НАЦІОНАЛЬНА ЕКОНОМІКА

УДК 338.14
DOI: https://doi.org/10.32782/2415-8801/2024-2.2

Гвоздь М.Я.
кандидат економічних наук, доцент,
доцент кафедри менеджменту організацій,
Національний університет «Львівська політехніка»

Морозов М.Я.
аспірант кафедри менеджменту організацій,
Національний університет «Львівська політехніка»

ЗАХИСТ ДАНИХ В ЕПОХУ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ЯК ЕЛЕМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА: ВИКЛИКИ ТА РІШЕННЯ

У статті визначено, що у сучасній епосі цифрової трансформації захист даних стає критично важливим елементом інформаційної безпеки для підприємств у зв'язку зі зростанням кількості кіберзагроз, підвищеною цінністю даних, потребою відповідності регулятивним вимогам, зростанням обсягів даних та впливом на репутацію підприємства. Дослідження цієї проблематики є надзвичайно актуальним, оскільки воно допомагає розуміти виклики, з якими стикаються підприємства в контексті цифрової трансформації, а також пропонує конкретні рішення і стратегії для ефективного захисту даних. Метою статті є аналіз сучасних викликів, з якими стикаються підприємства під час цифрової трансформації, що впливають на їхню інформаційну безпеку, а також надання пропозицій щодо ефективного захисту даних, зокрема через програми, спрямовані на підвищення адаптивності захисту інформації. Виокремлено три основні підходи до поділу викликів щодо захисту інформації з якими стикаються підприємства під час переходу до цифрової трансформації та їх вплив на безпеку даних, зокрема: технологічний, організаційний та стратегічний. Узгоджене поєднання цих трьох підходів дозволяє створити комплексну систему захисту інформації, яка забезпечує ефективність, надійність та відповідність стандартам безпеки. Досліджується необхідність інтеграції захисту інформації у стратегічне бізнес-планування підприємств і запропоновано шляхи вирішення цього завдання. Акцентовано увагу на тому, що підприємствам, особливо тим, які знаходяться в зоні ризику, важливо розглядати кібербезпеку як невід'ємну складову свого бізнесу. Це означає не лише встановлення базових заходів захисту, але й активну інвестицію у програми, спрямовані на підвищення адаптивності системи захисту інформації. Інтегруючи основні інструменти, такі як аналіз ризиків, системи моніторингу, плани реагування на інциденти, навчання персоналу та застосування сучасних технологій, підприємства можуть стати більш стійкими до потенційних кіберзагроз. Постійне вдосконалення і підтримка цих заходів дозволять ефективно адаптуватися до нових загроз і зберігати високий рівень захисту інформації у довгостроковій перспективі.

Ключові слова: *захист даних, цифрова трансформація, інформаційна безпека, діджиталізація, кібербезпека, адаптивність.*

DATA PROTECTION IN THE ERA OF DIGITAL TRANSFORMATION AS AN ELEMENT OF ENTERPRISE INFORMATION SECURITY: C HALLENGES AND SOLUTIONS

Gvozd Maryana, Morozov Mykola
Lviv Polytechnic National University

In the modern era of digital transformation, data protection is becoming a critically important element of information security for enterprises due to the increase in the number of cyber threats, the increased value of data, the need to comply with regulatory requirements, the growth of data volumes and the impact on the reputation of the enterprise. The study of this issue is extremely relevant, as it helps to understand the challenges faced by enterprises in the context of digital transformation, and also offers specific solutions and strategies for

effective data protection. The purpose of the article is to analyze the modern challenges enterprises face during digital transformation, which affect their information security, as well as to provide proposals for effective data protection, particularly through programs aimed at increasing the adaptability of information protection. Three main approaches to the division of information protection challenges faced by enterprises during the transition to digital transformation and their impact on data security are distinguished, in particular: technological, organizational, and strategic. A harmonious combination of these three approaches allows you to create a comprehensive information protection system that ensures efficiency, reliability, and compliance with security standards. The necessity of integrating information protection into the strategic business planning of enterprises is investigated and ways of solving this task are proposed. Attention is focused on the fact that it is important for enterprises, especially those at risk, to consider cyber security as an integral part of their business. This means establishing basic protection measures, and actively investing in programs aimed at increasing the adaptability of the information protection system. By integrating key tools such as risk analysis, monitoring systems, incident response plans, staff training, and the use of modern technology, businesses can become more resilient to potential cyber threats. Continuous improvement and support of these measures will allow us to effectively adapt to new threats and maintain a high level of information protection in the long term.

