DOI: https://doi.org/10.30837/EK.2024.034
Шейко І.А.,
к.е.н., доцент, доцент кафедри економічної кібернетики та управління економічною безпекою,
Харківський національний університет радіоелектроніки,
ORCID: https://orcid.org/0000-0002-5770-3677
Степаненко Р.Д.,
здобувач вищої освіти,
Харківський національний університет радіоелектроніки
ORCID: https://orcid.org/0009-0008-0586-0903
Батіг В.В.,
здобувач вищої освіти,
Харківський національний університет радіоелектроніки
ORCID: https://orcid.org/0009-0007-3883-3648

РИЗИКИ ТА ЗАГРОЗИ ЕКОНОМІЧНІЙ БЕЗПЕЦІ ПІДПРИЄМСТВА В КОНТЕКСТІ ЦИФРОВОГО РОЗВИТКУ

Організації в усіх галузях все більше покладаються на цифрові технології для виконання роботи. Зрештою, ці нові технології – штучний інтелект та машинне навчання, Інтернет речей, хмарні обчислення, максимізують швидкість, гнучкість, ефективність і прибутковість для організацій, які їх використовують [1]. Незалежно від того, чи має на меті компанія оптимізувати свою діяльність, прийняти нові бізнес-моделі чи покращити взаємодію з клієнтами, це часто є рушійною силою, що стоїть за рішенням організації прийняти нові цифрові ініціативи [2].

Оскільки технології все більше інтегруються в усі аспекти бізнесу, цифровий ризик стає все більшою проблемою для компаній у всьому світі. Він

охоплює широкий спектр потенційних негативних наслідків, що випливають із цифрових технологій і процесів. Це включає [3]:

– природно цифрові ризики: загрози, які не існували б без цифрових технологій, як-от витоки даних, атаки програм-вимагачів, збої в роботі хмарних служб і зміщення алгоритмів штучного інтелекту.

– традиційні ризики, що посилюються цифровими засобами: проблеми, які існують, але трансформуються або загострюються цифровізацією, включаючи репутаційну шкоду через соціальні медіа, збої в ланцюзі поставок після кібератак і фінансове шахрайство через цифрові канали.

Швидка еволюція цифрових ризиків відрізняє їх від традиційних загроз. Зважаючи на тісно пов’язані між собою цифрові системи та безпрецедентний масштаб і швидкість, з якою ці ризики можуть матеріалізуватися, компаніям дуже важливо чітко усвідомлювати нюанси цифрових технологій і те, як вони фундаментально змінюють увесь ландшафт ризиків.

У дослідженні Deloitte як фактори, здатні активізувати цифрові ризики названі такі: експоненційне зростання розумних (smart) приладів; зміна споживацьких очікувань та демографічні зміни; поширення цифрової інфраструктури да широкосмугового Інтернету; поява технологічних інновацій та схильність до їх використання.

Цифровізація економіки відкриває значні можливості для зростання та інновацій, але також створює нові ризики та загрози для економічної безпеки. Основними викликами у цифрову епоху є кіберзлочинність, технологічна залежність, порушення конфіденційності даних та соціально-економічна нерівність. На основі аналізу джерел [1-4] в цьому досліджені систематизовано вісім основних типів ризиків, представлених на рис. 1.

Кожен тип ризику має свої особливості прояву та методи боротьби з ним.

Рисунок 1 – Типи цифрових ризиків

Кіберзлочинність стала одним із найсерйозніших ризиків для бізнесу та держав. Атаки на фінансові установи, викрадення даних і збої в роботі критичних інфраструктур можуть призвести до значних економічних втрат і зниження довіри до цифрових систем.

Зокрема, збільшення кількості атак програм-вимагачів і фішингових схем є прямою загрозою для компаній та громадян. За даними Європейського агентства з кібербезпеки, найбільш розповсюдженими типами кібератак з червня 2023 по липень 2024 стали відмова у доступі (DoS/DDoS – атаки), програми вимагачі, витік даних, загрози соціальної інженерії (провокування персоналу компаній на дії, що сприяють порушенню кібербезпеки), шкідливе програмне забезпечення (рис. 2) [2].

