DOI: https://doi.org/10.30837/EK.2023.031

Тохтамиш Н.І.,
старший викладач кафедри економічної кібернетики
та управління економічною безпекою,
Харківський національний університет радіоелектроніки
ORCID: https://orcid.org/0009-0009-5572-8553
Курденко О.В.,
старший викладач кафедри економічної кібернетики
та управління економічною безпекою,
Харківський національний університет радіоелектроніки
ORCID: https://orcid.org/0000-0002-2127-230X
Шарко С.М.,
здобувач,
Харківський національний університет радіоелектроніки
ORCID: https://orcid.org/0009-0009-2419-1810

ЕКОНОМІЧНА БЕЗПЕКА ПІДПРИЄМСТВА В КОНТЕКСТІ ЦИФРОВОГО РОЗВИТКУ: НОВІ МОЖЛИВОСТІ ТА ЗАГРОЗИ

Економічна безпека є ключовою характеристикою стабільного функціонування та досягнення необхідних показників розвитку як окремих суб’єктів господарювання, так і суспільства в цілому.

Безпека економічних процесів характеризується численними політико-правовими та економічними механізмами та інструментами захисту економічних інтересів. У широкому розумінні економічну безпеку можна розглядати як здатність інституційно-організаційної системи захищати інтереси суб'єктів господарювання на основі міжнародних і національних правових норм щодо та дотримання національних традицій і цінностей господарювання. Інноваційні

інформаційно-комп’ютерні технології, що становлять основу цифрової економіки, відіграють значну роль у розвитку всіх сторін суспільства. Процеси цифровізації особливо суттєво впливають на господарську діяльність суб’єктів господарювання, а отже, і на забезпечення їх економічної безпеки [1].

Цифрова трансформація підприємства відкриває унікальні можливості щодо забезпечення його економічної безпеки за рахунок впровадження сучасних технологій у бізнес-процеси. Цей підхід передбачає не лише встановлення сучасного обладнання або програмного забезпечення, але і фундаментальні зміни в підходах до управління, корпоративної культури, зовнішніх комунікаціях. Як наслідок підвищуються продуктивність кожного працівника і рівень задоволеності клієнтів, а саме підприємство здобуває репутацію прогресивної і сучасної організації. Тому цифровізація процесів, на наш погляд, актуальна не тільки на рівні окремих підприємств: цілі галузі обирають для себе цей шлях розвитку як єдину можливість відповідати умовам навколишнього світу, що стрімко змінюються. Завдяки цьому цифрова трансформація промисловості, роздрібної торгівлі, державного сектору та інших сфер вже сьогодні змінює життя кожної людини і кожного [1].

Метою дослідження є аналіз та систематизація цифрових інструментів, що сприяють підтримці економічної безпеки підприємства.

Вплив цифрових технологій на економічний розвиток підприємства в сучасних умовах визначається їхньою стратегічною роллю в забезпеченні економічної безпеки. Цифрові інновації, такі як штучний інтелект, блокчейн, інтернет речей та аналітика даних, стали ключовими факторами, що формують економічну ландшафт підприємств [1].

У цьому дослідженні зосереджено увагу на таких аспектах позитивного впливу цифрових технологій на показники економічної безпеки підприємства як:

– підвищення продуктивності та ефективності операцій;

– збереження конфіденційних даних та швидка реакція на кібер-загрози;

– організація стабільних каналів комунікації із партнерами, клієнтами, постачальниками;

– отримання актуальної інформації про хід реалізації бізнес-процесів у реальному часі

– проведення надійних та безпечних фінансових трансакцій;

– організація навчання персоналу з кібербезпеки, безпечній роботі в онлайн-режимі.

Одним із аспектів позитивного впливу цифрових технологій є підвищення продуктивності та ефективності операцій. Впровадження автоматизованих систем управління, виробництва та обслуговування дозволяє підприємствам оптимізувати робочі процеси, зменшуючи витрати часу та ресурсів.

