

Електронний журнал «Ефективна економіка» включено до переліку наукових фахових видань України з питань економіки (Категорія «Б», Наказ Міністерства освіти і науки України № 975 від 11.07.2019). Спеціальності – 051, 071, 072, 073, 075, 076, 292. Ефективна економіка. 2025. № 9.

DOI: <http://doi.org/10.32702/2307-2105.2025.9.7>

УДК 004.658:15

Л. М. Буяк,

д. е. н., професор, завідувач кафедри економічної кібернетики та інформатики, Західноукраїнський національний університет

ORCID ID: <https://orcid.org/0000-0002-7115-6497>

Ю. С. Семененко,

PhD (д. філос. з економіки), Старший викладач кафедри економічної кібернетики та інформатики, Західноукраїнський національний університет

ORCID ID: <https://orcid.org/0009-0000-8334-9766>

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ЯК ІНСТРУМЕНТ ПІДВИЩЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ

L. Buiak,

Doctor of Economic Sciences, Professor, Head of the Department of Economic Cybernetics and Informatics, West Ukrainian National University

Y. Semenenko,

PhD in Economics, Senior Lecturer of the Department of Economic Cybernetics and Informatics, West Ukrainian National University

INFORMATION TECHNOLOGIES AS A TOOL FOR ENHANCING THE ECONOMIC SECURITY OF ENTERPRISES

Стаття присвячена дослідженню ролі інформаційних технологій у зміцненні економічної безпеки підприємств в умовах глобальної цифрової трансформації. Сучасне бізнес-середовище характеризується високою динамікою, зростанням кількості кіберзагроз, інформаційних атак, фінансових шахрайств та нестабільністю ринків, що суттєво підвищує рівень ризиків для суб'єктів господарювання. У таких умовах забезпечення економічної безпеки виходить за межі традиційних інструментів фінансового чи організаційного контролю та потребує інтеграції сучасних інформаційних технологій, здатних забезпечити моніторинг, аналіз, прогнозування та оперативне реагування на негативні впливи зовнішнього і внутрішнього середовища.

У статті розглянуто теоретичні засади економічної безпеки підприємства та визначено місце інформаційних технологій у її структурі. Обґрунтовано, що застосування сучасних цифрових рішень дозволяє підвищити рівень прозорості фінансово-господарської діяльності, мінімізувати ймовірність економічних правопорушень, забезпечити захист інформаційних ресурсів та створити умови для зростання конкурентоспроможності. Визначено важливі аспекти впровадження інформаційних технологій у систему економічної безпеки, серед яких моніторинг фінансових показників, інтеграція систем управлінського обліку та бізнес-аналітики, розвиток внутрішніх інструментів кіберзахисту та побудова ефективних механізмів управління ризиками.

Проведено аналіз економічного ефекту від використання ІТ у сфері безпеки, впливу на зниження витрат, підвищення продуктивності управлінських процесів, скорочення термінів прийняття рішень та покращення прогнозування розвитку бізнесу. Інформаційні технології виступають не лише інструментом підтримки операційної діяльності, а й фактором стратегічного розвитку, який забезпечує інтеграцію систем безпеки в загальну корпоративну стратегію.

Формування комплексної системи економічної безпеки на основі інформаційних технологій є необхідною умовою стійкого функціонування підприємств в умовах сучасних викликів. Запропоновані підходи та результати дослідження можуть бути використані для розробки практичних рекомендацій з удосконалення політики економічної безпеки, мінімізації ризиків та підвищення ефективності управління підприємством.

The article is devoted to the study of the role of information technologies in strengthening the economic security of enterprises in the context of global digital transformation. The modern business environment is characterized by high dynamics, an increase in the number of cyber threats, information attacks, financial fraud, and market instability, which significantly raises the level of risks for business entities. Under such conditions, ensuring economic security goes beyond traditional financial or organizational control tools and requires the integration of modern information technologies capable of providing monitoring, analysis, forecasting, and rapid response to negative influences of the external and internal environment.

The article examines the theoretical foundations of the economic security of enterprises and defines the place of information technologies in its structure. It is substantiated that the use of modern digital solutions makes it possible to increase the transparency of financial and economic activities, minimize the likelihood of economic offenses, ensure the protection of information resources, and create conditions for improving competitiveness. Important aspects of implementing information technologies in the system of economic security are identified, including the monitoring of financial indicators, the integration of management accounting and business analytics systems, the development of internal cybersecurity tools, and the establishment of effective risk management mechanisms.

An analysis of the economic effect of using IT in the field of security is carried out, particularly its impact on cost reduction, the improvement of

managerial process productivity, the shortening of decision-making time, and the enhancement of business development forecasting. Information technologies act not only as a tool for supporting operational activities but also as a factor of strategic development, ensuring the integration of security systems into the overall corporate strategy.

The formation of a comprehensive system of economic security based on information technologies is considered a necessary condition for the sustainable functioning of enterprises under modern challenges. The proposed approaches and research results can be used to develop practical recommendations for improving economic security policies, minimizing risks, and enhancing the efficiency of enterprise management.