Keywords: *data protection, digital transformation, information security, digitization, cyber security, adaptability.*

Постановка проблеми. В епоху цифрової трансформації підприємства все частіше інтегрують передові технології у свої основні бізнес-процеси, прагнучи підвищити ефективність, сприяти інноваціям і забезпечувати вищу цінність для клієнтів. Ця концептуальна зміна, відкриваючи нові можливості, одночасно підвищує вразливість цих підприємств до складних кіберзагроз і порушень інформаційної безпеки. Таким чином, формулювання проблеми випливає з критичного парадоксу: коли підприємства використовують потужність цифрових технологій для досягнення конкурентної переваги, вони ненавмисно наражаються на безліч ризиків інформаційної безпеки, починаючи від крадіжки даних і фінансового шахрайства, до шкоди репутації. Отже, вимога щодо захисту конфіденційної інформації стає не просто технічною проблемою, а стратегічною необхідністю, що підкреслює актуальність і терміновість розробки надійних механізмів захисту інформації, адаптованих до цифрового середовища підприємств. Ця комбінація можливостей і ризиків висвітлює поточну та актуальну проблему забезпечення захисту інформації в рамках цифрової трансформації підприємств.

Аналіз останніх досліджень і публікацій. Проблематика захисту даних в епоху цифрової трансформації як елемент інформаційної та економічної безпеки підприємства дедалі більше викликає зростаючий інтерес як у вітчизняних, так і в зарубіжних теоретиків та практиків. Зокрема значний вклад у розвиток цього питання зробили Б. Дергалюк, О. Дворник [5], М. Біличенко, Н. Касьянова, Л. Сопільник, Р. Скриньковський, М. Ковалів [3], О. Ємельяненко, П. Друкер, Д. Бредлі, М. Вейд, Б. Гебремескел, А. Болтон [9] та інші.

Для подальшого розвитку інформаційної безпеки підприємств в епоху цифрової трансформації необхідно проводити дослідження у цьому напрямі. Подальші дослідження допоможуть розробити нові стратегії та технології для захисту даних, розв'язати невирішені проблеми. безпеки і підвищити стійкість підприємств у цифровому світі. Також, ці дослідження сприятимуть розвитку міжнародної співпраці та створенню нових стандартів безпеки, що є важливими для забезпечення захищеності даних у масштабах глобальної мережі.

Постановка завдання. Метою статті є аналіз сучасних викликів, з якими стикаються підприємства під час цифрової трансформації, що впливають на їхню інформаційну безпеку, а також надання пропозицій щодо ефективного захисту даних, зокрема через програми, спрямовані на підвищення адаптивності захисту інформації.

Виклад основного матеріалу дослідження. У сучасному цифровому світі, швидкі темпи технологічного прогресу та високий рівень цифрової трансформації призвели до значного збільшення обсягів електронних даних, які обробляються та зберігаються підприємствами. Ця цифрова трансформація відкриває безліч можливостей для розвитку та оптимізації бізнесу, проте разом з цим вона приносить і значні виклики, зокрема щодо забезпечення безпеки цих даних.

Захист даних у цифрову епоху стає критично важливим завданням для підприємств будь-якого масштабу та сфери діяльності. Порушення конфіденційності, цілісності чи доступності цих даних може призвести до серйозних фінансових втрат, втрати довіри з боку клієнтів та партнерів, а також негативно вплинути на репутацію підприємства.

У цьому контексті пропонується проаналізувати виклики та ризики, пов'язані з захистом даних в епоху цифрової трансформації, а також розглянути ефективні стратегії та рішення для їх вирішення. Висвітлюючи роль захисту даних як ключового елемента інформаційної безпеки підприємства, ми прагнемо допомогти бізнесу

адаптуватися до сучасних викликів та забезпечити стабільну та безпечну роботу в цифровому середовищі.