Рисунок 2 – Найбільш розповсюджені типи кібератак у країнах ЄС з червня 2023 по липень 2024 [2]

Кібератаки негативно впливають на діяльність усіх секторів економіки та суспільного життя, проте особливо активними стали кібератаки на такі сектори (рисунок 3): публічне управління, транспорт, банківській сектор, бізнес-послуги та цифрова інфраструктура. Означені сектори прийняли на себе більше половини інцидентів з порушення кіберезпеки.

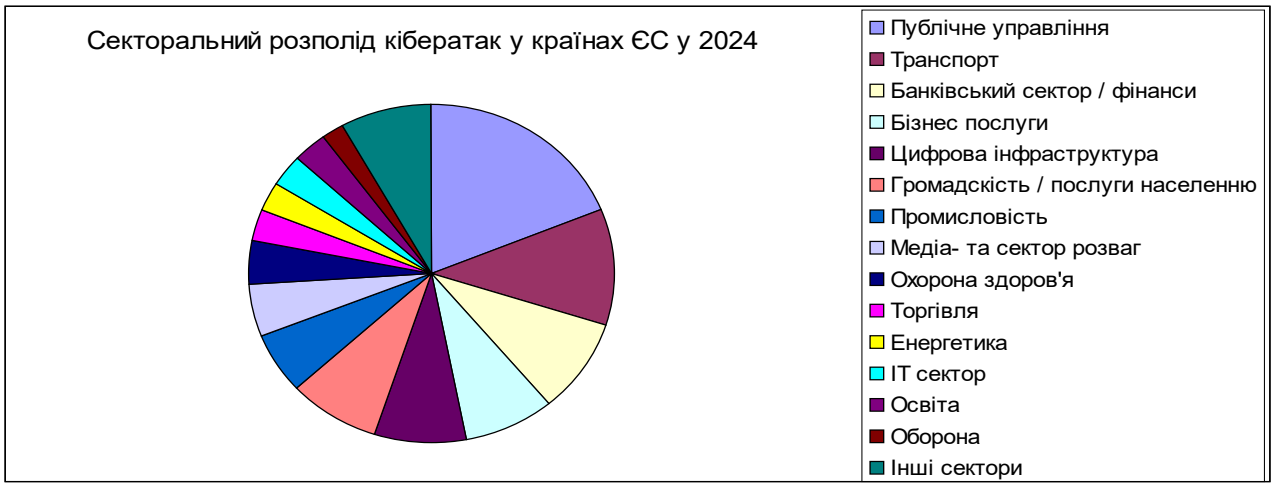

Рисунок 3 – Секторальний розподіл кібератак у країнах ЄС з липня 2023 по червень 2024 рр.

Ризик втрати даних та конфіденційності передбачає здатність компанії захищати особисту інформацію, дані клієнтів. Кіберзлочинці можуть легко зловживати цим типом даних, щоб завдати шкоди або зловживати ідентифікацією співробітників або клієнтів.

Збереження конфіденційності даних у цифрову епоху стає все більш проблематичним. Витоки персональної та фінансової інформації можуть не лише завдати шкоди окремим користувачам, але й негативно впливати на національну безпеку. Недостатні заходи захисту інформації часто є результатом низької культури кібербезпеки та відсутності регуляторних механізмів.

Так, за даними європейського агентства з кібербезпеки щомісяця викрадається понад 10 терабайт даних, програмне забезпечення-вимагач є однією з найбільших кіберзагроз у ЄС, а фішинг зараз визначено як найпоширеніший вихідний вектор таких атак. Розподілені атаки типу «відмова в обслуговуванні» (DDoS) також вважаються одними з найбільших загроз. За оцінками, на кінець 2020 року річний збиток світової економіки від кіберзлочинності сягнув 5,5 трильйонів євро, що вдвічі перевищує показник 2015 року [1].

Щоб уникнути конфіденційності даних компаніям варто запровадити суворі заходи кібербезпеки, зокрема керування ідентифікацією та доступом, багатофакторну автентифікацію та політику паролів. Набуває важливості також постійне навчання та підвищення обізнаності персоналу щодо ризиків втрати даних.

