УДК 658.15:004

В. П. Горин,
д. е. н., професор, професор кафедри фінансів
ім. С. І. Юрія, Західноукраїнський національний університет
ORCID ID: https://orcid.org/0000-0002-6048-8330
В. В. Костецький,
к. е. н., доцент, доцент кафедри фінансових технологій та банківського бізнесу,
Західноукраїнський національний університет
ORCID ID: https://orcid.org/0000-0002-0179-9526

DOI: 10.32702/2306-6814.2026.9.57

ЦИФРОВІ ІНСТРУМЕНТИ УПРАВЛІННЯ ФІНАНСОВОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА

V. Horyn,
Doctor of Economic Sciences, Professor, Professor of S. Yuriy Department of Finance, West Ukrainian National University
V. Kostetskyi,
PhD in Economics, Associate Professor, Associate Professor of Department of Financial Technologies
and Banking Business, West Ukrainian National University

DIGITAL TOOLS FOR MANAGING ENTERPRISE FINANCIAL SECURITY

У статті систематизовано цифрові інструменти управління фінансовою безпекою підприємства в умовах воєнної нестабільності. Визначено чотири функціональні групи таких інструментів: моніторинг фінансового стану, аналітика та прогнозування, автоматизація фінансових процесів, кібербезпека та захист фінансових даних. Для кожної групи охарактеризовано різновиди цифрових продуктів та їхню роль у мінімізації конкретних загроз фінансовій безпеці підприємства. Окрему увагу приділено продуктам, що мають практичне застосування в Україні. На основі порівняльного аналізу інструментів за критеріями характеру впливу на фінансову безпеку, складності інтеграції та тривалості ефекту від впровадження встановлено, що різні групи інструментів виконують неоднакову роль у забезпеченні фінансової стійкості підприємства. Ідентифіковано системні бар'єри впровадження цифрових рішень в умовах воєнного стану: висока вартість повнофункціональних платформ, складність їхньої інтеграції з наявною IT-інфраструктурою, дефіцит цифрових компетенцій персоналу та зростаюча залежність від зовнішніх провайдерів. Обгрунтовано, що фінансова безпека підприємства досягається не через окремі інструменти, а через побудову цілісної цифрової екосистеми, елементи якої є взаємодоповнювальними.

The article systematises digital tools for managing enterprise financial security under conditions of wartime instability. The study addresses a practical gap: while digital transformation of financial management is actively discussed in the literature, a structured classification of relevant instruments with an assessment of their applicability under heightened uncertainty has not been developed. Four functional groups of digital tools are identified: financial condition monitoring, analytics and forecasting, financial process automation, and cybersecurity and financial data protection. For each group, the principal instrument types are characterised along with their role in mitigating specific threats to enterprise financial security, with emphasis on solutions available in the Ukrainian market.

Copyright © The Author(s). This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

A comparative analysis of the instruments across three criteria — nature of impact on financial security (direct or indirect), integration complexity, and time horizon of implementation effect — reveals that the groups perform fundamentally different roles. Monitoring and cybersecurity tools exert a direct protective effect on financial flows and assets, whereas analytical platforms and automation solutions generate an indirect effect by improving the quality of managerial decisions and reducing operational risk.

The article identifies systemic barriers to the adoption of digital solutions under martial law: the high cost of full-featured platforms such as ERP and SIEM systems; the complexity of integrating them with legacy IT infrastructure; a deficit of digital competencies among financial management personnel; and growing dependency on external providers whose continuity of service is uncertain in wartime conditions.

The study concludes that enterprise financial security is achieved not through individual instruments in isolation, but through the construction of a coherent digital ecosystem in which tools across all four groups complement one another. The practical value of this framework lies in supporting evidence-based selection of digital instruments with regard to enterprise scale, risk profile, and resource constraints.

Ключові слова: фінансова безпека підприємства, цифрові інструменти, ERP-системи, BI-платформи, автоматизація фінансових процесів, кібербезпека, SIEM, RPA, фінансовий менеджмент, цифрова трансформація.

Key words: enterprise financial security, digital tools, ERP systems, BI platforms, financial process automation, cybersecurity, SIEM, RPA, financial management, digital transformation.

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

Сучасні умови діяльності підприємств в Україні визначаються впливом масштабної війни та пов'язаними з нею високим рівнем невизначеності й ризиків, посиленням нестабільності ринкового середовища, порушенням логістичних ланцюгів, зниженням платоспроможності контрагентів, загрозами фізичній та інформаційній інфраструктурі. У воєнних реаліях фінансова безпека підприємства формується під впливом загроз різного походження. Зовнішні джерела ризику пов'язані, перш за все, із високим рівнем волатильності валютного курсу, інфляційними процесами, обмеженням доступу підприємств до фінансових ресурсів, спонтанними змінами у державному регулюванні, втратою ринків збуту. Внутрішні загрози фінансовій безпеці підприємства обумовлені прорахунками в управлінні, які спричиняють зниження ліквідності, зростання дебіторської заборгованості, ускладнення контролю за фінансовими потоками та підвищення імовірності зловживань у кризових умовах. Традиційні підходи до управління фінансами підприємства орієнтовані переважно на стабільні умови діяльності, що визначає їхню недостатню ефективність в умовах воєнної економіки. За цих обставин стратегічної ваги набуває завдання щодо вироблення нової парадигми забезпечення фінансової безпеки підприємства, у якій домінуватимуть вимоги оперативності, гнучкості та здатності до швидкого реагування на динамічні зміни середовища. У контексті становлення сучасної філософії корпоративного управління значні перспективи має використання у фінансовому менеджменті інформаційних систем та цифрових технологій, які забезпечують інтеграцію даних, автоматизацію фінансових процесів, а також застосування аналітичних методів нового покоління.