Інформація, як колись так і сьогодні, є другим найважливішим ресурсом підприємств, після працівників. Варто розглянути, що несе за собою порушення інформаційної безпеки, які основні виклики стоять перед підприємствами щодо захисту інформації та яких постулатів рекомендовано дотримуватись, щоб втілити його у життя.

Виокремлюють три основні підходи до поділу викликів щодо захисту інформації [1]:

– ***Технологічний підхід.*** Технологічні виклики цифрової трансформації зосереджені навколо складнощів інтеграції та захисту потоку нових технологій. Оскільки різні підприємства використовують надзвичайно різні технолоігії із унікальними векторами вразливостей. Це можуть бути хмарні обчислення, пристрої Інтернету речей, мобільні рішення, смарт контракти та штучний інтелект. Це розширення цифрового сліду вимагає багатогранного підходу до безпеки для захисту даних на різних платформах і пристроях. Крім того, темпи, з якими з'являються нові технології, часто випереджають можливості організацій оновлювати свої заходи кібербезпеки, що призводить до потенційних прогалин у механізмах захисту. Основна проблема полягає в тому, щоб забезпечити цілісність, конфіденційність і доступність даних серед нових загроз, що потребує постійних інновацій у технологіях і практиках безпеки. Це включає в себе впровадження надійного шифрування, використання передових систем виявлення загроз, регулярні оцінки безпеки та постійного моніторингу технологічного розвитку для завчасного попередження і усунення вразливостей.

– ***Організаційний підхід.*** Організаційні проблеми в цифровій трансформації підприємства виникають із внутрішньої динаміки, включаючи культуру, структуру та поведінку співробітників, які впливають на ефективність заходів захисту інформації. Значною перешкодою є поширена недостатня обізнаність працівників щодо безпеки інформації. Навіть з простого факту, що інформація сама по собі є конфіденційною і забороненою для передачі третім особам, не кажучи вже про недостатню обізнаність щодо кіберзахисту, що робить їх сприйнятливими до фішингових атак, соціальної інженерії та інших форм цифрових атак. Крім того, часто існує розбіжність між цілями команд безпеки та ширшими бізнес-цілями, що призводить до недостатньої підтримки та ресурсів для реалізації ефективних стратегій безпеки. Часто люди консервативні у використанні ресурсів і технологій. Тому при появі чогось нового часто зустрічається колективний опір. Опір змінам і постійне використання застарілих систем ускладнюють ці проблеми, створюючи неефективність і вразливі місця в безпеці. Вирішення цих проблем вимагає побудови сильної культури обізнаності про безпеку, забезпечення підтримки ініціатив із захисту інформації керівництвом, сприяння співпраці між відділами та інтеграції міркувань безпеки в усі бізнес-процеси та рішення.

– ***Стратегічний підхід.*** Стратегічні виклики передбачають розробку та підтримку комплексного підходу до захисту інформації, що відповідає глобальним нормативним вимогам і міжнародним стандартам, а також підтримує довгострокові цілі підприємства. Навігація в складному нормативному середовищі, включно з дотриманням Загального регламенту захисту даних (GDPR, що є стандартом для ЄС), акти щодо сумісності і підзвітності медичного страхування (PIPEDA, PHIPA, HIPAA) та інших міжнародних стандартів, як-от ISO/IEC 27001, є серйозною проблемою. Ці нормативні акти передбачають суворі заходи щодо захисту даних і конфіденційності, що вимагає всебічного підходу до захисту інформації, який включає оцінку ризиків, управління даними та управління відповідністю. Підприємства повинні розробити стратегії, які не тільки забезпечують дотримання цих правил, але й захищають від динамічного середовища загроз. Стратегічне планування також має враховувати ризики третіх сторін, управління якими має вирішальне значення в підключеній цифровій екосистемі, і потребу в чіткому плані реагування на інциденти, що може пом'якшити вплив порушень інформаційної безпеки.