Як приклад наслідків витоку даних, модна привести дані інциденту з авіакомпанією British Airways. Влітку 2018 року авіакомпанія British Airways зазнала витоку даних, у результаті якого були скомпрометовані дані та дані кредитних карток приблизно від 380 000 до 500 000 клієнтів. Хакери викрали імена, адреси, електронні адреси, номери кредитних карток і коди безпеки карток. За словами експертів із безпеки даних, атака на ланцюг поставок на сторонні платіжні служби на веб-сайті British Airways була використана за допомогою

ін’єкції зловмисного коду JavaScript, який передавав платіжні дані невідомим зловмисникам. ICO (Офіс інформаційного комісара) наклав штраф у розмірі 183 мільйони фунтів стерлінгів, що є найбільшим штрафом у 2018 році, але в жовтні 2020 року British Airways сплатила значно меншу суму – лише 20 мільйонів фунтів стерлінгів (26 мільйонів доларів США) за те, що не захистила особисті записи та фінансові дані. клієнтів і постраждалих суб’єктів даних. Таким чином, виток даних спричинив не тільки репутаційні, але і фінансові втрати.

Особливу актуальність набуває ризик дефіциту персоналу та компетентностей. Так, згідно з даними Європейської комісії, сектор ІКТ разом із сектором науки, технологій, інженерії та математики (STEM) відчуває на собі брак кваліфікованого персоналу. Хоча брак робочої сили може бути ознакою динамічної економіки та давати працівникам певний вплив, він може мати негативний вплив на компанії та економіку в цілому та затримати цифровий та зелений перехід. Згідно з даними дослідження, 17 країн ЄС у 2021 році відчували брак персоналу у секторі ІТ. У 2022 році дефіцит персоналу у секторі ІКТ Європейського Союзу склав 4 %, а попит на фахівців з ІТ зріс у порівнянні з 2012 роком на 80 % (а на розробників програмного забезпечення – на 88 %). За період 2012-2022 р. кількість зайнятих у секторі ІКТ зросла майже удвічі.

Країни з найбільшим дефіцитом на ІТ-персонал – це Німеччина, Італія, Швейцарія, а також країни Північної Європи та Бенілюксу. У 2014 році Європейська комісія попередила, що до 2020 року в Європі буде не вистачати до 900 000 ІТ-персоналу. Пізніше німецька консалтингова фірма Empirica скоротила цю цифру до 500 тис. Наприклад, в Амстердамі технологічні стартапи складаються приблизно з 70 % іноземців (переважно з Бразилії, Франції, Туреччини, України та Індії), у Фінляндії зараз не вистачає понад 7000 розробників програмного забезпечення. За оцінками уряду Данії, до 2030 року в Данії не вистачатиме 19 000 спеціалістів з ІТ та електроніки. У Німеччині існує серйозна нестача ІТ-фахівців, проблема, яка проявляється майже

в усіх регіонах Німеччини. У 2016 році в Італії більше 30 000 вакансій для розробників програмного забезпечення та аналітиків були незаповненими, причому на Мілан припадає 20% цього дефіциту. Але така проблема дефіциту IT-персоналу є глобальною: у Сінгапурі протягом наступних 3 років знадобиться 42 000 IT-фахівців [1]. З іншого боку, у Східній та Південній Європі існує відносна надлишок технічних кадрів, що відображається в нижчих зарплатах у цих регіонах.

IT-індустрія впевнено перетворюється на один із флагманів економіки України та стає невід'ємною частиною її міжнародного іміджу. Але одним із найбільших викликів для майбутнього IT-індустрії в Україні є дефіцит кадрів.

За оцінками GlobalLogic, щорічно в Україні створюється близько 40 000 робочих місць в IT-секторі. Зважаючи на те, що попит на інженерів цих спеціальностей щорічно зростає приблизно на 30 %, але реальна кількість працевлаштованих інженерів зростає лише на 18%, що свідчить про значне перевищення попиту над пропозицією [8].