Прискорена цифровізація фінансового менеджменту супроводжується усе більш активним застосуванням бізнес-структурами хмарних платформ, систем автоматизованого моніторингу, інструментів на основі штучного інтелекту. Але цифровізація поряд із позитивними наслідками, сама по собі також може стати джерелом додаткових ризиків для фінансової безпеки підприємства, пов'язаних із кіберзагрозами, посиленням залежності від зовнішніх провайдерів, втратою контролю над фінансовими даними та ін. Отже, виникає практична необхідність систематизувати наявні цифрові інструменти управління фінансовою безпекою, оцінити їхні можливості та обмеження в умовах підвищеної нестабільності, характерної для воєнного часу.

АНАЛІЗ ОСТАННІХ НАУКОВИХ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

Питання інтеграції цифрових технологій у діяльність бізнес-сектору все більш помітно представлені у наукових публікаціях вітчизняних і зарубіжних вчених. Вони відображені у працях таких науковців, як О. Барановський, А. Берл, І. Бланк, З. Варналій, О. Вільямсон, М. Дженсен, А. Єпіфанов, О. Ареф'єва та інші. Серед останніх публікацій з цієї тематики доцільно відзначити праці: Н. Демчишака, Р. Шевчука і К. Гоменюк, які зз-

начають, що в умовах переходу до вартісно-орієнтованого управління фінансами цифрові інструменти дають можливість формувати більш гнучку фінансову стратегію і автоматизувати управління ризиками підприємства [1]; О. Захаркіна, А. Бойка та Л. Сокол, які обгрунтовують, що в сучасній бізнес-екосистемі фінансова стійкість підприємств нерозривно пов'язана з ефективним використанням цифрових інновацій, а підприємства з вищим рівнем цифрової зрілості демонструють більшу здатність протистояти надзвичайним обставинам [2]; А. Мехеда та З. Варналія, які акцентують увагу на необхідності адаптації механізму фінансової безпеки підприємства до умов цифрового середовища через визначення ключових рис цифрової економіки, її позитивних і негативних аспектів для підприємницьких структур [6]. Г. Коптєва при дослідженні ролі цифрових технологій та інструментів у забезпеченні фінансової безпеки бізнес-процесів у контексті порівняння світових та українських практик доводить, що цифровізація фінансової безпеки в Україні є не тільки реакцією на кризові виклики, а й важливим елементом інтеграції у європейський цифровий простір [4]. П. Нікіфоров та О. Марусяк звертають увагу на необхідності стратегічного, комплексного підходу до впровадження цифрових інструментів в управління фінансовою безпекою підприємства, на особливій ролі людського чинника, цифрових компетенцій персоналу та морально-етичного виміру цифровізації фінансового управління [8]. Попри зростання уваги до інтеграції цифрових технологій в управління бізнес-процесами та, зокрема, фінансовою безпекою підприємства, підходи до систематизації таких інструментів поки не вироблені, як залишається відкритим питання про бар'єри їхнього впровадження в Україні.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ (ПОСТАНОВКА ЗАВДАННЯ)

Мета статті полягає у систематизації та порівняльному аналізі цифрових інструментів управління фінансовою безпекою підприємства, ідентифікації бар'єрів їхнього впровадження в умовах підвищеної нестабільності, зумовленої воєнним станом в Україні.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

В умовах цифровізації економіки формування ефективної системи фінансового менеджменту суб'єкта господарювання нерозривно пов'язане із застосування інформаційних систем. Постійне зростання обсягів даних та ускладнення бізнес-процесів визначають необхідність переходу в управлінні фінансами до інтегрованих, технологічно підтриманих рішень. До позитивних наслідків інтеграції інформаційних систем у систему фінансового управління на підприємстві належать:

— підвищення оперативності й точності збору, опрацювання й аналізу фінансової інформації, яка формує інформаційне підгрунтя для вироблення більш виважених управлінських рішень. Автоматизація облікових, аналітичних та звітних процедур знижує ризик людських помилок, прискорює формування фінансової звітності й підвищує її достовірність, що важливо для забезпечення високого динамізму управління та його адаптації до мінливих реалій. Крім цього, інформаційні системи вирішують проблему фрагментації фінансових даних, що є критичною для крупних бізнес-структур. Вони забезпечують інтеграцію ізольованих інформаційних масивів в єдине інформаційне середовище, у якому фінансові показники стають відображенням усіх бізнес-процесів;

— підвищення якості фінансового планування і прогнозування показників діяльності підприємства. Зокрема, впровадження на підприємствах ERP, BI та інших інформаційних систем забезпечує можливості моделювання показників та сценаріїв розвитку, оцінювання фінансових ризиків та прогнозування наслідків управлінських рішень. Це позитивно впливає на обгрунтованість показників фінансового плану, інвестиційних стратегій, сприяє раціоналізації політики управління витратами;

— підвищення прозорості фінансової діяльності підприємства, зниження ризику фінансових порушень та помилок у фінансовій звітності. Функціонал інтегрованих інформаційних систем інтегрує фінансові дані в режимі, близькому до реального часу, щоб можна було виявляти відхилення й загрози фінансовій стабільності на ранніх стадіях їхнього виникнення, а отже розробляти засоби реагування на них;

— розширення аналітичних можливостей в управлінні фінансами на рівні підприємства, що за високого рівня турбулентності розвитку набуває особливого значення. Використання технологій бізнес-аналітики (BI), штучного інтелекту й data-аналізу змінює акценти з обліку на інтерпретацію фінансових даних, що відкриває перспективи для причинно-наслідкового аналізу, а також сценарного моделювання та оцінювання альтернативних управлінських рішень.

Головна мета інтеграції інформаційних систем у фінансовий менеджмент підприємства полягає у підвищенні ефективності управління його фінансовими ресурсами шляхом автоматизації обробки фінансових даних, забезпечення своєчасного доступу до достовірної інформації та підтримки процесу прийняття управлінських рішень. Інформаційні системи забезпечують об'єднання різних фінансових процесів (бюджетування, управління доходами і витратами, аналіз фінансових результатів, управління грошовими потоками) у єдине інформаційне середовище, що підвищує прозорість фінансових операцій, покращує контроль за використанням ресурсів, зменшує ризики помилок і забезпечує аналітичну підтримку стратегічного та оперативного управління фінансами підприємства.

