

теоретико-методологічне підґрунтя як базису розвитку фінансових відносин на кожному конкретному етапі функціонування національної економіки, здатних забезпечити відповідний рівень фінансової безпеки. Зокрема, заслуговує на особливу увагу позиція, згідно з якою стверджується, що «...державний борг повинен перебувати на такому рівні, що в разі раптового зростання потреби у видатках нові запозичення сприймалися як позитивний сигнал»¹⁹. В умовах сучасного критичного стану фінансової безпеки питання боргової політики набувають особливого значення. Відповіді на них є досить своєчасними для врахування в реальній практиці, а тому стануть предметом більш детального оцінювання в наступних частинах цієї монографії.

1.2. Фінансова безпека організацій: якісні зрушення та нові орієнтири на основі цифрових технологій

*(О. Є. Гудзь, доктор економічних наук, професор,
Державний податковий університет)*

З огляду на глибокі трансформації, які переживає сучасне бізнес-середовище, актуальність і цінність розгляду якісних зрушень та нових орієнтирів фінансової безпеки організацій на основі цифрових технологій є надзвичайно високою. Ключовими аргументами, що обґрунтовують таку позицію, є зростання загроз фінансовій безпеці, адже військова агресія росії, економічна турбулентність і кіберзагрози створюють нові виклики для фінансової стійкості організацій, а традиційні методи управління ризиками втрачають ефективність, що потребує переосмислення стратегій фінансової безпеки, якісних зрушень і нових орієнтирів на основі цифрових технологій.

Практично «безпека є однією із ключових передумов існування як колективу, так і окремих індивідів. Саме безпека існує первинною потребою особистості, а важливість її забезпечення проявляється на фізіологічному рівні. У разі незадоволення таких базових потреб людина опиняється за межами стабільної та ефективної участі в суспільному й економічному житті, знижуючи її продуктивність і працездатність. Загалом безпека є складною категорією, за допомогою якої

¹⁹ Козюк В. В. Оптимальний рівень боргового навантаження: глобальні макрофінансові зрушення та швидкоплинні очкування. *Фінанси України*. 2012. № 1. С. 78–92.

відображається потреба, відчуття та кінцеві результати цілеспрямованої діяльності індивіда, а також станом, у межах якого забезпечується захист життєво важливих інтересів учасників соціально-економічної системи від потенційних загроз і небезпеки, що спрямовано на нормальне функціонування різноманітних процесів»²⁰.

Фактично проблеми фінансової безпеки організацій сьогодні набули системного характеру, охоплюючи як зовнішні, так і внутрішні чинники. А «метою системи фінансової безпеки підприємств є забезпечення його стійкого і максимально ефективного функціонування, створення високого потенціалу розвитку і зростання в майбутньому»²¹, оскільки ризики не лише загрожують стабільності організацій, а й вимагають переосмислення безпекових стратегій.

Так, «початок широкомасштабної війни та введення воєнного стану призвели до виникнення реальних ризиків та загроз в управлінні фінансовою безпекою»²², оскільки «не відновившись повністю від шоку, спричиненого гібридною війною, яку розв'язала росія у 2014 р., будучи додатково ослабленою пандемією COVID-19, держава в результаті повномасштабного вторгнення росії в Україну зазнала нових викликів щодо фінансової безпеки суб'єктів підприємництва»²³. «Через широкомасштабну війну росії проти України українська економіка зазнала найбільших втрат за часів своєї незалежності. За універсальним показником – ВВП – найгіршим в економічній історії України був 1994 р., коли ВВП скоротився на 22,9 %, а інфляція становила 401 %. За даними Міністерства економіки, у 2022 р. ВВП України зменшився на 32 % при порівняно помірному індексі інфляції, який становив 30 %. Навіть з погляду статистики, це гарний результат, адже масштаби війни, руйнувань і шкоди, завданих росією, давали

²⁰ Коленда Н. В. Поняття соціально-економічної безпеки підприємства. *Економіка і суспільство*. 2016. № 7. С. 672–678, 673.

²¹ Вівчар О. І. Практичний базис системи фінансової безпеки підприємницьких структур: нові виклики та можливості. *Modeling the development of the economic systems*. 2021. № 3. С. 8–13. DOI : <https://doi.org/10.31891/mdes/2023-7-1>

²² Калюжна К. В., Басараб О. А. Забезпечення фінансової безпеки в Україні в умовах воєнного стану. *Фінансова безпека України: сучасний стан правового регулювання та перспективи розвитку* : матеріали IX Міжнародної науково-практичної конференції, м. Ірпінь, 26 жовтня 2023 року. Ірпінь : Державний податковий університет, 2023. 312, [103–106] с.

²³ Актуалітети фінансової безпеки суб'єктів підприємництва України в умовах війни та повоєнний час / Варналій З. С., Чеберяко О. В., Микитюк О. П., Бондаренко С. М. *Academy review*. 2024. № 1 (60). С. 123–140. DOI 10.32342/2074-5354-2024-1-60-9

підстави для найпесимістичних прогнозів скорочення ВВП на 50 % і більше»²⁴. А «зростання витрат на фінансування сектору безпеки та оборони, а також компенсації громадянам, постраждалим від воєнних дій, веде до значних фінансових збитків»²⁵. Підтримуємо тих науковців, які вважають, що «формування фінансової безпеки під час війни передбачає захист суб'єкта від дестабілізуючих впливів як внутрішніх, так і зовнішніх загроз, потрібних для підтримки операційної функціональності. Без нейтралізації загроз ефективне функціонування стає недосяжним, що призводить до потенційного зниження значень ключових функціональних параметрів»²⁶. Саме тому експерти передбачають зростання до 2029 року лише ринку кібербезпеки в Україні на понад 50 %, що свідчить про стратегічну важливість проблем фінансової безпеки для національної економіки та вітчизняних організацій. Наголосимо, що «забезпечення фінансової безпеки суб'єктів підприємництва – це дуже складний і багаторівневий процес, де мають бути своєчасно виявлені кожний виклик, ризик або загроза та вжиті своєчасні заходи для запобігання підвищенню рівня небезпеки, виникненню або посиленню фінансової кризи. Для цього недостатньо застосовувати традиційні методи управління, а потрібно розробити механізми забезпечення фінансової безпеки суб'єктів підприємництва, які охоплюватимуть спеціалізовані засоби та ґрунтуватимуться на відповідних принципах»²⁷.

