ISSN 2306-5478

УДК 657
https://doi.org/10.31713/ve4202539
JEL: M40

Скаковська С. С. [1; ORCID ID: 0000-0002-3415-9613],
к.е.н., доцент,
Зінкевич О. В. [1; ORCID ID: 0000-0002-8908-9368],
к.е.н., доцент

[1]Національний університет водного господарства та природокористування, м. Рівне

РЕАЛІЗАЦІЯ ІННОВАЦІЙНИХ СИСТЕМНИХ РІШЕНЬ У СФЕРІ КІБЕРЗАХИСТУ ТА ЗБЕРЕЖЕННЯ ЦІЛІСНОСТІ БУХГАЛТЕРСЬКИХ І ФІНАНСОВИХ МАСИВІВ ДАНИХ ПРИ ВИКОНАННІ ОБОВ'ЯЗКІВ ВІДДАЛЕНО

У цій публікації проводиться детальне вивчення новітніх викликів та потенційних небезпек, зумовлених масштабним впровадженням формату дистанційної праці. Зважаючи на інтенсивне розширення сфери експлуатації передових інформаційних систем, робота зосереджується на аналізі фундаментальних ризиків для цифрової безпеки фінансових активів та облікової документації. Особливий акцент зроблено на труднощах, що виникають під час організації захисту конфіденційної інформації на віддалених серверах, зокрема через критичні загрози від нелегітимного проникнення, мережевого фішингу та роботи через вразливі канали зв'язку.

Обговорюються ефективні стратегії та методи мінімізації кіберризиків, такі як впровадження багаторівневих систем автентифікації, використання шифрування, регулярні оновлення програмного забезпечення та навчання персоналу основам кібергігієни. Стаття також містить рекомендації розробки політик кібербезпеки та оптимізації організації роботи бухгалтерських підрозділів в умовах віддаленої роботи, що сприяє підвищенню захисту бухгалтерських даних та забезпеченню інноваційного, безперебійного функціонування підприємств.

Ключові слова: інновації; комунікація; кібербезпека; віддалена робота; організація праці; цифрові технології; захист бухгалтерських даних; інформаційні технології; системні інновації.

Актуальність теми. Цифрова трансформація формує нові можливості щодо підвищення ефективності управління фінансовою безпекою, але водночас збільшує ризики та виклики, пов'язані з кіберзагрозами та технологічною залежністю. У таких умовах ключовим завданням стає впровадження інноваційних методів

управління фінансовою безпекою, які дозволяють мінімізувати ризики та забезпечити стабільність бізнесу.

На наше переконання, фінансова безпека підприємства – це комплексна система заходів та інструментів, спрямованих на забезпечення стабільності фінансової діяльності, захищеність економічних інтересів, ефективне управління ризиками та реалізацію стратегій сталого розвитку в умовах конкурентного середовища. Фінансово-економічна безпека підприємства розглядається як складна система, яка об'єднує різні взаємопов'язані елементи. Вони сприяють оптимальному управлінню корпоративними ресурсами у всіх напрямах діяльності. Конкретний зміст і структура цієї системи залежать від особливостей підприємства, його ресурсного потенціалу, характеру ринкової діяльності та застосовуваних управлінських практик та системних інноваційних рішень [1].

Аналіз останніх досліджень. Процеси цифрової трансформації відкривають принципово нові горизонти для вдосконалення механізмів управління фінансовою стійкістю, проте паралельно з цим вони генерують додаткові загрози та складні виклики, зумовлені зростанням інтенсивності кібератак та посиленням технологічної вразливості організацій. У подібних обставинах пріоритетним стратегічним завданням стає інтеграція передових інноваційних підходів до менеджменту фінансової безпеки, котрі здатні нівелювати потенційні ризики та гарантувати довгострокову стабільність функціонування бізнес-структур. У вітчизняному науковому дискурсі вагомий теоретичний і практичний внесок у дослідження проблематики фінансової безпеки здійснили такі вчені, як Панченко В., Докієнко Л., Василишин С. та інші відомі дослідники. Попри наявні напрацювання, аспект фундаментального впливу цифрових інновацій на систему забезпечення фінансової безпеки все ще характеризується фрагментарністю вивчення, що стає надзвичайно актуальним для України в контексті стрімких глобальних трансформацій та безпекових викликів сьогодення.

