DOI: https://doi.org/10.30837/EK.2024.021

Полозова Т.В.,
д.е.н., професор, завідувач кафедри економічної кібернетики та управління економічною безпекою,
Харківський національний університет радіоелектроніки
ORCID: https://orcid.org/0000-0001-9956-8816
Ткаченко А.Г.,
здобувач вищої освіти,
Харківський національний університет радіоелектроніки
ORCID: https://orcid.org/0000-0002-6714-7731
Осадчук І.О.,
здобувач вищої освіти,
Харківський національний університет радіоелектроніки
Осадчук М.О.
здобувач вищої освіти,
Харківський національний університет радіоелектроніки

МЕХАНІЗМИ МІНІМІЗАЦІЇ РИЗИКІВ ЕКОНОМІЧНОЇ БЕЗПЕКИ В ПРОЦЕСІ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ПІДПРИЄМСТВ

Цифрові технології значно змінюють основні компоненти економічної безпеки, впливаючи на фінансову, інформаційну, кадрову та інші сфери. Вивчення цих аспектів дозволяє розробити ефективні стратегії для зниження ризиків та підвищення конкурентоспроможності. Традиційні підходи до економічної безпеки потребують оновлення з урахуванням цифрових змін. Через це розробка нових моделей, інструментів і методів забезпечення економічної безпеки є актуальним напрямом досліджень.

Актуальність дослідження економічної безпеки підприємства в контексті розвитку цифрових технологій обумовлена кількома ключовими чинниками:

а) *зростання ролі цифрових технологій у бізнесі*. Сучасний бізнес все більше залежить від цифрових рішень, таких як автоматизація, аналіз великих даних, штучний інтелект і Інтернет речей (IoT). Цифровізація відкриває нові можливості для підприємств, але водночас збільшує вразливість до ризиків, пов'язаних із кіберзагрозами, технічними збоями та втратами даних;

б) *збільшення цифрових ризиків*. Зростання кіберзагроз, таких як хакерські атаки, витік конфіденційної інформації та зловживання персональними даними, технологічні збої, дефіцит кваліфікованих кадрів, невідповідність використання цифрових технологій правовим нормам ставить під загрозу фінансову стабільність та репутацію компаній. У цьому контексті економічна безпека підприємств залежить від їхньої здатності протистояти цифровим викликам;

в) *конкурентний тиск та технологічна інтеграція*. Успіх підприємств на ринку залежить від їхньої здатності інтегрувати цифрові технології у свою діяльність. Проте надмірна цифровізація без належної оцінки ризиків може призвести до зростання витрат, низької ефективності та зниження економічної стійкості;

г) *необхідність збереження балансу між інноваціями та стабільністю*. Інновації є важливим драйвером розвитку, але їх реалізація потребує значних фінансових і людських ресурсів. Непродумані інвестиції у цифрові технології можуть підірвати економічну безпеку підприємств. Отже, важливо досліджувати способи забезпечення балансу між впровадженням технологій та збереженням економічної стабільності;

д) *динамічність зовнішнього середовища*. Умови ринку та регуляторна політика швидко змінюються, особливо з огляду на цифрові трансформації. Підприємства повинні адаптуватися до цих змін, забезпечуючи свою економічну безпеку в умовах зростаючої невизначеності.

Питання економічної безпеки розглядаються багатьма вітчизняними та закордонними науковцями та експертами.

Так, Гринкевич С., Когут М., Станкевич М. [1] зазначають, що економічна безпека підприємства «…сприяє уникненню фінансових труднощів, банкрутства та збереженню конкурентоспроможності». Автори також вказують, що «…розвиток технологій із світовим масштабом, таких як штучний інтелект, блокчейн або інтернет речей, можуть змінювати економічний вимір та створювати нові можливості, але вони також можуть ставити питання безпеки даних, кібербезпеки та роботизації робочої сили…» [1] та виділяють внутрішні та зовнішні фактори, що визначають рівень економічної безпеки підприємства.