Ключові слова: *Інформаційні технології, економічна безпека, цифрова трансформація, управління ризиками, впровадження IT-рішень.*

Keywords: *Information technologies, economic security, digital transformation, risk management, IT solutions implementation.*

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичним завданнями. У сучасних умовах глобальної цифрової трансформації та зростання рівня невизначеності бізнес-середовища проблема забезпечення економічної безпеки підприємств набуває особливої актуальності. Зростання кіберзагроз, фінансових шахрайств, нестабільність ринків та висока конкуренція створюють додаткові ризики для суб'єктів господарювання. Традиційні методи фінансового контролю та організаційного управління вже не гарантують належного рівня захищеності та стійкості підприємств у довгостроковій перспективі.

Інформаційні технології стають інструментом не лише для підвищення ефективності управління, але й для формування сучасних систем економічної безпеки. Використання цифрових рішень дозволяє здійснювати оперативний

моніторинг фінансових показників, прогнозувати ризики, забезпечувати інформаційну безпеку та інтегрувати механізми кіберзахисту в загальну корпоративну стратегію.

Але виникають певні складнощі під час впровадження таких рішень, значні інвестиційні витрати, потреба у кваліфікованому персоналі, швидкі темпи технологічного оновлення, а також ризики залежності від постачальників ІТ-рішень. Недостатня увага до цих проблем може призвести до неефективності впроваджених систем, зниження рівня економічної безпеки та втрати конкурентних позицій.

Виникає необхідність у комплексному дослідженні ролі інформаційних технологій у зміцненні економічної безпеки підприємств. Такий підхід дозволить розробити науково обґрунтовані методи впровадження ІТ-рішень, оцінки їх ефективності та формування стратегій, спрямованих на мінімізацію ризиків і підвищення стійкості бізнесу в умовах сучасних викликів.

Аналіз останніх досліджень та публікацій. Вивченням питання підвищення економічної безпеки з використанням інформаційних технологій займається велика кількість Українських та іноземних вчених. Тетяна Сімкова та Юрій Копча досліджують забезпечення економічної безпеки підприємств в умовах інноваційного розвитку [1]. Р.Г. Сніщенко та В.І.Гринчуцький обґрунтовують роль інформаційної безпеки як одного з елементів економічної безпеки [2]. Варналій З.С. та Бондаренко С.М. аналізують поняття фінансової безпеки Українських підприємств в воєнний та післявоєнний періоди [3]. Проте питання використання інформаційних технологій як інструменту підвищення економічної безпеки підприємств потребує подальшого вивчення та дослідження.

Мета статті. Метою статті є дослідження ролі інформаційних технологій у забезпеченні економічної безпеки підприємств в умовах цифрової трансформації та зростання ризиків у бізнес-середовищі. У роботі аналізується теоретичний і практичний потенціал застосування сучасних ІТ-рішень для моніторингу фінансових показників, управління ризиками,

кіберзахисту та підвищення прозорості господарської діяльності. Проводиться оцінка впливу цифрових технологій на зниження ймовірності економічних правопорушень, оптимізацію управлінських процесів і підвищення ефективності прийняття рішень. Стаття має на меті визначити головні напрями інтеграції ІТ у систему економічної безпеки підприємств та сформулювати рекомендації щодо підвищення їх конкурентоспроможності й стійкості до зовнішніх і внутрішніх загроз.

Виклад основного матеріалу. У сучасному бізнес-середовищі економічна безпека набуває статусу одного з основних чинників стійкого розвитку підприємства. Вона виступає основою захисту від загроз, що виникають унаслідок економічної нестабільності, зростання конкуренції чи трансформацій глобальних ринків. Саме через призму економічної безпеки визначається здатність підприємства не лише зберігати поточні позиції, але й формувати умови для довгострокового зростання.

Економічна безпека підприємства розглядається як комплексний стан захищеності його ресурсів, процесів і стратегічних інтересів від внутрішніх та зовнішніх викликів, що можуть перешкоджати стабільному розвитку та знижувати конкурентоспроможність. Вона формується на перетині фінансових, організаційних та технологічних чинників, але водночас виходить за межі окремих функціональних напрямів, охоплюючи весь цикл господарської діяльності. Сучасне розуміння економічної безпеки зміщується від вузького трактування, що зосереджувалося переважно на фінансових показниках, до ширшого підходу, який включає ризик-менеджмент, інформаційний захист та здатність підприємства адаптуватися до змін середовища.

Структура економічної безпеки ґрунтується на взаємодії кількох ключових елементів. Фінансова стійкість, яка визначає здатність підприємства підтримувати ліквідність, забезпечувати прибутковість і контролювати рівень боргових зобов'язань. Виробнича складова, що характеризує безперервність технологічних процесів і якість продукції чи

послуг. Важливим аспектом є кадровий потенціал, адже кваліфікація персоналу та ефективність його роботи безпосередньо впливають на здатність підприємства протидіяти ризикам. Також важливою є інформаційна складова, яка охоплює захист комерційних даних, стабільність інформаційних систем і можливість використання аналітики для прийняття рішень. Додатково до цього формується інноваційна складова, що забезпечує довгостроковий розвиток та дозволяє підприємству відповідати на технологічні виклики ринку.

