися: навчання персоналу (82%), оцінка ризиків (74%), тестування систем (68%) [15].

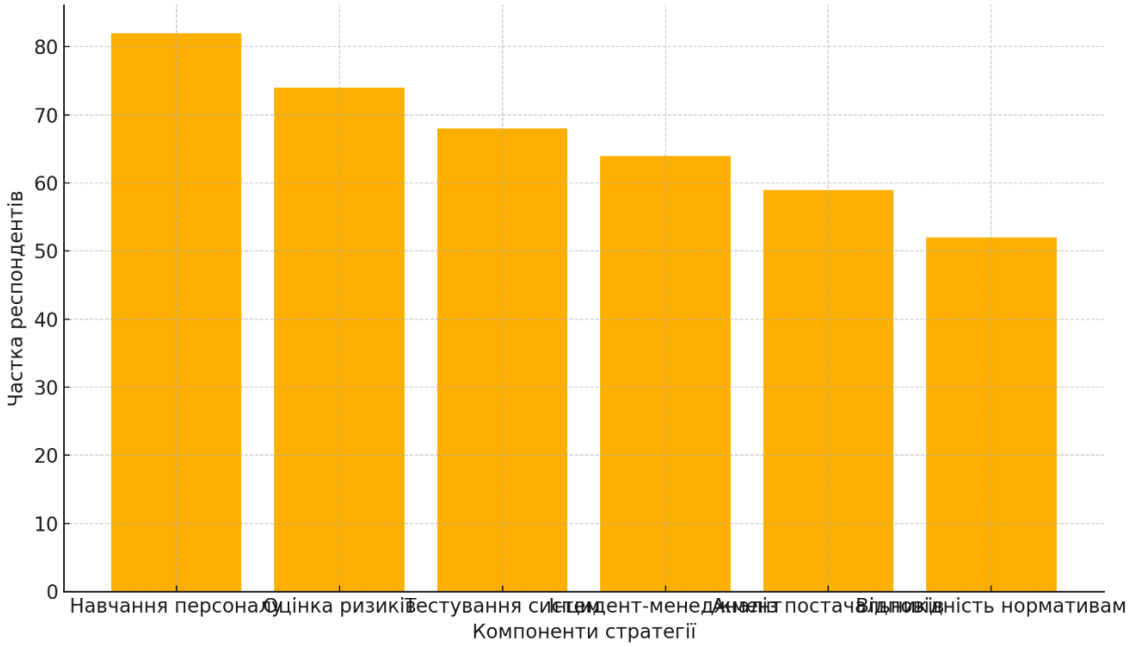

Рисунок 3 – Пріоритети в реалізації стратегії кібербезпеки за опитуванням CIO, % *Джерело: побудовано автором за даними PwC, Deloitte, IBM [15]*

Аналітичний коментар. Рисунок 3 ілюструє, що ключовим викликом у реалізації стратегії є людський чинник. Попри наявність технічних засобів захисту, близько 70% витоків пов’язані з діями персоналу – несвоєчасне оновлення, ігнорування інструкцій, слабкі паролі. Таким чином, навчання персоналу та розробка внутрішніх інструкцій є критично важливими заходами [16]. Сучасна корпоративна культура має передбачати не лише технічну

грамотність, але й створення мотиваційного середовища для дотримання політик безпеки – від керівництва до рядового працівника.

Водночас системна недооцінка аналізу кіберризиків постачальників (59%) створює вразливості в логістичних ланцюгах. Типовими прикладами є атаки через скомпрометовані API, зовнішніх консультантів, платформи зберігання даних. Інциденти типу Kaseya (2021) або MOVEit (2023) довели, що слабка ланка часто знаходиться поза периметром безпеки основної компанії [17]. У цьому контексті особливої уваги потребують B2B-взаємодії з компаніями, які не підпадають під жорстке регулювання – саме вони можуть стати «входом» для атаки на більших гравців.

У сучасних корпораціях кібербезпека дедалі частіше виводиться на рівень ради директорів. Розробляються KPI: середній час виявлення загроз (MTTD), реагування (MTTR), відсоток успішних фішинг-симуляцій, швидкість патч-менеджменту, частка систем, що відповідають вимогам комплаєнсу. У компанії Nestlé, наприклад, впроваджено щорічний аудит ISMS згідно з ISO/IEC 27001 та незалежне оцінювання від Ernst & Young [18]. Подібні практики дедалі частіше вимагаються і міжнародними партнерами при укладанні контрактів, особливо у високоризикових галузях (фармацевтика, оборонна промисловість, фінансові сервіси).

Стратегія кібербезпеки є не просто технічним пакетом заходів, а частиною загального стратегічного управління. Вона має забезпечити адаптивність, відповідність міжнародним стандартам і стійкість до нових ризиків у глобальному цифровому середовищі. Її реалізація вимагає лідерства, постійного моніторингу загроз, розвитку людського капіталу та інвестицій у цифрову культуру безпеки.