М. Кравченко та Ф. Немировський [2] при визначені поняття «економічна безпека» дотримуються комплексного підходу: «економічна безпека – це комплекс управлінських, організаційних і правових заходів, що забезпечують стабільне та ефективне функціонування підприємства через оптимізацію ресурсів, адаптацію до економічних ризиків і небезпек, гармонізацію відносин між внутрішнім і зовнішнім середовищем, підтримку конкурентоспроможності та довгострокову стійкість при врахуванні інтересів усіх зацікавлених сторін» [2].

На думку авторів статті [3] «економічна безпека – це стан, характеризує здатність суб'єкта господарювання забезпечити ефективне використання ресурсів та підприємницьких можливостей для запобігання можливих загроз та досягнення стабільного функціонування та цілей бізнесу». В економічній безпеці автори виділяють фінансову, виробничо-збутову, кадрову та техніко-технологічну складові та три основних елементи: незалежність (контроль над власними ресурсами), стійкість (стабільність діяльності) та розвиток (удосконалення показників діяльності) [3].

Науковець В. І. Міщенко [4] визначив ключові завдання організації державного регулювання, контролю та нагляду за процесами використання

цифрових технологій, а саме: встановлення чітких технічних умов, регламентів і стандартів; створення надійних і гнучких систем управління ризиками; підтримка належного рівня управління цифровими технологіями шляхом формування відповідних управлінських структур; безпечне та надійне управління даними та цифровими моделями; забезпечення та підтримка необхідного рівня кібербезпеки підприємств і громадян; захист прав людини, справедливості та різноманіття, а також підтримка сталого розвитку.

Багато міжнародних агенцій вказують на підвищення ризику кібератак для сучасних підприємств, що стають більш інтегрованими до глобальних мереж, а значить і більш вразливими до атак. Так, 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 [5].

У звіті Europol [6] приділено увагу розвитку кіберзлочинної економіки, яка охоплює діяльність організованих груп, їхню структуру, процеси залучення фахівців, організацію кібератак і отримання економічного зиску від злочинних дій. У звіті також розглядаються зміни, що відбулися на європейському ринку після початку російсько-української війни. Основним ресурсом цієї нелегальної економіки є викрадені дані, які добуваються та продаються через різноманітні кібернапади. Зростання кількості інцидентів у сфері інформаційної безпеки в умовах цифровізації економіки пов’язане з масштабним впровадженням і ускладненням цифрових технологій. Більшість загроз для інформаційної, а отже, і економічної безпеки походить від самих цифрових інструментів. Вразливості, що є основними ризиками в інформаційній безпеці, присутні в різних компонентах цифрової екосистеми: вебсайтах, мобільних додатках, офіційних ресурсах підприємств, підключених мережевих пристроях та серверах компаній тощо.

У Європейському Союзі підприємства використовують різні методи для забезпечення куберзахисту. Так, за даними Статистичної служби Eurostat [7], найбільш поширені методи захисту даних та протидії кібератакам це аутентифікація за складним паролем, резервування важливих даних з використанням хмарних технологій, мережений контроль доступу (табл. 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 IT 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 IT безпеки	35	35
Оцінка IT ризиків	33	32
Мають як мінімум два механізму аутентифікації		31
Використовують біометрію для ідентифікації	9,6	13

Джерело: Eurostat [7].

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.

На основі узагальнення теоретичних джерел [1-4, 8] в роботі пропонується сім ключових інструментів забезпечення економічної безпеки підприємства під час цифрової трансформації (рис. 1). Основні інструменти мінімізації ризиків для економічної безпеки включають стратегії та заходи, спрямовані на зниження негативного впливу внутрішніх та зовнішніх загроз.