Виклад основного матеріалу. Сьогодні інформаційно-комунікаційні технології займають визначальне місце у забезпеченні життєдіяльності бізнесу, охоплюючи всі ланки бухгалтерського та фінансового обліку.

Масове впровадження дистанційного режиму праці, що стало вимушеною відповіддю на пандемію COVID-19 та повномасштабну військову агресію проти української держави, радикально змінило

 ISSN 2306-5478

принципи побудови бухгалтерського менеджменту. Паралельно з перевагами гнучкості, нововведення породили складні виклики у сфері забезпечення кіберзахисту. Бухгалтерські дані, що містять у собі персональну та корпоративну фінансову таємницю, залишаються пріоритетною ціллю для кіберзлочинців, оскільки їх вразливість неминуче тягне за собою прямі грошові збитки та суттєве погіршення іміджу підприємства в очах партнерів.

За умов переходу на віддалені формати взаємодії об'єктивно зростає критична необхідність у забезпеченні та застосуванні інноваційних системних рішень та безкомпромісного захисту конфіденційної звітності, що безпосередньо зумовлює високу актуальність теми цієї статті та потребує глибокого аналізу існуючих стратегій кіберзахисту.

Метою даного дослідження є аналіз ролі цифрових інновацій у забезпеченні та управлінні фінансовою безпекою підприємств.

Пріоритетним завданням цієї праці є виокремлення спектру актуальних кібернетичних небезпек, що супроводжують масштабну дистанціалізацію бізнес-процесів, та проєктування системних стратегій безпеки для облікових даних із використанням потенціалу інноваційних інформаційних платформ. Зокрема, у тексті проводиться критичний огляд змін у механіці бухгалтерського обліку під впливом віддаленої моделі управління, а також класифікуються основні дестабілізуючі чинники (цифрові загрози та латентні ризики, характерні для функціонування фінансових департаментів у віддаленому доступі). Дослідницький інтерес зосереджений на пошуку та систематизації новітніх методів захисту інформаційного капіталу підприємства, які є придатними для розгортання в умовах віддаленої роботи. Підсумком роботи є створення практичних моделей зниження кіберризиків, що дозволяють підвищити рівень захищеності бухгалтерії, а також проведення порівняльного аналізу успішних галузевих практик із впровадження систем кіберзахисту для оцінки їхнього реального впливу на стабільність бізнесу.

Сучасна епоха всеохоплюючої глобалізації та інноваційних перетворень характеризується масовим переходом українських та світових підприємств на рейки віддаленого виконання посадових обов'язків. Ця тенденція набула надзвичайної динаміки під впливом кризи охорони здоров'я, спричиненої COVID-19, що змусило менеджмент багатьох установ у стислі терміни перебудовувати робочі алгоритми згідно з актуальними вимогами часу. Віддалений формат

перестав сприйматися як тимчасове розв'язання проблеми, перетворившись на вагомий тренд, що залишається визначальним у постпандемічний період.

На теренах України спостерігається активна практика використання дистанційної праці в IT-сфері та галузях сервісного обслуговування як фундаментального способу організації виробничого процесу. Корпоративний сектор та малий бізнес поступово еволюціонують до впровадження гнучких гібридних моделей, які вдало комбінують традиційні офісні заходи з віддаленим доступом до робочих місць. Це створює умови для раціоналізації бюджетів шляхом скорочення витрат на оренду приміщень, забезпечує співробітникам баланс між роботою та особистим життям завдяки гнучкості, а також дозволяє акумулювати інтелектуальний капітал, залучаючи фахівців із найвіддаленіших куточків країни чи світу. У глобальному масштабі функціонування в дистанційному режимі остаточно трансформувалося у загальноприйняту норму ділової активності.

Провідні світові технологічні гіганти, зокрема Google, Microsoft та Meta (Facebook), вже офіційно задекларували свої довгострокові стратегії щодо пролонгації або навіть масштабного розширення політик віддаленої зайнятості як фундаментального принципу корпоративної культури. Жорстка конкурентна боротьба за інтелектуальний капітал на міжнародному ринку праці змушує організації динамічно коригувати власні бізнес-алгоритми та технічну інфраструктуру згідно з новими вимогами, надаючи персоналу реальну можливість виконувати професійні обов'язки з будь-якої географічної локації планети. Водночас масштабна зміна парадигми роботи створює для бухгалтерських та фінансових департаментів комплекс критичних викликів, до яких належать цифрова безпека, гарантування безперебійного доступу до масивів даних, складність процедур контролю й аудиту, а також питання ефективної комунікації та адаптації кадрового складу. Дистанційний формат об’єктивно підвищує ймовірність здійснення цілеспрямованих кібератак та несанкціонованого розголошення конфіденційної звітності. Відтак, бухгалтерські реєстри потребують безкомпромісної охорони, що робить обов'язковим впровадження новітніх інструментів захисту, таких як системи багатофакторної перевірки автентичності, криптографічне шифрування інформаційних потоків та систематичний апгрейд використовуваного софту.