РОЗДІЛ 2. АНАЛІЗ СТАНУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В МІЖНАРОДНИХ КОМПАНІЯХ

2.1. Основні типи атак на корпоративні інформаційні системи

Корпоративні інформаційні системи є ключовою мішенню для кіберзловмисників у глобальному бізнес-середовищі. Ці системи містять конфіденційну інформацію, критичні бізнес-процеси, платіжні дані, комунікаційну інфраструктуру та доступ до партнерських платформ. Уразливість хоча б одного компонента IT-архітектури здатна спричинити фінансові, репутаційні та юридичні наслідки міжнародного масштабу [19].

Загалом атаки на корпоративні системи класифікуються за цілями, механізмом проникнення, тривалістю дії, масштабом впливу та джерелом походження. Найбільш поширеними типами є:

- **Ransomware (шифрувальне ПЗ)** — блокує доступ до даних і вимагає викуп за розшифрування. Наприклад, атака на Colonial Pipeline у 2021 році призвела до зупинки стратегічної інфраструктури в США [20].
- **Phishing / Spear Phishing** — атаки через підроблені листи або повідомлення, спрямовані на отримання облікових даних. Особливо небезпечні в транснаціональних компаніях з великим штатом працівників, де складно забезпечити уніфіковану політику верифікації.
- **DDoS (Distributed Denial of Service)** — масове перевантаження серверів, що призводить до відмови в обслуговуванні (часто використовується у сфері цифрової конкуренції чи політичного тиску). DDoS-атаки дедалі частіше координуються через бот-мережі, які використовують заражені IoT-пристрої.
- **Zero-day Exploits** — використання ще не виявлених або не оновлених вразливостей у програмному забезпеченні. Найбільш ризикованими є атаки через офісні додатки, SCADA-системи та промислові контролери.

- **Business Email Compromise (BEC)** — компрометація офіційної корпоративної переписки з метою отримання доступу до платіжних доручень, контрактів або банківських даних. За статистикою, в середньому компанія втрачає понад 120 тис. дол. США на одну успішну атаку BEC [21].
- **Supply Chain Attacks** — проникнення в основну компанію через слабо захищеного постачальника або підрядника. Відомим прикладом є інцидент SolarWinds, що уразив тисячі організацій у 2020 році [21].

Особливу загрозу становлять **комбіновані атаки**, що поєднують фішинг, зловмисне ПЗ та соціальну інженерію. Такі методи найчастіше використовуються проти компаній, що працюють у фінансовому, оборонному, енергетичному секторах. У деяких випадках застосовуються цілі сценарії — багатоступеневе проникнення з початковим скаутингом, заміною доменів, перехопленням трафіку та симуляцією внутрішньої корпоративної пошти.

Таблиця 2.1

Класифікація основних типів атак на корпоративні IT-системи

№	Тип атаки	Механізм дії та ціль	Галузі підвищеного ризику
1	Ransomware	Блокування даних, шифрування, вимога викупу	Логістика, промисловість, медицина
2	Phishing / Spear Phishing	Викрадення облікових даних через e-mail	Банки, страхування, держсектор
3	DDoS	Перевантаження серверів з виведенням з ладу	Онлайн-комерція, хмарні сервіси
4	Zero-day Exploits	Використання невідомих вразливостей	Телеком, виробництво, IoT-сервіси
5	Business Email Compromise	Зміна платіжних реквізитів, шахрайство	B2B-контракти, юриспруденція
6	Supply Chain Attacks	Проникнення через сторонній підрядник	ERP/CRM-системи, державні контракти

Джерело: складено автором за [19–21]

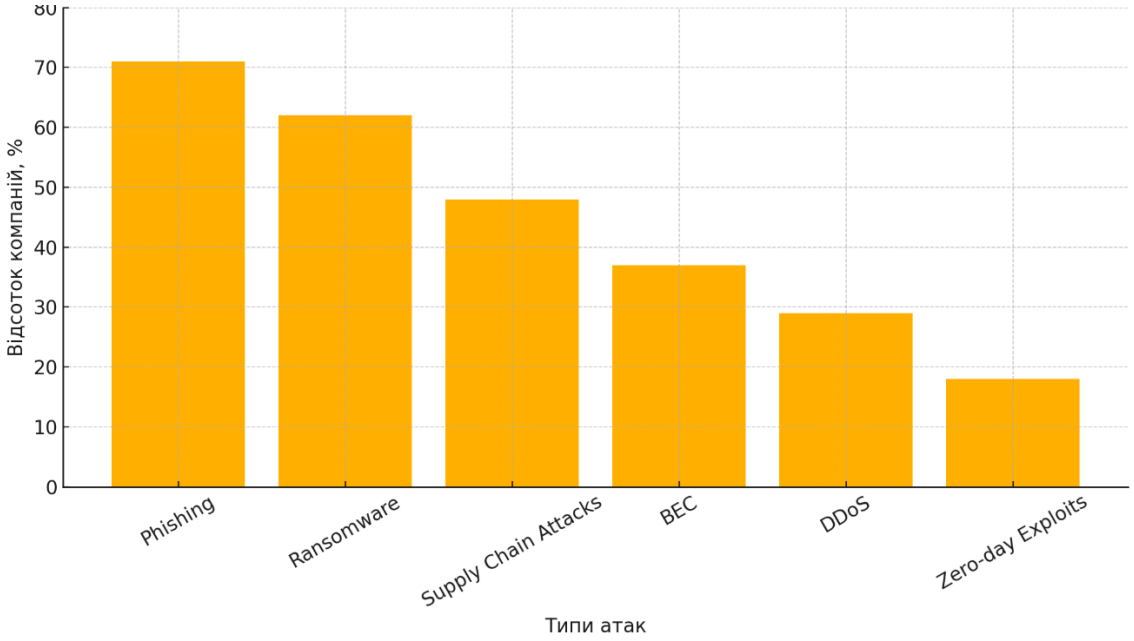

Рисунок 2.1 – Частка компаній, які зазнали різних типів атак у 2022–2023 рр., % *Джерело: побудовано автором за даними CrowdStrike, IBM, ENISA [22]*