Ефективне провадження інформаційних систем у фінансовий менеджмент підприємства має базуватися на певних принципах: достовірності інформації, який передбачає використання точних та перевірених даних для прийняття фінансових рішень; своєчасності, який означає оперативне оновлення фінансової інформації та швидкий доступ до неї користувачів; інтегрованості як об'єднання різних інформаційних потоків у межах єдиної інформаційної системи задля узгодженості фінансових, виробничих та управлінських даних; безперервності, який визначає необхідність постійного функціонування інформаційної системи та регулярного оновлення інформаційних ресурсів; безпеки фінансової інформації та її захисту від несанкціонованого

Copyright © The Author(s). This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

доступу, втрати чи спотворення; адаптивності, тобто здатності інформаційної системи пристосовуватися до змін у внутрішньому та зовнішньому середовищі організації.

Позитивний потенціал інформаційних систем у фінансовому менеджменті реалізується за умови свідомого вибору інструментів відповідно до конкретних загроз та операційного контексту діяльності підприємства. Особливої гостроти ця теза набуває в умовах воєнного періоду, позначеного якісними змінами у фінансових ризиках вітчизняного бізнесу, посиленням вимог до оперативності, стійкості та захищеності фінансових процесів. Інтеграція інформаційних систем в управління фінансовою безпекою передбачає використання широкого спектру інструментів, які відрізняються функціональним призначенням, архітектурою, вартістю впровадження та рівнем складності. Відповідно до функціонального підходу, ці інструменти доцільно розмежувати на такі групи: для моніторингу фінансового стану; аналітики та прогнозування; автоматизації фінансових процесів; кібербезпеки та захисту даних. Кожна група цифрових інструментів вирішує специфічні завдання, проте в комплексі вони формують цілісну цифрову екосистему управління фінансовою безпекою підприємства (рис. 1).

До базових функцій управління фінансовою безпекою підприємства належить моніторинг фінансового стану, призначений забезпечити безперервне відстеження ключових фінансових показників, своєчасне виявлення відхилень від планових значень та сигналізування про потенційні загрози. Враховуючи високий рівень нестабільності доходів, непередбачуваність витрат та ризики знищення активів, які супроводжують воєнний період, оперативне реагування на ці виклики вимагає актуальних даних у режимі реального часу. Для вирішення цього завдання призначені такі різновиди цифрових продуктів моніторингу:

— ERP-системи (англ. Enterprise Resource Planning — планування ресурсів підприємства), тобто інтегровані платформи, які об'єднують фінансовий облік, управління запасами, розрахунки з контрагентами, бюджетування та звітність у єдине інформаційне середовище. З позицій управління фінансовою безпекою ERP-системи забезпечують консолідоване уявлення про фінансовий стан підприємства, мінімізують ризик помилок унаслідок ручного введення даних та створюють аудиторський слід усіх операцій. Слід зазначити, що ERP-системи є наскрізним інструментом, який охоплює функції одразу кількох груп, однак у даній класифікації віднесений до групи моніторингу як тієї сфери, де їхня роль є

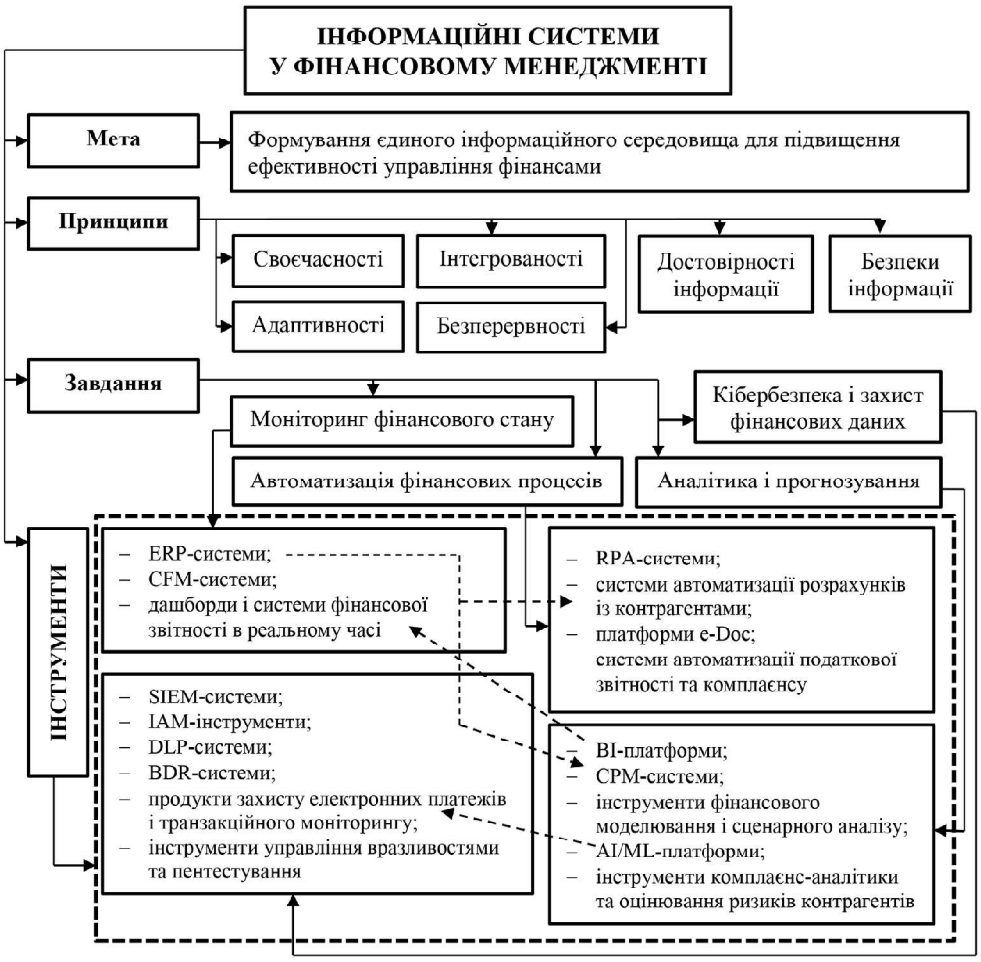

Рис. 1. Концептуальні основи застосування інформаційних систем у фінансовому менеджменті підприємства

Примітки: пунктирні стрілки вказують на перетинання функціоналу цифрових продуктів.
Джерело: побудовано авторами самостійно.