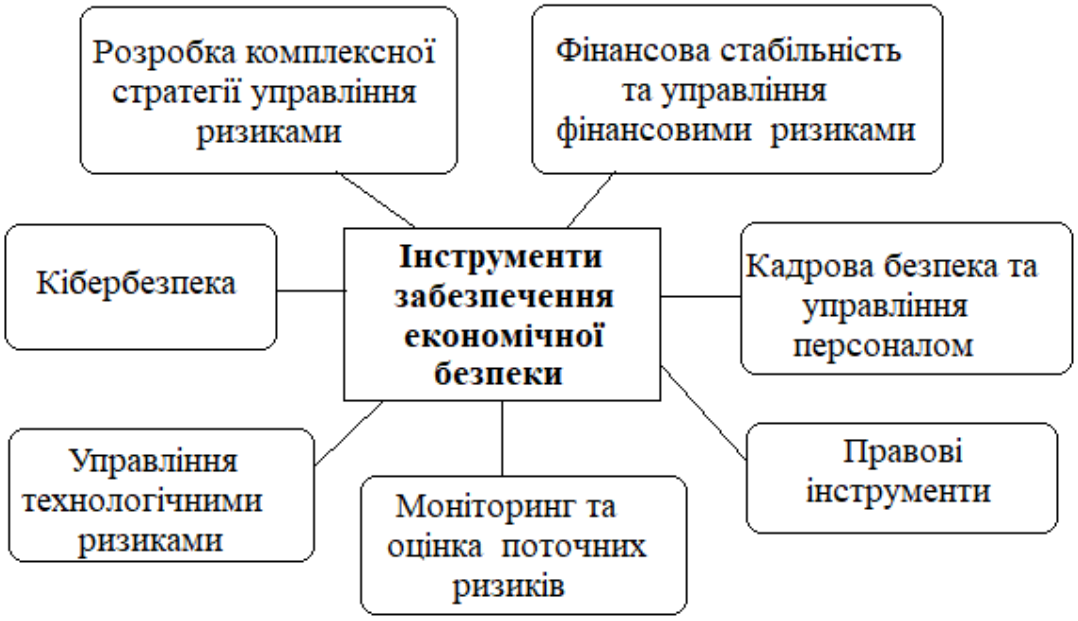

Рисунок 1– Інструменти забезпечення економічної безпеки підприємства при впроваджені цифрових інновацій

Так, розробка комплексної стратегії управління ризиками на підприємстві включає процедуру ідентифікації та оцінки ризиків, засобів їх зменшення/компенсації та процедуру регулярного моніторингу тенденцій розвитку поточних ризиків. Використання кількісних та якісних методів для визначення ймовірності виникнення ризиків і їх потенційного впливу на підприємство чи економіку в цілому дозволить менеджменту підприємства ефективно пріоритизувати ризики та розробити відповідні стратегії. Підготовка до непередбачених ситуацій шляхом створення запасних планів та механізмів реагування забезпечать швидке відновлення діяльності у разі кризових подій.

Інструменти кібербезпеки включають апаратні та програмні засоби ідентифікації загроз. Встановлення надійних систем захисту від кібератак, використання шифрування даних, багатофакторної автентифікації, регулярних оновлень програмного забезпечення та антивірусних засобів допомагає запобігти витоку конфіденційної інформації та збереженню стабільності інформаційних систем.

Фінансова стабільність і управління фінансовими ризиками передбачає диверсифікацію активів (розподіл активів по різних секторах, валютах, ринках і географічних регіонах для зменшення ризику фінансових втрат при зміні умов на окремих ринках), страхування та проведення стрес-тестування (Перевірка фінансової стійкості компанії через моделювання різних негативних сценаріїв: економічні кризи, коливання валютних курсів, зміни на ринку праці).

Управління технологічними ризиками включає інвестиції в інновації та дослідження та забезпечення надійної інфраструктури. Вкладення в розвиток нових технологій для зниження залежності від застарілих або уразливих систем. Це включає автоматизацію процесів, впровадження штучного інтелекту, Інтернету речей (IoT) для моніторингу та контролю за бізнес-процесами. Резервні енергетичні системи, хмарні обчислення та великі дані для безпеки і доступності інформації стануть у нагоді для забезпечення захисту від інфраструктурних збоїв.

