DOI: https://doi.org/10.25140/2411-5215-2025-2(42)-337-360
УДК 004.056:330.131.7:658.155:338.47:338.48
JEL Classification: O33; G32; G33; L92; Q16

Олена Вікторівна Шишкіна
доктор економічних наук, професор,
професор кафедри фінансів, банківської справи та страхування,
Національний університет «Чернігівська політехніка» (Чернігів, Україна)
E-mail: shyshkina.olena.v@gmail.com. **ORCID:** http://orcid.org/0000-0002-8946-1027
ResearcherID: F-3208-2014. **Scopus Author ID:** 58995081900

Тарас Тарасович Бойчук
аспірант
Національний університет «Чернігівська політехніка» (Чернігів, Україна)
E-mail: taras.boychuk.cv@ukr.net. **ORCID:** https://orcid.org/0009-0000-9073-8620

Дмитро Володимирович Євчук
аспірант
Національний університет «Чернігівська політехніка» (Чернігів, Україна)
E-mail: dimon.evchuk@gmail.com. **ORCID:** https://orcid.org/0009-0006-9585-638X

ВПЛИВ ЦИФРОВИХ ТЕХНОЛОГІЙ НА ФІНАНСОВИЙ РИЗИК-МЕНЕДЖМЕНТ ТА БЕЗПЕКУ ТРАНСПОРТНИХ І АГРАРНИХ ПІДПРИЄМСТВ

У статті досліджено багатогранний вплив цифрових технологій на фінансовий ризик-менеджмент та безпеку транспортних і аграрних підприємств України. Проаналізовано ключові цифрові технології, що впроваджуються в цих секторах, включаючи Інтернет речей, Великі дані (Big Data) та аналітику, штучний інтелект, хмарні обчислення та системи управління. Виявлено, що цифрові технології є каталізатором нових ризиків (ризики інвестицій *у технології, кіберризики тощо) і модифікатором традиційних (операційних, ринкових, кредитних та інших). Вивчено вплив цифровізації на безпеку підприємств. Визначено нові види загроз, такі як кібератаки на критичну інфраструктуру, витік та компрометація даних, несанкціонований доступ до систем управління, а також ризики, пов'язані з ланцюгом постачання програмного забезпечення. Підкреслено, що рівень кібербезпеки в обох галузях часто є недостатнім через брак інвестицій, кваліфікованих кадрів, застарілу інфраструктуру та низьку обізнаність персоналу. Узагальнено проблеми, виявлені у процесі аналізу, до яких віднесено недостатню інтеграцію управління новими ризиками в існуючі системи, фінансовий та кадровий дефіцит, відставання нормативно-правової бази, складність кількісної оцінки впливу кіберінцидентів, взаємозалежність систем, та посилення загроз в умовах воєнного часу. Сформульовано необхідність розробки та впровадження комплексного, інтегрованого підходу до фінансового ризик-менеджменту та забезпечення безпеки.*

Ключові слова: *цифрові технології; фінансовий ризик-менеджмент; цифровізація; транспортні підприємства; аграрні підприємства; кіберризики; безпека; кібербезпека,*
Табл.: 4. Бібл.: 14.

Постановка проблеми. Сучасний етап розвитку економіки характеризується стрімкою цифровою трансформацією, яка проникає в усі сфери діяльності, включаючи транспортний та аграрний сектори. Впровадження інноваційних цифрових технологій, таких як штучний інтелект (AI), великі дані (Big

Data), Інтернет речей (IoT), блокчейн, смартконтракти, хмарні обчислення відкриває нові можливості щодо підвищення ефективності, оптимізації процесів та ухвалення обґрунтованих рішень на підприємствах цих галузей.

Водночас цифровізація генерує нові виклики, які серед іншого пов'язані з фінансовими ризиками й безпекою. Кіберзагрози та необхідність забезпечення кібербезпеки критичної інфраструктури, залежність від функціонування складних технологічних систем, а також реалізація ризиків, пов'язаних з обробкою великих обсягів даних стають ключовими загрозами ефективному розвитку транспортних та аграрних підприємств.

Використання цифрових технологій підприємствами транспортної галузі дозволяє підвищити результативність управління автопарком, забезпечити моніторинг стану транспортних засобів, оптимізувати маршрути, запровадити безпілотні системи та інтелектуальні транспортні системи та реалізувати інші потреби. Варто зазначити, що неефективне управління фінансовими ризиками, пов'язаними з впровадженням і використанням цих технологій та недостатній рівень кібербезпеки можуть призвести до значних фінансових втрат, збоїв у роботі, аварій та навіть загрози життю людей.

Прогресивні підприємства аграрного сектору використовують цифрові технології для точного землеробства, моніторингу врожайності, управління ланцюгами поставок, прогнозування цін та погодних умов та інших процесів. Фінансові ризики в зазначеній галузі можуть бути пов'язані з інвестиціями в нові технології та зумовлені волатильністю ринків. При цьому кіберзагрози можуть спричинити втрату даних про врожайність, зрив посівних кампаній та згенерувати інші критичні наслідки.

