https://doi.org/10.31891/2307-5740-2024-330-67
УДК 330

ЧАЙКОВСЬКА Інна
Хмельницький національний університет
https://orcid.org/0000-0001-7482-1010
e-mail: inna.chaikovska@gmail.com
ТКАЧ Тарас
Хмельницький національний університет
https://orcid.org/0009-0008-6522-065X
e-mail: tkachti@ukr.net
ЧАЙКОВСЬКИЙ Максим
Хмельницький національний університет
https://orcid.org/0000-0002-9596-6697
e-mail: max.chaikovskyi@gmail.com

РОЛЬ СУЧАСНИХ ІНФОРМАЦІЙНИХ СИСТЕМ ТА ТЕХНОЛОГІЙ У ЗАБЕЗПЕЧЕННІ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА В УМОВАХ DIGITAL-ЕКОНОМІКИ

У статті розглянуто вплив наскрізної автоматизації та цифровізації на економіку та економічну безпеку підприємства. Встановлена двохаспектність даного впливу: як нові можливості та нові загрози і ризики. У роботі запропоновано сформувати цифрову екосистему як складову економічної безпеки підприємства з метою забезпечення економічної безпеки підприємства в умовах Digital-економіки. Дана цифрова екосистема повинна поєднувати використання новітніх технологій (штучний інтелект, машинне навчання, хмарні обчислення, аналітика великих даних, прогнозне моделювання, розширена та віртуальна реальність, промисловий Інтернет речей) разом із новітніми інформаційними системами (ERP, HRM, MES, CRM, PRM, SCM та ін.) з метою збору, зберігання, обробки та поширення інформації стосовно різних аспектів економічної безпеки підприємства. Дана інформація сприятиме активному виявленню, аналізу, оцінці впливу ризиків на функціонування підприємства в умовах Digital-економіки, а також для прийняття ефективного обґрунтованого управлінського рішення з метою управління ризиками (управлінськими, інформаційними, кадровими, технологічними та ін.). Саме такий підхід дозволить підвищити рівень економічної безпеки підприємства за умов цифровізації.

Ключові слова: Digital-економіка, цифровізація, інформаційні технології, інформаційні системи, економічна безпека підприємства, штучний інтелект.

CHAIKOVSKA Inna, TKACH Taras, CHAIKOVSKYI Maksym
Khmelnytskyi National University

THE ROLE OF MODERN INFORMATION SYSTEMS AND TECHNOLOGIES IN ENSURING THE ECONOMIC SECURITY OF THE ENTERPRISE IN THE CONDITIONS OF THE DIGITAL ECONOMY

The article examines the impact of end-to-end automation and digitization on the economy and economic security of the enterprise. The two-facetedness of this influence is established: as new opportunities and new threats and risks. Among the possibilities: optimization of work, improvement of interaction with clients and development of new business models, improvement of efficiency and productivity of work, personalization of the offer, study of innovative sources of income, etc. It has been established that modern information systems provide complex data management capabilities, which allows enterprises to use the power of their data. This includes the ability to collect, store and analyze vast amounts of data, enabling more informed decisions. They also offer robust reporting and visualization tools, allowing companies to understand and display complex data in a more accessible way. Technologies such as artificial intelligence (AI), machine learning (ML) and data analytics help to understand market trends, consumer behavior and competitive dynamics. They provide real-time monitoring of business operations, enabling quick decision-making and immediate response to threats and opportunities. Among the problems: in the Digital economy, enterprises are exposed to a wide range of risks that can have a significant impact on their economic security. These risks can come from many different sources, such as cyber threats, technology disruptions and market volatility. The work proposes to form a digital ecosystem as a component of the economic security of the enterprise in order to ensure the economic security of the enterprise in the conditions of the Digital economy. This digital ecosystem should combine the use of the latest technologies (artificial intelligence, machine learning, cloud computing, big data analytics, predictive modeling, augmented and virtual reality, industrial Internet of Things) together with the latest information systems (ERP, HRM, MES, CRM, PRM, SCM, etc.) for the purpose of collecting, storing, processing and disseminating information regarding various aspects of the economic security of the enterprise. This information will contribute to the active detection, analysis, and assessment of the impact of risks on the operation of the enterprise in the conditions of the Digital economy, as well as to the adoption of an effective, substantiated management decision for the purpose of risk management (management, information, personnel, technological, etc.). This approach will allow to increase the level of economic security of the enterprise under the conditions of digitalization.