Збалансованість зазначених елементів визначає рівень економічної безпеки в цілому. Якщо один із компонентів виявляється ослабленим, підприємство стає вразливим до кризових явищ, навіть за умов стабільності інших складових. Тому система економічної безпеки потребує постійного моніторингу та адаптації, щоб відповідати реальним викликам середовища. У сучасних умовах саме інтеграція різних напрямів в єдину стратегію дозволяє підприємству не лише зберігати стійкість, але й розвивати конкурентні переваги.

Сучасна цифрова економіка формує середовище, у якому підприємства все більше залежать від ефективного використання інформаційних технологій для захисту власних ресурсів. Зростання складності бізнес-процесів, поява нових ризиків і загроз вимагають розробки комплексних підходів до забезпечення економічної безпеки. У цьому контексті ІТ-рішення набувають нової ролі вони одночасно є інструментом оптимізації управління і засобом протидії негативним впливам внутрішніх та зовнішніх чинників.

Одним із ключових напрямів використання ІТ є впровадження аналітичних систем, здатних виявляти закономірності в даних, прогнозувати фінансові ризики та формувати обґрунтовані управлінські рішення. Їхнє застосування дозволяє підвищувати прозорість діяльності та мінімізувати ймовірність стратегічних прорахунків. Паралельно з цим важливе значення має кіберзахист, який забезпечує збереження інформаційних активів і недопущення несанкціонованого доступу до корпоративних даних. Оскільки

інформація стає ключовим економічним ресурсом, втрата контролю над нею здатна спричинити серйозні фінансові збитки та підрив довіри до підприємства.

Важливою частиною є системи моніторингу фінансових потоків, які забезпечують своєчасне виявлення аномалій у розрахунках, запобігають шахрайським операціям і підтримують баланс ліквідності. Вони інтегрують у єдину платформу бухгалтерські, банківські та управлінські дані, що підвищує якість контролю над ресурсами. Аналітика, кіберзахист і моніторинг утворюють взаємодоповнювану систему, здатну зміцнити економічну безпеку підприємства у динамічному цифровому середовищі.

Оцінка економічної безпеки підприємства ґрунтується на поєднанні кількісних та якісних методологічних підходів, що дають змогу комплексно визначити рівень захищеності бізнесу від внутрішніх і зовнішніх загроз. У науковій літературі виділяють декілька базових напрямів, які різняться за об'єктом дослідження, способом вимірювання та інструментарієм інтерпретації результатів.

Одним із базових підходів є індикаторний, що передбачає використання системи ключових показників фінансової та виробничої діяльності. Він дає змогу визначати граничні значення, відхилення від яких сигналізують про зростання загроз. Однак такий підхід часто потребує глибшої аналітики, оскільки окремі індикатори не завжди відображають реальну картину ризиків. У цьому контексті застосовують інтегральні моделі, де за допомогою багатофакторного аналізу формують узагальнений показник рівня економічної безпеки.

Важливу роль відіграє функціональний підхід, орієнтований на оцінку безпеки за складовими: фінансовою, інноваційною, виробничою, інформаційною. Такий поділ дозволяє виявити проблемні місця у структурі підприємства та спрямувати ресурси на їхнє посилення. Окреме місце посідає ресурсно-орієнтований підхід, що акцентує увагу на ефективності

використання активів і здатності компанії протистояти загрозам завдяки власному потенціалу.

Сучасна практика активно інтегрує ризик-орієнтовані методології, які ґрунтуються на прогнозуванні ймовірності настання негативних подій та оцінюванні їхніх наслідків. Вони передбачають моделювання сценаріїв та використання ІТ-інструментів для кількісного визначення ступеня небезпеки. Завдяки цьому управлінці отримують не лише оцінку поточного стану, а й основу для розробки превентивних стратегій.

У результаті поєднання різних методологічних підходів формується багатовимірна картина економічної безпеки, що забезпечує можливість ухвалювати стратегічні рішення на основі об'єктивної та динамічної інформації.

Сучасні умови господарювання створюють умови в яких економічна безпека підприємства дедалі більше визначається здатністю до цифрової трансформації та ефективного управління ризиками. Цифровізація бізнес-процесів створює нові можливості для моніторингу фінансових потоків, аналізу ринкової динаміки та прогнозування потенційних загроз, водночас формуючи новий спектр ризиків, пов'язаних із кіберзлочинністю, інформаційними витоками та технологічною залежністю.

Економічна безпека у цифровому середовищі не обмежується захистом ресурсів. Вона передбачає створення системи адаптивного реагування на виклики, що виникають унаслідок швидкої зміни технологій. Управління ризиками в такому контексті набуває стратегічного значення, оскільки дозволяє визначати критичні точки у бізнес-моделі, формувати сценарії розвитку та мінімізувати втрати від непередбачуваних подій.