Схематичне представлення викликів захисту інформації наведено на рис. 1.

Все це підкреслює, наскільки важко забезпечити всеосяжний захист інформації в умовах цифрової трансформації. Також варто відзначити, що дотримання всіх цих вимог суттєво сповільнює процес цифровізації бізнес-процесів підприємства, оскільки для цього потрібно додаткові таланти, час та ресурси. З іншої сторони вся мета цифровізації полягає в тому, щоб забрати частину обов'язків з працівника і передати їх цифровим механізмам. Таким чином, автоматизувати процеси підприємства для більшої ефективності. Отже, парадокс і основний виклик переходу до цифрової моделі полягає в оптимальному забезпеченні ідеального балансу між інвестиціями в розробки та технології, що зроблять підприємство більш швидким та ефективним, і водночас дотримання надійного захисту інформації, який сповільнює процес цифровізації.

Один із хороших способів для підприємств, які знаходяться в зоні ризику – це програма, спрямована на підвищення адаптивності захисту інформації. Адаптивність описує здатність системи поглинати збої та потрясіння та успішно працювати, незважаючи на них. Підприємства повинні

Рис. 1. Схематичне відображення викликів захисту інформації

Джерело: розроблено авторами

розглядати кібербезпеку як невід'ємну складову бізнесу, використовуючи основні інструменти:

– ***Пріоритезація масивів даних і бізнес-ризиків, залучення топ-менеджменту.*** Підприємства повинні провести ретельне відображення та класифікацію даних, щоб зрозуміти, де зберігаються конфіденційні чи критичні дані та як вони поширюються в організації. Оцінку ризиків слід проводити регулярно, щоб визначити та визначити пріоритетність ризиків, пов'язаних з різними типами даних. Реалізація передбачає підхід "згори донизу", починаючи з вищого керівництво, щоб пріоритети виставлялись відповідно відповідно до бізнес-цілей.

– ***Мобілізація провідних працівників задля демонстрації цінності масивів даних.*** Впровадження може передбачати розробку спеціальних навчальних програм, які висвітлюють конкретні сценарії безпеки, з якими можуть зіткнутися співробітники, показуючи прямий вплив витоку даних на бізнес та їхні особисті інтереси. Гейміфікацію та звичайні вправи можна використовувати для закріплення цих концепцій, роблячи навчання більш привабливим і таким, що запам'ятовується. Необхідно також створити механізми зворотного зв'язку, щоб спонукати співробітників повідомляти про потенційні проблеми безпеки, без осудження.

– ***Інтеграція захисту інформації у міжкомпанійні процеси***. Щоб ефективно інтегрувати кібербезпеку, підриємства можуть почати з впровадження принципів "безпека за замовчуванням" у розробку продуктів та процеси комунікації між відділеннями. Це може включати регулярні перевірки безпеки на кожному етапі життєвого циклу продукту, а також використання автоматизованих інструментів для забезпечення виконання принципів безпеки. Крім того, відділ кібербезпеки може допомогти забезпечити послідовне застосування стандартів і принципів безпеки в усіх інших відділах.

– ***Інтеграція механізмів реагування на інциденти в усі бізнес процеси та їхнє покращення за допомогою реалістичних тестів.*** Підприємства повинні розробити план реагування на інциденти, у якому детально описано конкретні ролі та обов'язки в різних відділах. Необхідно провести навчання та симуляційні вправи, щоб кожен знав свою роль у разі витоку інформації. Рекомендовано планово ініціювати тестові інциденти, щоб автоматизувати реакцію і проводити ітераційне вдосконалення навичок відділень.

– ***Переведення функції захисту інформації в технології для збільшення масштабованості.*** Реалізація цієї практики передбачає вбудовування функцій безпеки безпосередньо в нові технології. Це дозволить автоматизувати роботу моніторингу безпеки. Може реалізовуватись використанням надійних методів шифрування для зберігання та передачі даних, сторонніх сервісів які виявляють загрозу і попережєають про ризики. Необхідно

запланувати регулярні перевірки безпеки та оновлення, щоб забезпечити ефективність заходів безпеки в міру зростання підприємства і руху технологій вперед.