Keywords: human capital; Digital economy, digitization, information technologies, information systems, economic security of the enterprise, Artificial Intelligence.

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Стрімкий розвиток технологій в епоху Digital-економіки здійснює значний вплив на всі сфери нашого життя. Технології виступають каталізатором змін, і економічний розвиток не є винятком, адже вони змінюють робочі процеси, методи виробництва та моделі споживання. Проте технології не лише стимулюють інновації та сприяють розвитку можливостей, але й створюють низку проблем для традиційних моделей економічного розвитку, що робить ще актуальнішим питання економічної безпеки.

У сучасній Digital-економіці питання економічної безпеки підприємства є критичним. Економічна безпека, загалом, означає наявність стабільного доходу або інших ресурсів для підтримки рівня життя як на сьогоднішній момент, так і у перспективі. Однак, у контексті підприємства, вона набуває дещо іншого значення. Це стосується здатності компанії підтримувати відповідний рівень економічного розвитку, а також можливість забезпечувати своє фінансове благополуччя, особливо в умовах численних викликів і невизначеності, характерних для Digital-економіки, яка передбачає використання різноманітних інформаційних систем та технологій.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Серед науковців, які досліджували проблеми забезпечення економічної безпеки в умовах Digital-економіки, можна виділити наступних: Брітченко І. [2], Гавловська Н.І. [1], Гончар В. [7], Дикань В. [5], Кухар О. [3], Панченко О.А. [4], Полусмяк Ю. [6], Рудніченко Є.М. [1], Шматковська Т. [2] та ін.

Науковці приходять до єдиної думки, що автоматизація та цифровізація в умовах Digital-економіки має значний вплив на економічні процеси та економічну безпеку зокрема.

У роботі [1, с.173-174] Рудніченко Є.М., Гавловська Н.І. та ін. відмічають, що надзвичайно швидкий розвиток технологій та впровадження практично у всі сфери життя суспільства штучного інтелекту обумовлюють трансформаційні процеси не лише у виробничих процесах, а й у менеджменті.

Як зазначається колективом авторів Т. Шматковська, І. Брітченко, С. Войтович, П. Лошонці, І. Лорві, І. Кулик, С. Бігун у роботі [2, с.153], використання цифрових програмних продуктів для обробки фінансово-господарської облікової інформації значно спрощує управління, аналіз і контроль діяльності підприємств, установ, організацій. Таким чином, фінансова безпека всіх суб'єктів, задіяних у бізнес-процесах, може протидіяти потенційним ризикам і загрозам фінансовій стабільності та успішності розвитку як окремих підприємств, так і фінансового ринку в цілому. А також науковці зазначають, що сучасна цифрова трансформація підприємств має незаперечні переваги у здійсненні діяльності, новітні інформаційні технології та корпоративні програмні продукти мають бути інтегровані в бізнес-процеси та забезпечувати стратегічне управління такими процесами. Відповідно, розробка стратегії цифрової безпеки підприємства має ґрунтуватися на концепції, що базується на наступних основних принципах: цифрова та інформаційна безпека підприємства має бути унікальною, виходячи з його організаційної структури, спеціалізації виробництва та наявності цифрових технологій; функціонування системи цифрової безпеки підприємств може бути забезпечено лише за умови комплексної безпеки всіх її функціональних складових; ефективна цифрова безпека підприємства можлива лише за умови добре продуманої концепції та відповідних заходів безпеки.

У роботі [3, с. 150] відмічається, що успішне виконання функцій підприємств та їх стійке позиціонування на ринку можливі лише за умови забезпечення їх економічної безпеки. Процес цифровізації впливає на рівень економічної безпеки підприємства через позитивний вплив вдосконалених цифрових технологій на компоненти безпеки. Використання цифрової економіки створює багато позитивних моментів у бізнес-діяльності, сприяє досягненню цілей та забезпечує економічну безпеку.

Панченко О.А. у роботі [4, с.30] відзначає, що інформаційні технології можуть як забезпечувати стабільність і безпеку, так і загрожувати цим двом компонентам. З одного боку, інформаційні технології можна використовувати для поширення та обміну ідеями та стратегіями в області безпеки, а з іншої - інформаційні технології можуть бути використані таким чином, щоб загрожувати стабільності і безпеки держави.