Крім того, цифрові технології розширюють можливості в сфері аналізу та прогнозування економічних тенденцій. Використання аналітичних інструментів дозволяє підприємствам здійснювати більш точне прогнозування попиту на товари і послуги, оптимізувати запаси та планувати виробництво з урахуванням ринкових умов.

Проте, разом із перевагами, виникають і певні ризики. Зокрема, зростання залежності від цифрових технологій може відкрити підприємства перед новими загрозами в сфері кібербезпеки. Важливо розвивати ефективні стратегії захисту від кібератак та забезпечувати стійкість інформаційних систем.

Так, у дослідженні [1] систематизовані проблеми економічної безпеки підприємства на сучасному етапі, з’ясовано, що кібербезпека вважається одним з головних елементів забезпечення економічної безпеки в умовах цифрової економіки. До основних проблем економічної безпеки автори віднесли:

– проблеми захисту даних підприємства від кібератак;

– дію зовнішніх кібер-шахраїв;

– недостатню обізнаність та рівень цифрових навичок персоналу, який не завжди діє з алгоритмами кібербезпеки: розкриває листи від невідомих адресатів, ділиться персональними даними на сторінках у соціальних мережах, розкриває конфіденційні дані;

– забезпечення захисту корпоративних даних на належному рівні в умовах стрімкого розвитку цифрових інструментів в економіці.

У звіті Europol [2] фокусується увага на економіці кіберзлочинів: кількості груп, організація їх роботи від найма спеціалістів до проведення кібератак та отриманні економічної вигоди від злочинних дій. У звіті проаналізовано, які зміни відбулися на європейському ринку після початку російської-української війни. Основним товаром цієї незаконної економіки є викрадені дані, які купуються та створюються за допомогою різних кібератак.

Зростання кількості порушень інформаційної безпеки в умовах цифровізації економіки пов’язаний з постійним ускладненням і зростанням масштабів застосування цифрових технологій. І тут варто зазначити, що більшість загроз інформаційного характеру, а згодом, і економічної безпеки криється в самих цифрових технологіях. Вразливості (так називають загрози в світі інформаційної безпеки) є у веб-сайтах та мобільних додатках, на офіційному сайті підприємства, в підключених комутаторах і серверах компанії тощо.

Інформаційні атаки, в першу чергу, спрямовані на знаходження вразливості і отримання інформації, в кінцевому підсумку можуть привести до прямих фінансових втрат (крадіжка грошових коштів, що знаходяться на електронному рахунку, проведення фальшивих транзакцій і угод тощо), упущену вигоду (через витік даних і втрати конкурентних переваг), а також до зниження ділової репутації і, як наслідок, втрати капіталізації підприємства. Таким чином, проглядається пряма залежність між ступенем розвитку і впровадженням цифрової економіки в

господарську діяльність підприємств і їх економічною безпекою, в тому числі і кібербезпекою [3].

Європейська агенція з кібербезпеки ENISA при аналізі кіберзагроз протягом 2023 р. [4] зосереджує увагу на таких восьми основних групах загроз:

– програми-вимагачі – тип атаки, коли зловмисники захоплюють контроль над активами цілі та вимагають викуп в обмін на повернення доступності активу

– шкідливе програмне забезпечення – будь-яке програмне забезпечення, призначене для виконання несанкціонованого процесу, який матиме негативний вплив на конфіденційність, цілісність або доступність системи

– соціальна інженерія – широкий спектр діяльності, яка намагається використати людську помилку або людську поведінку з метою отримання доступу до інформації чи послуг

– загрози проти даних – набір загроз, спрямованих на джерела даних з метою отримання несанкціонованого доступу та розголошення, а також маніпулювання даними для втручання в поведінку систем;

– відмова в обслуговуванні – атаки відбуваються, коли користувачі системи або служби не можуть отримати доступ до відповідних даних, послуг або інших ресурсів. Цього можна досягти шляхом виснаження служби та її ресурсів або перевантаженням компонентів мережевої інфраструктури;

– кампанії дезінформації зростають, що стимулюється збільшенням використання платформ соціальних мереж та онлайн-медіа;

– атака на ланцюг постачання – спрямована на відносини між організаціями та їхніми постачальниками. Щоб атаку можна було класифікувати як атаку на ланцюг поставок, цілями мають бути як постачальник, так і клієнт.