Аналіз графіку показує, що у 2022–2023 роках найпоширенішими були фішинг (71%), атаки типу ransomware (62%) та інциденти в ланцюгах постачання (48%). При цьому DDoS-атаки були зафіксовані здебільшого як супровід основного інциденту, а не як самостійний інструмент. Це свідчить про зміну тактики: атаки стають більш прихованими, тривалими та інтелектуально керованими.

Реагування на загрози вимагає не лише технічної готовності, а й розбудови процедурної та юридичної відповідальності: хто і як повідомляє про інцидент, які дії є дозволеними для локалізації, як підтримується зв’язок із партнерами та регуляторами. Особливо актуальним є впровадження механізмів відновлення довіри після атаки — публічні звіти, зовнішні аудити, компенсації клієнтам.

Крім того, важливо впроваджувати тестування на проникнення (penetration testing) та створення внутрішніх груп «червоних команд» (red teams), які імітують поведінку реального зловмисника в корпоративній мережі. Це дозволяє виявити приховані вразливості до того, як ними скористаються хакери. Аналіз типів атак на корпоративні системи свідчить про необхідність системного й проактивного підходу до кіберзахисту. Сучасні загрози змінюються швидше, ніж

традиційні моделі захисту. Тому компанії повинні не лише інвестувати в технології, а й переглядати процеси взаємодії всередині організації, формувати культуру кібербезпеки, проводити регулярні тренінги та перевірки. Ефективне управління кіберризиками забезпечує не лише стабільність роботи, а й формує довіру з боку міжнародних партнерів, інвесторів і споживачів.

2.2. Вразливості корпоративної IT-інфраструктури

Однією з ключових проблем захисту інформаційної безпеки в міжнародному менеджменті є вразливості корпоративної IT-інфраструктури, які створюють передумови для кіберінцидентів. Ці вразливості мають багатошарову природу та стосуються як технічних, так і організаційних аспектів функціонування компаній. У глобальному контексті ці недоліки особливо критичні для транснаціональних корпорацій, які оперують у різних юрисдикціях з неоднаковими рівнями регуляції та цифрової зрілості. Основні категорії вразливостей включають:

- **Програмні вразливості** — помилки у програмному коді, ненадійні оновлення, відсутність патчів. Згідно з даними NIST, понад 24% атак у 2023 році були зумовлені неоновленим ПЗ [23].
- **Конфігураційні вразливості** — неправильні налаштування мережевого обладнання, хмарних платформ чи міжмережевих екранів (firewalls). Особливо часто це трапляється у середовищах, де облікові записи адміністраторів не мають обмежень доступу.
- **Людський фактор** — низький рівень цифрової гігієни, слабкі паролі, нехтування протоколами багатофакторної автентифікації. У доповіді IBM зазначено, що 95% усіх інцидентів мали людське походження [24].
- **Складність IT-архітектури** — численні інтегровані модулі, відсутність централізованого моніторингу, використання різнотипного обладнання у філіях. Це ускладнює своєчасне виявлення загроз та кореляцію подій у SIEM-системах.

- **Слабкий захист кінцевих точок (endpoints)** — неоновлені антивіруси, відсутність контролю USB-пристроїв, використання незахищених особистих ноутбуків для роботи у віддаленому режимі.

Таблиця 2.2

Основні категорії вразливостей в IT-інфраструктурі компаній

№	Категорія вразливості	Опис проблеми та наслідки	Частка в загальній кількості інцидентів, %
1	Програмні	Неоновлене ПЗ, застарілі бібліотеки	24
2	Конфігураційні	Недбалі налаштування мереж та firewall	18
3	Людський фактор	Фішинг, слабкі паролі, ігнорування MFA	27
4	Складна архітектура	Розподілені системи без централізованого захисту	15
5	Захист кінцевих точок	Відсутність контролю USB та AV	16

Джерело: складено автором за даними NIST, IBM, ENISA [23–25]

Згідно з аналітичними звітами провідних аналітичних центрів, таких як ISACA та Forrester, ризики, пов’язані з вразливостями інфраструктури, зростають на фоні глобального тренду діджиталізації та переходу на віддалені формати роботи. Зокрема, лише за 2023 рік кількість інцидентів, пов’язаних з незахищеними хмарними середовищами, зросла на 32% порівняно з попереднім роком. Цей тренд є характерним як для малих підприємств, що лише починають впровадження цифрових рішень, так і для міжнародних корпорацій, які керують розгалуженою IT-інфраструктурою на кількох континентах.