Водночас українські виші здатні підготувати не більше 15-20 тис. IT-фахівців різних напрямків. Крім того, багато випускників працевлаштовуються за кордоном або віддають перевагу фрілансу. IT-спеціалісти також активно навчаються на численних приватних курсах. У середньостроковій перспективі можливе збільшення до 35 тис. випускників бакалаврів за рахунок піку народжуваності в 2008-2013 рр. Це покращує ситуацію, але все ще не дозволяє покрити суттєву нестачу IT-персоналу [9].

Внаслідок повномасштабного вторгнення 70,8 % IT-компаній провели незаплановану релокацію, чверть з них – повну. Так, 16,7 % компаній провели повну чи часткову релокацію за кордон переважно у Польщу, Німеччину, США, Португалію, Болгарію, Чехію, Румунію, Молдову, Іспанію, Канаду; 81,5 % релокованих закордон IT-компаній все ж планують повертати бізнес в Україну за умови скасування воєнного стану та повного припинення бойових дій [10].

Також компанії, які стали на шлях цифрової трансформації, можуть стикнутися із ризиком відповідності –ризик, пов'язаний з необхідністю дотримання нормативних вимог, викликаними новою технологією та обсягом даних, які створює організація. Такі вимоги поширюються на усі дані, що збирає компанія від клієнтів: отримання згоди на обробку персональних даних, вимоги до їх збереження, захисту та обробки, використання ліцензійного програмного забезпечення.

З будь-якою новою технологією часто потрібно впроваджувати нові вимоги чи правила, інакше компанія не буде відповідати нормативним вимогам щодо бізнес-операцій, збереження даних та інших бізнес-практик. Оскільки нові технології продовжують з'являтися, вимоги до відповідності також змінюються. З цієї причини менеджмент компанії повинен переконатися, що вона в режимі реального часу відповідає вимогам законодавства.

Однак управління ризиками відповідності не обмежується тільки контуром управління підприємством. Стосунки компанії із третіми сторонами також можуть загрожують їй невідповідністю, і через це компанія буде нести відповідальність за те, щоб будь-який постачальник або з яким вона співпрацює вздовж ланцюга постачання, не відповідає нормативним вимогам.

Яскравим прикладом реалізації ризику цифрової відповідності в діловій практиці ЄС є дії Загального регламенту захисту даних (GDPR) проти таких компаній, як Meta (раніше Facebook). У 2023 році Комісія із захисту даних Ірландії оштрафувала Meta на 1,2 мільярда Євро за передачу даних користувачів із ЄС до США без достатніх гарантій, порушуючи суворі правила конфіденційності даних GDPR. GDPR передбачає, що особисті дані громадян ЄС не можуть передаватись за межі ЄС, якщо не забезпечено відповідний захист. Покладення Meta на стандартні договірні положення було визнано недостатнім. Накладений на штраф підкреслив слабкі сторони системи захисту даних Meta, що викликало занепокоєння серед клієнтів і зацікавлених сторін. це рішення змусило Meta

переоцінити методи обробки даних і механізми відповідності, збільшивши операційні витрати. Цей випадок підкреслює фінансові, репутаційні та операційні ризики недотримання цифрових норм.

Ризик відповідності тісно пов'язаний із *ризиком третіх сторін*. Сьогодні організації практично в кожній галузі працюють із третіми сторонами, будь то постачальники, продавці, підрядники чи постачальники послуг.

Будь-яка організація покладається на треті сторони для виконання кількох бізнес-функцій, які мають вирішальне значення для ваших бізнес-операцій. Однак аутсорсинг будь-якій третій стороні неминуче створює ризик, наприклад юридичні, логістичні, фінансові або репутаційні проблеми. Наприклад, будь-які ризики, пов'язані з інтелектуальною власністю компанії – даними, операціями, фінансами, інформацією про клієнтів або іншою конфіденційною інформацією, вважаються ризиками третіх сторін, якщо ці треті сторони мають доступ до ваших мереж і систем.