 ISSN 2306-5478

Фахівцям бухгалтерських служб критично важливо гарантувати стабільну та постійну можливість оперування фінансовою документацією і спеціалізованими обліковими платформами. Реалізація цього завдання передбачає необхідність спрямування капітальних інвестицій у розвиток хмарних рішень та архітектуру віддаленого підключення, що характеризується максимальним ступенем захищеності інформаційних каналів. Водночас дистанційний формат трудової діяльності створює додаткові перешкоди для здійснення якісного внутрішнього контролю та проведення аудиторських перевірок.

Це зумовлює нагальну потребу у формуванні принципово нових методологічних підходів до нагляду за фінансовими трансакціями та розробки алгоритмів оперативного виявлення можливих зловживань чи помилок. Крім того, такий специфічний режим функціонування може негативно впливати на продуктивність взаємодії між обліковим персоналом та іншими структурними одиницями організації. Для нейтралізації цієї загрози стає принципово важливим впровадження високотехнологічних засобів комунікації та систематизація регулярних відеоконференцій і онлайн-брифінгів. Зрештою, трансформація робочих місць вимагає від бухгалтерів опанування додаткових компетенцій, насамперед у сегменті передових IT-рішень та фундаментальних принципів кібернетичної гігієни.

Компаніям слід організовувати регулярне навчання та підвищення кваліфікації співробітників.

Дистанційна робота створює додаткові загрози для кібербезпеки. Серед основних загроз можна виділити:

- несанкціонований доступ (збільшується ризик несанкціонованого доступу до конфіденційної інформації, оскільки домашні мережі та особисті пристрої часто мають слабший захист);

- фішинг (зловмисники активно використовують фітингові атаки для отримання доступу до облікових записів та конфіденційної інформації);

- шкідливе програмне забезпечення (збільшується ризик зараження пристроїв шкідливим програмним забезпеченням, оскільки працівники використовують різні програми та додатки);

- незахищені мережі (використання незахищених Wi-Fi мереж у громадських місцях або вдома може призвести до перехоплення даних).

Явище несанкціонованого доступу до масивів даних ідентифікується як фундаментальний дестабілізуючий фактор кіберзахисту в сучасних умовах віддаленої роботи. Спектр основних небезпек складається з:

- експлуатації облікових записів: через використання вразливих або ідентичних паролів на різних ресурсах, хакери отримують можливість незаконного володіння правами доступу працівників;

- використання соціально-інженерного інструментарію: через обман та маніпулювання довірою, зловмисники виманюють у штатних одиниць критично важливу інформацію;

- ризиків відкритого віддаленого доступу: впровадження засобів віддаленого зв'язку без суворої системи безпеки стає точкою входу для зовнішніх атак на цілісність корпоративних систем.

Різні форми фішингу та альтернативні вектори кібернападів залишаються основними механізмами компрометації безпеки для тієї категорії працівників, чия діяльність організована поза офісом.

Відкриті та незахищені мережі бездротового зв’язку Wi-Fi часто функціонують без застосування належних протоколів шифрування, що створює сприятливі умови для зловмисників щодо перехоплення інформаційних потоків, які транслюються через такі канали. Деструктивні суб’єкти мають можливість проектувати фальшиві точки доступу Wi-Fi з метою прихованого збору та аналізу мережевого трафіку співробітників компаній. Крім того, експлуатація вразливих мережевих з’єднань без активації захищених VPN-тунелів суттєво підвищує ймовірність несанкціонованого витоку конфіденційних відомостей у відкритий простір. Облікові та фінансові департаменти характеризуються критично високим рівнем вразливості до інцидентів у сфері кібербезпеки з огляду на величезні масиви фінансової та комерційної таємниці, які вони систематично опрацьовують. Такі деструктивні наслідки можуть бути зумовлені наступними чинниками:

- крадіжка фінансових даних через отримання доступу до фінансових звітів, платіжних реквізитів та іншої конфіденційної інформації, що може призвести до фінансових втрат;

- маніпуляції з бухгалтерськими даними (зміна бухгалтерських даних, що призводять до неправильних фінансових звітів та втрат);

- зараження шкідливим програмним забезпеченням, що може призвести до втрати або шифрування важливих даних.