Одним із стратегічних інструментів зменшення вразливостей є Zero Trust Architecture (ZTA) — концепція, за якої жоден пристрій або користувач не вважається надійним за замовчуванням. Це дозволяє забезпечити мікросегментацію мережі, динамічне виявлення аномалій, автоматичне відключення підозрілих сесій. Компанії, які впровадили ZTA, у середньому на 48% швидше реагують на інциденти безпеки та демонструють нижчі втрати даних у порівнянні з традиційними підходами. Особливо ефективною ця модель є для організацій з високим рівнем регуляторного нагляду, таких як банківська сфера, охорона здоров’я та оборонна промисловість.

Також зростає роль інструментів безперервного сканування вразливостей (CVMS), які інтегруються в DevOps-процеси та дозволяють виявляти загрози ще на етапі розробки ПЗ. Наприклад, у середовищах AWS чи Azure можна налаштувати автоматичне сповіщення про критичні вразливості зі сторонніх джерел (наприклад, CVE). Такий підхід є ключовим у скороченні «часу до виправлення» (time-to-fix) та підвищенні адаптивності IT-екосистеми. Встановлення «сенсорних точок» у критичних вузлах дозволяє в режимі реального часу фіксувати аномальну поведінку, автоматизувати формування звітів та запобігати повторному виникненню інцидентів.

Окрім технічних рішень, важливою є побудова інституційної культури безпеки, коли кожен працівник розуміє свою роль у підтриманні кіберстійкості. Це включає регулярні тренінги, політику «без винятків», оновлення регламентів відповідно до NIST Cybersecurity Framework. Особливу роль у цьому відіграє CISO (Chief Information Security Officer), який координує політики захисту на глобальному рівні. Створення локальних груп реагування на інциденти (Incident Response Teams) у кожному підрозділі дозволяє пришвидшити локалізацію загроз і мінімізувати шкоду.

Загалом, побудова стійкої корпоративної IT-інфраструктури вимагає поєднання технічних, організаційних та кадрових рішень. Без системного підходу до виявлення і усунення вразливостей компанії ризикують втратити конкурентоспроможність і довіру партнерів у міжнародному середовищі. Особливо небезпечним є нехтування заходами безпеки в періоди злиття чи придбання компаній (M&A), коли інфраструктура інтегрується без повної перевірки відповідності політик безпеки. Саме в такі моменти зловмисники можуть скористатися «тимчасовими вікнами» в захисті.

2.3. Оцінка ризиків і вразливостей у міжнародному менеджменті

Ефективне управління інформаційною безпекою в системі міжнародного менеджменту неможливе без належної оцінки ризиків та ідентифікації

вразливостей. У транснаціональних компаніях ці процеси потребують урахування багатьох чинників — геополітичного контексту, регуляторного середовища, розподіленої IT-архітектури та міжкультурних відмінностей в управлінні інцидентами. Сучасний ризик-менеджмент у сфері кібербезпеки має виходити за межі класичних сценаріїв і опиратися на інтегровані моделі оцінювання.

Натомість традиційний підхід до управління ризиками — з використанням простих контрольних списків і реагування post-factum — більше не є ефективним в умовах глобалізованої економіки. Нові типи загроз, такі як supply chain attacks, deepfake-based frauds або атакувальні моделі на базі штучного інтелекту, змушують компанії переглядати підходи до ідентифікації вразливих місць. Крім технічного компонента, зростає значення культурних та управлінських ризиків — наприклад, ситуацій, коли співробітники з різних країн мають різне уявлення про етику поводження з даними або протокол реагування на інцидент.

Інтегровані моделі оцінки ризиків (наприклад, методологія FAIR — Factor Analysis of Information Risk) дозволяють кількісно виразити ризик у грошовому еквіваленті, що полегшує обґрунтування інвестицій у безпеку для керівництва компанії. Наприклад, в одній зі світових FMCG-корпорацій упровадження моделі FAIR дозволило скоротити витрати на кіберстрахування на 17%, оскільки компанія змогла чітко аргументувати реальний рівень захищеності ключових процесів.

Для ефективної оцінки ризиків також доцільно впроваджувати інструменти сценарного аналізу та статистичне моделювання на базі машинного навчання. Наприклад, побудова моделей класифікації інцидентів дозволяє виявити закономірності в поведінці атакувальних бот-мереж, а прогнозні моделі впливу (impact simulation) — змоделювати наслідки успішного злому хмарної CRM-системи. Такі підходи вже впроваджуються в транснаціональних компаніях (SAP, Siemens, Cisco), що мають глобальні центри кібераналітики.

Таблиця 2.4

Етапи процесу оцінювання ризиків в міжнародному менеджменті

Етап	Назва етапу	Опис процесу
1	Ідентифікація активів	Визначення ресурсів, що потребують захисту
2	Виявлення загроз	Аналіз потенційних сценаріїв атак та типів порушників
3	Визначення вразливостей	Аудит систем, виявлення конфігураційних, технічних і людських вад
4	Оцінювання наслідків	Прогноз фінансових та операційних втрат у разі інциденту
5	Пріоритезація	Побудова карти ризиків, визначення критичних напрямів реагування

Джерело: систематизовано автором на основі ISO/IEC 27005:2022, NIST RMF, FAIR Framework [26–28]

Як показано на рисунку 6, процес оцінювання кіберризиків у міжнародних компаніях має послідовну логіку: від ідентифікації активів до пріоритезації заходів реагування. Цей підхід дозволяє адаптувати механізми оцінювання до мультикультурного середовища, де одна і та ж загроза може мати різний пріоритет залежно від регіону. Наприклад, у країнах з жорстким законодавством щодо конфіденційності даних (наприклад, Німеччина чи Південна Корея) вразливості, пов’язані з персональними даними, отримують вищий рівень пріоритету, ніж у юрисдикціях із менш суворими нормами.