домінуючою [9]. Широке представлення в Україні отримали ERP-платформи Microsoft Dynamics 365 Finance та SAP S/4HANA, які відзначаються високим рівнем функціональності щодо фінансового контролінгу, управління ризиками та консолідованої звітності для холдингових структур. ERP-платформа Microsoft Dynamics 365 Finance має вбудовані інструменти моніторингу ключових показників ефективності (KPI), підтримує інтеграцію з Power BI для побудови аналітичних дашбордів, а її хмарна архітектура важлива для збереження даних в умовах воєнного часу та ризиків фізичного знищення офісної інфраструктури підприємства [7];

— CFM-системи (англ. Cash Flow Management Systems), або спеціалізовані рішення для планування, відстеження та оптимізації руху грошових коштів. На відміну від ERP-систем, CFM-системи фокусуються виключно на ліквідності та платоспроможності підприємства, що актуально для бізнесів із нерівномірними чи непрогнозованими грошовими потоками. Для великих підприємств зі складною структурою рахунків, банківських відносин та валютних операцій поширені TMS-платформи (управління платіжними операціями і ліквідністю). Вони забезпечують цілісне управління платіжними операціями, розрахунками з банками, валютними конвертаціями та управлінням ліквідністю підприємства. Застосування цих інструментів сприяє уникненню касових розривів, затримок платежів і неефективного розподілу коштів між рахунками. Водночас, ці цифрові інструменти відкривають перспективи розробки сценарних прогнозів ліквідності підприємства, а також автоматичного генерування попереджень про негативні зміни. В Україні серед CFM-систем широке застосування отримали платформи Xero, Finmap та інші, які надають можливості для моніторингу грошових потоків, автоматичної звірки банківських виписок, контролю заборгованості та касових розривів тощо. Вони інтегровані з низкою вітчизняних банківських установ, що дає можливість отримувати актуальні дані про рух коштів у режимі реального часу;

— дашборди і системи фінансової звітності в реальному часі, тобто цифрові інструменти візуалізації фінансових даних, які агрегують інформацію з різних джерел та представляють її у зручному форматі для прийняття управлінських рішень. Ключовою перевагою цих продуктів є високий рівень оперативності, коли менеджмент підприємства отримує реальне уявлення про фінансовий стан без необхідності очікування на підготовку фінансової звітності. Поширеним в Україні інструментом візуалізації даних є Looker Studio від Google, який надає можливості створення інтерактивних фінансових дашбордів на основі даних з різних джерел, але не має спеціалізованих фінансових аналітичних модулів.

Поряд з моніторингом фінансового стану, важливим аспектом управління фінансовою безпекою підприємства є аналітика та прогнозування показників, адже більшість загроз не виникають раптово, а формуються поступово і можуть бути виявлені на ранній стадії за допомогою аналітичних інструментів. Попри те, що в умовах воєнного часу посилюється невизначеність перспектив зміни ситуації, а отже виникають сумніви щодо доцільності прогнозування як такого, у бізнес-середовищі воно навпаки є більш затребуваним. Оскільки підприємства змушені працювати у воєнних реаліях, коли традиційні моделі, побудовані на історичних даних мирного часу, втрачають прогностичну силу, зростає інтерес до використання цифрових інструментів сценарного аналізу, стрес-тестування, адаптивного прогнозування та ін. Ця група цифрових інструментів управління фінансовою безпекою охоплює такі їх різновиди:

— BI-платформи — програмні рішення для акумуляції, обробки, аналізу та візуалізації великих масивів фінансових і операційних даних, які, на відміну від дашбордів, забезпечують глибокий аналіз причинно-наслідкових зв'язків між ними, виявлення аномалій, побудову аналітичних кубів та багатовимірний аналіз показників. З позицій управління фінансовою безпекою бізнесу BI-платформи спрямовані на виявлення нетипових відхилень у фінансових операціях, які можуть свідчити про помилки, зовнішні маніпуляції чи шахрайство [5]. Серед BI-платформ широке застосування в Україні отримали Microsoft Power BI (входить до екосистеми Microsoft 365), Tableau (поширені у крупному бізнесі та фінансовому секторі) та інші. Вони надають можливості щодо візуалізації та глибокого аналізу даних, побудови інтерактивних звітів та дашбордів, а також передбачають функції прогнозування на основі вбудованих алгоритмів;

— CPM-системи (управління ефективністю діяльності) — інтегровані платформи, функціонал яких поєднує бюджетування, прогнозування, фінансову консолідацію та стратегічне планування. У контексті забезпечення фінансової безпеки суб'єкта господарювання CPM-системи забезпечують безперервний цикл планування-виконання-аналізу, що дає можливість оперативно корегувати фінансову стратегію підприємства відповідно до змін у зовнішніх умовах його функціонування. В умовах воєнної невизначеності ця функція є особливо цінною для побудови та порівняння альтернативних сценаріїв розвитку підприємства;

— інструменти фінансового моделювання і сценарного аналізу, призначені для оцінювання впливу різних сценаріїв розвитку подій на фінансовий стан підприємства через побудову фінансових моделей (дисконтування грошових потоків, аналіз чутливості, симуляції Монте-Карло, стрес-тестування). Такі інструменти призначені для оцінювання фінансової стійкості підприємства до внутрішніх та зовнішніх шоків (втрати ключових контрагентів, різкого падіння реалізації, зростання витрат та ін.). На практиці ця функція підтримується як спеціалізовані модулі CPM-системи, а також розширені можливості Microsoft Excel у поєднанні з надбудовами для фінансового моделювання;

— AI/ML-платформи — клас цифрових інструментів, які використовують для виявлення прихованих закономірностей у фінансових даних, автоматичного прогнозування показників та ідентифікації аномалій. Перевагою AI/ML-платформ є їхня здатність обробляти великі масиви неструктурованих даних, а також адаптуватись без перепрограмування до змін середовища.