Цифрова трансформація водночас слугує інструментом посилення економічної безпеки. Використання аналітичних платформ, систем штучного інтелекту та автоматизованих засобів контролю забезпечує більш точне прогнозування ризиків і підвищує прозорість операційної діяльності. Це створює передумови для переходу від реактивного до превентивного

управління, де загрози не лише виявляються на ранніх етапах, але й активно нейтралізуються завдяки технологічним рішенням.

Взаємозв'язок економічної безпеки з цифровою трансформацією та управлінням ризиками є двостороннім, трансформаційні процеси відкривають нові можливості для зміцнення безпеки, але водночас породжують ризики, які потребують постійного контролю та гнучких підходів до управління. Саме баланс між інноваційним розвитком і превентивним ризик-менеджментом визначає здатність підприємства зберігати стійкість і конкурентоспроможність у цифровій економіці.

У сучасній економіці інформаційні технології є основою, на якій формується конкурентоспроможність підприємств. Їхнє призначення полягає не лише в автоматизації рутинних завдань, а й у створенні середовища, що забезпечує постійний доступ до актуальної інформації, швидку обробку даних і підтримку процесів прийняття рішень. Завдяки цьому підприємства отримують можливість реагувати на зміни ринку з мінімальними затримками та більшою точністю у прогнозуванні.

Сутність інформаційних технологій у бізнесі проявляється в інтеграції цифрових інструментів у ключові процеси управління. Це включає оптимізацію комунікацій, побудову прозорої фінансової системи, підвищення продуктивності персоналу та розвиток механізмів стратегічного планування. Такі технології не зводяться лише до програмного забезпечення чи технічного обладнання, вони утворюють цілісну систему взаємодії людей, процесів та інфраструктури.

У контексті економічної безпеки інформаційні технології стають інструментом підвищення стійкості бізнесу. Їх застосування дозволяє швидко виявляти загрози, проводити аналітику ризиків і формувати ефективні заходи протидії. Вони створюють умови, за яких управлінські рішення ґрунтуються на перевірених даних, що знижує ймовірність помилок та зменшує вразливість підприємства до зовнішніх і внутрішніх чинників.

Інформаційні технології в бізнесі набувають значення стратегічного ресурсу, що впливає на довгострокову стабільність підприємства. Вони забезпечують не лише оперативне управління, а й формування нових моделей розвитку, здатних відповідати вимогам цифрової економіки та забезпечувати стійку конкурентну позицію на ринку.

Ефективність забезпечення економічної безпеки підприємства значною мірою визначається якістю застосованих інформаційних рішень. Сучасні цифрові інструменти створюють умови для комплексного захисту, що охоплює як інформаційну, так і фінансову сферу діяльності компанії (рис.1). Вони спрямовані на своєчасне виявлення загроз, їх оцінку та формування механізмів реагування, що дозволяє мінімізувати ризики та забезпечувати стабільність розвитку.