 ISSN 2306-5478

Впровадження актуальних інноваційних технологічних рішень у сфері безпеки даних дозволяє ефективно протидіяти вектору кіберзагроз і підтримувати високий рівень конфіденційності стратегічно важливої інформації. Шифрування вважається ключовим та безкомпромісним методом захисту, що забезпечує стійкість систем до несанкціонованого втручання. Воно трансформує інформаційний потік у такий вигляд, що його візуалізація та змістовне сприйняття стають доступними лише після завершення операції зворотного перетворення за допомогою відповідного криптографічного ключа.

Методологія захисту може бути впроваджена у практику через наступні функціональні напрями:

- системне шифрування дискового простору: використовується як базовий метод охорони всієї інформації на накопичувачах типу SSD чи HDD (наприклад, через штатний засіб BitLocker у середовищі Windows або аналогічне рішення FileVault у macOS);

- диференційоване шифрування файлових об'єктів та папок: дозволяє забезпечити ізольований захист для окремих одиниць зберігання, виступаючи важливим інструментом посилення безпеки конфіденційних бухгалтерських архівів;

- захист даних у динаміці (під час транзиту): нейтралізує ризики перехоплення інформації в процесі її обміну між вузлами мережі, що стає можливим завдяки інтеграції мережевих протоколів HTTPS та засобів автентифікації SSL/TLS.

Система багаторівневої автентифікації (MFA) визнана критично важливим заходом для забезпечення цілісності та конфіденційності користувацьких акаунтів. Її призначення полягає у створенні додаткових ступенів захисту, які доповнюють стандартні методи ідентифікації. Виділяють три основні площини підтвердження прав доступу:

- інформаційний рівень (парольна комбінація): є первинним кроком автентифікації, що традиційно застосовується в більшості цифрових платформ;

- матеріальний рівень (смартфон чи токен): включає використання повідомлень із кодами підтвердження, апаратних автентифікаторів або мобільних додатків для перевірки легітимності входу;

- персоналізований рівень (біометрія): базується на ідентифікації через біометричні маркери, такі як унікальний папілярний візерунок або антропометричні дані обличчя.

Впровадження MFA суттєво мінімізує ймовірність успішного несанкціонованого доступу, змушуючи зловмисників долати багаторівневу структуру оборони.

Поряд із цим, регулярне оновлення прикладного та системного програмного забезпечення є основоположним принципом кібербезпеки. Процес оновлення спрямований на деактивацію відомих прогалин у безпеці та впровадження нових інструментів протидії загрозам. Цей напрям захисту може бути реалізований за допомогою налаштування автоматичного отримання оновлень або через планове інспектування систем на предмет наявності нових версій ПЗ та їх подальшу установку в ручному режимі за необхідності.

Для суб'єктів бізнесу рекомендується апробація оновлень в ізольованих тестових контурах перед їх масштабуванням на промислове (продуктивне) середовище. Дотримання регламенту своєчасного оновлення системного та прикладного програмного забезпечення допомагає мінімізувати ризики експлуатації відомих кібернетичних вразливостей.

Віртуальні приватні мережі (VPN) формують захищений тунель для даних під час їх передачі через потенційно небезпечні мережеві середовища, зокрема публічні точки доступу Wi-Fi. Ключовий перелік переваг від використання VPN складається з:

- криптографічний захист трафіку: VPN-з'єднання забезпечує маскування всіх даних, що передаються між кінцевим вузлом та сервером, роблячи інформацію недоступною для сторонніх осіб;

- запобігання перехопленню: надійний бар'єр проти мережевих атак типу «Man-in-the-middle» у публічних мережах;

- безпечне підключення до корпоративної екосистеми: VPN надає авторизованим користувачам можливість безпечного доступу до внутрішніх ресурсів підприємства з будь-якої географічної локації.

Отже, застосування VPN є обов'язковою передумовою для забезпечення кіберстійкості процесів віддаленої роботи та комплексного захисту конфіденційної інформації.

