Ганна В. Єфімова[1], Артем В. Іващенко[2]

ДОСЛІДЖЕННЯ ВПЛИВУ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ НА ЕКОНОМІЧНІ АСПЕКТИ КІБЕРБЕЗПЕКИ В БІЗНЕС СЕРЕДОВИЩІ

Досліджено вплив цифрової трансформації на економічні аспекти кібербезпеки в бізнес середовищі. Розглянуто основні виклики та можливості, які виникають у процесі впровадження новітніх технологій. Проаналізовано економічні наслідки кіберзагроз та запропоновано стратегії для підвищення рівня кіберзахисту бізнесу.

Ключові слова: *цифрова трансформація, кібербезпека, бізнес середовище, кіберзагрози, стратегії кіберзахисту.*

Рис. 2. Літ.20.

DOI: 10.32752/1993-6788-2024-1-274-163-174

Anna V. Efimova, Artem V. Ivashchenko

STUDY OF THE IMPACT OF DIGITAL TRANSFORMATION ON THE ECONOMIC ASPECTS OF CYBERSECURITY IN THE BUSINESS ENVIRONMENT

The impact of digital transformation on the economic aspects of cybersecurity in the business environment has been investigated. The main challenges and opportunities arising from the implementation of new technologies have been considered. The economic consequences of cyber threats have been analyzed, and strategies for improving business' cybersecurity have been proposed.

Keywords: *digital transformation, cybersecurity, business environment, cyber threats, cybersecurity strategies.*

Peer-reviewed, approved and placed: *20.04.2024.*

Постановка проблеми. Нові технології мають великі перспективи. Вони створюють нові шляхи і можливості для більш процвітаючого майбутнього. Але вони також ставлять нові виклики. Хоча цифрові технології засліплюють блиском і досконалістю своїх застосувань, вони поки що не принесли очікуваних дивідендів у вигляді зростання продуктивності праці в повному обсязі.

Дійсно, за останні кілька десятиліть сукупне зростання продуктивності сповільнилося в багатьох економіках. Як наслідок, темпи економічного зростання стали нижчими. [1-2]

Водночас нерівність у доходах і пов'язані з нею диспропорції зросли, особливо в розвинених країнах, що спричинило соціальне невдоволення та політичний застій. У різних країнах спостерігається нерівномірна участь у нових можливостях, створених цифровою трансформацією. [3] Багато хто залишається позаду, як серед галузей і фірм, так і серед робочої сили та різних верств суспільства. Фірми, що перебувають на технологічному рубежі, відірвалися від решти, здобувши домінування на ринках, що дедалі більше концентруються, і отримують більшу частку прибутку від нових технологій. У

[1] National University of Shipbuilding Admiral Makarov. Ukraine.
[2] National University of Shipbuilding Admiral Makarov. Ukraine.

той час як зростання продуктивності в цих компаніях було високим, в інших компаніях воно стагнувало або сповільнювалося, що пригнічувало сукупне зростання продуктивності. Зростаюча автоматизація завдань низької та середньої кваліфікації змістила попит на робочу силу в бік навичок вищого рівня, що негативно вплинуло на заробітну плату та робочі місця на нижньому кінці спектру кваліфікацій. Оскільки нові технології сприяють зростанню капіталу, досягненню бізнес-результатів за принципом «переможець отримує все» та розвитку навичок вищого рівня, розподіл доходів від капіталу та праці став більш нерівномірним, а дохід зміщується від праці до капіталу.

Однією з важливих причин таких результатів є те, що політика та інституції повільно пристосовуються до трансформацій, що розгортаються. Щоб реалізувати потенціал сучасних розумних машин, політика також має бути розумнішою. Вони повинні швидше реагувати на зміни, щоб повною мірою скористатися потенційними можливостями підвищення продуктивності та економічного зростання, а також боротися зі зростаючою нерівністю, оскільки технологічні прориви створюють переможців і переможених.

Це питання може здатися простим, але воно є одним із найважливіших для компаній у всьому світі. Незважаючи на численні зусилля з удосконалення цифрових систем протягом останніх десятиліть, кібербезпека залишається надзвичайно актуальною проблемою.