Крім того, візуалізація етапів у вигляді циклічної схеми або графа дозволяє ефективно комунікувати ризики не лише між IT-фахівцями, а й з керівництвом компанії, не технічними підрозділами та зовнішніми стейкхолдерами. Це особливо актуально у великих холдингах і корпораціях, де управління ризиками інтегрується в систему корпоративного управління ESG (Environmental, Social, Governance).

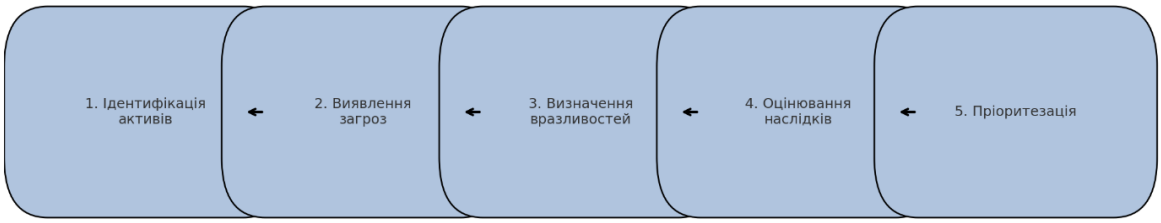

Рисунок 2.3 Ключові етапи оцінювання кіберризиків у міжнародних компаніях. Побудовано автором на основі FAIR Institute, 2023 [27]

Важливо також враховувати контекст міжнародного менеджменту, де до ризиків кібербезпеки додаються такі чинники, як політична нестабільність у країнах присутності, ризики інсайдерів серед локального персоналу, складність дотримання локального законодавства з передачі персональних даних. Такі фактори потребують використання крос-національних сценаріїв ризиків, у тому числі з урахуванням постійного моніторингу геополітичної обстановки.

Ключовим є також постійний перегляд ризиків — не рідше ніж щоквартально, із залученням представників IT, правового департаменту, служби безпеки та операційних підрозділів. Це дозволяє не лише підтримувати актуальність карти ризиків, але й своєчасно адаптувати плани реагування.

Таким чином, комплексна оцінка ризиків у міжнародному менеджменті є основою для розробки ефективної кіберстратегії. Вона дозволяє не лише мінімізувати ймовірність інцидентів, але й забезпечити довіру інвесторів, відповідність міжнародним стандартам і безперервність бізнесу навіть у кризових умовах.

РОЗДІЛ 3. ШЛЯХИ ПІДВИЩЕННЯ РІВНЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У МІЖНАРОДНОМУ МЕНЕДЖМЕНТІ

3.1. Стратегії забезпечення інформаційної безпеки в міжнародному менеджменті

Ефективне функціонування міжнародних компаній у цифрову епоху вимагає цілісного стратегічного підходу до захисту інформаційних активів. З огляду на зростання масштабів кіберзагроз, особливо в умовах геополітичної нестабільності, керівники компаній дедалі частіше розглядають інформаційну безпеку як один з ключових пріоритетів корпоративної стратегії. У цьому контексті важливо формувати адаптивні стратегії, що поєднують технологічні, організаційні й культурні аспекти.

Однією з базових стратегій є застосування моделі Zero Trust Architecture (ZTA), яка базується на принципі «нікому не довіряй, завжди перевіряй». Цей підхід передбачає постійну перевірку автентичності користувачів і пристроїв, незалежно від їхнього розташування. У транснаціональних компаніях із децентралізованою інфраструктурою ZTA дозволяє ефективно контролювати доступ до критичних ресурсів навіть за умов роботи з віддалених регіонів світу.

Іншою важливою стратегією є впровадження Security by Design — концепції, яка передбачає вбудування механізмів захисту ще на етапі проєктування IT-систем і сервісів. Це дозволяє зменшити вразливості, пов’язані з людським фактором або технічними помилками. Наприклад, у банківському секторі використання принципів Security by Design дає змогу уникати багатьох атак типу SQL-ін’єкцій або міжсайтового скриптингу (XSS).

Також варто згадати модель DevSecOps, яка інтегрує питання безпеки безпосередньо в процеси розробки програмного забезпечення та обслуговування IT-систем. На відміну від традиційного підходу, де захист впроваджується після завершення розробки, у DevSecOps безпека супроводжує продукт на всіх етапах його життєвого циклу. Це дозволяє не лише скоротити витрати на ліквідацію інцидентів, а й мінімізувати часові втрати на реагування.