Найвпливовішими зовнішніми загрозами для фінансової безпеки організацій вищезазначені дослідники вважають:

воєнні ризики та геополітичну нестабільність, оскільки продовження бойових дій на території України спричиняють руйнування інфраструктури, релокацію організацій, втрату активів і невизначеність у плануванні;

²⁴ Свириденко Ю. Українська економіка пережила найважчий рік за часи незалежності: як ми вистояли та що далі. URL : <https://www.epravda.com.ua/columns/2022/12/30/695585/>

²⁵ Актуалітети фінансової безпеки суб'єктів підприємництва України в умовах війни та повоєнний час / Варналій З. С., Чеберяко О. В., Микитюк О. П., Бондаренко С. М. *Academy review*. 2024. № 1 (60). С. 123–140. DOI 10.32342/2074-5354-2024-1-60-9

²⁶ Матвійчук В. І., Матушевський О. В. Формування фінансової безпеки суб'єкта господарювання в умовах воєнного стану. *Економіка і організація управління*. 2023. № 4 (52). С. 118–131. DOI 10.31558/2307-2318.2023.4.13

²⁷ Актуалітети фінансової безпеки суб'єктів підприємництва України в умовах війни та повоєнний час / Варналій З. С., Чеберяко О. В., Микитюк О. П., Бондаренко С. М. *Academy review*. 2024. № 1 (60). С. 123–140. DOI 10.32342/2074-5354-2024-1-60-9

«суттєвими загрозами є інфляційні процеси, знецінення національної валюти, нарощування зовнішньої заборгованості країни; ресурсні обмеження, стрибки цін, подорожчання паливно-енергетичних ресурсів, зростання тарифів, незахищеність прав власності, повномасштабна російсько-українська війна»²⁸;

залежність від міжнародної фінансової підтримки, адже затримки чи скорочення обсягів допомоги впливають на державні програми підтримки бізнесу, кредитування та інвестиційний клімат;

«незмінною для підприємств в Україні залишається проблеми зростання цін на сировину, матеріали та товари, що суттєво впливають на фінансову безпеку підприємств. Зокрема, збільшення цін призводить до збільшення виробничих витрат, скорочення маржі прибутку та потенційного зниження рентабельності. Крім того, проблему спричиняє навантаження на грошові потоки підприємств, погіршуючи їх здатність інвестувати, сплачувати борги та підтримувати операційну діяльність»²⁹;

глобальні економічні деформації, які впливають на коливання валютних курсів, інфляцію, зміни в ланцюгах постачання, а енергетичні кризи створюють додаткові фінансові ризики.

Потрібно констатувати, що «на сучасному етапі розвитку економіки України зростає кількість, вагомість та складність загроз фінансовій безпеці суб'єктів господарювання. Неналежна протидія деструктивним чинникам, недосконалість нормативно-правового забезпечення фінансової діяльності суб'єктів господарювання, неефективність механізму захисту прав власників зумовлюють зниження рівня фінансової безпеки підприємницьких структур. Негативний вплив цих чинників посилений наявністю корупційних схем на різних ланках державної влади. Наслідком цього є зростання рівня тінізації економіки та значне поширення масових протиправних захоплень підприємств» [³⁰, с. 123].

²⁸ Актуалітети фінансової безпеки суб'єктів підприємництва України в умовах війни та повоєнний час / Варналій З. С., Чеберяко О. В., Микитюк О. П., Бондаренко С. М. *Academy review*. 2024. № 1 (60). С. 123–140. DOI 10.32342/2074-5354-2024-1-60-9.

²⁹ Матвійчук В. І., Матушевський О. В. Формування фінансової безпеки суб'єкта господарювання в умовах воєнного стану. *Економіка і організація управління*. 2023. № 4 (52). С. 118–131. DOI 10.31558/2307-2318.2023.4.13

³⁰ Крупка М. І., Яструбецька Л. С. Фінансова безпека суб'єктів господарювання : підручник. Львів : ЛНУ імені Івана Франка, 2018. 320 с.

Найвпливовішими внутрішніми загрозами для фінансової безпеки організацій можемо виділити:

нестабільність доходів і платоспроможності, адже більшість організацій стикаються з нерівномірними грошовими потоками, зниженням попиту та труднощами з обслуговуванням боргів;

недостатню цифрову трансформацію, а відсутність сучасних ІТ-рішень у фінансовому управлінні обмежує здатність організацій оперативно реагувати на загрози;

кадрові проблеми та дефіцит кваліфікованих фахівців, через міграцію, мобілізацію й демографічні зміни ускладнює управління фінансами та ризиками;

низьку фінансову грамотність управлінського персоналу та обмежене розуміння складних фінансових інструментів і ризиків, що знижує ефективність стратегічних рішень.

Водночас гострими секторальними проблемами для фінансової безпеки організацій є:

банківський сектор, оскільки, незважаючи на те, що банки демонструють стійкість, ризики ліквідності, корпоративного кредитування та операційних втрат залишаються актуальними;

аграрний сектор залишається особливо вразливим не лише до кліматичних змін, а й до логістичних порушень і нестабільності валютного фінансування.

А гострими інституційними та регуляторними проблемами для фінансової безпеки організацій вважаємо:

недосконалість нормативно-правового поля;

надто повільна адаптація законодавства до цифрових фінансових інструментів і кібербезпеки;

обмеженість державних механізмів страхування ризиків;

відсутність ефективних моделей гарантування фінансової стабільності для малого та середнього бізнесу.