Аналіз останніх досліджень та публікацій. Дослідженню загального становлення цифрової трансформацій та вплив кіберпезпеки на економічні аспекти у бізнес середовищі, присвячені публікації таких науковців, як А. Кузіор, Т. Васильєва, О. Кузменко [4], А. Аль-Тамімі [5], В. Гончар [10], А. Рамірез [19] та ін. Враховуючи швидкий розвиток технологій, з'являються нові типи кіберзагроз, які потребують негайного вивчення. Наприклад, питання захисту від атак на квантові комп'ютери або проблеми безпеки у хмарних обчисленнях залишаються недостатньо дослідженими. А. Рамірез і В. Гончар обговорювали загальні аспекти, але залишається багато невирішених питань у сфері регуляторного забезпечення кібербезпеки, особливо в контексті міжнародного співробітництва та гармонізації нормативних актів. Багато дослідників не приділили достатньо уваги питанням інтеграції кібербезпеки в стратегічне планування бізнесу. Важливо вивчити, як бізнес може оптимізувати витрати на кіберзахист, інтегруючи його в основні бізнес-процеси, а також як розробляти ефективні стратегії кібербезпеки, що відповідають вимогам сучасного бізнесу. Наприклад, використання блокчейн-технологій для підвищення прозорості та незламності систем захисту або розробка нових методів управління кіберризиками, що базуються на аналізі великих даних та машинного навчання.

Потреба в розробці нових методів для прогнозування та моделювання кіберзагроз і їх економічного впливу зростає. Це дозволить бізнесу бути більш підготовленим до можливих атак та мінімізувати економічні збитки.

Метою дослідження є дослідження впливу цифрової трансформації на кібербезпеку бізнесу, визначення основних ризиків, які можуть відобразитись на бізнес середовищі, та окреслення основних підходів до забезпечення кібербекзпеки бізнесу.

Основні результати дослідження. Цифрова трансформація означає впровадження цифрових рішень у бізнес-процесах організацій, що може призвести до значних змін у їхній діяльності. Така модифікація може вплинути на різні аспекти організації, наприклад, на користувацький досвід, бізнес-процеси, цільові ринки, клієнтів, відносини з клієнтами. Прискорене використання технологій бізнес-організаціями під час пандемії COVID-19 також призвело до багатьох гострих викликів [4]. Нові технології, такі як штучний інтелект, великі дані та аналітика, блокчейн, хмарні обчислення, Інтернет речей та промисловий Інтернет речей, є ключовими факторами для цифрової трансформації. Завдяки значним перевагам бізнеси прискорюють процес цифрової трансформації. Велика різниця полягає в тому, що протягом перших 50 років комп'ютери підтримували бізнес-процеси, автоматизуючи функції бек-офісу, такі як облік, виставлення рахунків, обробка даних, адміністративна робота тощо. Проте з моменту появи Інтернету в середині 1990-х років обчислювальна та мережева інфраструктура еволюціонувала до того, що тепер вони є головним джерелом передової бізнес-цінності, що надається безпосередньо клієнтам, діловим партнерам, співробітникам та іншим зацікавленим сторонам. Значною мірою це пов'язано з повним перепроектуванням мережі, яке відбулося лише за останні кілька років. Перетин кібербезпеки з цифровою трансформацією є ключовим центром у динамічному цифровому ландшафті. Організації прагнуть тримати крок з розвитком технологій.

Цифрова трансформація – це більше, ніж лише оновлення технологій. Це комплексна метаморфоза, яка впливає на всі аспекти організації. Інтеграція цифрових технологій змінює основу бізнес-операцій, від операційних процесів до взаємодії з клієнтами. Привабливість цифрових потужностей, однак, приносить із собою збільшену потребу в надійних кіберзаходах. Поки бізнес використовує цифрові інновації для отримання конкурентної переваги, він також повинен посилити заходи кібербезпеки, оскільки кіберзагрози продовжують зростати. Цей складний баланс між захистом і прогресом відкриває можливості для глибокого дослідження взаємозв'язку між кібербезпекою та цифровою трансформацією. Однак кібербезпека стала серйозним викликом для компаній, і для забезпечення неперервності бізнесу вони повинні забезпечити безпеку своїх інструментів та артефактів цифрової трансформації. Тому важливо, щоб компанії, які переходять до цифрової трансформації, надавали пріоритет кібербезпеці та переконувалися, що їхні системи захищені від потенційних загроз [4, 5].

Фінансові та економічні системи все більше залежать від багатьох цифрових систем і великих даних. Цей висхідний тренд дозволяє існувати соціально-економічним об'єктам. Розуміння ключових ідей глобальної цифрової економіки гарантує стабільне функціонування фінансової системи [4]. У зв'язку з цим існує багато проблем і проблем, пов'язаних, по-перше, з довірою до цифрових систем; по-друге, визначення сили цифрової довіри для поєднання бізнесу [5], політики, громадської, соціальної та особистої інформації; по-третє, визначення впливу ключових індикаторів на цифрову еволюцію [6] з огляду на глобальну пандемію [7-9].