Кадрова безпека та управління персоналом включають програми навчання та підвищення кваліфікації, належну політику найму та утримання кваліфікованих кадрів, створення мотиваційних програм та системи винагород для зменшення ризиків, пов'язаних з відтоком талановитих співробітників.

Системи безперервного навчання і розвитку співробітників (навчання впродовж життя) дозволяють адаптувати персонал до нових технологій, мінімізуючи ризики через відсутність необхідних навичок.

Правові інструменти та регулювання включають захист інтелектуальної власності та адаптацію системи управління та бізнес-процесів підприємства до змін у законодавстві. Важливим є також Залучення до міжнародних угод та стандартів для забезпечення економічної безпеки на глобальному рівні, зокрема у боротьбі з фінансовими злочинами, кіберзлочинністю та незаконними економічними операціями.

Моніторинг та оцінка ризиків включає апарат з аналізу та оцінки ризиків в також системи раннього попередження. Технології аналітики великих даних та

хмарні обчислення дозволяють проводити аналіз великої кількості даних для прогнозування можливих загроз і виявлення трендів, що можуть негативно вплинути на економічну безпеку.

Впровадження автоматизованих систем для моніторингу економічних, політичних та технологічних змін, які можуть вказувати на потенційні ризики для безпеки.

Ці інструменти дозволяють знизити рівень загроз та посилити стійкість підприємств, державних інститутів і економічних систем у цілому до змін, що відбуваються в умовах глобалізації, цифровізації та постійних технологічних інновацій.

Впроваджуючи цифрові інновації підприємства для забезпечення економічної безпеки та стійкості діяльності можуть використовувати цифрові технології. На основі аналізу літературних джерел систематизовано Цифрові інструменти для забезпечення економічної безпеки підприємства при впроваджені цифрових інновацій (табл. 2).

Компанії по всьому світу, що працюють в різних секторах економіки, використовують цифрові технології для мінімізації ризиків та підтримки економічної безпеки (табл. 3). Ці приклади демонструють, як великі компанії впроваджують цифрові стратегії з урахуванням можливих ризиків, зокрема в аспектах кібербезпеки та захисту даних. Вони зуміли зберегти баланс між інноваціями та стійкістю бізнесу, що дозволяє їм адаптуватися до змін у цифровому середовищі. Розуміючи ці приклади, компанії можуть вчитися на сценаріях реального світу та визначати пріоритетність цифрових інвестицій, щоб забезпечити свою фінансову та операційну стабільність.

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 (рис. 2).

Таблиця 2 – Цифрові інструменти для забезпечення економічної безпеки підприємства при впроваджені цифрових інновацій

Цифрові технологій	Напрям використання для підтримки кіберстійкості
Аналіз великих даних	Контент-аналіз відкритих публікацій та соціальних мереж для протидії розповсюдженню дезінформації Аналіз незвичної поведінки контрагентів та конкурентів
Штучний інтелект, машинне навчання	Виявлення багатоканальних атак для інформаційної безпеки Динамічне виявлення онлайн-фішингових електронних листів нульового дня Створення бази знань щодо реакцій на кіберзагрози
Інтернет речей (IoT)	Апаратура для кіберзахисту (вважається більш надійним, ніж програмний захист) Збір та керування даними датчиків, контроль та моніторинг виробничої інфраструктури Медіа-спостереження із забезпеченням конфіденційності користувачів, безпеки медіа-ресурсів та вимог до пам'яті вузла-датчика
Криптологія	Ідентифікація користувачів Захист даних та інформації
Нейроні мережі та пошук даних (Data mining)	Виявлення та класифікація кібератак Ідентифікація користувачів
Хмарні обчислення	Покращуюсь використання IoT Скорочення часу реакції у випадку гібридної атаки
Smart-контракти з використанням технології Blockchain	Мінімізація ризику, що стосується третіх осіб – розумний контракт реалізується автоматично при настанні події, незалежно від дій контрагентів.

Джерело: сформовано авторами на основі [5–9].