Схожої думки дотримуються В. Дикань, Н. Фролова та Цзян Пань у роботі [5, с.21], які відмічають, що поряд зі значними перевагами реалізації суб'єктами малого та середнього бізнесу цифрових змін, пов'язаних з оптимізацією бізнес-процесів, покращенням комунікації з партнерами, клієнтами та співробітниками, підвищенням прозорості бізнес-процесів та економічної інформації, активізацією інноваційної діяльності бізнес- суб'єктів і розбудовою сучасної інформаційної інфраструктури, слід звернути увагу і на суттєві виклики цифровізації, зумовлені посиленням залежності від цифрових технологій.

С. Решетов, Ю. Полусмяк у роботі [6, с.12] наголошують на ризиках цифрової трансформації для економічної безпеки держави, а саме на зростанні рівня безробіття. По-перше, автоматизація процесів залишить частину населення без роботи. По-друге, можуть виникнути нові потреби та вимоги ринку щодо нових професій та трансформація існуючих. Ще одним потужним ризиком є зростання кіберзлочинності

(викрадення персональних даних, коштів з рахунків, збір великої кількості конфіденційної та комерційної інформації, блокування діяльності тощо).

У роботі [7, с.52-54] В. Гончар та К. Полупанова відобразили функціональну характеристику технологій систем програмного забезпечення економічної безпеки підприємства (таблиця 1).

Таблиця 1

Функціональна характеристика технологій систем програмного забезпечення економічної безпеки підприємства [8]

Види технологій	Функціональне завдання (мета реалізації)	Список замовлених дій (кроків) (алгоритм технології)
1. Основні технології		
1.1. Технології ідентифікації загроз	Визначення реальних ризиків, загроз і небезпек та їх ідентифікація	- моніторинг ризиків, загроз і небезпек - накопичення даних та їх поточна систематизація - виявлення загроз у наборі стандартних прогнозованих загроз - систематизація даних про непередбачувані загрози
1.2. Технології тестування системи ЕБП	Оцінка здатності системи економічної безпеки підприємства забезпечити необхідний рівень безпеки бізнесу	- діагностика системи моніторингу загроз - діагностична здатність інформаційно-комунікаційної системи - діагностика можливості оперативної оцінки фінансового стану підприємства - діагностика можливостей систем внутрішнього контролю - аналіз інноваційності технологій безпеки та стану їх забезпечення - діагностика пристосувального механізму - аналіз наявності та ефективності засобів правового захисту
1.3. Технології оцінки класу небезпеки	Оцінка стану та рівня економічної безпеки підприємства	- розрахунок показників - порівняти їх значення з визначеними параметрами - розрахунок узагальнюючих показників - оцінка рівня небезпеки
1.4. Технології захисту від загроз і небезпек	Захист економічної системи підприємства від негативного впливу реальних загроз і ризиків та їх деструктивних наслідків	- перелік дій за умов рейдерського захоплення - за умов захоплення (викрадення) працівників - загрози життю і свободі працівників та їх близьких - проникнення невідомих осіб до місць зберігання інформації та майна - непередбачений збій в обліково-інформаційній системі
2. Допоміжні технології		
2.1. Технології обліково-аналітичного забезпечення	Надання обліково-аналітичної інформації для функціонування адаптованої системи економічної безпеки підприємства	- організація первинного та зведеного (синтетичного та аналітичного) обліку операцій і процесів (у тому числі трансформаційних), а також пов'язаних з ними активів, капіталу та зобов'язань для моніторингу загроз і небезпек - організація звітності в системі ЕБП - проведення аналітичних розрахунків показників аналізу господарської діяльності та фінансового стану - обробка, накопичення, зберігання та передача обліково-аналітичних даних у системі управління ЕБП
2.2. Технології внутрішньо-господарського контролю	Контроль ефективності управлінських рішень у системі економічної безпеки підприємства	- контроль за дотриманням корпоративної політики ЕБП - контролює збереження майна та інших корпоративних ресурсів - контроль за дотриманням техніки безпеки - контроль комерційної таємниці - моніторинг ефективності заходів захисту.
2.3. Технології інформаційно-комунікаційного забезпечення	Оцифрування та автоматизація збору, накопичення, зберігання та передачі даних, а також зовнішніх і внутрішніх комунікацій	- автоматизація збору, накопичення та передачі інформації про загрози та небезпеки бізнес-процесів та трансформаційних перетворень - автоматизована інформаційно-обліково-аналітична система - системи автоматизації внутрішнього контролю - оцифрування конфіденційної інформації - цифровізація системи забезпечення та поточного управління ЕБП
2.4. Технології управління	Забезпечення ефективності економічної безпеки підприємства	- розробка політики корпоративної безпеки - прогнозування ймовірності трансформаційних перетворень та ймовірності виникнення ризиків і загроз - організація охоронної діяльності - планування та організація економічної безпеки - моніторинг ефективності інноваційних технологій, механізмів та засобів безпеки - запобігання руйнівним наслідкам загроз, витоку конфіденційної інформації та прикладної шкоди репутації підприємства