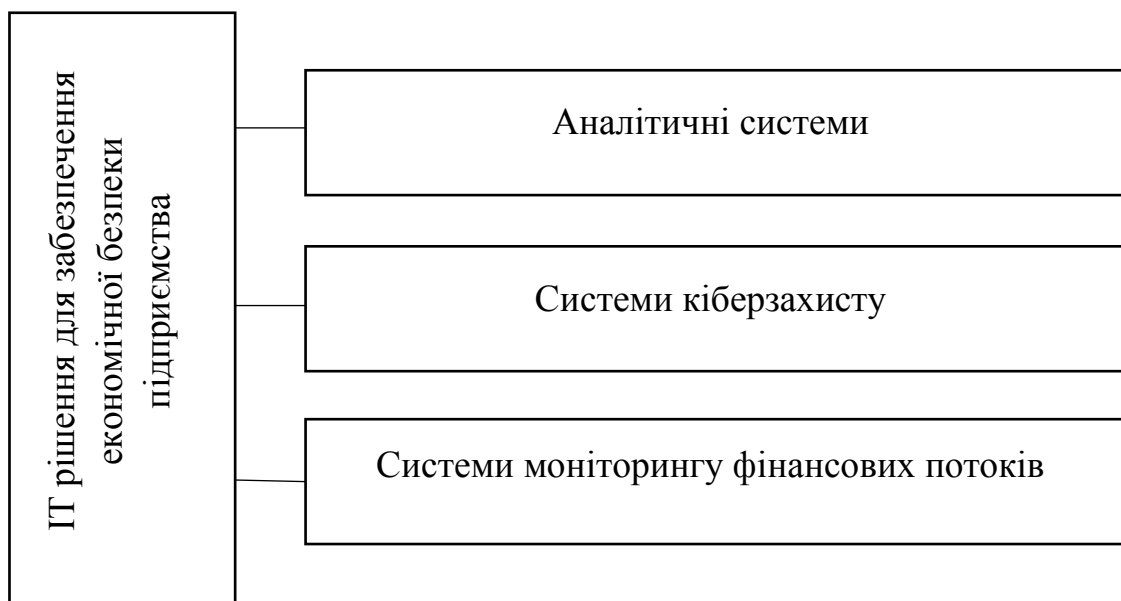


Рисунок 1. Типи ІТ рішень для забезпечення економічної безпеки підприємства

В умовах постійної зміни ринкової кон'юнктури аналітика стає основою для управлінських рішень. Аналітичні системи дають змогу обробляти великі масиви даних у режимі реального часу та формувати багатовимірні моделі діяльності підприємства. Вони виявляють закономірності, що непомітні за традиційного аналізу, і дозволяють прогнозувати можливі ризики. Застосування таких інструментів забезпечує

раннє попередження про фінансові загрози, підвищує якість планування та створює інформаційну базу для своєчасного реагування на негативні фактори. Аналітичні системи не лише відображають поточний стан, а й допомагають будувати сценарії розвитку подій, що перетворює їх на ключовий елемент стратегічного управління безпекою.

З розвитком цифрових технологій підприємства дедалі більше залежать від надійності інформаційної інфраструктури. Загрози у вигляді хакерських атак, витоків даних або шкідливого програмного забезпечення можуть мати прямий економічний ефект, включно з фінансовими втратами та репутаційними ризиками. Системи кіберзахисту створюють багаторівневий бар'єр, що включає інструменти аутентифікації, шифрування, аналізу трафіку та виявлення вторгнень. Їхня функція полягає не лише у відбитті атак, а й у забезпеченні безперервності бізнес-процесів за рахунок швидкого відновлення роботи систем після інцидентів. Кіберзахист формує цифровий щит підприємства, що гарантує захист ключових активів і зменшує вплив зовнішніх загроз на економічну стабільність.

Фінансова сфера традиційно є найбільш вразливою для внутрішніх і зовнішніх загроз. Використання систем моніторингу дозволяє підприємствам отримувати повну картину руху коштів і вчасно реагувати на будь-які відхилення. Такі системи автоматично виявляють підозрілі операції, знижують ризик шахрайства та запобігають нелегальним фінансовим діям. Крім того, вони створюють умови для підвищення прозорості обліку та ефективності використання ресурсів. Моніторинг фінансових потоків інтегрується з бухгалтерськими та управлінськими системами, утворюючи єдине середовище для контролю й оптимізації фінансів. У результаті підприємство отримує інструмент не лише для захисту, а й для стратегічного управління капіталом.

Використання інформаційних технологій змінює саму логіку функціонування системи економічної безпеки підприємства. У сфері фінансової стабільності ІТ-інструменти забезпечують більш точний контроль

за рухом грошових потоків, автоматизують процеси виявлення підозрілих транзакцій і дають змогу прогнозувати ризики ліквідності. Це зменшує ймовірність внутрішніх зловживань та підвищує довіру партнерів.

В управлінні кадровими ризиками технології створюють інструменти для оцінки продуктивності персоналу, моніторингу кваліфікації й вчасного виявлення ознак недобросовісної поведінки. Аналітичні моделі допомагають прогнозувати потреби в кадрах і знижувати ризики плинності, що особливо важливо в умовах дефіциту кваліфікованих спеціалістів.

У площині інформаційної безпеки ключову роль відіграє кіберзахист. Системи шифрування, багаторівнева аутентифікація та інструменти управління доступом мінімізують ризики несанкціонованого втручання у внутрішні ресурси. Завдяки цьому зберігається комерційна таємниця та стратегічна інформація, що напряду впливає на конкурентоспроможність.

На рівні операційної діяльності технології сприяють зменшенню виробничих ризиків. Автоматизовані системи управління виробництвом підвищують точність прогнозів щодо попиту, оптимізують запаси та дозволяють виявляти неефективність у реальному часі. Це знижує ймовірність фінансових втрат через перебої у виробництві чи постачанні.

Інформаційні технології створюють нові інструменти для активного управління ризиками, перетворюючи економічну безпеку на динамічний процес.

Традиційні механізми безпеки здебільшого ґрунтувалися на фізичному контролі та адміністративних регламентах. Вони включали охорону приміщень, перевірку фінансової документації вручну, внутрішні інструкції та звітність. Такі підходи мали високу залежність від людського фактора, що обмежувало їхню ефективність у ситуаціях із великою кількістю даних і високою швидкістю змін.

Цифрові інструменти захисту змінили цей підхід. Вони забезпечують безперервний моніторинг, працюють з великими обсягами інформації й дозволяють виявляти ризики ще на ранніх етапах.

Важливою перевагою цифрових рішень є їхня гнучкість і масштабованість. Системи кіберзахисту оновлюються відповідно до нових загроз, тоді як традиційні заходи зазвичай мають статичний характер. Сучасні IT-інструменти інтегруються між собою, формуючи комплексну багаторівневу систему захисту, що практично неможливо відтворити лише адміністративними методами.