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

Схема ілюструє дві сторони використання цифрових технологій. З одного боку, поширення процесів цифровізації призводить до підвищення загроз для бізнесу – кібератаки, законодавче регулювання, втрата даних, необхідність підвищувати кваліфікацію персоналу. З іншого боку цифрова трансформація також і надає цифрові інструменти для боротьби з цими загрозами: аналітика великих даних, хмарні обчислення, криптографія та шифрування, нейроні мережі та пошук даних.

Таблиця 3 – Приклади використання цифрових інструментів для забезпечення економічної безпеки компаніями

Компанія, галузь	Цифрові інструменти	Програма оцінки ризиків та її результати
Siemens електроніка	«Vision 2020+»: операційна система IoT Mindsphere, Mendix – платформа розробки додатків, цифрові послуги.	Використання багатоступеневих систем захисту, моніторинг можливих кіберзагроз в реальному часі, програма підвищення культури кібербезпеки персоналу. Це дозволило Siemens зберігати стабільність операцій і мінімізувати вплив цифрових загроз, одночасно збільшуючи ефективність виробничих процесів через автоматизацію та передові аналітичні рішення.
General Electric (електро-, приладову-дування,	«Industrial Internet» з фокусом на підключення підприємств до Інтернету речей (IoT) для підвищення ефективності та скорочення витрат	Компанія створила надійну архітектуру кібербезпеки: себе виявлення аномалій, багатофакторну аутентифікацію, шифрування даних і постійну перевірку безпеки своїх виробничих систем
Netflix медіа	Використання великих даних (Big Data) для персоналізації контенту та передбачення поведінки користувачів	Шифрування даних. Netflix створила систему моніторингу для вчасного виявлення та реагування на кіберзагрози. Компанія має політику тестування та відновлення даних після можливих атак або технічних збоїв
Walmart, ритейл	Використовують аналітики даних та штучного інтелекту для прогнозування попиту, управління запасами та оптимізації ланцюгів поставок	Walmart вживає заходів для забезпечення безпеки персональних даних клієнтів, використовуючи методи шифрування і мультифакторну аутентифікацію для захисту обробленої інформації.
Toyota, автомобіле-будування	Впровадження IoT в автомобільні технології та виробничі процеси, створення інтелектуальних автомобілів та використання даних для оптимізації виробництва	Використання криптографічних методів для захисту збережених даних
Bank of America, фінансова установа	Мобільний банкінг та онлайн-платформи	Застосування штучного інтелекту в управлінні ризиками та кредитуванні. Аналітика великих даних при прийнятті рішень про кредитування
PayPal, онлайн-платежі	Мобільний банкінг та онлайн-платформи.	Використання штучного інтелекту і машинного навчання для покращення виявлення та запобігання шахрайству. Шифрування даних.

Джерело: сформовано авторами на базі [8-11].