У роботі [8, с. 623] використовується поняття цифрової безпеки підприємства (на відміну від інформаційної складової економічної безпеки підприємства), та зазначається, що враховуючи сучасні умови цифрової трансформації, доцільно запровадити цифрову безпеку підприємства як стан цифровізації в економічній науці, а не інформаційної, що забезпечує економічні та інформаційні інтереси підприємства в поточний період та його стратегічну економічну безпеку в довгостроковій перспективі на основі відповідних технологій сучасному стану промислової революції (у цьому контексті – Індустрія 4.0).

ВИДІЛЕННЯ НЕВИРІШЕНИХ РАНІШЕ ЧАСТИН ЗАГАЛЬНОЇ ПРОБЛЕМИ, КОТРИМ ПРИСВЯЧУЄТЬСЯ СТАТТЯ

Зважаючи на значну кількість досліджень у даному напрямку [1-8], питання ролі сучасних інформаційних систем та технологій у забезпеченні економічної безпеки підприємства в умовах Digital-економіки вивчено недостатньо та вимагає подальших досліджень.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Метою статті є дослідження ролі сучасних інформаційних систем та технологій у забезпеченні економічної безпеки підприємства в умовах Digital-економіки.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Значні досягнення в сфері технологій прямо чи опосередковано вплинули на всі галузі. Щоб залишатися конкурентоспроможними та процвітати в економіці, що розвивається, галузям довелося адаптуватися до цих технологічних досягнень та впливів, таких як наскрізна автоматизація та цифровізація, що спричинило зміни у їх функціонуванні.

Цифровізація галузей промисловості, спричинена прогресом у технологіях, перетворює традиційні процеси на цифрові робочі процеси, дозволяючи компаніям оптимізувати роботу, покращити взаємодію з клієнтами та розробити нові бізнес-моделі. Також вона створює нові можливості для компаній використовувати цифрові платформи, хмарні обчислення та аналітику даних для підвищення ефективності, персоналізації пропозицій і вивчення інноваційних джерел доходу.

Завдяки прогресу в робототехніці та штучному інтелекті рутинні та повторювані завдання вдалося автоматизувати та виконувати за допомогою технології, що підвищило ефективність і продуктивність праці.

Технології також видозмінили процес виробництва: передові технології виробництва, такі як 3D-друк, зменшують витрати на створення прототипів, прискорюють виробництво та сприяють персоналізації. Ці зміни підвищують ефективність, знижують витрати та збільшують охоплення ринку для багатьох галузей, а також сприяють глобальній електронній комерції, дозволяючи компаніям охоплювати клієнтів у всьому світі та змінюючи традиційні моделі роздрібної торгівлі.

Для багатьох галузей промисловості технології підвищили важливість даних і аналітики для прийняття рішень. Технології, що розвиваються, такі як аналітика великих даних, машинне навчання та прогнозне моделювання, надають цінну інформацію для бізнесу, дозволяючи організаціям оптимізувати роботу, орієнтуватися на клієнтів і розробляти інформовані стратегії на основі аналізу на основі даних, що дозволяє компаніям краще адаптуватися до змін ринку та підвищувати рівень задоволення клієнтів.

Удосконалення технологій сприяло швидкому розвитку Digital-економіки, де бізнес переважно здійснюється за допомогою мережі Інтернет, що відкриває нові шляхи для економічної діяльності, дозволяючи компаніям легко виходити на глобальні ринки та клієнтів. Digital-економіка також надає нові можливості для підприємців, малого бізнесу та компаній для розширення свого охоплення та масштабу.

Отже, Digital-економіка видозмінила бізнес-операції, що призвело до збільшення залежності від сучасних інформаційних систем і технологій. Ці інструменти відіграють вирішальну роль у забезпеченні економічної безпеки підприємства, особливо в динамічному взаємопов'язаному світі.