Інформаційні технології у сфері економічної безпеки формують багаторівневу систему захисних і управлінських інструментів, які дозволяють зменшувати ризики, забезпечувати стабільність і підтримувати конкурентні позиції підприємства.

Ці системи виступають базовим рівнем цифрового забезпечення економічної безпеки, оскільки вони структурують дані, автоматизують процеси й унеможливають частину ризиків, пов'язаних із людським фактором (рис.2).

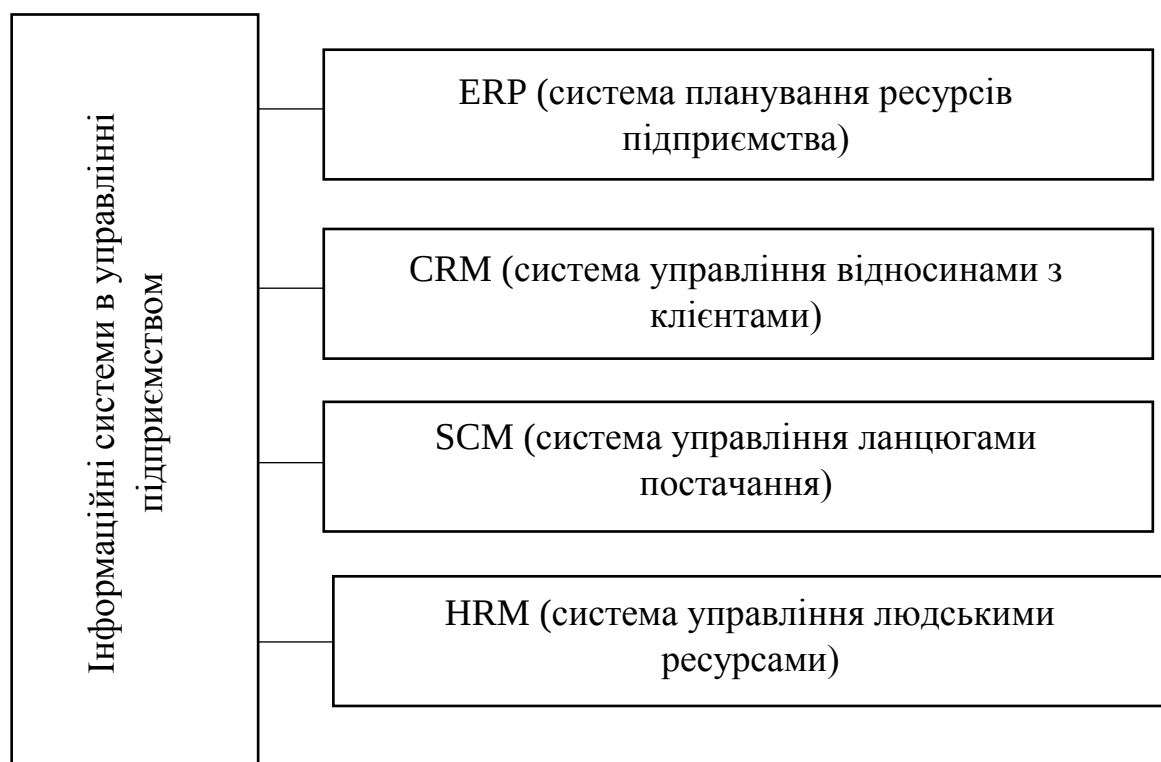


Рисунок 2. Інформаційні системи в управлінні підприємством

ERP системи забезпечують централізоване управління ресурсами підприємства. Для економічної безпеки важливим є прозорість фінансових операцій, контроль витрат і планування закупівель. ERP зменшує ризик шахрайства через автоматичне узгодження даних у різних підрозділах та забезпечує швидке виявлення відхилень.

CRM системи спрямовані на управління відносинами з клієнтами. Їх значення для безпеки полягає в захисті бази клієнтів від витоку, а також у моніторингу репутаційних ризиків. Вона допомагає вчасно реагувати на зміни в поведінці клієнтів, що знижує ймовірність фінансових втрат і шахрайських дій.

SCM забезпечує контроль ланцюгів постачання. Для безпеки це означає зменшення ризиків перебоїв у постачанні, своєчасне виявлення ненадійних партнерів і оптимізацію логістики. Система мінімізує фінансові втрати від зривів контрактів або несвоєчасних поставок.

HRM автоматизує управління персоналом. З погляду безпеки це контроль кадрових ризиків, моніторинг продуктивності працівників, управління доступом до інформації та прогнозування потреб у кадрах. HRM дозволяє виявляти слабкі місця у системі мотивації й попереджати витік знань.

BI-системи надають можливість працювати з великими масивами даних аналізуючи їх у режимі реального часу. Для економічної безпеки вони виконують критичну функцію — оцінку фінансової стійкості підприємства. Системи прогнозують рух капіталу, відстежують динаміку доходів і витрат, формують сценарії розвитку залежно від змін ринкових умов. Завдяки інтеграції BI з ERP і CRM вдається оперативно виявляти ризики неплатоспроможності та приймати рішення щодо оптимізації фінансових потоків. Це дає змогу знижувати вразливість підприємства до зовнішніх і внутрішніх загроз.