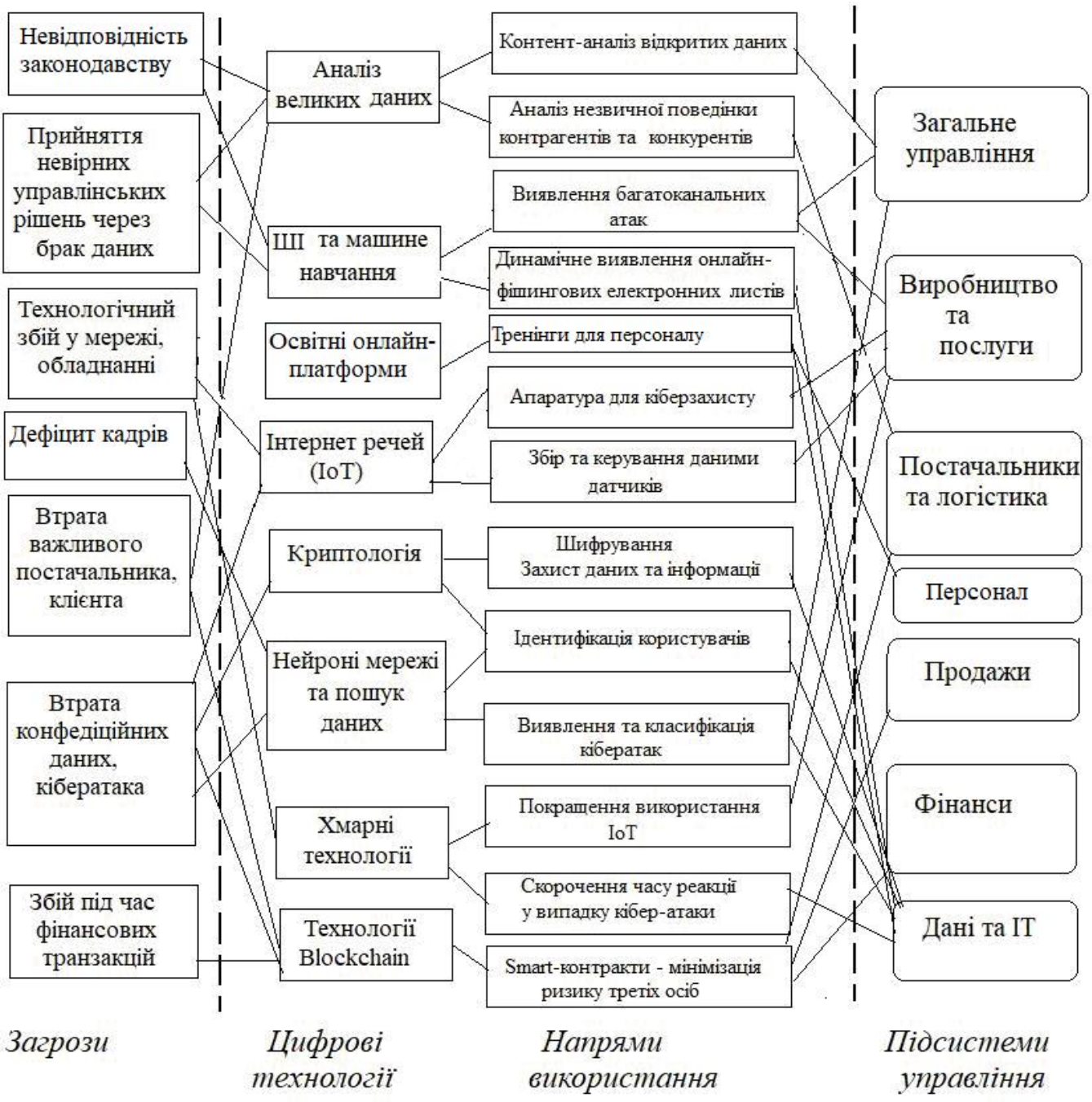

Рисунок 2 – Схема взаємозв’язку між підсистемами підприємства, загрозами та цифровими технологіями з напрямами їх використання

Інтеграція цифрових технологій у бізнес-процеси може значно підвищити ефективність і конкурентоспроможність компанії. Однак важливо здійснювати цей

процес обережно, щоб не втратити економічну стійкість. На основі аналізу теоретичних підходів в досліджені систематизовані ключові рекомендації для підприємств щодо інтеграції цифрових технологій без втрати стійкості:

а) *розробка стратегії цифрової трансформації.* Така стратегія цифрової трансформації повинна визначити довгострокову ціль та задачі, значення цільових показників, які цифрові технології (штучний інтелект, аналітика даних, автоматизація тощо) найбільше підходять для досягнення цілей. Покрокове впровадження нових технологій дозволить уникнути ризиків, пов'язаних з одночасною зміною всіх процесів. Це дозволить краще оцінити ефективність кожного етапу й адаптувати стратегію за потреби;

б) *досягнення балансу між цифровими інноваціями та стабільною роботою підприємства*. Хоча цифрові технології можуть суттєво поліпшити продуктивність, важливо не поспішати із заміною традиційних процесів без належного тестування та оцінки. Інтенсивність впровадження інновацій не повинна відображатися на сталості роботи підприємства.