Сучасні інформаційні системи [9] забезпечують платформу для зберігання, обробки та розповсюдження інформації. Вони є невід'ємною частиною підтримки ефективної роботи, покращення процесу прийняття рішень і підвищення продуктивності. Автоматизуючи рутинні завдання, ці системи звільняють ресурси, дозволяючи підприємству зосередитися на стратегічних цілях.

Крім того, ці системи забезпечують комплексні можливості керування даними, що дозволяє підприємствам використовувати потужність своїх даних. Це включає в себе здатність збирати, зберігати й аналізувати величезні обсяги даних, що дозволяє приймати більш обґрунтовані рішення. Вони також пропонують надійні інструменти звітності та візуалізації, що дозволяє компаніям розуміти та відображати складні дані більш доступним способом.

Такі технології, як штучний інтелект (AI), машинне навчання (ML) і аналітика даних, допомагають зрозуміти ринкові тенденції, поведінку споживачів і динаміку конкуренції. Вони забезпечують моніторинг бізнес-операцій у режимі реального часу, дозволяючи швидко приймати рішення та негайно реагувати на загрози та можливості.

AI та ML, зокрема, мають потенціал для трансформації бізнес-операцій. Вони можуть аналізувати великі обсяги даних, щоб виявити закономірності та тенденції, які людям буде важко, якщо не неможливо, виявити. Це може призвести до більш точного прогнозування, підвищення ефективності роботи та кращого розуміння потреб і переваг клієнтів.

Однак, використання цих систем і технологій створює свої проблеми.

У Digital-економіці підприємства піддаються широкому спектру ризиків, які можуть мати значний вплив на їх економічну безпеку. Ці ризики можуть походити з багатьох різних джерел, таких як кіберзагрози, технологічні збої та нестабільність ринку.

Зокрема, кіберзагрози набувають все більшого поширення в Digital-економіці. Загрози кібербезпеці становлять значний ризик для економічної безпеки, потенційно можуть порушити роботу, скомпрометувати конфіденційні дані та заплямувати репутацію підприємства. Тому важливо впровадити надійні заходи безпеки для захисту цілісності інформаційної системи. Ці загрози можуть приймати різні форми, починаючи від витоку даних, що відкриває конфіденційну інформацію про клієнтів, і закінчуючи атаками програм-вимагачів, які блокують компанії у їхніх власних системах, доки не буде сплачено викуп. Наслідки таких атак можуть бути надзвичайно руйнівними, що призведе до втрати довіри клієнтів, регулятивних санкцій і значних фінансових втрат.

В Україні у 2023 році кількість кібератак зросла, порівняно з 2022 роком, на 15,9% до 2543 інцидентів. Про це повідомила прессслужба Держспецзв'язку [10], передає Інтерфакс-Україна. За даними урядової команди реагування на комп'ютерні надзвичайні події CERT-UA, 347 кібератак було зафіксовано на уряд та урядові організації, 276 – на місцеві органи влади, 175 – на організації у секторі безпеки та оборони, 127 – комерційні організації. Ще 92 рази було атаковано енергетичний сектор, 81 – телеком, 38 – освітні установи. 32 – транспортну галузь, 30 – фінансовий сектор, 25 – IT-сектор, 15 – ЗМІ, 12 – медичні установи. Лише за другу половину 2023 року зафіксували та розслідували 1,46 тис кіберинцидентів.

З метою мінімізації кіберзагроз необхідно здійснювати наступний комплекс заходів (рис. 1):

Рис.1. Комплекс заходів з метою мінімізації кіберзагроз для бізнесу

1. Ідентифікація кіберзагроз: розпізнавання різних форм кіберзагроз, які можуть вплинути на підприємство, наприклад витоки даних, атаки програм-вимагачів, фішингові шахрайства та атаки на відмову в обслуговуванні.

2. Оцінка ризику: оцінювання потенційного впливу цих загроз на діяльність, репутацію та фінансовий стан підприємства.

3. Заходи профілактики: запровадження надійних рішень кібербезпеки, включаючи брандмауери, шифрування, системи виявлення вторгнень і безпечну політику паролів.

4. Навчання співробітників: проведення регулярних тренінгів, щоб ознайомити співробітників з кіберзагрозами та найкращими методами їх запобігання.

5. Регулярний аудит: проведення постійного аудиту кібербезпеки для виявлення та усунення вразливостей у цифровій інфраструктурі підприємства.

6. План реагування на інциденти: розробка комплексного плану реагування на інциденти, щоб керувати діями підприємства у разі кібератаки.