ISSN 2306-6814
Copyright © The Author(s). This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

У контексті управління фінансовою безпекою AI/ML-інструменти застосовують насамперед для виявлення шахрайських транзакцій, оцінювання кредитних ризиків контрагентів та прогнозування касових розривів. В Україні доступними рішеннями цього класу є хмарні платформи Microsoft Azure Machine Learning та Google Vertex AI, а також бібліотека Prophet з відкритим кодом для стратегічного прогнозування фінансових часових рядів;

— інструменти комплаєнс-аналітики та оцінювання ризиків контрагентів, які призначені для перевірки фінансового стану та надійності партнерів на основі даних відкритих реєстрів. Ці інструменти набувають особливої ваги в умовах воєнного часу, коли зростає кількість фіктивних структур, схемних операцій та контрагентів, які можуть мати зв'язки з росією. В Україні серед цих інструментів верифікації представлені найперше платформи YouControl, CFIN, які агрегують дані з реєстрів фіскальних органів, органів юстиції, судових реєстрів, санкційних списків та інших джерел. Завдяки цьому, у підприємств є можливість перевірки власних контрагентів на предмет дотримання ними санкційного законодавства, що важливо для управління репутаційними ризиками.

Поряд із аналітикою та прогнозуванням, забезпечення фінансової безпеки підприємства залежить від автоматизації фінансових процесів, яка покликана усунути ручну працю з рутинних операцій та мінімізувати операційні ризики. На практиці причини фінансових втрат зазвичай пов'язані із помилками у рутинних процесах — через некоректне введення даних, затримки у проведенні платежів, дублювання операцій чи порушення вимог податкового законодавства. У цьому контексті автоматизація виступає інструментом підвищення надійності фінансових процесів і, відповідно, стійкості підприємства до внутрішніх загроз.

В умовах воєнного часу значення таких інструментів суттєво посилюється через скорочення персоналу, вимушену релокація підприємств, перехід до онлайн-формату роботи тощо. Це створює додаткове навантаження на фінансові підрозділи підприємства, яке компенсувати без технологічної підтримки досить складно. Відтак автоматизація забезпечує безперервність фінансових операцій навіть за умов обмежених кадрових ресурсів, що прямо впливає на здатність підприємства підтримувати ліквідність і виконувати свої зобов'язання.

До цієї групи цифрових інструментів управління фінансовою безпекою підприємства доцільно зараховувати:

— системи автоматизації розрахунків із контрагентами, спрямовані на впорядкування грошових потоків підприємства. Вони забезпечують автоматичне розпізнавання рахунків-фактур, їхнє погодження, контроль строків проведення платежів, управління дебіторською заборгованістю тощо. У ситуації погіршення платіжної дисципліни такі системи виконують функцію захисту ліквідності підприємства, дають йому можливість оперативно реагувати на прострочення та зменшувати обсяг "заморожених" коштів;

— платформи електронного документообігу, призначені для управління фінансовою документацією підприємства в електронному форматі з підтримкою кваліфікованого електронного підпису (КЕП). Вони не лише підвищують швидкість обробки документів, але й знижують ризики їхньої втрати, підробки або несанкціонованого доступу. Враховуючи зумовлену війною територіальну розосередженість персоналу, що характерно для значної частини підприємств, електронний документообіг фактично стає основою функціонування фінансової системи компанії. Фактичним стандартом серед цифрових інструментів цього виду в Україні залишається M.E.Doc, однак вона має певні прогалини щодо захисту від кібервірусів;

— системи автоматизації податкової звітності та комплаєнсу забезпечують відповідність діяльності підприємства вимогам чинного законодавства шляхом автоматичного формування, перевірки і подання звітності, а також оперативного врахування змін регуляторного середовища. З огляду на нестабільність норм податкового законодавства, особливо у період воєнного стану, такі системи дозволяють мінімізувати ризики штрафів і фінансових санкцій. У цій ніші варто відзначити платформи Checkbox (автоматизація фіскальних операцій та робота з ПРРО, інтегрується з обліковими системами та e-commerce платформами) та Corezoid (поширена в установах фінансового сектору);

— системи роботизованої автоматизації процесів (RPA), які забезпечують відтворення типових дій користувача (копіювання даних між системами, звірка документів, формування звітів, заповнення форм та ін.) у різних інформаційних системах без необхідності їх глибокої інтеграції. На відміну від спеціалізованих систем документообігу та податкової звітності, RPA не потребує глибокої інтеграції і може автоматизувати процеси навіть у застарілих системах, виконуючи роль сполучної ланки між різними програмними рішеннями. Додатковою перевагою RPA-систем є формування так званого audit trail (аудиторського сліду), що передбачає автоматичну фіксацію всіх виконаних дій, змін даних і послідовності операцій, що підвищує прозорість фінансових процесів, полегшує внутрішній контроль і створює передумови для своєчасного виявлення помилок і зловживань. Для фінансової безпеки ключовим ефектом є зниження ризику людських помилок та прискорення обробки фінансової інформації. В Україні широко представлені такі платформи RPA, як UiPath (популярна у суб'єктів малого бізнесу через наявність безкоштовної версії) та Blue Prism, яка вирізняється вищим рівнем безпеки, але через високу вартість і складність впровадження доступна переважно крупним компаніям.