в) *інвестування у кібербезпеку*. Поширення цифрових технологій супроводжується значним збільшенням кіберзагроз. Тому важливо інвестувати в кібербезпеку, застосовувати багаторівневі системи захисту даних і регулярно оновлювати програмне забезпечення для запобігання атакам. Тренінги персоналу дозволять підготувати його до нових викликів;

г) *адаптивність організаційної структури*. Більш гнучка організаційна структура з перерозподілом ролей, повноважень та обов'язків покращує комунікацію та контроль, мотивує персонал до особистого розвитку, зменшує внутрішній опір змінам;

д) *навчання персоналу*. Програми підвищення цифрових навичок персоналу дозволять зробити цифрових перехід на підприємстві менш ризиковим;

е) *оцінка економічної ефективності впровадження цифрових технологій*. Оцінка ефективності дозволить обрати найкращий варіант впровадження цифрових технологій з кількох альтернатив. Тестування цифрових технологій в межах окремого відділу/бізнес-процесу перед повним їх впровадженням дозволить виявити потенційні проблеми та оцінити вплив на економічну безпеку;

ж) *управління змінами* через прозорість, комунікації із стейкголдерами та усіма рівнями персоналу, організація зворотного зв'язку;

з) *постійний моніторинг після впровадження цифрових інновацій*. Регулярний аналіз результатів цифрової трансформації із заявленими цілями дозволить підприємству виявити сильні та слабкі позиції, а також необхідність корегування стратегії підприємства. Технології швидко розвиваються, тому компанії повинні бути готові до постійного оновлення своїх систем і стратегій для збереження конкурентоспроможності та економічної стійкості.

Ці рекомендації допоможуть бізнесам інтегрувати цифрові технології без значних втрат для економічної стійкості, забезпечивши ефективність і адаптивність у довгостроковій перспективі.

Таким чином, цифрові технології мають глибокий і багатогранний вплив на різні аспекти економічної безпеки. Для мінімізації ризиків та оптимізації переваг необхідно забезпечити баланс між технологічними інноваціями та захистом ключових компонентів економічної безпеки.

Перелік джерел посилань

1. Гринкевич С., Когут М., Станкевич М. Еволюція теоретичних концепцій економічної безпеки підприємства. *Економіка та суспільство*. 2023. № 50. https://doi.org/10.32782/2524-0072/2023-50-70

2. Кравченко М., Немировський Ф. Теоретичні підходи до визначення поняття «економічна безпека підприємства». *Наукові інновації та передові технології*. 2024. № 11(39). С. 932-943.

3. Мірошниченко Я., Фощій П., Угрімова І. Поняття, зміст та функціональні складові економічної безпеки промислового підприємства. *Вісник Національного технічного університету «Харківський політехнічний інститут»*. 2023. № 5. С. 84-88.

3. Адаменко Т. М. Система економічної безпеки підприємства: підхід до формування. *Економіка Менеджмент Підприємництво*. 2013. № 25(II). С. 265-273. URL: http://eme.ucoz.ua/publ/zbirniki/25_ii_2013/adamenko_t_m_/39-1-0-333

4. Міщенко В. І. Механізми регулювання процесів цифровізації для забезпечення національно укоріненої стійкості економічного розвитку. *Економічний простір.* 2024. № 189. С. 283-290.

5.Cisco Comp. Digital Vortex: how digital disruptions is redefining industries. June 2015. URL: http://surl.li/eqrtod.

6.Europol Internet organized crime threat assessment (IOCTA) 2023. Publications Office of the European Union, Luxembourg. URL: http://surl.li/qhsutt.

7. Eurostat Security policy: measures, risks and staff awareness by size class of enterprise URL: http://surl.li/hgqfwu.

8. Schwertner K. Digital transformation of business. *Trakia Journal of Sciences*, 2017. Vol. 15. Suppl. 1. pp. 388-393.

9. Siemens. Vision 2020+: Shaping the future Siemens. Press Conference. Munich, 2 August, 2018. URL: http://surl.li/vwiqua

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

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