Погоджуємося з думкою, що «безпеку варто розглядати не лише як стан захищеності інтересів від зовнішніх або внутрішніх чинників, але й потребу в забезпеченні динамічної та статичної стійкості, підвищення рівня адаптації до викликів, а також подальшого ефективного розвитку підприємства» [31, с. 6], а також «фінансова безпека

³¹ Медведєва І. Б., Погосова М. Ю. Діагностування безпеки промислового підприємства у трирівневій системі фінансових відносин : монографія. Харків : Видавництво ХНЕУ, 2011. 264 с.

підприємства полягає в захищеності фінансових інтересів та потенціалу від ризиків і загроз зовнішнього та внутрішнього середовища, що спрямовано на забезпечення фінансової стабільності й оптимального рівня фінансування бізнесових процесів у коротко- та довгостроковій перспективі» [32, с. 145].

Щоб нівелювати означені загрози та проблеми щодо зміцнення фінансової безпеки організацій в умовах нестабільності та високої турбулентності середовища, доцільно використовувати цифрові рішення, які сьогодні можуть відігравати ключову роль. «У сучасній бізнес-екосистемі забезпечення фінансової стійкості часто пов'язане з ефективним використанням цифрових інновацій для управління ризиками. Важливість інформаційних технологій у цьому процесі вже не обмежується традиційними методами; сучасні підходи містять у собі цілісні системи, котрі відповідають за моніторинг і мінімізацію потенційних загроз»³³.

Розглянемо найбільш ефективні технології та інструменти, які вже демонструють практичну цінність для зміцнення фінансової безпеки організацій:

штучний інтелект (далі – ШІ): моделі ШІ аналізують великі обсяги фінансових даних для виявлення аномалій, шахрайства або ознак фінансової нестабільності й на цій основі здійснюють прогнозування різноманітних ризиків і загроз, «аналітика великих даних використовується для глибшого розуміння взаємодії ризиків та причинно-наслідкових факторів»³⁴;

машинне навчання забезпечує антиципацію загроз і ризиків, автоматично виявляє потенційні ризики ще до їхньої реалізації, зокрема в кредитному скорингу, управлінні дебіторською заборгованістю тощо;

блокчейн-рішення забезпечують прозорість транзакцій, захист від підробок і несанкціонованого доступу, «технологія блокчейн забезпечує безпрецедентний рівень прозорості та підзвітності фінансових операцій»³⁵;

³² Марченко О. С. Економічна безпека підприємства : навчальний посібник. Харків : Право, 2022. 246 с.

³³ Захаркін О. О., Бойко А. В., Сокол Л. В. Цифрові технології та інструменти забезпечення фінансової безпеки бізнесу. *Проблеми сучасних трансформацій. Серія Економіка та управління*. 2023. № 10. DOI : <https://doi.org/10.54929/2786-5738-2023-10-08-02>

³⁴ Там само.

³⁵ Там само.

інструменти кіберзахисту, як-от: багаторівнева автентифікація, шифрування даних, системи виявлення вторгнень (IDS / IPS) є критично важливими для захисту фінансових операцій та фінансової інформації;

автоматизовані системи управління ризиками (ERM) за допомогою інтеграції ризик-менеджменту з цифровими платформами дають змогу централізовано моніторити фінансові, операційні та стратегічні ризики, забезпечують оперативне реагування на зміни у фінансовому середовищі й дотримання нормативних вимог у реальному часі;

хмарні технології та цифрові платформи забезпечують гнучкість і масштабованість, дають змогу швидко адаптувати фінансові моделі до змін ринку, оптимізувати витрати на IT-інфраструктуру та підвищення доступності аналітичних інструментів;

електронний документообіг і цифрова ідентифікація знижують ризики фальсифікацій і підробки, адже цифрові підписи, верифікація особи та автоматизований аудит знижують ризики шахрайства та забезпечують прозорість фінансових операцій через електронні платформи, які дають нагоду відстежувати всі етапи фінансових транзакцій;

FinTech-рішення, цифрові банки, інноваційні сервіси, мобільні додатки, онлайн-кредитування, автоматизоване управління грошовими потоками, інтеграція з ERP / CRM забезпечують повну синхронізацію фінансових даних з операційною діяльністю організацій.

Саме «стрімкий розвиток цифрових інновацій вимагає від бізнесу постійного оновлення стратегічних підходів та управлінських практик для досягнення конкурентоспроможності й надійності в нестабільному економічному середовищі»³⁶. Водночас «основними функціональними елементами безпеки підприємств є: захист комерційної таємниці і конфіденційної інформації; комп'ютерна безпека; внутрішня безпека; безпека будівель і споруд; фізична безпека; технічна безпека; безпека зв'язку; безпека перевезень вантажів і осіб; екологічна безпека; конкурентна розвідка тощо» [³⁷, с. 97], а «основою взаємовідносин між суб'єктами економічної діяльності в цифровій економіці є інтегровані продукти-сервіси, так звані продуктово-сервісні системи (Product-Service Systems – PSS), що складаються з матеріальних

³⁶ Захаркін О. О., Бойко А. В., Сокол Л. В. Цифрові технології та інструменти забезпечення фінансової безпеки бізнесу. *Проблеми сучасних трансформацій. Серія Економіка та управління*. 2023. № 10. DOI : <https://doi.org/10.54929/2786-5738-2023-10-08-02>

³⁷ Вівчар О. І. Управління економічною безпекою підприємств: соціогуманітарні контексти : монографія. Тернопіль : ФОП Паляниця В. А., 2018. 515 с.

продуктів, нематеріальних сервісів, програмних компонентів і коопераційної мережі, а також організаційних принципів і технологій, що підтримують взаємодію між цими компонентами в рамках цілісної інтегрованої архітектури продукту-сервісу» [³⁸, с. 57].

Сьогодні вже маємо добірку успішних кейсів впровадження цифрових технологій, які суттєво посилили фінансову безпеку організацій.