Для контролю ризиків третіх сторін варто регулярно переглядати стосунки зі сторонніми особами та здійснювати постійний моніторинг, щоб гарантувати, що компанія буде миттєво в курсі будь-яких недоліків.

З цифровою трансформацією пов'язаний також і *технологічний ризик*. Впровадження будь-якою цифрової інновації передбачає обов'язковий етап навчання, що може вплинути на якість бізнес-операцій.

З розвитком нових цифрових технологій стають актуальними кілька нових ризиків, пов'язаних із застосуванням нових технологій, які, можливо, не були такими очевидними, як раніше. Наприклад, потенційна недоступність критично важливих систем через збої в електроживленні, несумісність обладнання, втрата даних може безпосередньо вплинути на ваші бізнес-процеси та співробітників, іноді навіть повністю зупинити роботу.

У [11] до сфер, що пов'язані із ризиками цифрової трансформації відносять: Інтернет речей та хмарну інфраструктуру.

Яскравим прикладом збитків для бізнесу в результаті використання хмарних технологій та Інтернету речей є DDoS-атака 2016 року на Dyn, компанію, що розробляє хмарну інтернет-інфраструктуру. Dyn, великий провайдер DNS, зазнав розподіленої атаки типу «відмова в обслуговуванні» (DDoS), здійсненої ботнетом Mirai. Ботнет складався із заражених пристроїв IoT, таких як камери та маршрутизатори. Атака перевантажила сервери Dyn, порушивши роботу кількох відомих компаній, зокрема Amazon, Netflix, Spotify і Twitter.

У результаті кібератаки постраждалі компанії зазнали втрат доходу та додаткових витрат для пом'якшення наслідків. Інцидент виявив, що не можна сильно покладатися на незахищені пристрої Інтернету речей і централізовані хмарні сервіси, похитнувши довіру клієнтів.

Щоб уникнути технологічних ризиків компанія має створити та оновлювати план аварійного відновлення, який враховує будь-які технології, без яких неможливі бізнес-операції компанії. Корисним також буде регулярно створювати резервні копії своїх даних у кількох локальних і зовнішніх місцях, щоб забезпечити доступ до найважливішої інформації навіть у разі збою.

Інколи автоматизація може негативно впливати на бізнес-процеси, створюючи додаткові ризики. Наприклад, деякі рішення автоматизації можуть призвести до несумісності програмного забезпечення або створювати зайву операційну складність.

У той же час, більше застосування програмного забезпечення означає більшу ймовірність витоку даних. Через це важливо своєчасно оновлювати ПЗ та в останній версії виправлені усі слабкі місця.

Інструменти автоматизації на основі штучного інтелекту також можуть створювати ризики, які часто важко передбачити в довгостроковій перспективі через постійні зміни природи самої технології. Впровадження такого типу автоматизації часто може призвести до збоїв у роботі, збільшення складності та посилення вразливості до кіберзагроз.

Щоб уникнути ризиків автоматизації менеджмент компанії має досліджувати будь-які потенційні ризики, створені програмним забезпеченням автоматизації, і налаштувати інструменти для їх усунення.

Ризик помилок персоналу (соціальної інженерії) також повинен бути врахований. Так, соціальна інженерія має своєю метою примусити спостерігача/співрозмовника/клієнта/партнера робити так, як вигідно компанії. Через використання технік соціальної інженерії кіберзлочинчі можуть переконати персонал зробити небезпечні кроки, що дозволять стороннім особам отримати доступ до конфіденційної інформації: наприклад, відкрити лист від незнайомого адресата, встановити додаток або комп'ютерну гру, зайти на Інтернет сайт. Таким чином, соціальна інженерія перетворилася на некерований ризик, який заслуговує на окрему категорію. Спроби соціальної інженерії варіюються від фішингових атак через електронну пошту, зловживання соціальними мережами, тощо.

Найпоширенішим типом атак соціальної інженерії є, ймовірно, фішинг – спроба змусити користувачів обійти повсякденні заходи кібербезпеки та надати конфіденційні дані, такі як імена користувачів і паролі, інформацію про банківський рахунок, номери соціального страхування та дані кредитних карток.