У звіті компанії Cisco вказуються такі дані: у 86 % організацій була хоча б одна спроба співробітників потрапити на фітинговий сайт; 70 % організацій мали

користувачів, які отримували шкідливу рекламу в браузері; у 48% фірм виявлено діяльність зловмисного програмного забезпечення, що викрадає інформацію [3].

У Європейському Союзі підприємства використовують різні методи для забезпечення кіберзахисту. Так, за даними Статистичної служби Eurostat [5], найбільш поширені методи захисту даних та протидії кібератакам це аутентифікація за складним паролем, резервування важливих даних з використанням хмарних технологій, мережений контроль доступу (таблиця 1).

Таблиця 1 – Основні інструменти захисту даних, що використовуються підприємствами ЄС

Відсоток підприємств ЄС, що використовують такі інструменти захисту даних	2019	2022
Мають як мінімум один елемент ІТ безпеки	85	92
Аутентифікація за складним паролем	76	82
Резервне копіювання даних (хмарне зберігання)	75	78
Мережевий контроль доступу	64	65
VPN	42	49
Ведення журналів після інцидентів безпеки	45	45
Моніторинг виявлення підозрілої активності		41
Шифрування даних, документів та електронної пошти	38	36
Тестування ІТ безпеки	35	35
Оцінка ІТ-ризиків	33	32
Мають як мінімум два механізму аутентифікації		31
Використовують біометрію для ідентифікації	9,6	13

Джерело: Eurostat [5]

Таким чином, європейські підприємства активно використовують цифрові інструменти у протидії кіберзагрозам. Крім того, більшість підприємств має окремі політики та протоколи щодо захисту даних та організації кібербезпеки підприємства.

Кібератаки також призводять до значних економічних збитків для підприємств та організацій.

Економічні збитки в результаті кіберзлочинів і кібератак становлять значну загрозу для підприємств в епоху цифрових технологій. Поширений характер цих загроз може мати далекосяжні наслідки, впливаючи на різні аспекти діяльності та фінансового стану компанії.

По-перше, прямі фінансові втрати виникають через крадіжку конфіденційної інформації, фінансове шахрайство та виплату викупу. Кіберзлочинці часто атакують корпоративні бази даних, витягуючи цінні дані, як-от інформацію про клієнтів, інтелектуальну власність і фінансові записи. Грошові втрати, понесені через ці порушення, можуть бути значними, що вплине на негайну ліквідність і довгострокову фінансову стабільність компанії.

Крім того, не можна ігнорувати непрямі витрати від кіберінцидентів. Збої в роботі, простої та втрата продуктивності можуть бути результатом необхідності розслідування та усунення наслідків атаки. Підприємствам може знадобитися інвестувати в заходи кібербезпеки, проводити судово-медичні аналізи та впроваджувати нові протоколи безпеки, що несе додаткові витрати.

У звіті Центру стратегічних та міжнародних досліджень (CSIS) проаналізовані економічні наслідки кіберзлочинів [6]. У звіті наводяться дані, що кількість нових випущених зловмисних програм коливаються від 300 000 до мільйона вірусів та інших шкідливих програмних продуктів щодня. Автори роблять висновок, що монетизація викрадених даних, яка завжди була проблемою для кіберзлочинців, здається, стала менш складною через розвиток «чорних ринків» кіберзлочинності та використання цифрових валют [6].