Сучасні системи управління ризиками базуються на алгоритмах машинного навчання й моделюванні сценаріїв. Вони дозволяють визначати

ймовірність виникнення кризових ситуацій, оцінювати потенційні збитки та формувати стратегії мінімізації наслідків. Для економічної безпеки це означає перехід від реактивного підходу до проактивного. Технології прогнозування особливо важливі в умовах нестабільної економіки, коли підприємства повинні швидко адаптуватися до змін у фінансових ринках, валютних коливаннях чи законодавчому середовищі.

До систем кіберзахисту належать антивірусні програми, міжмережеві екрани, системи багаторівневої автентифікації, інструменти управління доступом та технології шифрування. Їхня роль в економічній безпеці визначальна, адже інформація є ключовим стратегічним ресурсом. Захист даних запобігає витоку комерційної таємниці, недопущенню шахрайських операцій і втраті конкурентних переваг. Сучасні підходи передбачають створення комплексних систем кіберзахисту, які не тільки відбивають атаки, а й здатні прогнозувати можливі загрози.

Впровадження інформаційних технологій у сферу економічної безпеки потребує послідовного підходу, що поєднує технічну, організаційну та управлінську складові. Спершу проводиться діагностика існуючого стану системи безпеки, виявляються найбільш вразливі процеси та джерела ризиків. Далі формується концепція цифрового захисту, у якій визначаються цілі, ресурси та пріоритети. Важливим етапом є адаптація вибраних технологічних рішень до специфіки бізнесу, універсальних моделей не існує. Після цього відбувається технічне впровадження, інтеграція з уже діючими системами та налаштування механізмів контролю. Завершальним кроком виступає тестування, підготовка персоналу і запуск повноцінної експлуатації з постійним удосконаленням.

Ефективність автоматизації визначається узгодженістю між технологічними можливостями системи та реальними потребами бізнесу. Ключове значення має підтримка з боку керівництва, оскільки без стратегічного бачення ІТ-рішення можуть залишитися фрагментарними. Важливою є також якість даних, адже неточна чи застаріла інформація

знижує достовірність аналітики та прогнозів. Рівень кваліфікації персоналу визначає, наскільки швидко нові інструменти інтегруються в робочі процеси. Додатковим фактором є побудова системи з урахуванням гнучкості, що дозволяє реагувати на зміну загроз і масштабувати рішення відповідно до зростання підприємства.

Найбільш поширеною проблемою є висока вартість сучасних технологій, що обмежує доступ підприємств до комплексних систем захисту. Не менш важливим чинником є людський фактор, опір змінам, недостатня готовність працівників до використання нових інструментів, брак знань у сфері кібербезпеки. Додаткову складність становить фрагментарність рішень, коли різні системи не узгоджуються між собою, створюючи проблемні місця у захисті. Ризиком є й залежність від зовнішніх постачальників, що може призводити до втрати контролю над критичними даними чи сервісами.

Сучасні IT-рішення не існують у відриві від загальної цифрової інфраструктури підприємства. Їхня ефективність визначається рівнем інтеграції з системами управлінського обліку, фінансової аналітики, логістики та кадрового менеджменту. Водночас важливим є взаємозв'язок із зовнішніми сервісами, зокрема банківськими платформами, державними реєстрами та системами контрагентів. Така взаємодія створює умови для комплексного моніторингу й забезпечення прозорості транзакцій, проте водночас підвищує вимоги до кіберзахисту. Саме збалансування внутрішньої інтеграції та зовнішньої взаємодії формує цілісність економічної безпеки.

Використання інформаційних технологій у сфері безпеки змінює структуру витрат підприємства, зменшуючи операційні втрати та підвищуючи ефективність управління ресурсами. Автоматизація процесів контролю дозволяє мінімізувати витрати, пов'язані з дублюванням функцій і помилками персоналу. Водночас впровадження систем аналітики знижує ймовірність шахрайських дій та фінансових маніпуляцій, що прямо впливає на збереження капіталу. Первинні інвестиції у технології можуть бути

значними, однак довгостроковий ефект проявляється через скорочення непродуктивних витрат і підвищення прозорості фінансових потоків.

ІТ-рішення для безпеки сприяють підвищенню швидкості обробки даних і зменшенню часу, необхідного для виявлення та усунення ризиків. Автоматизовані механізми аналізу дозволяють керівникам оперативно отримувати достовірну інформацію про стан підприємства, що скорочує цикл прийняття управлінських рішень. Це створює можливість для своєчасного реагування на загрози уникаючи додаткових втрат. Підвищення продуктивності також досягається за рахунок зменшення навантаження на персонал, який замість виконання рутинних завдань зосереджується на стратегічних функціях.