Щоб уникнути ризику соціальної інженерії компанії варто приділити увагу тренінгу з питань кібербезпеки для всіх своїх співробітників, наголошуючи на важливості звітування про фішинг. Компанія може запустити випадкову симуляцію кібератаки та регулярно перевіряти здатність співробітників виявляти спроби фішингу, винагороджуючи успіх і забезпечуючи додаткове навчання для всіх співробітників, які мають труднощі із розпізнанням інцидентів безпеки.

У епоху цифрових технологій управління ризиками стало критично важливим аспектом організаційної стратегії, оскільки компанії стикаються зі зростаючим набором цифрових ризиків. Для мінімізації ризиків необхідно впроваджувати комплексні стратегії, що включають розвиток кібербезпеки, регулювання технологічного сектору та підтримку інновацій. Лише баланс між

використанням цифрових можливостей та управлінням загрозами дозволить забезпечити стійку економічну безпеку у цифрову епоху.

Першим кроком в управлінні цифровими ризиками є проведення комплексної оцінки ризиків. Організації повинні визначити потенційні загрози, такі як хакерство, фішинг, програми-вимагачі та вразливі місця системи. Крім того, слід оцінити ризики, пов'язані з цифровою трансформацією, як-от застарілі системи управління або неналежне управління даними.

Ефективне управління цифровими ризиками ґрунтується на впровадженні превентивних заходів і створенні стратегій реагування. Ключові практики включають [12]:

– інфраструктуру кібербезпеки: встановлення надійних брандмауерів, шифрування та багатофакторної автентифікації.

– навчання співробітників: навчання персоналу розпізнаванню фішингу та інших кіберзагроз.

– відповідність нормативним вимогам: забезпечення дотримання законів про захист даних, таких як GDPR або CCPA, шляхом регулярних перевірок.

Цифрові ризики є динамічними, що вимагає постійного моніторингу та адаптації. Розширена аналітика та інструменти на основі ШІ можуть забезпечити виявлення загроз у реальному часі. Регулярне оновлення протоколів безпеки та підтримка планів реагування на інциденти забезпечують готовність до нових викликів.

Перелік джерел посилань

1. What is digital risk? https://www.proofpoint.com/au/threat-reference/digital-risk.

2. Bevin L. 10 common types of digital risks. ZenGRC. 31.05.2024. URL: https://www.zengrc.com/blog/common-types-of-digital-risks/.

3. Airbus Protect. Digital Risk-management: a business-aligned approach. 27.09.2024. URL: https://www.protect.airbus.com/blog/digital-risk-management-a-business-aligned-approach/.

4. Deloitte. Managing risk in digital transformation. URL: https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-ra-managing-risk-in-digital-transformation-1-noexp.pdf.

5. The European Union Agency for Cybersecurity (ENISA) Threat Landscape 2024. September 2024. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.

6. European Commission: Directorate-General for Employment, Social Affairs and Inclusion, *Employment and social developments in Europe* 2023, Publications Office of the European Union, 2023, https://data.europa.eu/doi/10.2767/089698.

7. LuxInnivation. Software Developers in Europe & the world: A study of the Attractiveness of top tech cities for software developers (luxinnovation.lu) URL: http://surl.li/gtccuo (дата звернення 05.10.2022).

8. IT Ukraine Association Результати національного досліження IT-індустрії (2021). URL: https://itukraine.org.ua/results-of-a-national-study-of-the-it-industry.html (дата звернення 08.10.2022).

9. IT в Україні: цифри, перспективи та бар'єри. 2021. Липень, 25. http://surl.li/fwhknl (дата звернення 07.10.2022).

10. IT Ukraine Association. Дослідження Do IT Like Ukraine: IT-індустрія зростає попри все. 13.12.2022. URL: https://itukraine.org.ua/it-reports-do-it-like-ukraine/.

11.Digital Adoption Top 5 digital transformation risks. 31.05.2024. URL: https://www.digital-adoption.com/digital-transformation-risks/.

12.McKinsey&Company. Digital risk: transforming risk management for the 2020s. URL: http://surl.li/hvypuo.