Як державний, так і приватний сектори стають жертвами сплеску атак з використанням програм-вимагачів. Оскільки до 2025 року кіберзлочинність коштуватиме світу 10,5 трильйонів доларів США щорічно, бізнес повинен розглядати кібербезпеку як невід'ємну частину своїх стратегій цифрової трансформації. Кібератаки не лише небезпечні тим, що викривають конфіденційні дані, але й тим, що вимагають значних витрат і часу на врегулювання. Захистивши свої дані, організації можуть зосередитися на інноваціях та продовженні роботи. Ми бачимо, як багато компаній інвестують у кібер-сховища – комплексні рішення для відновлення, які захищають наскрізну IT-систему, щоб захистити свої дані. Захищаючи кожну частину свого бізнесу, компанії знижують ризик атак і стають більш кіберстійкими в довгостроковій перспективі [13].

Незважаючи на те, що безпека зараз враховується в рівнянні інвестиційних рішень, лідери не повинні сприймати безпеку як «податок», а радше як стимул для венчурного бізнесу. Новий статус безпеки як інвестиції в бізнес також означає, що особам, які приймають рішення, необхідно враховувати економічну віддачу від цих інвестицій (ROI). Розрахунок рентабельності інвестицій у кібербезпеку має два аспекти: економічна ефективність витрат на безпеку для захисту внутрішніх активів, процесів і людей підприємства та те, наскільки безпека сприяє позитивній зовнішній цінній пропозиції, представленій клієнтам, партнерам і зацікавленим сторонам [13].

Ефективні лідери розуміють, що кібербезпека – це не ізольована IT-проблема, а критична бізнес-функція, яка впливає на всі аспекти діяльності організації. Вони стежать за тим, щоб обговорення кібербезпеки не обмежувалося лише IT-відділом, а стало регулярним елементом розмов у залі засідань ради директорів.

Бізнес-одиниці є дуже гетерогенними, що призводить до різноманітності технологічних систем, що застосовуються в організаціях. Сучасні технології, такі як Інтернет речей, можуть допомогти організаціям покращити кібербезпеку [9].

В. Гончар [10] розробила теоретичні та практичні рекомендації щодо покращення економічної безпеки в цифровій економіці. А саме, було проведено дослідження впливу цифрових технологій на підприємницьку діяльність в Україні, виявивши, що бізнеси все більше використовують інформаційні та комунікаційні технології. Проте були виявлені різниці на основі розміру та сектору, запропоновано методологію для оцінки рівня цифрової трансформації країни в цьому контексті, яка може допомогти уніфікувати вивчення умов, пов'язаних з підприємництвом та інноваціями. Однак у дослідженні не було виявлено значного зв'язку між рівнями ефективності компаній, що вивчалися, та їхнім ступенем цифровізації через низьку участь персоналу у цих проектах. Висновок полягає в тому, що хоча бізнеси використовують все більше технологій у всіх секторах, включаючи банківський, оскільки це збільшує гнучкість і можливості продажу, а також зменшує внутрішні витрати, такі як час, витрачений на перепідготовку працівників, які можуть ще не бути ознайомленими або не мати достатніх

навичок, необхідних у поточний момент, з урахуванням швидких змін, що відбуваються у всьому світі, потрібно більше залучати персонал у ці проекти, якщо вони мають вплив на рівні ефективності бізнесу. Тому дії повинні спрямовуватися не лише на підтримку стійкості підприємства проти ризиків, пов'язаних із загрозами кібербезпеки, але й на сприяння покращенню кваліфікації персоналу, необхідної для виконання більш складних завдань, що виникають внаслідок автоматизації бізнес-процесів завдяки впровадженню технологій у всіх секторах, включаючи банківський, де це збільшує гнучкість і можливості продажу, а також зменшує внутрішні витрати, такі як час, витрачений на перепідготовку працівників [8].

У іншій статті Кузіор та ін. [4] описали зближення процесів цифровізації між країнами на основі таких факторів, як використання Інтернету, метрики інфраструктури та доступ до ІКТ. У цьому дослідженні використовувався коефіцієнт варіації для визначення сигма-збіжності. Розроблено економетричну модель, яка описує вплив рівнів кібербезпеки країни, легкість здійснення бізнесу та індекси боротьби з відмиванням грошей на цифровий розвиток. Мета цього дослідження полягала в розумінні ключових визначників, які формують ризик використання фінансових інструментів для відмивання грошей та фінансування тероризму в контексті глобальних цифрових тенденцій.

Крім того, в дослідженні Путрі та ін. [12] був представлений приклад переходу від довідника до цифровизації в Індонезії. Були використані якісні дослідницькі підходи, такі як вивчення та опис подій через взаємодію з іншими, ментальні образи та сприйняття. Вони були засновані на думці громадськості, щоб сприяти використанню цифровизації у громадському бізнесі та послугах і дотримуватися тенденцій, помічених відповідними сторонами, а також сприяти урядовому сектору у розвитку послуг та оцінці ефективності концепцій за допомогою рамки кібербезпеки "шість складників" (SWCSF) та Системи електронного уряду (SPBE), якою використовується багато урядових агентств.