– ***Диференціювання захисту найважливіших активів.*** Ця практика вимагає ідентифікації критичних даних задля застосування багаторівневих засобів контролю безпеки базуючись на рівнях чутливості інформації. Наприклад, критичні бази даних можуть бути ізольовані в захищених сегментах мережі із суворим контролем доступу та моніторингом у реальному часі, тоді як менш конфіденційну інформацію можна захистити за допомогою базових заходів безпеки.

– ***Налаштування системи активного захисту, щоб забезпечувати відповідь на атаки в реальному часі.*** Впровадження систем активного захисту передбачає встановлення передових систем виявлення та запобігання атакам, які постійно відстежують мережеву та системну діяльність на предмет незвичайної поведінки. Ці системи мають бути інтегровані з централізованою системою управління інформацією про безпеку та подіями, щоб забезпечити аналіз у реальному часі, сповіщення та скоординовану реакцію на підприємстві.

– ***Проактивність у захисті***. Організації конкурсів пошуку вразливостей підприємств. Це може бути організовано короткотривалим конкурсом, коли протягом декількох днів оголошується легітимним атакувати ресурси підприємства з метою виявлення невідомих вразливостей. Можна також відкривати сервіси та ресурси для постійного сканування "білими хакерами", які у випадку успішного виявлення вразливостей, отримають винагороду.

Для підприємств, особливо тих, які знаходяться в зоні ризику, важливо розглядати кібербезпеку як невід'ємну складову свого бізнесу. Це означає не лише встановлення базових заходів захисту, але й активну інвестицію у програми, спрямовані на підвищення адаптивності системи захисту інформації. Інтегруючи запропонований комплекс інструменти, підприємства можуть стати більш стійкими до потенційних кіберзагроз. Постійне вдосконалення і підтримка цих заходів дозволять ефективно адаптуватися до нових загроз і зберігати високий рівень захисту інформації у довгостроковій перспективі.

Висновки з проведеного дослідження. У контексті цифрової трансформації, де обсяги даних зростають і кіберзагрози стають більш складними, забезпечення інформаційної безпеки стає критичним завданням для підприємств будь-якого розміру і галузі. Ефективний захист даних потребує поєднання технологічних, організаційних і стратегічних заходів. Тільки комплексний підхід дозволить створити стійку систему інформаційної безпеки. Використання стратегічних підходів дозволяє підприємствам ефективно управляти ризиками та адаптуватися до змін у цифровому середовищі. Розуміння загроз і прийняття свідомих рішень щодо захисту даних є важливими для забезпечення успіху і стійкості бізнесу в епоху цифрової трансформації. Захист даних повинен бути постійним процесом, який враховує нові технології, виклики та стандарти безпеки.

Успішна цифрова трансформація підприємств потребує сильної інформаційної безпеки, що базується на комплексному підході до захисту даних і активному управлінні ризиками. Це є ключовим елементом забезпечення конкурентоспроможності та стійкості в умовах сучасного цифрового середовища.

Стаття має практичне значення для бізнесу, оскільки надає конкретні інструменти і стратегії для підвищення інформаційної безпеки в умовах цифрової трансформації. Це допомагає підприємствам ефективно відповідати на виклики сучасного цифрового середовища та забезпечувати стійкість та надійність їхніх інформаційних ресурсів.

Перспективним напрямом подальших досліджень у галузі захисту даних підприємств в епоху цифрової трансформації є аналіз взаємозв'язку між цифровою трансформацією підприємств і їхньою інформаційною безпекою з огляду на зміну бізнес-процесів, структури IT-інфраструктури та інші аспекти.