7. Планування відновлення та безперервності бізнесу: розробка стратегії для відновлення після кібератак і забезпечення безперервності діяльності підприємства.

Технологічні збої, ще один ризик у Digital-економіці, також можуть вплинути на економічну безпеку підприємства. Швидкі зміни в технологіях можуть зробити продукти або послуги компанії застарілими, загрожуючи її позиції на ринку та прибутку. Крім того, нестабільність ринку, яка характеризується непередбачуваними коливаннями ринкових умов, може суттєво вплинути на прибутковість та економічну стабільність бізнесу.

Щоб пом'якшити ці ризики, підприємства повинні прийняти проактивний підхід до своєї економічної безпеки. Це передбачає виявлення потенційних загроз і вразливостей, а також впровадження заходів для протидії їм. Наприклад, підприємства можуть інвестувати в надійні рішення кібербезпеки для захисту своїх цифрових активів. Застосування розширених заходів безпеки, таких як брандмауери, системи шифрування та виявлення вторгнень, може допомогти захистити від кіберзагроз.

Це включає створення потужної системи безпеки, регулярне тестування та оновлення заходів безпеки, а також навчання персоналу найкращим практикам безпеки. Це також передбачає розробку комплексного плану аварійного відновлення, щоб гарантувати швидке відновлення бізнесу в разі порушення безпеки чи іншої катастрофи.

Впровадження сучасних інформаційних систем і технологій — це не одноразова подія, а безперервний процес, який вимагає регулярних оновлень, щоб йти в ногу з розвитком технологій і мінливими потребами бізнесу. Це також вимагає культури навчання та адаптації серед працівників, щоб максимізувати переваги цих інструментів.

Це передбачає постійне навчання та розвиток, щоб переконатися, що співробітники знають новітні технології та розуміють, як їх ефективно використовувати [11]. Це також означає сприяння культурі інновацій, коли співробітників заохочують досліджувати нові способи використання технологій для покращення бізнес-операцій і результатів.

Тому, з метою забезпечення економічної безпеки підприємства в умовах Digital-економіки підприємствах, слід сформувати цифрову екосистему як складову економічної безпеки підприємства (рис. 2).

Дана цифрова екосистема повинна поєднувати використання новітніх технологій (штучний інтелект, машинне навчання, хмарні обчислення, аналітика великих даних, прогнозне моделювання, розширена та віртуальна реальність, промисловий Інтернет речей) разом із новітніми інформаційними системами (ERP, HRM, MES, CRM, PRM, SCM та ін.) з метою збору, зберігання, обробки та поширення інформації стосовно різних аспектів економічної безпеки підприємства. Дана інформація сприятиме активному виявленню, аналізу, оцінці впливу ризиків на функціонування підприємства в умовах Digital-економіки, а також для прийняття ефективного обґрунтованого управлінського рішення з метою управління ризиками (управлінськими, інформаційними, кадровими, технологічними та ін.). Саме такий підхід дозволить підвищити рівень економічної безпеки підприємства за умов цифровізації.