Так, після 2022 року українські банки активно впроваджували безготівкові операції, мобільні додатки та системи онлайн-ідентифікації, що допомогло підвищити операційну ефективність, зменшити ризики шахрайства, а також забезпечити стабільність функціонування банківських структур у періоди значної турбулентності середовища. Звернемо увагу, що цифрові трансформації позитивно впливали на дохідність банків до війни, але під час кризи їхня роль стала більш потужною.

Наголосимо, що загалом у світі фінтех-компанії (Revolut, Monzo, Raunoer) замінили традиційні банки за багатьма функціями (кредитування, перекази, управління ризиками) і, як результат, знизили свої витрати на обслуговування клієнтів, забезпечили швидке масштабування, високий рівень прозорості та захисту транзакцій. Тобто цифрові рішення стали джерелом нових доходів і конкурентною перевагою.

В Україні великі аграрні холдинги (зокрема, Kernel, МНР) використовують хмарні ERP-системи, ВІ-аналітику, автоматизовані фінансові дашборди та інтегрують цифрові платформи для моніторингу фінансових ризиків у реальному часі, що дає їм змогу підвищити точність прогнозування, зменшити втрати від валютних коливань і логістичних збоїв.

І в цьому контексті неможливо не згадати платформу «Дія», яка стала прикладом успішної цифровізації державних фінансових послуг (реєстрація бізнесу, податкові звіти, гранти), що сприяло зменшенню адміністративних витрат, підвищенню прозорості та доступності фінансової інформації для організацій.

А на додаток акцентуємо, що в дослідженнях науковців (зокрема, й Державного податкового університету) здійснено кореляційно-регресійний аналіз щодо взаємозалежності між інтенсивністю використання цифрових технологій і стійкістю фінансової безпеки організацій

³⁸ Мехед А. М., Варналій З. С. Фінансова безпека підприємств в умовах цифрової економіки. *Вісник університету банківської справи*. 2021. № 3 (42).

і виявлено позитивну висхідну динаміку між індексами цифрової трансформації та індикаторами фінансової безпеки, що підтверджує стратегічну важливість використання цифрових рішень. «Цифровізація є якісно новою парадигмою розвитку економіки й суспільства та зумовлює перетворення всіх сфер виробництва. У процесі цифрової трансформації змінюються формат виробленої продукції, підходи до розроблення та до виробництва такої продукції, формується новий уклад, який визначається новими форматами бізнес-процесів, цифрових продуктів, цифрових ринків, взаємовідносинами між суб'єктами підприємництва, що створює потребу в переосмисленні підходів до безпеки підприємства та адаптацію механізму фінансової безпеки згідно з вимогами цифрового середовища» [³⁹, с. 60].

Отже, визначення напрямів якісних зрушень і нових орієнтирів у сфері фінансової безпеки організацій на основі цифрових технологій вважаємо стратегічним рішенням, яке формується під впливом комплексу взаємопов'язаних чинників. Наведемо структурований огляд ключових детермінантів, які визначають напрям і глибину цифрової трансформації фінансової безпеки організацій.

Передусім це є мета, стратегічні цілі та тип організації. Місія та візія організації мають орієнтуватися на довгострокову стійкість, інноваційність та адаптивність до ризиків. Сфера діяльності організації (фінансові, виробничі, аграрні, ІТ-компанії) впливає на вибір пріоритетів у фінансовій безпеці, а розмір і структура організацій (великі, середні, малі) впливають на обсяги можливих інвестицій у складні ERM-системи чи хмарні рішення з базовим функціоналом.

Водночас вагоме значення для визначення напрямку й глибини цифрової трансформації фінансової безпеки організацій має наявний рівень цифрової зрілості, цифрової інфраструктури (ERP, CRM, BI-системи, хмарні сервіси тощо), компетентності й здатності персоналу працювати з аналітичними платформами, ШІ, кіберзахистом, цифрова культура, тобто готовність персоналу до змін, відкритість до інновацій, підтримка з боку керівництва тощо.

Фінансово-економічні чинники відіграють значну роль щодо вибору напрямку й глибини цифрової трансформації фінансової безпеки організацій, оскільки визначають доступність інвестицій у цифрові

³⁹ Мехед А. М., Варналій З. С. Фінансова безпека підприємств в умовах цифрової економіки. *Вісник університету банківської справи*. 2021. № 3 (42).

технології, наявність ресурсів для впровадження цифрових рішень (потрібно враховувати не лише ціну впровадження, а й обслуговування, навчання, оновлення), можливість адекватного оцінювання ризиків, рівня загроз (валютних, кредитних, операційних), потребу в конкретних технологіях.

Вибір напрямку й глибини цифрової трансформації фінансової безпеки організації відбувається й з огляду на регуляторне та правове середовище, оскільки важливо враховувати нормативні вимоги до стандартів кібербезпеки, фінансової звітності, захисту даних, податкові стимули й обмеження, що впливають на вибір технологій, особливо в умовах післявоєнного відновлення, та міжнародні стандарти: ISO 27001, GDPR, Basel III, що важливо для організацій, які працюють на глобальному ринку. А «забезпечення фінансової стабільності у кризовий період потребує принципово нового підходу до управління фінансовою системою з метою підтримки її збалансованості (збільшення спроможності до акумуляції та ефективного розміщення фінансових ресурсів), підвищення стійкості (зменшення залежності від зовнішніх впливів)»⁴⁰.