Сучасні цифрові технології розширюють можливості прогнозу аналітики, що підсилює здатність підприємства передбачати ймовірні загрози та адаптувати стратегію управління ризиками. Завдяки аналізу великих обсягів даних стає можливим виявлення прихованих тенденцій і раннє попередження кризових ситуацій. Це дозволяє мінімізувати наслідки непередбачуваних подій і зменшувати фінансові втрати від коливань ринку. Прогнозна аналітика підвищує гнучкість підприємства, формуючи підґрунтя для більш стійкого функціонування у мінливому середовищі.

Інформаційні технології перестають виконувати виключно технічну функцію й перетворюються на елемент стратегічного управління. Їх інтеграція у корпоративну стратегію дозволяє сформувати цілісну систему економічної безпеки, яка охоплює фінансову, організаційну та репутаційну складові. Це забезпечує не лише збереження активів, а й створює додану вартість через підвищення довіри інвесторів, партнерів і клієнтів. У результаті підприємство отримує конкурентну перевагу, яка базується на стабільності, передбачуваності та здатності до довгострокового розвитку.

Висновки. Економічна безпека підприємства в умовах цифрової трансформації визначається здатністю ефективно інтегрувати інформаційні технології у систему управління та захисту ресурсів. Використання сучасних

цифрових рішень дозволяє мінімізувати ризики фінансових втрат, інформаційних атак і репутаційних загроз, створюючи основу для стабільного розвитку.

Використання спеціалізованих систем забезпечує прозорість бізнес-процесів, контроль фінансових потоків і захист даних, що знижує ймовірність шахрайських дій та операційних помилок. Інструменти бізнес-аналітики підвищують точність оцінки фінансової стабільності, сприяють ранньому виявленню ризиків і дозволяють оперативно коригувати управлінські стратегії. Засоби кіберзахисту формують додатковий рівень безпеки, що унеможливорює витік інформації та забезпечує захист корпоративних даних.

Практичний ефект впровадження інформаційних технологій проявляється у скороченні витрат, зростанні продуктивності управлінських процесів та зменшенні часу прийняття рішень. Це створює умови для швидшого реагування на зовнішні виклики та внутрішні загрози, знижуючи рівень невизначеності у діяльності підприємства. Цифрові технології сприяють формуванню інтегрованої системи ризик-менеджменту, що підвищує здатність підприємства адаптуватися до динамічного ринкового середовища.

Комплексне впровадження інформаційних технологій у систему економічної безпеки дозволяє поєднати контроль ресурсів, ефективність управління та стратегічну стійкість, що є ключовою умовою успішного функціонування підприємств у сучасному цифровому середовищі.

Література

1. Сімкова Т., Копча Ю. Стратегічні імперативи забезпечення економічної безпеки підприємства в умовах інноваційного розвитку під впливом невизначеності і ризиків. Економічний аналіз. 2025. Том 35. № 1. С. 167-177. DOI: <https://doi.org/10.35774/econa2025.01.167>

2. Сніщенко Р. Г., Гринчуцький В. І. Інформаційна безпека як складова економічної безпеки суб'єктів господарювання. Економічний аналіз. 2020. Том 30. № 1. Частина 1. С. 241-248. DOI: <https://doi.org/10.35774/econa2020.01.01.241>

3. Varnalii, Z., & Bondarenko, S. (2023). Financial security of Ukrainian enterprises during the war and post-war period. *University Economic Bulletin*, 18(1), 106-113. DOI: <https://doi.org/10.31470/2306-546X-2023-56-106-113>

4. Семененко, Ю. (2024). Хмарні технології як фактор підвищення ефективності діяльності компанії. *Herald of Khmelnytskyi National University. Economic Sciences*, 334(5), 211-218. DOI: <https://doi.org/10.31891/2307-5740-2024-334-29>

References

1. Simkova, T. and Kopcha, Yu. (2025), “Strategic imperatives of ensuring the economic security of the enterprise in the conditions of innovative development under the influence of uncertainty and risks”, *Economic Analysis*, vol. 35, no. 1, pp. 167–177. <https://doi.org/10.35774/econa2025.01.167>

2. Snishchenko, R.H. and Hrynychutskyi, V.I. (2020), “Information security as a component of the economic security of business entities”, *Economic Analysis*, vol. 30, no. 1, part 1, pp. 241–248. <https://doi.org/10.35774/econa2020.01.01.241>

3. Varnalii, Z. and Bondarenko, S. (2023), “Financial security of Ukrainian enterprises during the war and post-war period”, *University Economic Bulletin*, vol. 18, no. 1, pp. 106–113. <https://doi.org/10.31470/2306-546X-2023-56-106-113>

4. Semenenko, Y. (2024), “Cloud technologies as a factor in improving the efficiency of the company’s activities”, *Herald of Khmelnytskyi National University. Economic Sciences*, vol. 334, no. 5, pp. 211–218. <https://doi.org/10.31891/2307-5740-2024-334-29>

Стаття надійшла до редакції 04.09.2025 р.