Цифрова трансформація – це глобальне явище, яке привертає увагу в кожній галузі та стимулює великі інвестиції. Однак цифрова трансформація не є єдиною метою; це багатогранний підхід, який залежить від цілей відповідної галузі та цифрової зрілості. Таким чином, цифрова трансформація – це шлях зміни монолітного бізнес-підходу до повністю оцифрованих бізнес-концепцій [7].

Протягом останніх років звичайні компанії зазнавали атаки, які призводила до втрати даних або проблем із відповідністю. Однак варто зазначити, що деякі організації, які зазнали порушень, не зазнали жодних втрат даних, проблем з відповідністю чи збоїв через чудову готовність до безпеки [11].

Якщо дивитися на бізнес-одиниці, які досягли більшого успіху в протистоянні атакам і захисті своїх даних, кілька підходів виділяються як найкращі практики.

- інтеграція систем для створення єдиної архітектури безпеки;
- поширення інформації про загрози в усій компанії;

- забезпечення роботи захисних засобів на всіх ділянках мережі;
- автоматизація більшої частини методів безпеки.

Впровадження цих практик безпеки у своїх мережах, компанії зможуть прийняти цифрову трансформацію, мінімізуючи проблеми безпеки та відповідності.

Однією з головних проблем у цифровій трансформації є злиття нових технологій, таких як штучний інтелект, великі дані та аналітика, блокчейн, хмарні обчислення та послуги, Інтернет речей і промисловий Інтернет речей та інші. У зв'язку з цим Хмарні обчислення та послуги досягають нового покоління штучного інтелекту, застосовуваного у все більшій кількості промислових програм із безпрецедентними результатами [9]. Окрім цього, Інтернет речей об'єднує промислові пристрої та об'єкти в рамках промислових ланцюжків створення вартості та інфраструктури, але щодня генерує терабайти даних, для роботи з якими потрібні Big Data та Analytics. Тому цифрова трансформація має величезний вплив на промислові системи та процеси, а також на ключовий показник ефективності (KPI). Крім того, нові технології також матимуть величезний вплив на реалізацію циркулярної економіки в промислових секторах, парадигми сучасної цифрової трансформації в промислових, державних і приватних обговореннях щодо зменшення парникового ефекту. На цьому тлі цифрова трансформація привернула велику увагу в усіх промислових, державних і приватних організаціях, що кардинально змінить підходи до операційної діяльності в усіх секторах [12]. Отже, трансформацію бізнес-одиниць через оцифрування та нові технології можна назвати технологічною хвилею, такою як третя, а тепер і четверта промислова трансформація. У цьому контексті четверта індустріальна трансформація оптимізує комп'ютеризацію третьої шляхом оцифрування, мереж бездротової інфраструктури, інтелектуальних алгоритмів тощо, яка сьогодні відома як парадигма цифрової трансформації. Таким чином, оцифрування та технології цифрової трансформації створюють і, відповідно, змінюють ринкові пропозиції, бізнес-процеси або бізнес-моделі, які є результатом використання обох. Однак внутрішня складність цифрової трансформації також робить обізнаність про кібербезпеку обов'язковою умовою.

Кібербезпека має справу з наявністю кіберзловмисників із їх репертуаром кіберзлочинних атак. Таким чином, кібербезпека розуміється як сукупність знань щодо технологій, процесів і практик, призначених для захисту комп'ютерних систем, мереж, ресурсів інфраструктури та інших від атак кіберзлочинців, пошкоджень, маніпуляцій або несанкціонованого доступу.

Існує декілька ключових стратегій кібербезпеки, які застосовуються в бізнес середовищі та можуть сприяти покращенню економічних аспектів, а саме: многошарова безпека та управління ризиками.

Многошарова безпека (рис.1) є стратегією, яка включає створення кількох рівнів захисту, що працюють разом для забезпечення комплексного захисту інформаційних систем. Цей підхід забезпечує додаткові рівні безпеки, що ускладнює для зловмисників доступ до критичної інформації.

Основні компоненти многошарової безпеки:

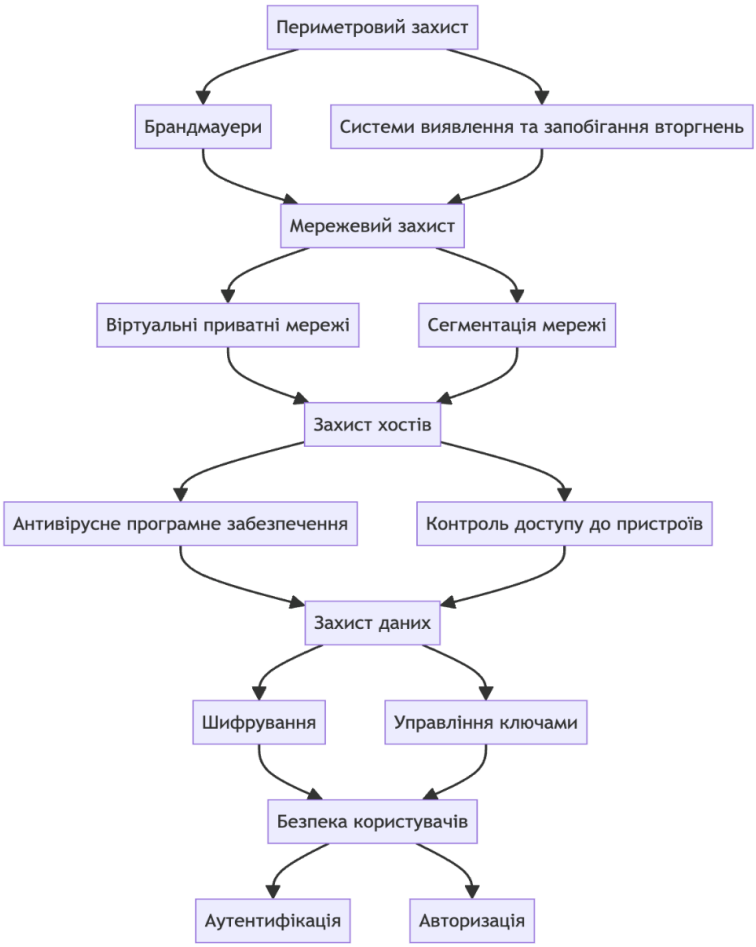

Рис. 1. Схема многошарової безпеки (Defense in Depth)

1. Периметровий захист:

Брандмауери (Firewalls): Використовуються для контролю вхідного та вихідного мережевого трафіку на основі визначених правил безпеки. Вони захищають мережу від несанкціонованого доступу. Системи виявлення та запобігання вторгнень (IDS/IPS): IDS (Intrusion Detection Systems) виявляють потенційні загрози, тоді як IPS (Intrusion Prevention Systems) не лише виявляють, але й активно запобігають вторгненням.

2. Мережевий захист:

Віртуальні приватні мережі (VPN): Забезпечують безпечне з'єднання між користувачами та корпоративною мережею через інтернет, використовуючи шифрування. Сегментація мережі: Розділення мережі на менші сегменти для обмеження руху зловмисників у разі проникнення.

3. Захист хостів:

Антивірусне програмне забезпечення: Виявляє та видаляє шкідливе програмне забезпечення на окремих пристроях. Контроль доступу до пристроїв: Забезпечує, що тільки авторизовані пристрої можуть підключатися до мережі.

4. Захист даних:

Шифрування: Перетворює дані в закодований формат, який може бути розшифрований тільки авторизованими користувачами. Управління ключами: Забезпечує безпечне зберігання та управління криптографічними ключами.

5. Безпека користувачів:

Аутентифікація: Перевірка особи користувача за допомогою паролів, біометрії або інших методів. Авторизація: Визначає рівень доступу користувачів до ресурсів на основі їх ролей і прав.

Управління ризиками (рис.2) в контексті кібербезпеки є критично важливим елементом захисту бізнесу від можливих загроз. Цей процес включає ідентифікацію, оцінку, та пом'якшення ризиків, що дозволяє мінімізувати потенційні збитки від кіберінцидентів.

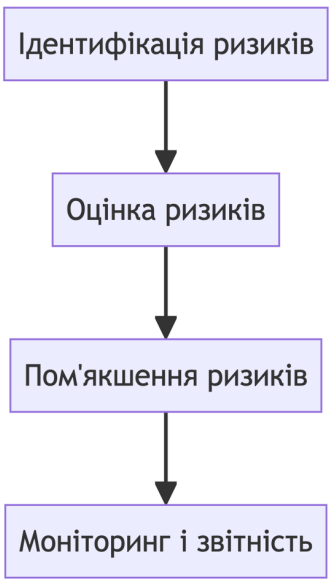

Рис. 2. **Схема многошарової безпеки (Defense in Depth)**

Основні етапи управління ризиками:

1. Ідентифікація ризиків:

Виявлення всіх можливих загроз і вразливостей, які можуть вплинути на інформаційні системи. Використання різних методів, таких як анкетування, аналіз даних, аудити безпеки.

2. Оцінка ризиків:

Визначення ймовірності та потенційного впливу кожного ризику. Використання кількісних та якісних методів оцінки для пріоритизації ризиків.

3. Пом'якшення ризиків:

Розробка та впровадження заходів для зменшення ймовірності або впливу ризиків. Включає використання технічних, адміністративних та фізичних заходів.