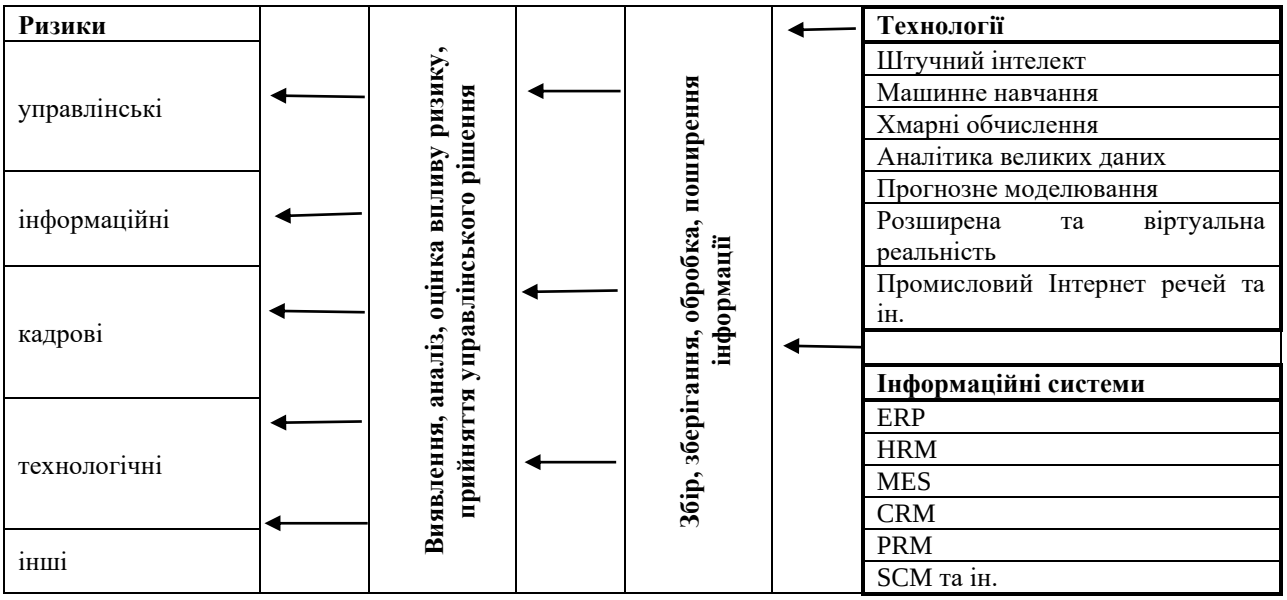

Рис. 2. Цифрова екосистема в структурі економічної безпеки підприємства

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Таким чином, можна зробити висновок, що забезпечення економічної безпеки підприємств в умовах Digital-економіки має враховувати двохаспектність використання сучасних інформаційних систем та технологій, а саме необхідність мінімізації потенційних ризиків та загроз, пов’язаних з активним розвитком та використанням цифрових технологій, з однієї сторони, а також ефективне використання можливостей, які цифрові технології надають, з іншої.

Отже, сучасні інформаційні системи та технології є життєво важливими для забезпечення економічної безпеки підприємства в Digital-економіці. Вони надають інструменти, необхідні для навігації в складному бізнес-середовищі, збереження конкурентоспроможності та захисту від потенційних ризиків. Однак, їх ефективне впровадження потребує стратегічного підходу, уваги до кібербезпеки та необхідності постійного навчання та адаптації.

Крім того, підприємства повинні застосовувати інноваційні технології для підвищення ефективності роботи та конкурентоспроможності на ринку. Використання таких технологій, як штучний інтелект, машинне навчання та великі дані, може допомогти підприємствам прогнозувати ринкові тенденції, оптимізувати роботу та випереджати конкурентів.

У роботі запропоновано сформувати цифрову екосистему як складову економічної безпеки підприємства з метою забезпечення економічної безпеки підприємства в умовах Digital-економіки. Дана цифрова екосистема повинна поєднувати використання новітніх технологій (штучний інтелект, машинне

навчання, хмарні обчислення, аналітика великих даних, прогнозне моделювання, розширена та віртуальна реальність, промисловий Інтернет речей) разом із новітніми інформаційними системами (ERP, HRM, MES, CRM, PRM, SCM та ін.) з метою збору, зберігання, обробки та поширення інформації стосовно різних аспектів економічної безпеки підприємства. Дана інформація сприятиме активному виявленню, аналізу, оцінці впливу ризиків на функціонування підприємства в умовах Digital-економіки, а також для прийняття ефективного обґрунтованого управлінського рішення з метою управління ризиками (управлінськими, інформаційними, кадровими, технологічними та ін.). Саме такий підхід дозволить підвищити рівень економічної безпеки підприємства за умов цифровізації.

Література

1. Цифрова економіка та її вплив на розвиток організацій / Рудніченко Є. М., Гавловська Н. І., Суходоля С. А., Лісовський І. В., Ядуха С. Й. // Вісник Хмельницького національного університету. Економічні науки. – 2020. - № 4. – Т. 1. - С.172-176.

2. Modern information and communication technologies in the Digital economy in the system of economic security of the enterprisest / Shmatkovska, I. Britchenko, S. Voitovych, P. Lošonczi, I. Lorvi, I. Kulyk, S. Begun // AD ALTA: Journal of Interdisciplinary Research. – 2022. – P.153-156.

3. Digital transformation as a factor in ensuring economic security of enterprises / O. Kukhar, Y. Kravchyk, O. Brechko // Baltic Journal of Economic Studies. – 2023. - Vol. 9. - № 5. – P. 143-152.

4. Панченко О. А. Інформаційні технології в забезпеченні державної безпеки / О.А. Панченко // Science Review. – 2020. - № 5(32). - С. 30-35.