Окрему увагу слід приділяти формуванню культури кібербезпеки серед працівників. За даними дослідження IBM (2023), понад 43% інцидентів пов’язані з людським фактором — зокрема, недотриманням протоколів або фішингом. У зв’язку з цим компанії впроваджують програми підвищення обізнаності, регулярне тестування за допомогою фішингових симуляцій та сертифікацію співробітників (наприклад, через платформи типу Cybrary або KnowBe4).

Інституційний рівень стратегії також передбачає створення центрів реагування на інциденти (SOC — Security Operations Centers), які здійснюють цілодобовий моніторинг активності, виявлення аномалій та координацію дій у разі кризових ситуацій. За даними Deloitte, транснаціональні корпорації з SOC демонструють на 35% менший середній час реагування на загрози порівняно з компаніями без таких підрозділів.

З огляду на багатовимірність міжнародного середовища, ефективною є також стратегія побудови мультинаціональних альянсів у сфері кіберзахисту. Наприклад, участь у глобальних об'єднаннях типу FIRST (Forum of Incident Response and Security Teams) дозволяє обмінюватися даними про нові загрози в реальному часі, отримувати підтримку від партнерів та дотримуватися уніфікованих протоколів реагування. У табл. 7 систематизовано ключові стратегічні підходи до забезпечення інформаційної безпеки в міжнародному менеджменті.

Таблиця 3.1

Основні стратегії забезпечення інформаційної безпеки в міжнародних компаніях

Стратегія	Суть підходу	Приклади застосування

Zero Trust Architecture	Контроль доступу на основі автентифікації і мінімізації довіри	Хмарні сервіси, віддалена робота
Security by Design	Інтеграція безпеки ще на етапі проєктування	Банківський софт, IoT-пристрої
DevSecOps	Інтеграція безпеки в життєвий цикл розробки	CI/CD у великих IT-компаніях
Культура кібербезпеки	Навчання персоналу, поведінковий моніторинг	Тренінги, фішингові симуляції
SOC	Центри моніторингу й реагування на інциденти	24/7 операційні центри
Кіберальянси	Участь у міжнародних платформах обміну інформацією	FIRST, Global Cyber Alliance

Джерело: систематизовано автором за даними IBM (2023), Deloitte (2022), NIST SP 800-207 [29–31]

Таким чином, стратегічне забезпечення інформаційної безпеки повинно не лише відповідати технічним стандартам, але й враховувати динаміку міжнародного законодавства, рівень цифрової зрілості компаній, політичну стабільність регіону та міжкультурні відмінності у підходах до приватності та захисту даних. Важливо також усвідомлювати роль кібербезпеки як складової репутаційного капіталу транснаціональних корпорацій: інциденти витоку даних можуть спричинити значні фінансові та іміджеві втрати, особливо в умовах глобальної конкуренції.

У підсумку, ефективна стратегія інформаційної безпеки в міжнародному менеджменті повинна бути комплексною, адаптивною до контексту конкретної країни та чутливою до культурних особливостей. Поєднання технологічних інструментів, інституційних механізмів і людського капіталу створює основу для стійкої цифрової трансформації.

3.2. Інституційні підходи до управління кібербезпекою в міжнародних компаніях

Інституційний підхід до управління кібербезпекою ґрунтується на впровадженні структурних, процедурних і кадрових механізмів, які

забезпечують цілісне реагування на загрози у цифровому середовищі. Для транснаціональних компаній важливим чинником є гармонізація цих механізмів на рівні глобальних штаб-квартир і регіональних представництв, з урахуванням локальних юридичних вимог і технологічних відмінностей [1].

Ключовим елементом інституційного підходу виступає створення позиції Chief Information Security Officer (CISO), який координує реалізацію політик безпеки, управляє ризиками й організовує взаємодію між IT-підрозділами, HR, юридичними службами та зовнішніми аудиторами [2]. У компаніях із розвиненою структурою управління CISO має окремий департамент або функціональну вертикаль, що звітує напряму CEO або Раді директорів.

Другим важливим компонентом є формування внутрішніх організаційних структур на кшталт Комітетів з кібербезпеки, які забезпечують міжфункціональну координацію. Такі комітети, як правило, розглядають звіти з моніторингу інцидентів, погоджують бюджети на безпекові заходи, ініціюють зовнішні аудити та затверджують політики резервного копіювання, шифрування і зберігання даних.

Зростаючу роль відіграють також внутрішні тренінгові центри або платформи підвищення цифрової обізнаності. Наприклад, Nestlé створила у 2022 році власну Академію кіберграмотності, яка охоплює понад 70 000 співробітників у 189 країнах світу [3]. Такий підхід дозволяє уніфікувати поведінкові моделі персоналу стосовно електронної безпеки, захисту конфіденційної інформації та реагування на фішинг.

Не менш важливою складовою є запровадження внутрішньої системи управління інцидентами (Incident Response Plans, IRP). У міжнародних компаніях ця система зазвичай стандартизована відповідно до NIST SP 800-61, яка включає етапи виявлення, аналізу, стримування, ліквідації та післяінцидентного аналізу [4]. Також використовуються цифрові платформи управління безпековими подіями — наприклад, IBM QRadar, Splunk Enterprise Security або Microsoft Sentinel [1].