4. Моніторинг і звітність:

Постійний моніторинг ризиків та ефективності заходів безпеки.

Регулярне звітування та оновлення стратегії управління ризиками відповідно до нових загроз.

Висновки. В умовах цифрової трансформації кібербезпека набуває критичної ролі. Цифрова трансформація перетворила бізнес-середовище, перехід організаційних процесів до ІТ-рішень призвів до значних змін у різних аспектах діяльності компаній. Вона впливає на кілька елементів, таких як користувацький досвід, операції, ринки, клієнти, відносини та культурні відмінності. Нові технології, включаючи штучний інтелект, великі дані та аналітику, технологію блокчейн, хмарні обчислення та послуги, приводять до цифрової трансформації по всьому світу, одночасно збільшуючи кібербезпечні ризики для бізнесу, які переживають цей процес. Компанії, які проходять процес цифрової трансформації, стають більш вразливими перед кібератаками та порушеннями безпеки. Кібербезпека є важливою складовою цифрової трансформації, оскільки вона допомагає запобігти перервам через злочинну діяльність або несанкціонований доступ з боку атакувальників, які прагнуть змінити, знищити або вимагати чутливу інформацію від користувачів. Тому організації, які впроваджують ЦТ, повинні надавати пріоритет кібербезпеці, щоб забезпечити успішний перехід без будь-яких перерв, спричинених порушеннями безпеки.

Дослідження підкреслює, що цифрова трансформація – це складний та постійний процес, для якого організації повинні бути свідомими нових технологій та пов'язаних з ними ризиків безпеки. Переходячи свої основні операції до ІТ-рішень, компанії повинні забезпечити відповідні заходи для захисту даних та мереж від несанкціонованого доступу або злочинних дій. За результатами дослідження рекомендується впровадження шифрування або полісів кіберстрахування для зменшення цих ризиків під час цифрової трансформації. В перспективі необхідно розробити рекомендації для компаній щодо набуття всеосяжних знань про кіберзагрози протягом всього бізнес-процесу, що включатиме виявлення потенційних вразливостей на початкових етапах і активне їх вирішення.

1. Brynjolfsson, E, D Rock and C Syverson (2021), “The productivity J-curve: How intangibles complement general purpose technologies”, American Economic Journal: Macroeconomics 13(1): 333-372. URL: https://www.aeaweb.org/articles?id=10.1257/mac.20180386

2. Goldin, I, P Koutroumpis, F Lafond and J Winkler (2022), “Why is productivity slowing down?”, OMPTEC Working paper. URL: https://www.inet.ox.ac.uk/files/2022-7-WP-Paper-2-Why-is-Productivity-Slowing-Down-OMPTEC-FoW-FoD-Ian-copy_2022-06-09-133241_hfcj.pdf

3. Santos, Gilberto & Magalhres, Maria & Carvalho, Sandro & Pinto, Ricardo & Fйlix, Maria Joro & Rosak-Szyrocka, Joanna. (2022). DIGITAL TRANSFORMATION AND GLOBAL INEQUALITY. International Journal for Quality Research. 16. 1297-1314. 10.24874/IJQR16.04-22. URL: https://www.researchgate.net/publication/365602122_DIGITAL_TRANSFORMATION_AND_GLOBAL_INEQUALITY

4. Kuzior, A.; Vasylieva, T.; Kuzmenko, O.; Koibichuk, V.; Brozek, P. Global Digital Convergence: Impact of Cybersecurity, Business Transparency, Economic Transformation, and AML Efficiency. URL: https://www.researchgate.net/publication/364971598_Global_Digital_Convergence_Impact_of_Cybersecurity_Business_Transparency_Economic_Transformation_and_AML_Efficiency

5. Saeed, S.; Altamimi, S.A.; Alkayyal, N.A.; Alshehri, E.; Alabbad, D.A. Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. Sensors 2023, 23, 6666. URL: https://doi.org/10.3390/ s23156666

6. How Digital Transformation Has Impacted Security and How to Minimize Risk, BrandPost Jul 26, 2018 URL : https://www.csoonline.com/article/565927/how-digital-transformation-has-impacted-security-and-how-to-minimize-risk.html

7. Cybersecurity in the Digital Business Transformation Era. By Peerapong Jongvibool June 18, 2018 URL: https://www.fortinet.com/blog/industry-trends/cybersecurity-in-the-digital-business-transformation-era

8. Digital Transformation: An Overview of the Current State of the Art of Research. Sascha Kraus, Paul Jones. URL: https://journals.sagepub.com/doi/full/10.1177/21582440211047576

9. What is the digital economy and how is it transforming business? URL: https://www.weforum.org/agenda/2022/05/digital-economy-transforming-business/