5. Забезпечення економічної безпеки малого та середнього бізнесу в умовах цифровізації / В. Дикань, Н. Фролова, Цзян Пань // Інфраструктура ринку. – 2021. – Вип. 62. - С.21-27.

6. Решетов С. Вплив цифрової трансформації економіки на економічну безпеку / С. Решетов, Ю. Полусмяк // Management and entrepreneurship: trends of development. – 2020. - № 4 (22). - P. 8-16.

7. Gonchar V. Development of economic security of enterprises in the conditions of transformations / V. Gonchar, K. Polupanova // Public Security and Public Order. – 2022. - № 29. - P. 44-58.

8. Economic Security of the Enterprise Within the Conditions of Digital Transformation / Y. Samoilenko, I. Britchenko, L. Levchenko, P. Lošonczi, O. Bilichenko, O. Bodnar //. Economic affairs. – 2022. - № 67(04). – P. 619-629.

9. Чайковська І.І. Розробка моделі інформаційної системи управління знаннями на проєктно-орієнтованому підприємстві /І.І. Чайковська, В.В. Лук'янова, М.Ю. Чайковський // Modeling the development of the economic systems. - 2023. - №2. - С. 153-158.

10. Кількість кібератак у 2023 році зросла на 16% - Держспецзв'язку. URL: https://www.epravda.com.ua/news/2024/01/31/709355/

11. Чайковська І.І. Трансформація ролі людського капіталу в умовах Digital-економіки / І.І. Чайковська, Т.І. Ткач, Б.А. Поперечний // Modeling the development of the economic systems. - 2024. - №1. - С. 189-194.

References

1. Cufrova ekonomika ta ii vpluv na rozvutok organizaciy / Rudnichenko E. M., Gavlovska N. I., Suhodolya S. A., Lisovskuy I.V., Yaduha S. Y. // Herald of Khmelnytskyi National University. – 2020. - № 4. – T. 1. - S.172-176.

2. Modern information and communication technologies in the Digital economy in the system of economic security of the enterprisest / Shmatkovska, I. Britchenko, S. Voitovych, P. Lošonczi, I. Lorvi, I. Kulyk, S. Begun // AD ALTA: Journal of Interdisciplinary Research. – 2022. – P.153-156.

3. Digital transformation as a factor in ensuring economic security of enterprises / O. Kukhar, Y. Kravchyk, O. Brechko // Baltic Journal of Economic Studies. – 2023. - Vol. 9. - № 5. – P. 143-152.

4. Panchenko O. A. Infirmaciyni tehnologii v zabezpechenni derzhavnoi bezpeky / O.A. Panchenko // Science Review. – 2020. - № 5(32). - S. 30-35.

5. Zabezpechennya ekonomichnoi bezpeky malogo ta serednogobiznesu v umovah cufrovizacii / V. Dukan, N. Frolova, Czyan Pan // Infrastruktura runky. – 2021. – Vup. 62. - S.21-27.

6. Reshetov S. Vpluv cufrovoi transformacii ekonomiky na ekonomichnu bezpeku / S. Reshetov, Yu. Polusmyak // Management and entrepreneurship: trends of development. – 2020. - № 4 (22). - P. 8-16.

7. Gonchar V. Development of economic security of enterprises in the conditions of transformations / V. Gonchar, K. Polupanova // Public Security and Public Order. – 2022. - № 29. - P. 44-58.

8. Economic Security of the Enterprise Within the Conditions of Digital Transformation / Y. Samoilenko, I. Britchenko, L. Levchenko, P. Lošonczi, O. Bilichenko, O. Bodnar //. Economic affairs. – 2022. - № 67(04). – P. 619-629.

9. Chaikovska I.I. Rozrobka modeli informaciynoi sistemy upravlinnya znannyamy na proektno-orientovanomu pidpruemstvi / I.I. Chaikovska, V.V. Lukyanova, M.Yu. Chaikovskyi // Modeling the development of the economic systems. - 2023. - №2. - S. 153-158.

10. Kilkist kiberatak u 2023 roci zrosla na 16% - Derzhspeczvyazku. URL: https://www.epravda.com.ua/news/2024/01/31/709355/

11. Chaikovska I.I. Transformaciya roli lyudskogo kapitalu v umovah Digital-ekonomiky / I.I. Chaikovska, T.I. Tkach, B.A. Poperechnyi // Modeling the development of the economic systems. - 2024. - №1. - S. 189-194.