Для цілей дослідження слід звернути увагу на використання цифрових інструментів в управлінні ризиками сучасного підприємства.

Цифрова трансформація існуючих підприємств необхідна для підвищення їх конкурентоспроможності та капіталізації за рахунок кардинального підвищення продуктивності, зниження кількості залучених співробітників в ланцюжок

створення цінності і підвищення швидкості і якості прийняття управлінських рішень. Активне впровадження цифрових технологій в господарську діяльність підприємств усіх галузей економіки вносить зміни в систему виявлення, оцінки та мінімізації економічних ризиків і загроз економічній безпеці [7].

В сучасних умовах виникнення загроз збереження цифрових даних стає одним з основних напрямків забезпечення безпеки підприємства. В даний час атаки на системи зберігання даних стають все більш складним і повсякденним явищем, тому питання забезпечення кібербезпеки підприємства повинні виступати пріоритетним завданням у забезпеченні його економічної безпеки.

На основі аналізу літературних джерел [1,3,6,7] побудована схема взаємозв'язку між підсистемами підприємства, потенційними загрозами та цифровими технологіями з напрямами їх використання (рисунок 1).

Серед основних підсистем підприємство окремо виділені: загальне управління, виробництво та послуги, постачальники та логістика, продажі, фінанси та дані і IT.

Дана схема може послужити основою для вдосконалення процесів управління цифровими ризиками на сучасному підприємстві з урахуванням цифрової трансформації. Таке вдосконалення здатне суттєво підвищити рівень економічної безпеки підприємства в контексті цифрових та гібридних загроз.

На основі проведеного дослідження можна сформулювати ряд висновків. Так, економічні збитки для підприємств у результаті кіберзлочинів і кібератак охоплюють прямі фінансові наслідки, збої в роботі, репутаційну шкоду та правові наслідки. Щоб пом'якшити ці ризики, необхідна комплексна стратегія кібербезпеки, яка стосується як запобігання, так і реагування, визнаючи складний характер кіберзагроз, що розвивається, у сучасному взаємопов'язаному бізнес-середовищі.

Таким чином, цифрові технології, несучи можливості для підвищення конкурентоспроможності та ефективності бізнесу, вимагають від підприємств не лише високих інвестицій, але й удосконалення систем безпеки для забезпечення стійкого економічного розвитку.