10. Gonchar, V. The Transformation of Entrepreneurial Activity in the Conditions of the Development of the Digital Economy and a Methodology of Assessing Its Digital Security in Digital Technologies in the Contemporary Economy: Collective Monograph; Simanavi ciene, Ed.; Mykolas Romeris University Research: Vilnius, Lithuania, 2022; ISBN 9786094880506. URL: https://www.researchgate.net/publication/369214796_Digital_technologies_collective_monograph_2022

11. Cybersecurity Trends: Optimize for Resilience and Performance https://www.gartner.com/en/cybersecurity/topics/cybersecurity-trends

12. Digital McKinsey and Global Risk Practice Cybersecurity in a Digital Era URL: https://www.mckinsey.com/~/media/mckinsey/business%20functions/risk/our%20insights/cybersecurity%20in%20a%20digital%20era/cybersecurity%20in%20a%20digital%20era.pdf

13. The Crucial Role of Cybersecurity in Digital Transformation by Team EM URL: https://blog.emb.global/cybersecurity-in-digital-transformation/

14. Gull, H.; Saeed, S.; Iqbal, S.Z.; Bamarouf, Y.A.; Alqahtani, M.A.; Alabbad, D.A.; Alamer, A. An empirical study of mobile commerce and customers security perception in Saudi Arabia. Electronics 2022, 11, 293. URL: https://www.academia.edu/92049900/An_Empirical_Study_of_Mobile_Commerce_and_Customers_Security_Perception_in_Saudi_Arabia?uc-sb-sw=83097700

15. Anthi, E.; Williams, L.; Rhode, M.; Burnap, P.; Wedgbury, A. Adversarial attacks on machine learning cybersecurity defences in industrial control systems. J. Inf. Secur. Appl. 2021, 58, 102717. URL: https://www.sciencedirect.com/science/article/pii/S2214212620308607

16. Meeran, Y.A.; Shyry, S.P. Resilient Detection of Cyber Attacks in Industrial Devices. In Proceedings of the 2023 7th International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 11–13 April 2023; pp. 564–569. URL: https://www.researchgate.net/publication/373091797_Digital_Transformation_and_Cybersecurity_Challenges_for_Businesses_Resilience_Issues_and_Recommendations

17. Ameri, K.; Hempel, M.; Sharif, H.; Lopez Jr, J.; Perumalla, K. Design of a novel information system for semi-automated management of cybersecurity in industrial control systems. ACM Trans. Manag. Inf. Syst. 2023, 14, 1–35. URL: https://dl.acm.org/doi/10.1145/3546580

18. Buja, A.; Apostolova, M.; Luma, A. Enhancing Cyber Security in Industrial Internet of Things Systems: An Experimental Assessment. In Proceedings of the 2023 12th Mediterranean Conference on Embedded Computing (MECO), Budva, Montenegro, 14 June 2023; pp. 1–5. URL: https://www.semanticscholar.org/paper/Enhancing-Cyber-Security-in-Industrial-Internet-of-Buja Apostolova/ed087b19cb55a30f095b751d71adc3eb384f5b7a

19. Ramirez, R.; Chang, C.K.; Liang, S.H. PLC Cybersecurity Test Platform Establishment and Cyberattack Practice. Electronics 2023, 12, 1195. URL: https://www.mdpi.com/2079-9292/12/5/1195

20. 7 Building Blocks of an Effective Cyber Security Strategy By Eyal Katz November 16, 2021 URL : https://spectralops.io/blog/7-building-blocks-of-an-effective-cyber-security-strategy/

1. Brynjolfsson, E, D Rock and C Syverson (2021), "The productivity J-curve: How intangibles complement general purpose technologies", American Economic Journal: Macroeconomics 13(1): 333-372. URL: https://www.aeaweb.org/articles?id=10.1257/mac.20180386

2. Goldin, I, P Koutroumpis, F Lafond and J Winkler (2022), "Why is productivity slowing down?", OMPTEC Working paper. URL: https://www.inet.ox.ac.uk/files/2022-7-WP-Paper-2-Why-is-Productivity-Slowing-Down-OMPTEC-FoW-FoD-Ian-copy_2022-06-09-133241_hfcj.pdf

3. Santos, Gilberto & Magalhres, Maria & Carvalho, Sandro & Pinto, Ricardo & Fălix, Maria Joro & Rosak-Szyrocka, Joanna. (2022). DIGITAL TRANSFORMATION AND GLOBAL INEQUALITY. International Journal for Quality Research. 16. 1297-1314. 10.24874/IJQR16.04-22. URL: https://www.researchgate.net/publication/365602122_DIGITAL_TRANSFORMATION_AND_GLOBAL_INEQUALITY