Нарешті, ефективність інституційного підходу залежить від побудови системи регулярного моніторингу та звітності. Компанії формують KPI з кіберстійкості (кількість зірваних атак, час реагування, частка пройдених навчань тощо), які публікуються в ESG-звітах або корпоративних річних звітах [2]. Таким чином, безпека інтегрується в ширший контекст сталого розвитку (sustainability).

Інституціоналізація управління кіберризиками створює підґрунтя для довготривалої цифрової стійкості компаній у глобальному конкурентному середовищі. Вона забезпечує не лише технічну реакцію на інциденти, але й передбачає формування сталої культури безпеки, що охоплює всі рівні корпоративної структури – від топменеджменту до рядових співробітників.

Водночас, сучасні підходи до кібербезпеки все частіше інтегрують принципи корпоративного управління, спрямовані на прозорість та підзвітність. Зокрема, великі міжнародні корпорації дедалі частіше включають питання інформаційної безпеки до порядку денного наглядових рад, що сприяє підвищенню рівня стратегічного контролю. Крім того, підвищується роль незалежних зовнішніх аудитів, які дозволяють неупереджено оцінити рівень відповідності внутрішніх політик вимогам міжнародних стандартів та нормативів.

У цьому контексті перспективним є також запровадження системи Cybersecurity Maturity Model (CMM), яка дає змогу оцінювати рівень зрілості інфраструктури безпеки за п’ятибальною шкалою: від реактивного до оптимізованого рівня. Це дозволяє проводити бенчмаркінг та вибудовувати планові заходи з підвищення ефективності захисту на основі виявлених слабких місць.

3.3. Політики, стандарти й нормативне забезпечення кібербезпеки в міжнародних компаніях

Забезпечення високого рівня кібербезпеки в міжнародних компаніях неможливе без чіткого нормативно-правового підґрунтя та системи внутрішніх політик. Стандарти й політики відіграють ключову роль у формалізації процесів безпеки, регламентації дій працівників та забезпеченні відповідності глобальним і локальним нормам. Ці документи стають основою для управління ризиками, побудови систем захисту даних, формування культури інформаційної безпеки в організації.

Найбільш поширеними міжнародними стандартами, які застосовуються у сфері кібербезпеки, є ISO/IEC 27001, NIST Cybersecurity Framework, COBIT, CIS Controls та стандарт PCI DSS. Наприклад, ISO/IEC 27001 встановлює вимоги до створення, впровадження, підтримки та вдосконалення системи управління інформаційною безпекою (ISMS), яка охоплює всі аспекти безпеки – від технічних до організаційних [5].

NIST Cybersecurity Framework (CSF), розроблений у США, є гнучкою системою, яка дозволяє компаніям будь-якого масштабу оцінити поточний рівень безпеки, визначити бажаний стан та впровадити відповідні заходи. Він поділений на п’ять функцій – ідентифікація, захист, виявлення, реагування та відновлення – що дозволяє здійснювати комплексне управління загрозами [6].

Стандарти COBIT та CIS Controls допомагають формалізувати вимоги до IT-процесів, створення зон відповідальності, а також дають змогу ефективно інтегрувати вимоги безпеки в корпоративну IT-архітектуру. Зі свого боку, PCI DSS застосовується у компаніях, що працюють із платіжними системами, й містить жорсткі вимоги до шифрування, захисту даних карток та моніторингу транзакцій [7].

Крім міжнародних стандартів, важливу роль відіграють регіональні нормативи. Зокрема, в Європейському Союзі діє Загальний регламент про захист даних (GDPR), що накладає чіткі вимоги до обробки персональної інформації,

зокрема вимоги до інформування суб’єктів, отримання згоди, дотримання прав доступу, виправлення та забуття. Компанії, які не дотримуються GDPR, можуть стикатися з багатомільйонними штрафами [8].

В Україні застосовуються Закони «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основні засади забезпечення кібербезпеки України», а також нормативні документи Держспецзв’язку та НБУ. Багато міжнародних компаній адаптують свої політики до цих вимог, якщо ведуть діяльність в українському сегменті ринку або мають дочірні представництва [9].

Внутрішні політики компаній охоплюють низку ключових напрямів: політика контролю доступу, політика шифрування, політика поводження з мобільними пристроями, політика резервного копіювання, політика інцидент-менеджменту, політика роботи з постачальниками тощо. Наприклад, у компанії Siemens усі співробітники зобов’язані проходити щорічне навчання з інформаційної безпеки, а доступ до критичних систем регламентується багаторівневою системою авторизації [10].

Крім того, політики мають бути адаптивними до змін середовища. У зв’язку з розвитком гібридних форматів роботи (remote/hybrid), багато компаній оновлюють політики щодо BYOD (bring your own device), VPN-з’єднань, використання хмарних сервісів і забезпечення захисту на рівні «zero trust». Такі підходи забезпечують безпечне управління інфраструктурою навіть за умови територіального розподілу співробітників [11].