Проблема якісних зрушень у контурі фінансової безпеки організацій на основі цифрових технологій є архіважливою, особливо в українських реаліях, де цифровізація стає не просто трендом, а інструментом виживання та розвитку для організацій. Ключовими якісними зрушеннями, які варто ініціювати вже сьогодні для зміцнення фінансової безпеки організацій на основі цифрових технологій, є такі:

перехід до проактивного управління ризиками через цифрові інструменти, що передбачає інтеграцію систем штучного інтелекту та машинного навчання для прогнозування фінансових ризиків і виявлення аномалій у транзакціях, впровадження автоматизованих систем моніторингу для виявлення кіберзагроз, шахрайства та порушень фінансових протоколів у реальному часі;

розбудова цифрової кіберстійкості, впровадження Zero Trust архітектури (кожна транзакція, користувач і пристрій мають бути перевірені), шифрування даних та багаторівнева автентифікація для захисту фінансової інформації, аудит цифрових слідів (створення прозорих логів доступу до фінансових систем);

⁴⁰ Варналій З. С., Бондаренко С. М. Фінансова безпека підприємств України в умовах війни та повоєнного відновлення. *Економічний вісник університету*. 2023. № 56. С. 106–113. DOI : <https://doi.org/10.31470/2306-546X-2023-56-106-113>

активне використання Big Data й аналітики та фінансового прогнозування, побудова кореляційних матриць для виявлення залежностей між внутрішніми й зовнішніми фінансовими чинниками, інтеграція даних з ERP, CRM, банківських систем для формування єдиної аналітичної платформи;

розвиток цифрової компетентності персоналу, навчання фінансових аналітиків роботі з Python, Power BI, RPA для автоматизації фінансових процесів, формування цифрової культури (безпека, етика, відповідальність у роботі з даними);

розробка адаптивної фінансової стратегії на основі цифрових даних, перехід на цінносно-орієнтоване управління фінансами (фокус на створенні доданої вартості через цифрові рішення), запровадження гнучкого бюджетування та сценарного планування з використанням цифрових моделей;

інтеграція фінтех-рішень і відкритих API, розширення співпраці з фінтех-екосистемами для доступу до інноваційних платіжних рішень, кредитного скорингу, цифрової ідентифікації, впровадження Open Banking для розширення фінансових можливостей організації.

розробка стратегічних карт фінансової безпеки з цифровими KPI, використання бенчмаркінгу з міжнародними практиками цифрового фінансового захисту, постійне оцінювання й аудит фінансової безпеки в цифровому середовищі.

Якісні зрушення «визначають правильний з погляду підприємства спосіб використання комунікаційних та обчислювальних ресурсів, правила доступу на об'єкт, правила обігу з конфіденційною інформацією, а також процедури запобігання порушень режиму безпеки та реагування на них»⁴¹, оскільки «у кризових умовах та в умовах повномасштабного вторгнення на територію України, що характеризується швидкими змінами ресурсної бази та коливаннями цін на чинники виробництва, першочерговим завданням створення та функціонування системи фінансової безпеки є захист «життєвого простору» суб'єкта господарювання⁴². Водночас «система фінансової безпеки

⁴¹ Колодяжна І. В., Букріна К. А. Економічна безпека в системі сталого функціонування підприємства. *Науковий вісник Ужгородського національного університету. Серія: Міжнародні економічні відносини та світове господарство*. 2019. Випуск 23, частина 1. С. 135–140.

⁴² Матвійчук В. І., Матушевський О. В. Формування фінансової безпеки суб'єкта господарювання в умовах воєнного стану. *Економіка і організація управління*. 2023. № 4 (52). С. 118–131. DOI 10.31558/2307-2318.2023.4.13

підприємства змінюється і вимагає приділення значної уваги захисту інформаційних активів» [43, с. 58].

Водночас питання нових орієнтирів фінансової безпеки є стратегічним і глибоко резонуючим із сучасними викликами українських організацій. У контексті цифрової трансформації та нестабільного середовища нові орієнтири для зміцнення фінансової безпеки мають бути не просто технічними, а системно-інтегрованими. І не будемо забувати, що «крім імовірності настання загрози фінансовій безпеці, важливе значення має визначення обсягу можливих затрат, проте їх не завжди можливо оцінити в кількісному вираженні» [44, с. 99].

Наведемо сім ключових орієнтирів, які варто визначити вже сьогодні для зміцнення фінансової безпеки організацій:

ціннісне-орієнтоване управління фінансами, перехід від контролю витрат до управління створенням доданої вартості через цифрові рішення, запровадження цифрових стратегічних карт фінансової безпеки з KPI, що враховують ризики, фінансові інновації та стійкість;

інтелектуалізація управління фінансовими ризиками, активне використання штучного інтелекту та машинного навчання для прогнозування фінансових загроз і аномалій, розробка антиципативних моделей для реагування на зміни ринку, законодавства та технологій;

забезпечення кіберстійкості фінансових операцій, інтеграція кібербезпеки у фінансову стратегію (шифрування, багаторівнева автентифікація, моніторинг доступу), виявлення кіберризиків як елементів фінансової вразливості, особливо в умовах війни та релокації бізнесу;

використання цифрової аналітики для стратегічного планування, побудова кореляційних матриць між фінансовими показниками та цифровими чинниками (інновації, швидкість адаптації, цифрова компетентність), широке використання Big Data та хмарних платформ для інтеграції фінансових, операційних і ринкових даних;

впровадження фінтех-екосистеми як партнера фінансової безпеки, співпраця з фінтех-платформами для доступу до інноваційних рішень (цифрова ідентифікація, скоринг, смарт-контракти), впровадження відкритих API для інтеграції з банками, страховими системами, аудиторами;

⁴³ Мехед А. М., Варналій З. С. Фінансова безпека підприємств в умовах цифрової економіки. *Вісник університету банківської справи*. 2021. № 3 (42).

⁴⁴ Квасницька Р. С., Доценко І. О., Матвійчук Л. О. Оцінювання фінансової безпеки підприємства в системі забезпечення реалізації його фінансової стратегії. *Financial and Credit Activity Problems of Theory and Practice*. 2019. № 3. С. 95–102.

підвищення цифрової грамотності й етики персоналу, формування культури цифрової відповідальності (захист даних, етичне використання технологій, протидія шахрайству), навчання фінансових фахівців роботі з Python, Power BI, RPA, а також з цифровими ризик-моделями;

підвищення адаптивності до цифрових трансформацій, створення гнучких фінансових стратегій, здатних швидко адаптуватися до технологічних змін, підвищення цифрової зрілості як чинника фінансової стійкості організації.