4. Kuzior, A.; Vasylieva, T.; Kuzmenko, O.; Koibichuk, V.; Brozek, P. Global Digital Convergence: Impact of Cybersecurity, Business Transparency, Economic Transformation, and AML Efficiency. URL: https://www.researchgate.net/publication/364971598_Global_Digital_Convergence_Impact_of_Cybersecurity_Business_Transparency_Economic_Transformation_and_AML_Efficiency

5. Saeed, S.; Altamimi, S.A.; Alkayyal, N.A.; Alshehri, E.; Alabbad, D.A. Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. Sensors 2023, 23, 6666. URL: https://doi.org/10.3390/ s23156666

6. How Digital Transformation Has Impacted Security and How to Minimize Risk, BrandPost Jul 26, 2018 URL : https://www.csoonline.com/article/565927/how-digital-transformation-has-impacted-security-and-how-to-minimize-risk.html

7. Cybersecurity in the Digital Business Transformation Era. By Peerapong Jongvibool June 18, 2018 URL: https://www.fortinet.com/blog/industry-trends/cybersecurity-in-the-digital-business-transformation-era

8. Digital Transformation: An Overview of the Current State of the Art of Research. Sascha Kraus, Paul Jones. URL: https://journals.sagepub.com/doi/full/10.1177/21582440211047576

9. What is the digital economy and how is it transforming business? URL: https://www.weforum.org/agenda/2022/05/digital-economy-transforming-business/

10. Gonchar, V. The Transformation of Entrepreneurial Activity in the Conditions of the Development of the Digital Economy and a Methodology of Assessing Its Digital Security in Digital Technologies in the Contemporary Economy: Collective Monograph; Simanavi ciene, Ed.; Mykolas Romeris University Research: Vilnius, Lithuania, 2022; ISBN 9786094880506. URL: https://www.researchgate.net/publication/369214796_Digital_technologies_collective_monograph_2022

11. Cybersecurity Trends: Optimize for Resilience and Performance https://www.gartner.com/en/cybersecurity/topics/cybersecurity-trends

12. Digital McKinsey and Global Risk Practice Cybersecurity in a Digital Era URL: https://www.mckinsey.com/~/media/mckinsey/business%20functions/risk/our%20insights/cybersecurity%20in%20a%20digital%20era/cybersecurity%20in%20a%20digital%20era.pdf

13. The Crucial Role of Cybersecurity in Digital Transformation by Team EM URL: https://blog.emb.global/cybersecurity-in-digital-transformation/

14. Gull, H.; Saeed, S.; Iqbal, S.Z.; Bamarouf, Y.A.; Alqahtani, M.A.; Alabbad, D.A.; Alamer, A. An empirical study of mobile commerce and customers security perception in Saudi Arabia. Electronics 2022, 11, 293. URL: https://www.academia.edu/92049900/An_Empirical_Study_of_Mobile_Commerce_and_Customers_Security_Perception_in_Saudi_Arabia?uc-sb-sw=83097700

15. Anthi, E.; Williams, L.; Rhode, M.; Burnap, P.; Wedgbury, A. Adversarial attacks on machine learning cybersecurity defences in industrial control systems. J. Inf. Secur. Appl. 2021, 58, 102717. URL: https://www.sciencedirect.com/science/article/pii/S2214212620308607

16. Meeran, Y.A.; Shyry, S.P. Resilient Detection of Cyber Attacks in Industrial Devices. In Proceedings of the 2023 7th International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 11–13 April 2023; pp. 564–569. URL: https://www.researchgate.net/publication/373091797_Digital_Transformation_and_Cybersecurity_Challenges_for_Businesses_Resilience_Issues_and_Recommendations

17. Ameri, K.; Hempel, M.; Sharif, H.; Lopez Jr, J.; Perumalla, K. Design of a novel information system for semi-automated management of cybersecurity in industrial control systems. ACM Trans. Manag. Inf. Syst. 2023, 14, 1–35. URL: https://dl.acm.org/doi/10.1145/3546580

18. Buja, A.; Apostolova, M.; Luma, A. Enhancing Cyber Security in Industrial Internet of Things Systems: An Experimental Assessment. In Proceedings of the 2023 12th Mediterranean Conference on

Embedded Computing (MECO), Budva, Montenegro, 14 June 2023; pp. 1–5. URL: https://www.semanticscholar.org/paper/Enhancing-Cyber-Security-in-Industrial-Internet-of-Buja Apostolova/ed087b19cb55a30f095b751d71adc3eb384f5b7a

19. Ramirez, R.; Chang, C.K.; Liang, S.H. PLC Cybersecurity Test Platform Establishment and Cyberattack Practice. Electronics 2023, 12, 1195. URL: https://www.mdpi.com/2079-9292/12/5/1195

20. 7 Building Blocks of an Effective Cyber Security Strategy By Eyal Katz November 16, 2021 URL : https://spectralops.io/blog/7-building-blocks-of-an-effective-cyber-security-strategy/