Нарешті, важливим аспектом є регулярне оновлення політик відповідно до аудиторських перевірок, результатів тестування вразливостей (penetration testing) і нових вимог партнерів або регуляторів. Усе більшого значення набуває застосування динамічних систем адаптації політик до поточних загроз, зокрема з використанням штучного інтелекту й машинного навчання для виявлення аномалій у поведінці користувачів та мережевого трафіку. Такі інструменти дозволяють формувати адаптивні правила доступу в режимі реального часу, що значно підвищує ефективність систем кіберзахисту. Крім того, великі транснаціональні компанії активно залучаються до міжкорпоративних альянсів

(наприклад, Global Forum on Cyber Expertise), які сприяють обміну найкращими практиками та координації міжнародних стандартів у сфері безпеки. У великих компаніях цей процес координується спеціальними політичними офісами або комітетами, які відповідають за актуальність і відповідність усіх регламентуючих документів [12].

Список використаних джерел

1. Дорошенко О.І. Інформаційна безпека в системі управління транснаціональними корпораціями // *Економічна безпека*. – 2022. – №3. – С. 89–95.

2. ISO/IEC 27000:2018. Information technology – Security techniques – Information security management systems – Overview and vocabulary. URL: https://www.iso.org/standard/73906.html

3. Баєва В.М. Інформаційна безпека в цифровій економіці: виклики для менеджменту // *Науковий вісник ХНЕУ*. – 2021. – №2(304). – С. 112–118.

4. CyberEdge Group. 2023 Cyberthreat Defense Report. URL: https://cyber-edge.com/cdr/

5. Maersk cybersecurity case study. URL: https://www.maersk.com/news/articles/2023/maersk-cybersecurity-posture

6. IBM X-Force Threat Intelligence Index 2023. URL: https://www.ibm.com/reports/threat-intelligence

7. ENISA Threat Landscape Report 2023. URL: https://www.enisa.europa.eu

8. SolarWinds Cyberattack Analysis (CSIS). URL: https://www.csis.org/solarwinds

9. IBM X-Force Threat Intelligence Index 2023. URL: https://www.ibm.com/reports/threat-intelligence

10. FireEye APT10 and APT29 Reports. URL: https://www.fireeye.com/current-threats/apt-groups.html

11. Verizon Data Breach Investigations Report 2023. URL: https://www.verizon.com/business/resources/reports/dbir/

12. Kaseya ransomware attack summary. Reuters. URL: https://www.reuters.com/technology/us-software-firm-kaseya-hit-by-ransomware-attack-2021-07-02/

13. Verizon Data Breach Investigations Report 2023. URL: https://www.verizon.com/business/resources/reports/dbir/

14. Colonial Pipeline ransomware attack summary. CISA. URL: https://www.cisa.gov/news-events/news/colonial-pipeline-ransomware-attack

15. SolarWinds Cyberattack Analysis. CSIS. URL: https://www.csis.org/solarwinds

16. CrowdStrike Global Threat Report 2023. URL: https://www.crowdstrike.com/global-threat-report/

17. National Vulnerability Database (NVD). NIST. URL: https://nvd.nist.gov/

18. IBM X-Force Threat Intelligence Index 2023. URL: https://www.ibm.com/reports/threat-intelligence

19. ENISA Threat Landscape Report 2023. URL: https://www.enisa.europa.eu/topics/threat-risk-managemen

20. IBM Security. X-Force Threat Intelligence Index 2023. URL: https://www.ibm.com/reports/threat-intelligence

21. NIST Special Publication 800-207. Zero Trust Architecture. URL: https://csrc.nist.gov/publications/detail/sp/800-207/final

22. Deloitte. Cybersecurity Trends 2022. URL: https://www2.deloitte.com/us/en/pages/risk/articles/cybersecurity-trends.htm\

23. IBM Security. X-Force Threat Intelligence Index 2023. URL: https://www.ibm.com/reports/threat-intelligence (дата звернення: 05.06.2025).

24. Deloitte Cybersecurity Framework Overview 2022. URL: https://www2.deloitte.com/global/en/pages/risk/topics/cyber-risk.html (дата звернення: 05.06.2025).

25. Nestlé Global Cybersecurity Report 2023. URL: https://www.nestle.com/investors/annualreport (дата звернення: 05.06.2025).

26. NIST. Computer Security Incident Handling Guide. Special Publication 800-61 Rev.2. URL: https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final (дата звернення: 05.06.2025).

27. ISO/IEC 27001 Information Security Management. URL: https://www.iso.org/isoiec-27001-information-security.html (дата звернення: 05.06.2025)

28. NIST Cybersecurity Framework. URL: https://www.nist.gov/cyberframework (дата звернення: 05.06.2025).

29. PCI Security Standards Council. PCI DSS v4.0. URL: https://www.pcisecuritystandards.org (дата звернення: 05.06.2025).

30. Regulation (EU) 2016/679 (General Data Protection Regulation). URL: https://gdpr-info.eu (дата звернення: 05.06.2025).

31. Закон України «Про основні засади забезпечення кібербезпеки України». URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 05.06.2025).

32. Siemens. Data Privacy and Cybersecurity Standards. URL: https://www.siemens.com/global/en/company/sustainability/cybersecurity.html (дата звернення: 05.06.2025).

33. Deloitte. 2024 Global Future of Cyber Survey. URL: https://www2.deloitte.com/global/en/pages/risk/articles/global-future-of-cyber-survey.html (дата звернення: 05.06.2025).

34. EY Global Information Security Survey 2023. URL: https://www.ey.com/en_gl/cybersecurity (дата звернення: 05.06.2025).