Список використаних джерел:

1. Gerald C. Kane, Anh Nguyen Phillips, Jonathan R. Copulsky, Garth R. Andrus. The Technology Fallacy: How People Are the Real Key to Digital Transformation. 2022. URL: https://mitpress.mit.edu/9780262545112/the-technology-fallacy/

2. Проект Закону України про цифровий контент та цифрові послуги. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/38875

3. Sopilnyk L., Skrynkovskyy R., Kovaliv M., Zayats R., Malashko O., Yesimov S., Mykytiuk M. Development of Digital Economy in the Context of Information Security in Ukraine. *Path of Science*. 2020. Vol. 6. No. 5. P. 2023–2032. DOI: http://dx.doi.org/10.22178/pos.58-7

4. Дергалюк Б.В. Вплив цифрової трансформації на забезпечення економічної безпеки підприємства. *Економічний вісник НТУУ "Київський політехнічний інститут.* 2023. № 26. С. 65–68.

5. Дворник О. Стратегії, виклики та успішні практики в епоху цифрової трансформації бізнесу. *Development service industry management*. 2023. № 4. С. 107–111. URL: https://dsim.khmnu.edu.ua/index.php/dsim/article/view/68/48

6. Біличенко М.М., Касьянова Н.В. Вплив цифрової трансформації на формування системи економічної безпеки підприємства. *Бізнес Інформ*. 2023. № 7. С. 83–95.

7. Digital Vortex 2021. Digital Disruption In a COVID World. Global Center For Digital Business Transformation. 2021. URL: https://www.imd.org/contentassets/8c5b42807da941ee95c7be87d54e5db9/20210427-digitalvortex21-report-web-final.pdf

8. Gebremeskel B., Jonathan G., Yalew S. Information Security Challenges During Digital Transformation. *Procedia Computer Science*. 2023. Vol. 219. P. 44–51. DOI: https://doi.org/10.1016/j.procs.2023.01.262

9. Bolton A., Goosen L., Kritzinger E. Security aspects of an empirical study into the impact of digital transformation via unified communication and collaboration technologies on the productivity and innovation of a global automotive enterprise. Information and Cyber Security. 2020. P. 99–113 DOI: https://doi.org/10.1007/978-3-030-43276-8_8

References:

1. Kane G. C., Phillips A. N., Copulsky J. R., & Andrus G. R. (2022) The Technology Fallacy: How People Are the Real Key to Digital Transformation. Available at: https://mitpress.mit.edu/9780262545112/the-technology-fallacy/

2. Draft Law of Ukraine on digital content and digital services. Available at: https://itd.rada.gov.ua/billInfo/Bills/Card/38875

3. Sopilnyk L., Skrynkovskyy R., Kovaliv M., Zayats R., Malashko O., Yesimov S., & Mykytiuk M. (2020) Development of Digital Economy in the Context of Information Security in Ukraine. *Path of Science*, no. 6(5), pp. 2023–2032. DOI: http://dx.doi.org/10.22178/pos.58-7

4. Dergalyuk B. V. (2023) The impact of digital transformation on ensuring the economic security of the enterprise. *Economic Bulletin of NTUU "Kyiv Polytechnic Institute",* no. 26, pp. 65–68.

5. Dvornyk O. (2023) Strategies, challenges and successful practices in the era of digital business transformation. *Development Service Industry Management*, no. 4, pp. 107–111. Available at: https://dsim.khmnu.edu.ua/index.php/dsim/article/view/68/48

6. Bilichenko M. M., & Kasyanova N. V. (2023) The influence of digital transformation on the formation of the economic security system of the enterprise. *Business Inform*, no. 7, pp. 83–95.

7. Global Center For Digital Business Transformation. (2021). Digital Vortex 2021: Digital Disruption In a COVID World. Available at: https://www.imd.org/contentassets/8c5b42807da941ee95c7be87d54e5db9/20210427-digitalvortex21-report-web-final.pdf

8. Gebremeskel B., Jonathan G., & Yalew S. (2023) Information Security Challenges During Digital Transformation. *Procedia Computer Science*, no. 219, pp. 44–51. DOI: https://doi.org/10.1016/j.procs.2023.01.262

9. Bolton A., Goosen L., & Kritzinger E. (2020) Security aspects of an empirical study into the impact of digital transformation via unified communication and collaboration technologies on the productivity and innovation of a global automotive enterprise. Information and Cyber Security. P. 99–113. DOI: https://doi.org/10.1007/978-3-030-43276-8_8

E-mail: mariana.y.hvozd@lpnu.ua