Важливе значення щодо вибору напрямку та глибини цифрової трансформації фінансової безпеки організацій мають технологічні тренди й доступність інновацій і зовнішнє середовище й геополітичні чинники, оскільки саме вони стимулюють релокацію бізнесу, зміну моделей безпеки, перехід на цифрові формати у відповідь на глобальні ризики, кіберзагрози, нестабільність ринків, зміни в ланцюгах постачання.

Ефективність і адекватність вибору напрямку й глибини цифрової трансформації фінансової безпеки організацій найкраще оцінюється через систему кількісних та якісних показників, які відображають здатність організації протистояти ризикам, зберігати фінансову стійкість і забезпечувати стабільний розвиток, а «оцінка та моніторинг ризиків – це безперервний процес, який удосконалює процес виявлення та оперативного реагування на нові фінансові ризики»⁴⁵. Структуруємо перелік ключових індикаторів, згрупованих за напрямками:

I-й напрям – фінансово-економічні індикатори, що демонструють загальний фінансовий стан організації (індекс абсолютної ліквідності (здатність негайно покрити зобов'язання), індекс фінансової стійкості (частка власного капіталу в загальних активах), рентабельність активів / капіталу (ефективність використання ресурсів), індекс покриття зобов'язань (здатність обслуговувати борги), оборотність дебіторської заборгованості (рівень управління грошовими потоками);

II-й напрям – інтегральні та таксономічні індикатори, які демонструють загальний стан фінансової безпеки організації (індекс фінансової безпеки (синтетичний показник, що враховує кілька фінансових

⁴⁵ Матвійчук В. І., Матушевський О. В. Формування фінансової безпеки суб'єкта господарювання в умовах воєнного стану. *Економіка і організація управління*. 2023. № 4 (52). С. 118–131. DOI 10.31558/2307-2318.2023.4.13

параметрів (ліквідність, стійкість, прибутковість), таксономічний індикатор, що дає змогу порівнювати рівень безпеки між організаціями та в динаміці);

III-й напрям – індикатори ризиків і стабільності демонструють вразливість до зовнішніх фінансових впливів та ймовірності фінансової неспроможності (індекс ризику банкрутства (модель Альтмана, Таффлера, Терещенка тощо), індекс концентрації кредиторської заборгованості, частка простроченої дебіторської / кредиторської заборгованості, індикатор фінансової дисципліни);

IV-й напрям – ресурсні та соціальні ефекти демонструють інноваційну та інвестиційну активність, енергоефективність, технічну модернізацію й корпоративну відповідальність організацій (обсяг капіталовкладень у безпекові технології, рівень ресурсної безпеки, вплив стратегії безпеки на соціальну стабільність, інклюзивність і персонал);

V-й напрям – стратегічна узгодженість, що демонструє внутрішню збалансованість і зовнішню гармонізацію організацій (відповідність ресурсів меті та завданням фінансової безпеки, інтеграція стратегії безпеки з корпоративною стратегією розвитку).

Впровадження цифрових рішень для зміцнення фінансової безпеки передбачає не просто технічну модернізацію, а стратегічний процес, який охоплює управлінські, технологічні й аналітичні аспекти. Наведемо структуровану дорожню карту етапів, адаптовану до українських реалій та орієнтовану на організації, що прагнуть системно посилити свою фінансову безпеку й стійкість.

Етап 1 – діагностика та стратегічне планування передбачає оцінювання поточного рівня фінансової безпеки (аналіз ризиків, вразливостей, фінансових показників), визначення цілей цифрової трансформації (що саме має бути захищено: грошові потоки, дані, інвестиції, кредитні ризики), формування цифрової стратегії фінансової безпеки, її узгодження з корпоративною стратегією, визначення KPI.

Етап 2 – вибір технологій та інструментів передбачає аналіз доступних цифрових рішень (ERP, BI, блокчейн, ШІ, хмарні сервіси, системи кіберзахисту тощо), порівняння вартості й ефективності (оцінювання TCO (Total Cost of Ownership), ROI (Return on Investment), адаптація до специфіки організації (у фінансовому, виробничому, аграрному, IT-секторах, різні вимоги до безпеки).

Етап 3 – формування команди та навчання персоналу передбачає створення міжфункціональної робочої групи (ІТ, фінанси, аудит, стратегія), навчання та сертифікація (підвищення цифрової грамотності, кібергігієни, роботи з аналітичними платформами), залучення зовнішніх експертів (консалтинг, аудит, обґрунтування рішень).

Етап 4 – інтеграція цифрових рішень, що передбачає технічне впровадження (налаштування систем, інтеграція з існуючими платформами), автоматизацію процесів (управління ризиками, звітність, моніторинг транзакцій), забезпечення кіберзахисту (шифрування, багаторівнева автентифікація, резервне копіювання).

Етап 5 – моніторинг, оцінювання та корекція, що передбачає впровадження систем контролю (дашборди, аналітичні звіти, індикатори ефективності), аудит цифрової безпеки (регулярна перевірка відповідності стандартам: ISO, GDPR, НБУ), адаптація до змін середовища (оновлення технологій, реагування на нові загрози).

Етап 6 – масштабування та стратегічне оновлення, що передбачає розширення функціоналу (додаткові модулі, інтеграція з новими платформами), побудова цифрової екосистеми (об'єднання фінансової безпеки з управлінням ризиками, інвестиціями, інноваціями), підготовка до сертифікації та міжнародної інтеграції (для експорту, залучення інвесторів, участі в грантових програмах).

Фактично проведення якісних зрушень і впровадження нових орієнтирів для зміцнення фінансової безпеки організацій на основі цифрових технологій це є не просто технічне оновлення, а глибинна трансформація стратегічного мислення організацій. Такий підхід має ряд переваг, але й несе певні ризики, які варто враховувати під час розробки антикризових та інноваційних безпекових стратегій.