Кібербезпека є невід'ємною складовою фінансової безпеки підприємства, однак довгий час розглядалась як суто технічна сфера відповідальності IT-підрозділу, що не мала прямого відношення до фінансового менеджменту. Сучасна практика спростовує цей підхід, адже кіберінциденти мають прямі фінансові наслідки у вигляді втрати коштів, блокування фінансових операцій, витоку конфіденційних даних, репутаційних збитків та

регуляторних санкцій. В умовах масштабного вторгнення Україна стала одним із найбільш інтенсивних театрів кібервійни у світі — російські державні та проксі-структури здійснюють систематичні атаки на критичну інфраструктуру, фінансовий сектор і приватний бізнес. Відтак інструменти кібербезпеки доцільно розглядати як повноправну складову управління фінансовою безпекою підприємства, а їхні функціональні різновиди охоплюють:

— SIEM-системи управління інформацією і подіями безпеки (англ. Security Information and Event Management) — платформи для централізованого збору, кореляції та аналізу журналів подій з усіх інформаційних систем підприємства в режимі реального часу. З погляду управління фінансовою безпекою SIEM-системи підвищують ймовірність раннього виявлення підозрілих випадків у фінансових операціях (незвичних платежів у нічний час, доступу до фінансових систем з нетипових локацій або масового вивантаження фінансових даних) до їх реалізації у фінансових втратах. В Україні серед цих цифрових інструментів поширені IBM QRadar та Splunk, представлені через партнерську мережу у великому бізнесі та банківському секторі;

— IAM-інструменти захисту ідентичності та управління доступом (англ. Identity and Access Management) — рішення для контролю доступу до фінансових систем на основі принципу мінімальних привілеїв, коли кожен користувач має доступ лише до тих фінансових даних та операцій, які необхідні для виконання його функціональних обов'язків, а кожен сеанс роботи із фінансовою системою підприємства підтверджується багатофакторною автентифікацією. В умовах переходу підприємств на дистанційний режим діяльності, коли працівники входять до корпоративних систем через незахищені мережі, IAM-інструменти перетворились на базовий, але критично важливий рівень захисту фінансових систем. В Україні цей клас цифрових інструментів представлений насамперед рішеннями Microsoft Azure Active Directory (Entra ID), широко розповсюдженого в екосистемі Microsoft 365;

— DLP-системи запобігання витоку даних (англ. Data Loss Prevention) — інструменти контролю переміщення конфіденційних даних внутрі підприємства та за його межі. У контексті фінансової безпеки DLP-системи захищають від витоку фінансової звітності, банківських реквізитів, даних про контрагентів та комерційної таємниці, у тому числі від інсайдерської загрози. Зокрема, Platforma Varonis, представлена в Україні через партнерську мережу, спеціалізується на захисті даних та виявленні внутрішніх загроз. Вона забезпечує картування фінансових файлів і баз даних, виявляє надмірні права доступу та моніторить поведінку користувачів;

— BDR-системи резервного копіювання та відновлення даних (англ. Backup and Disaster Recovery) — цифрові інструменти для забезпечення безперервності фінансових операцій у разі кіберінциденту або фізичного знищення обладнання. В умовах воєнного часу, коли руйнування офісної інфраструктури є реальним ризиком для підприємств у зонах активних бойових дій, резервне копіювання з географічно розподіленим зберіганням даних перетворюється на стратегічний елемент фінансової безпеки. Наприклад, платформа Veeam Backup & Replication підтримує резервне копіювання до хмарних сховищ Microsoft Azure та Amazon AWS, що забезпечує зберігання фінансових даних компаній за межами України та зменшує ризик їхньої незворотної втрати;

— продукти захисту електронних платежів і транзакційного моніторингу, які призначені для виявлення шахрайських транзакцій та несанкціонованих платежів у реальному часі. Використовують алгоритми машинного навчання для аналізу зразків платіжної поведінки та автоматичного блокування підозрілих операцій, тому актуальні для підприємств із великим обсягом транзакцій або розгалуженою мережею авторизованих підписантів платіжних доручень. Для виконання цих функцій використовують уже згадувані AI/ML-платформи, які ефективні у питанні оперативного виявлення загроз у режимі реального часу;

— інструменти управління вразливостями та пентестування, призначені для систематичного виявлення вразливостей в IT-інфраструктурі підприємства (зокрема, сканери вразливостей, платформи для організації програм bug bounty, інструменти для проведення контрольованих тестів на проникнення та ін.). Для фінансової безпеки ці інструменти забезпечують проактивний підхід до захисту фінансової інформації, виявлення та усунення слабких місць в IT-інфраструктурі до їх експлуатації.

Систематизація цифрових інструментів управління фінансовою безпекою підприємства потребує логічного продовження у їхньому порівнянні за низкою критеріїв. Сучасний ринок програмного забезпечення пропонує широкий спектр цифрових продуктів, що ускладнює процес обгрунтованого вибору рішень для підприємств, які не мають можливості проводити власне масштабне тестування і орієнтуються переважно на ціновий чинник. Водночас, в умовах воєнного стану формується принципово відмінний профіль фінансових ризиків порівняно зі звичайним режимом господарювання, що змінює вимоги до інструментального забезпечення фінансового менеджменту. Зважаючи на контекст дослідження, для порівняння цифрових інструментів у якості критеріїв порівняння обрано характер впливу на фінансову безпеку підприємства, складність інтеграції та тривалість ефекту від впровадження. Рівень впливу на фінансову безпеку (прямий або опосередкований) розмежовує інструменти, які безпосередньо захищають фінансові потоки і активи підприємства, від тих, котрі підвищують якість управлінських рішень або операційну надійність, тим самим формуючи підгрунтя для підвищення фінансової стійкості. Критично важливим критерієм в умовах скорочення кадрового потенціалу фінансових підрозділів підприємств у воєнний час виступає також складність інтеграції цифрового інструменту. Щодо горизонту ефекту (короткостроковий чи довгостроковий), то він відображає, наскільки швидко підприємство отримує практичну віддачу від впровадженого програмного рішення, що важливо для з огляду на необхідність опе-

Copyright © The Author(s). This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

Таблиця 1. Порівняльний аналіз цифрових інструментів управління фінансовою безпекою підприємства