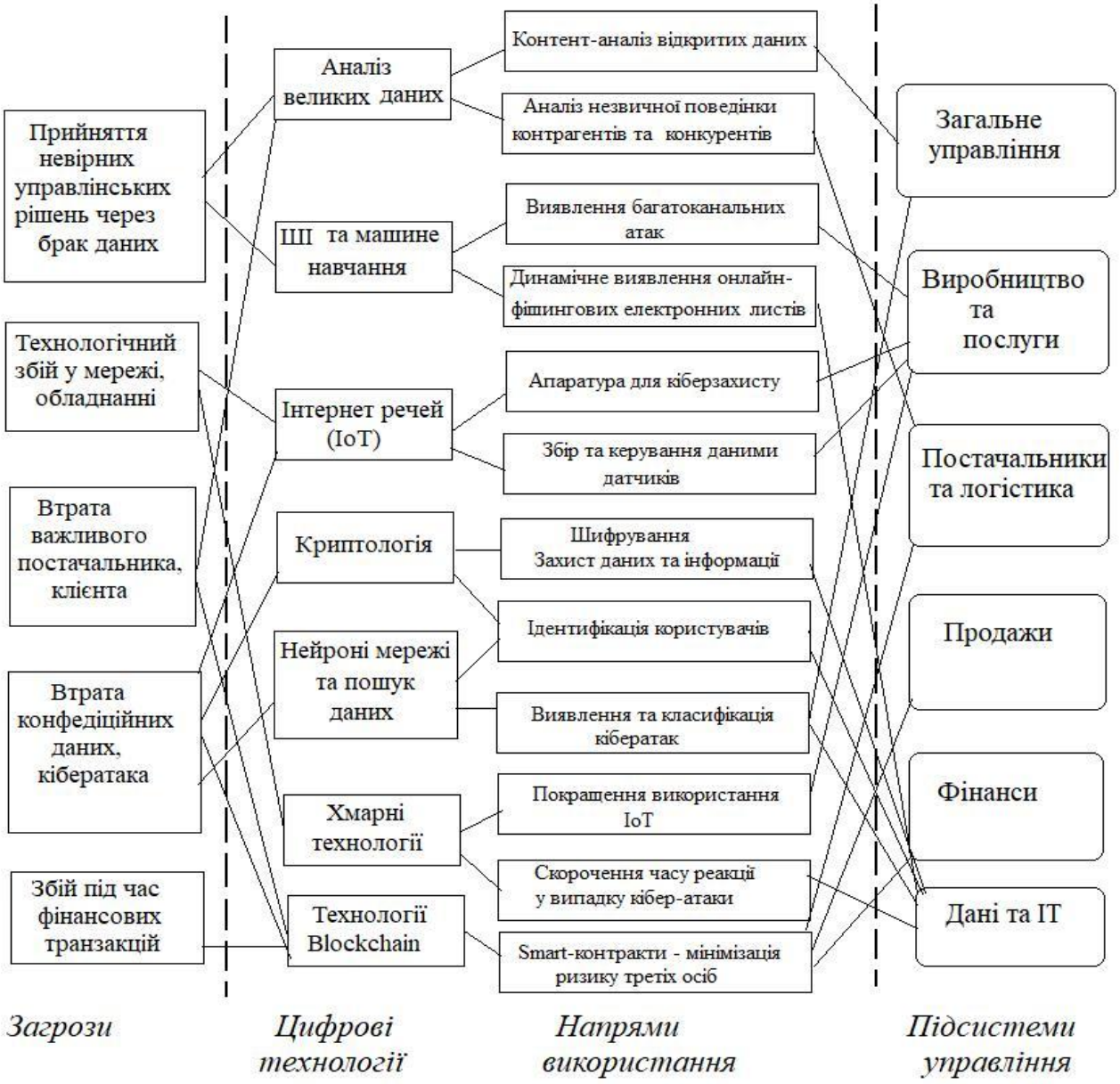

Рисунок 1 – Схема взаємозв'язку між підсистемами підприємства, загрозами та цифровими технологіями з напрямами їх використання

Перелік джерел посилання

1. Бакай В.Й. Забезпечення економічної безпеки підприємства на основі використання цифрових технологій. *Вісник Хмельницького національного університету.* 2020. № 4(1). С. 32-35.

2. Europol Internet organized crime threat assessment (IOCTA) 2023. Publications Office of the European Union, Luxembourg. URL: https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA%202023%20-%20EN_0.pdf.

3. Cisco Comp. Digital Vortex: how digital disruptions is redefining industries. June 2015. URL: https://www.cisco.com/c/dam/en/us/solutions/collateral/industry-solutions/digital-vortex-report.pdf.

4. European Union Agency for Cyber Security (ENISA) ENISA Threat Landscape 2022 (October 2022) URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022 (дата звернення: 14.11.2023).

5. Center for Strategic and International Studies (CSIS) Economic impact of cybercrime: no slowing down. February 2018. URL: https://csis-website-prod.s3. amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf.

6. Eurostat Security policy: measures, risks and staff awareness by size class of enterprise URL: https://ec.europa.eu/eurostat/databrowser/view/isoc_cisce_ra/default/table?lang=en.

7. Qi Y., Sun Y., Zhang Z. et al. The digital economy – technologies, trends, and influences. *Personal and Ubiquitous Computing*. 2023. № 27. С. 1521-1523. URL: https://doi.org/10.1007/s00779-023-01734-z.