Перевагами проведення якісних зрушень і впровадження нових орієнтирів для зміцнення фінансової безпеки організацій на основі цифрових технологій, потрібно вважати:

прозорість і контроль у реальному часі, оскільки автоматизовані системи дають змогу моніторити фінансові потоки, ризики та зобов'язання без затримок, що зменшує ймовірність людських помилок і маніпуляцій;

штучний інтелект і машинне навчання дають нагоду передбачати фінансові загрози на основі історичних даних і поведінкових моделей, що підвищує точність стратегічного планування;

хмарні рішення та цифрові платформи легко масштабуються відповідно до змін середовища, що забезпечує організації гнучкість і адаптивність, а також організації можуть швидко змінювати фінансові моделі без втрати ефективності;

оптимізація процесів (зокрема, документообіг, аудит, звітність) скорочує адміністративні витрати та зменшує потребу у фізичній інфраструктурі;

інтеграція з іншими системами сприяє поєднанню цифрових рішень з ERP, CRM, SCM, що допомагає формуванню єдиної екосистеми управління.

Недоліками та ризиками проведення якісних зрушень і впровадження нових орієнтирів для зміцнення фінансової безпеки організацій на основі цифрових технологій можуть бути:

зростання кіберзагроз і вразливостей, збільшення залежності від цифрових систем, що підвищує ризик хакерських атак, витік даних і фінансового шахрайства, через що виникає потреба в постійному оновленні систем кіберзахисту;

надмірна технологічна залежність, а втрата доступу до цифрових платформ (через технічні збої або санкції) може паралізувати фінансову діяльність, зростає ризик монополізації хмарних сервісів і втрати контролю над даними;

недостатня кваліфікація персоналу у сфері цифрової безпеки може знизити ефективність впроваджених рішень, тому виникає потреба в постійному навчанні та перепідготовці кадрів;

правова невизначеність через недосконалість нормативної бази щодо цифрових фінансових інструментів, особливо в умовах швидких змін, відсутність чітких механізмів відповідальності за порушення цифрової безпеки;

інвестиційна складність, адже впровадження якісних цифрових рішень потребує значних початкових вкладень, що може бути недоступним для малих і бюджетних організацій.

Наголосимо, що «для формування належного рівня фінансової безпеки підприємницьких структур потрібно створити ефективну систему управління фінансовою безпекою як на державному рівні, так і на рівні окремих суб'єктів господарювання» [⁴⁶, с. 208]. Отже, проведення

⁴⁶ Крупка М. І., Яструбецька Л. С. Фінансова безпека суб'єктів господарювання : підручник. Львів : ЛНУ імені Івана Франка, 2018. 320 с.

якісних зрушень і впровадження нових орієнтирів для зміцнення фінансової безпеки організацій на основі цифрових технологій в умовах воєнного стану змушує організації діяти не просто адаптивно, а проактивно, щоб зберегти фінансову стійкість, захистити ресурси та забезпечити безперервність діяльності, тобто «основне значення системи фінансової безпеки підприємств полягає в тому, що вона повинна мати попереджувальний характер» [⁴⁷, с. 10]. Наведемо систематизований перелік превентивних організаційних і кадрових заходів, які доцільно впровадити для зміцнення фінансової безпеки:

Організаційні превентивні заходи передбачають:

антикризове фінансове планування, формування сценаріїв розвитку подій (оптимістичний, песимістичний, базовий) і визначення критичних точок фінансової стабільності (ліквідність, кредитоспроможність, доступ до резервів);

реструктуризацію фінансових потоків, перенесення акценту на короткострокову платоспроможність, оптимізацію витрат, замороження неключових інвестицій;

цифровізацію фінансового контролю, впровадження хмарних систем звітності, електронного документообігу, онлайн-моніторингу ризиків, забезпечення резервного копіювання даних і кіберзахисту;

побудову внутрішнього центру фінансової безпеки, визначення відповідальних осіб за моніторинг ризиків, аудит, зв'язок з банками та державними структурами, розробку внутрішніх регламентів реагування на фінансові загрози;

переорієнтацію на локальні та стійкі ланцюги постачання, зменшення залежності від імпорту, валютних ризиків і нестабільних партнерів.

Кадрові превентивні заходи передбачають:

формування кризових команд, створення міжфункціональних груп (фінанси, ІТ, безпека, логістика) для оперативного реагування, делегування повноважень для швидкого прийняття рішень;

підвищення кваліфікації персоналу, навчання з фінансової грамотності, цифрових інструментів, кібергігієни, проведення вебінарів і тренінгів з антикризового управління й адаптивного планування;

⁴⁷ Вівчар О. І. Практичний базис системи фінансової безпеки підприємницьких структур: нові виклики та можливості. *Modeling the development of the economic systems*. 2021. № 3. С. 8–13. DOI : <https://doi.org/10.31891/mdes/2023-7-1>

психологічну підтримку та мотивацію, забезпечення емоційної стійкості команди через внутрішню комунікацію, гнучкий графік, підтримку, збереження ключових кадрів через адаптовані системи винагород;

проведення аудиту кадрових ризиків, здійснення діагностики вразливості до втрати персоналу (мобілізація, релокація, вигорання), розробку планів заміщення та резерву кадрів.

Отже, «ефективна реалізація заходів фінансової безпеки передбачає використання системного та комплексного підходу. Ключовим аспектом у цьому питанні виступає недопущення перевищення захисних заходів вартості об'єктів, які перебувають під таким захистом»⁴⁸. Водночас фінансова безпека «є єдиним організаційно-технічним комплексом, під час формування якого розробляється концепція забезпечення безпеки об'єкта чи політика безпеки. Її основу становить перелік обов'язкових заходів, які спрямовані на вироблення алгоритму дій щодо захисту заявленого об'єкта, як-от визначення складу служби безпеки, її місця в організаційній структурі підприємства; сфера її компетенції, прав і повноважень; варіанти дій у різних ситуаціях уникнення конфліктів між внутрішніми та зовнішніми структурними підрозділами» [⁴⁹, с. 137].