Інструмент	Вплив на фінансову безпеку	Вартість впровадження	Складність інтеграції	Ефект впровадження
Група 1. Моніторинг фінансового стану				
ERP-системи (універсальні)	Прямий	Висока	Висока	Д
CFM-системи/TMS	Прямий	Низька – середня	Низька	К
Дашборди реального часу	Опос.	Низька	Низька	К
Група 2. Аналітика та прогнозування				
BI-платформи	Опос.	Середня	Середня	Д
CPM-системи	Прямий	Висока	Висока	Д
Інструменти сценарного аналізу	Опос.	Низька – середня	Середня	К
AI/ML-платформи	Прямий	Висока	Висока	Д
Комплаєнс-аналітика	Прямий	Низька – середня	Низька	К
Група 3. Автоматизація фінансових процесів				
RPA-системи	Опос.	Середня –висока	Середня	К
Системи автоматизації розрахунків	Прямий	Середня	Середня	К
Електронний документообіг	Опос.	Низька – середня	Низька	К
Автоматизація податкової звітності	Прямий	Низька – середня	Низька	К
Група 4. Кібербезпека та захист даних				
SIEM-системи	Прямий	Висока	Висока	Д
IAM-інструменти	Прямий	Низька – середня	Низька –середня	К
DLP-системи	Опос.	Висока	Висока	Д
BDR-системи	Прямий	Середня	Середня	Д
Захист платежів / транзакційний моніторинг	Прямий	Середня–висока	Середня	К
Інструменти управління вразливостями	Опос.	Середня	Висока	Д

Примітки: Опос. — опосередкований; К — короткостроковий; Д — довгостроковий.
Джерело: побудовано автором самостійно.

ративного реагування на динамічні зміни зовнішнього середовища (табл. 1).

Незважаючи на переваги задіяння цифрових інструментів в управлінні фінансовою безпекою підприємства, їхнє впровадження в Україні наштовхується на низку бар'єрів, які набувають особливої гостроти в умовах воєнного часу:

— висока вартість впровадження повнофункціональних рішень. Зокрема, ERP-системи класу Microsoft Dynamics 365 Finance і SAP S/4HANA потребують значних початкових інвестицій, не враховуючи витрат на навчання персоналу, адаптацію під специфіку підприємства і подальшу технічну підтримку. Високий рівень витрат характерний для CPM-систем, платформ на основі ШІ та SIEM-рішень. В умовах невизначеності воєнного стану значні інвестиції у цифрові інструменти для значної частини підприємств, особливо у сегменті малого та середнього бізнесу недоступні. Проблема вартості набуває додаткового виміру у зв'язку з необхідністю оплати ліцензій та, відповідно, валютним ризиком;

— висока складність інтеграції низки цифрових інструментів з наявною IT-інфраструктурою підприємств. Успішне впровадження ERP, CPM і SIEM-систем неможливе без кваліфікованих фахівців з інформаційних технологій — системних адміністраторів, бізнес-аналітиків і спеціалістів із кібербезпеки. В умовах війни доступність таких кадрів знизилася через мобілізацію, міграцію та зростання попиту на IT-спеціалістів із боку оборонного сектору та міжнародних компаній. Проблеми інтеграції посилює також застарілість частини IT-інфраструктури вітчизняних підприємств та відсутність стандартизованих API для взаємодії між різними системами;

— дефіцит цифрових компетенцій у менеджменті та персоналу фінансових служб підприємств, оскільки ефективне використання складних аналітичних платформ, AI/ML-рішень чи SIEM-систем потребує відповідних знань і навичок. За оцінками О. Казак та Р. Дідушка [3], повноцінне використання цифрових інструментів фінансового менеджменту стримується низьким рівнем цифрової зрілості вітчизняного бізнесу, а 60% малих і середніх підприємств перебувають на базовому рівні цифровізації;

— ризики залежності від зовнішніх провайдерів і можливого припинення підтримки програмних продуктів. Частина глобальних постачальників IT-рішень після початку повномасштабного вторгнення прийняла рішення про вихід або обмеження діяльності в Україні, окремі хмарні платформи ввели додаткові обмеження щодо зберігання даних або транзакційних операцій. Залежність від хмарних рішень зовнішніх провайдерів також підвищує вразливість у разі збоїв інтернет-з'єднання через ракетні удари по енергетичній та телекомунікаційній інфраструктурі.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Результати дослідження продемонстрували, що в умовах воєнної нестабільності та зростання фінансових ризиків цифрові інструменти набувають визначального значення у формуванні ефективної системи управління фінансовою безпекою підприємства. Систематизація таких інструментів за функціональними групами (моніторинг фінансового стану, аналітика та прогнозування, автоматизація фінансових процесів, кібербезпека і захист даних) засвідчила, що кожна з них виконує специфічні завдання, проте лише їх інтегроване застосування забезпечує досягнення синергетичного ефекту. У цьому контексті фінансова безпека підприємства формується як результат побудови цілісної цифрової екосистеми, яка об'єднує доповнювані цифрові інструменти і здатна до безперервного функціонування та адаптації до змін зовнішнього середовища.

Порівняльний аналіз цифрових інструментів за критеріями впливу на рівень фінансової безпеки підприємства, складності інтеграції та тривалості ефекту від їхнього впровадження засвідчив, що різні групи інструментів мають

неоднакову роль у забезпеченні фінансової стійкості підприємства. Зокрема, інструменти моніторингу та кібербезпеки забезпечують безпосередній вплив на захист фінансових потоків і активів, тоді як аналітичні платформи та засоби автоматизації формують опосередкований ефект через підвищення якості управлінських рішень і зниження операційних ризиків. Впровадження складних цифрових рішень супроводжується значними організаційними та фінансовими витратами, а також потребує відповідного рівня цифрової зрілості підприємства, що обмежує їхню доступність для значної частини вітчизняного бізнесу.