Висновки. Підсумовуючи, слід зазначити, що впровадження віддаленої роботи є невід'ємним елементом еволюції як українського підприємництва, так і світової економічної системи, проте цей перехід генерує специфічні проблеми для підрозділів бухгалтерського обліку, які потребують ґрунтовного аналізу та вирішення. Пріоритетом стає реалізація інноваційних стратегій кіберзахисту, підвищення кваліфікації штату та експлуатація сучасних IT-інструментів для

 ISSN 2306-5478

мінімізації вразливостей. Розвиток навичок кібергігієни є фундаментом для побудови цілісної системи безпеки всередині компанії.

Внутрішня політика кібербезпеки організації має таку структуру:

Нормативи використання ідентифікаторів (паролів): формування вимог до створення унікальних та захищених парольних фраз, контроль за графіком їх регулярного оновлення та запобігання використанню ідентичних даних у різних програмних комплексах.

Політика адміністрування доступу: регулювання прав користувачів щодо взаємодії з базами даних, надання доступу виключно в обсязі, що відповідає робочим завданням, на базі міжнародного принципу «найменших привілеїв».

План антикризового реагування на інциденти: розробка методології дій при виникненні кіберзагроз, яка включає етапи діагностики, офіційного звітування, ізоляції уражених сегментів мережі та остаточного усунення шкідливих впливів.

Програма освітнього супроводу персоналу: систематична організація навчальних заходів та вебінарів із базової кібербезпеки, навчання способам детекції фішингових схем та протидії іншим формам соціальної інженерії.

1. Tkachenko V., Tkachenko I., Puzyrova P. Fundamentals of financial and economic security management of Ukrainian enterprises. *Research Papers in Economics and Finance*. 2020. Vol. 4(2). P. 41–51. URL: https://doi.org/10.18559/ref.2020.2. **2.** Попівняк Ю. М. Кібербезпека та захист бухгалтерських даних в умовах застосування новітніх інформаційних технологій. *Бізнес Інформ*. 2019. № 8. С. 150–157. URL: https://doi.org/10.32983/2222-4459-2019-8-150-157 **3.** Муравський В. В. Комп'ютерно-комунікаційна форма обліку : монографія. Тернопіль : ТНЕУ, 2018. 486 с. **4.** Германюк Н. В. Роль комунікацій в управлінні організаційним процесом. *Ефективна наука.* 2021. № 10. С. 1–6. **5.** Зайцева Н. В. Організація комунікацій в управлінській діяльності на основі сучасних інформаційних технологій. *Теоретичні і практичні аспекти економіки та інтелектуальної власності.* 2015. № 15. Том 1. С. 166–170. URL: https://doi.org/10.31498/2225-6407.11.2015.74772 **6.** Бадяєв О. Інноваційні підходи до кризового фінансового менеджменту в контексті цифрової трансформації. *Актуальні проблеми інноваційної економіки та права.* 2024. URL: https://doi.org/10.36887/2524-0455-2024-3-21. **7.** Василішин С. Удосконалення важелів цифровізації управління ризиками економічної безпеки та формування кібербезпеки облікової системи. *Вісник економіки.* 2021. № 1. С. 97–100. URL: https://doi.org/10.35774/VISNYK2021.01.097. **8.** Македон В., Стрижус М. Забезпечення економічної безпеки підприємства та конкурентоспроможності на основі інноваційного розвитку. *Ринкова інфраструктура.* 2024. Вип. 79. С. 167–172. URL: https://doi.org/10.32782/infrastruct79-28. **9.** Про аудит фінансової звітності та аудиторську діяльність : Закон України від 21 грудня 2017 р. № 2258-VIII. URL:

https://zakon.rada.gov.ua/laws/show/2258-19#Text. (дата звернення: 10.10.2025). **10.** Про бухгалтерський облік та фінансову звітність в Україні : Закон України від 16 липня 1999 р. № 996-XIV. URL: https://zakon.rada.gov.ua/laws/show/996- 14#Text. (дата звернення: 15.10.2025).