Водночас наголосимо, що для проведення якісних зрушень і визначення нових орієнтирів фінансової безпеки організацій на основі цифрових технологій важливо використовувати найефективніші цифрові технології нового покоління, які є не просто інструментами, а архітектурою нової фінансової безпеки й стійкості, яка дає змогу організаціям діяти швидко, точно й безпечно навіть в умовах воєнного стану.

І наостанок зазначимо, що проведення якісних зрушень і визначення нових орієнтирів фінансової безпеки організацій на основі цифрових технологій має передбачати й модернізацію фінансової поведінки в організації, яка є стратегічною культурою управління фінансовими

⁴⁸ Рожко О. Д., Нестеров Є. В. Теоретичні підходи до визначення фінансової безпеки підприємства. *Економіка та суспільство*. 2024. Випуск 65. DOI : <https://doi.org/10.32782/2524-0072/2024-65-79>

⁴⁹ Колодяжна І. В., Букріна К. А. Економічна безпека в системі сталого функціонування підприємства. *Науковий вісник Ужгородського національного університету. Серія: Міжнародні економічні відносини та світове господарство*. 2019. Випуск 23, частина 1. С. 135–140.

ресурсами та формує рівень її фінансової безпеки. Вплив фінансової поведінки на фінансову безпеку можна розглядати через кілька ключових аспектів:

стратегічну орієнтацію, адже організації, які дотримуються довгострокової фінансової стратегії, мають вищу стійкість до зовнішніх шоків, а поведінка, орієнтована на інвестиції в інновації та цифрову трансформацію, підвищує здатність адаптуватися до змін;

обачну фінансову поведінку, яка сприяє диверсифікації джерел доходу, страхуванню ризиків, створенню резервів, що знижує вразливість до криз, оскільки імпульсивні рішення (наприклад, надмірне кредитування або необґрунтовані витрати) можуть призвести до втрати платоспроможності та банкрутства;

фінансову дисципліну, адже регулярне виконання зобов'язань, прозора звітність, контроль дебіторської заборгованості вважаються ознаками збалансованої поведінки, яка зміцнює довіру контрагентів і банків, а порушення платіжної дисципліни, приховування витрат або маніпуляції з балансом зазвичай знижують кредитний рейтинг і підвищують ризики;

адаптивність до середовища, оскільки організації, що швидко реагують на зміни (валютні коливання, зміни податкової політики, воєнні ризики), демонструють вищу фінансову безпеку, а поведінка, що ігнорує зовнішні сигнали, призводить до стратегічної інерції та втрати конкурентоспроможності;

цифрову грамотність та інноваційність, оскільки використання цифрових інструментів для управління фінансами є ознакою проактивної поведінки, яка дає змогу краще контролювати ризики, а відмова від цифровізації – це обмеження доступу до сучасних механізмів захисту, прогнозування та оптимізації.

Отже, фінансова поведінка є дзеркалом внутрішньої культури фінансового управління, яке визначає здатність організації протистояти загрозам, зберігати стабільність, реалізовувати стратегічні цілі фінансової безпеки, і тому адекватна фінансова поведінка є важливою для проведення якісних зрушень і визначення нових орієнтирів фінансової безпеки організацій на основі цифрових технологій.

Підсумовуючи, зазначимо, що цифровізація існує новим фундаментом фінансової безпеки організацій, оскільки сучасні цифрові технології (штучний інтелект, машинне навчання, блокчейн, цифрові

платформи, хмарні сервіси) дають змогу автоматизувати управління ризиками, зменшити людський чинник і підвищити точність прогнозування, забезпечити моніторинг фінансових потоків у реальному часі, що критично важливо для адаптації до змін ринку та нормативного ландшафту. Крім того, спостерігаються принципові зрушення в підходах до фінансової безпеки, адже відбувається перехід від реактивного до проактивного управління ризиками: організації не лише реагують на загрози, а й передбачають їх, що зміщує акцент з контролю витрат на стратегічне управління фінансовими ресурсами, включно із інвестиціями в кіберзахист і цифрову інфраструктуру. Загалом новими орієнтирами фінансової безпеки організацій усе частіше визначають інтеграцію, гнучкість, адаптивність, оскільки вже фінансова безпека не розглядається ізольовано, а влітається в загальну цифрову стратегію організацій, а гнучкість у фінансовому плануванні, адаптація до цифрових викликів і створення доданої вартості стають ключовими індикаторами її якості. Водночас «основним напрямом державної політики має стати низка організаційних, правових, соціально-економічних та управлінських рішень щодо ефективного захисту суб'єктів підприємництва від зовнішніх і внутрішніх загроз» [50, с. 528]. А «в умовах нових викликів, негативних наслідків війни та суперечностей процесу реформ держава має спрямувати свої зусилля на забезпечення безпеки суб'єктів підприємництва. Створення унікальної системи фінансової безпеки є ключовою умовою для ефективного функціонування й подальшого розвитку підприємства» [51, с. 131]. Тобто в умовах війни та післявоєнного відновлення цифрові технології стають критичним інструментом для виживання, захисту, безпеки й розвитку бізнесу організацій та основою для проведення якісних зрушень і визначення нових орієнтирів фінансової безпеки організацій.

⁵⁰ Барановський О. І. Фінансова безпека в Україні (методологія оцінки та механізми забезпечення) : монографія. Київ : Київ. нац. торг.-екон. ун-т, 2014. 759 с.

⁵¹ Актуалітети фінансової безпеки суб'єктів підприємництва України в умовах війни та повоєнний час / Варналій З. С., Чеберяко О. В., Микитюк О. П., Бондаренко С. М. *Academy review*. 2024. № 1 (60). С. 123–140. DOI 10.32342/2074-5354-2024-1-60-9