Процес цифровізації управління фінансовою безпекою підприємств в Україні стримується низкою системних бар'єрів, серед яких визначальними є висока вартість впровадження комплексних рішень, складність їх інтеграції з наявною IT-інфраструктурою, дефіцит цифрових компетенцій персоналу, зростання залежності від зовнішніх провайдерів. Це зумовлює необхідність формування зваженого підходу до вибору цифрових інструментів з урахуванням масштабу діяльності підприємства, структури фінансових ризиків і ресурсних обмежень. Перспективи подальших досліджень пов'язані з розробленням методичних підходів до оцінювання ефективності цифровізації фінансової безпеки підприємства та формуванням адаптивних стратегій впровадження цифрових рішень в умовах воєнної економіки.

Література:

1. Демчишак Н., Шевчук Р., Гоменюк К. Цифрові технології та інструменти забезпечення фінансової безпеки підприємств у контексті вартісно-орієнтованого управління. Економіка та суспільство. 2025. № 73. URL: https://doi.org/10.32782/2524-0072/2025-73-53

2. Захаркін О., Бойко А., Сокол Л. Цифрові технології та інструменти забезпечення фінансової безпеки бізнесу. Проблеми сучасних трансформацій. Серія: економіка та управління. 2023. № 10. URL: https://doi.org/10.54929/2786-5738-2023-10-08-02

3. Казак О., Дідушок Р. Цифрова трансформація малого та середнього бізнесу України в умовах воєнного стану: виклики, можливості та стратегії адаптації. Європейський науковий журнал Економічних та Фінансових інновацій. 2025. № 3 (17). С. 558—567. URL: https://doi.org/10.32750/2025-0348

4. Коптєва Г. Цифровізація фінансової безпеки бізнес-процесів: світові та українські практики. Вісник Національного технічного університету "Харківський політехнічний інститут" (економічні науки). 2025. № 5. С. 3—8. URL: https://es.khpi.edu.ua/article/view/343129

5. Лелюк С. Цифрові продукти та інструменти Business Intelligence в бізнес-процесах фінансового менеджменту. Сталий розвиток економіки. 2025. № 3 (54). С. 461—468. URL: https://doi.org/10.32782/2308-1988/2025-54-69

6. Мехед А., Варналій З. Фінансова безпека підприємств в умовах цифрової економіки. Вісник університету банківської справи. 2021. № 3 (42). С. 55—61. URL: https://ser.net.ua/index.php/SER/article/view/440

7. Мікулицька Г. ERP після заборонених систем: 4 міфи, які стримують український бізнес. URL: https://speka.ua/technologies/erp-pislya-zaboronenix-sistem-4-mifi-yaki-strimuyut-ukrayinskii-biznes-vm4k33

8. Нікіфоров П., Марусяк О. Роль цифрових технологій у зміцненні фінансової безпеки підприємств: можливості, виклики та стратегічні підходи впровадження. Ефективна економіка. 2025. № 5. URL: https://nayka.com.ua/index.php/ee/article/view/6482

9. Що таке ERP-система управління підприємством та де її краще розмістити? URL: https://www.sim-networks.com/ukr/blog/enterprise-resource-planning-systems-and-cloud-infrastructure

References:

1. Demchyshak, N., Shevchuk, R. and Homeniuk, K. (2025), "Digital technologies and tools for ensuring financial security of enterprises in the context of value-oriented management", Ekonomika ta suspilstvo, [Online], vol. 73. https://doi.org/10.32782/2524-0072/2025-73-53.

2. Zakharkin, O., Boiko, A. and Sokol, L. (2023), "Digital technologies and tools for ensuring financial security of business", Problemy suchasnykh transformatsii. Seriia: ekonomika ta upravlinnia, vol. 10. https://doi.org/10.54929/2786-5738-2023-10-08-02.

3. Kazak, O. and Didushok, R. (2025), "Digital transformation of small and medium-sized enterprises in Ukraine under martial law: challenges, opportunities and adaptation strategies", Yevropeiskyi naukovyi zhurnal ekonomichnykh ta finansovykh innovatsii, [Online], vol. 3 (17), pp. 558—567. https://doi.org/10.32750/2025-0348.

4. Koptieva, H. (2025), "Digitalisation of financial security of business processes: global and Ukrainian practices", Visnyk Natsionalnoho tekhnichnoho universytetu "Kharkivskyi politekhnichnyi instytut" (ekonomichni nauky), vol. 5, pp. 3—8, available at: https://es.khpi.edu.ua/article/view/343129 (Accessed 17 April 2026).

5. Leliuk, S. (2025), "Digital products and Business Intelligence tools in financial management business processes", Stalyi rozvytok ekonomiky, vol. 3 (54), pp. 461—468. https://doi.org/10.32782/2308-1988/2025-54-69.

6. Mekhed, A. and Varnalii, Z. (2021), "Financial security of enterprises in the digital economy", Visnyk universytetu bankivskoi spravy, vol. 3 (42), pp. 55—61, available at: https://ser.net.ua/index.php/SER/article/view/440 (Accessed 17 April 2026).

7. Mikulytska, H. (2025), "ERP after banned systems: 4 myths that restrain Ukrainian business", available at: https://speka.ua/technologies/erp-pislya-zaboronenix-sistem-4-mifi-yaki-strimuyut-ukrayinskii-biznes-vm4k33 (Accessed 17 April 2026).

8. Nikiforov, P. and Marusiak, O. (2025), "The role of digital technologies in strengthening enterprise financial security: opportunities, challenges and strategic approaches to implementation", Efektyvna ekonomika, [Online], vol. 5, available at: https://nayka.com.ua/index.php/ee/article/view/6482 (Accessed 17 April 2026).

9. Sim-Networks (2021), "What is an ERP system and where is it better to deploy it?", available at: https://www.sim-networks.com/ukr/blog/enterprise-resource-planning-systems-and-cloud-infrastructure (Accessed 17 April 2026).

Отримано редакцією журналу / Received: 17.04.26
Прорецензовано / Revised: 28.04.26
Дата публікації / Published: 12.05.26

Copyright © The Author(s). This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).