REFERENCES:

1. Tkachenko V., Tkachenko I., Puzyrova P. Fundamentals of financial and economic security management of Ukrainian enterprises. *Research Papers in Economics and Finance*. 2020. Vol. 4(2). P. 41–51. URL: https://doi.org/10.18559/ref.2020.2. **2.** Popivniak Yu. M. Kiberbezpeka ta zakhyst bukhhalterskykh danykh v umovakh zastosuvannia novitnikh informatsiinykh tekhnolohii. *Biznes Inform*. 2019. № 8. S. 150–157. URL: https://doi.org/10.32983/2222-4459-2019-8-150-157 **3.** Muravskyi V. V. Kompiuterno-komunikatsiina forma obliku : monohrafiia. Ternopil : TNEU, 2018. 486 s. **4.** Hermaniuk N. V. Rol komunikatsii v upravlinni orhanizatsiinym protsesom. *Efektyvna nauka*. 2021. № 10. S. 1–6. **5.** Zaitseva N. V. Orhanizatsiia komunikatsii v upravlinskii diialnosti na osnovi suchasnykh informatsiinykh tekhnolohii. *Teoretychni i praktychni aspekty ekonomiky ta intelektualnoi vlasnosti*. 2015. № 15. Tom 1. S. 166–170. URL: https://doi.org/10.31498/2225-6407.11.2015.74772 **6.** Badiaiev O. Innovatsiini pidkhody do kryzovoho finansovoho menedzhmentu v konteksti tsyfrovoi transformatsii. *Aktualni problemy innovatsiinoi ekonomiky ta prava*. 2024. URL: https://doi.org/10.36887/2524-0455-2024-3-21. **7.** Vasylishyn S. Udoskonalennia vazheliv tsyfrovizatsii upravlinnia ryzykamy ekonomichnoi bezpeky ta formuvannia kiberbezpeky oblikovoi systemy. *Visnyk ekonomiky*. 2021. № 1. S. 97–100. URL: https://doi.org/10.35774/VISNYK2021.01.097. **8.** Makedon V., Stryzhus M. Zabezpechennia ekonomichnoi bezpeky pidpryiemstva ta konkurentospromozhnosti na osnovi innovatsiinoho rozvytku. *Rynkova infrastruktura*. 2024. Vyp. 79. S. 167–172. URL: https://doi.org/10.32782/infrastruct79-28. **9.** Pro audyt finansovoi zvitnosti ta audytorsku diialnist : Zakon Ukrainy vid 21 hrudnia 2017 r. № 2258-VIII. URL: https://zakon.rada.gov.ua/laws/show/2258-19#Text. (data zvernennia: 10.10.2025). **10.** Pro bukhhalterskyi oblik ta finansovu zvitnist v Ukraini : Zakon Ukrainy vid 16 lypnia 1999 r. № 996-XIV. URL: https://zakon.rada.gov.ua/laws/show/996- 14#Text. (data zvernennia: 10.15.2025).

ISSN 2306-5478

Skakovska S. S. [1; ORCID ID: 0000-0002-3415-9613],
Candidate of Economics (Ph.D.), Associate Professor,
Zinkevych O. V. [1; ORCID ID: 0000-0002-8908-9368],
Candidate of Economics (Ph.D.), Associate Professor

[1]*National University of Water and Environmental Engineering, Rivne*

IMPLEMENTATION OF INNOVATIVE SYSTEM SOLUTIONS IN THE FIELD OF CYBER PROTECTION AND MAINTAINING THE INTEGRITY OF ACCOUNTING AND FINANCIAL DATA SETS WHEN PERFORMING DUTIES REMOTELY

This publication provides a detailed study of the latest challenges and potential dangers caused by the large-scale implementation of the remote work format. Given the intensive expansion of the scope of operation of advanced information systems, the work focuses on the analysis of fundamental risks for the digital security of financial assets and accounting documentation. Particular emphasis is placed on the difficulties that arise when organizing the protection of confidential information on remote servers, in particular due to critical threats from illegitimate penetration, network phishing and work through vulnerable communication channels. Digital transformation creates new opportunities to improve the efficiency of financial security management, but at the same time increases the risks and challenges associated with cyber threats and technological dependence. In such conditions, the key task is to implement innovative financial security management methods that minimize risks and ensure business stability. In our opinion, the financial security of an enterprise is a comprehensive system of measures and tools aimed at ensuring the stability of financial activities, the protection of economic interests, effective risk management and the implementation of sustainable development strategies in a competitive environment. The financial and economic security of an enterprise is considered as a complex system that combines various interconnected elements. They contribute to the optimal management of corporate resources in all areas of activity. The specific content and structure of this system depend on the characteristics.

Keywords: innovation; communication; cybersecurity; remote work; work organization; digital technologies; accounting data protection; information technologies; system innovations.

Отримано: 20 жовтня 2025 року
Прорецензовано: 25 жовтня 2025 року
Прийнято до друку: 18 грудня 2025 року