З огляду на вищенаведене, необхідність глибокого розуміння взаємозв'язку між впровадженням цифрових технологій, управлінням фінансовими ризиками та забезпеченням безпеки транспортних і аграрних підприємств для підвищення їхньої стійкості, конкурентоздатності та сталого розвитку в умовах зростаючої цифрової економіки України набуває особливої актуальності в умовах сьогодення.

Аналіз останніх досліджень і публікацій. Аналіз сучасних досліджень, присвячених проблемі впливу цифрових технологій на фінансовий ризик-менеджмент і безпеку транспортних та аграрних підприємств, дозволяє стверджувати, що ця тематика набуває дедалі більшої актуальності в умовах цифрової трансформації економіки, посилення зовнішніх ризиків (у тому числі пов'язаними з військовими діями, кіберзагрозами, дестабілізацією логістичних ланцюгів тощо) та зростаючої потреби в забезпеченні сталого функціонування ключових галузей національного господарства.

Опрацювання результатів наукових робіт вітчизняних та іноземних учених дозволяють стверджувати, що зазначені дослідження охоплюють широке коло питань – від впровадження цифрових двійників і блокчейн-технологій до розвитку цифрової логістики, кіберзахисту фінансових операцій та

підвищення операційної безпеки підприємств. У центрі уваги науковців перебуває ідентифікація нових ризиків, що виникають у цифровому середовищі, пошук інструментів їхнього прогнозування та мінімізації, а також удосконалення механізмів стратегічного управління безпекою підприємствами аграрної і транспортної галузей.

Серед численних наукових робіт вважаємо доцільним зупинитись на здобутках окремих вітчизняних авторів і авторських колективів. Так, наприклад, колектив авторів на чолі з С. В. Коляденко досліджує концепцію смартпромисловості в аграрному секторі економіки в умовах цифровізації і визначає такі ключові компоненти аграрної смартпромисловості, як IoT, штучний інтелект, Big Data, хмарні технології і робототехніка та розглядає економічні переваги та виклики впровадження смарттехнологій в аграрному секторі [9].

А. М. Орел та, В. В. Дяченко хоча і акцентують основну увагу на банківських структурах, проте наголошують на важливості фінансової цифровізації, яка впливає на управління ризиками в аграрному секторі через кредитування, лізинг та страхування, звертаючи увагу на ризики кібератак, нестачу технічної експертизи та правову невизначеність [10].

В. А. Ковтун узагальнює особливості застосування інтелектуальних технологій загалом та аналітичних систем IT-технологій, зокрема, у галузі рослинництва та тваринництва та їх економічні наслідки [8]. Колективи авторів на чолі з Н. П. Юрчук [14] та Н. М. Горобець [7] розглядають питання розвитку цифрових технологій, у тому числі великих даних, у діяльності аграрних підприємств.

У галузі транспорту й логістики цікавими є напрацювання Ю. Попової та О. Чуприни [6], які наголошують на відновленні логістичних мереж із використанням цифрових технологій та пропонують розширення цифрового супроводження перевезень, автоматизацію маршрутів, впровадження IoT для контролю товарів та фінансових потоків.

Робота Богданюк І. В., Мандич С. М., які розглядаючи загрози безпеці підприємств у глобалізованому цифровому середовищі пропонують цифрову трансформацію системи охорони та управління ризиками на рівні логістичних об'єктів (елеватори, термінали, транспорт) [7].

Опрацьовані дослідження вітчизняних науковців демонструють високу актуальність впровадження цифрових технологій у фінансовий ризик-менеджмент і безпеку аграрних і транспортних підприємств. Серед ключових напрямів досліджень останніх років особливо виділяються такі напрямки: автоматизоване управління ризиками; цифрові моделі логістики; захист фінансових операцій; прозорість міжнародних ланцюгів; цифрова інфраструктура повоєнного відновлення.

Серед опрацьованих наукових робіт іноземних науковців вважаємо доцільним зупинитись на працях таких авторів. Т. Й. Мелессе, К. Франсіозі, В. Ді Паскуале та С. Ріємма досліджують використання цифрових двійників

у харчовому ланцюгу постачання. Доводять як ці технології дозволяють створити віртуальну модель реальних процесів агровиробництва для прогнозування, моделювання ризиків і оперативного реагування, що сприяє покращенню управління ризиками, зниженню втрат продукції, а також безпеці логістики та контролю фінансових потоків [4].

С. С. Дешмукх та С. К. Беті аналізують як цифрові інструменти впливають на розвиток агротехнологічних стартапів у країнах, що розвиваються, а також розглядають проблеми кібербезпеки, обмеженого фінансування, відсутності ІТ-інфраструктури. Цікавим з науково-практичного погляду є запропонована авторами інтеграція блокчейн-платформ і AI-рішень для покращення прозорості та керованості ризиками в агробізнесі [3].

Л. Чжоу детально аналізує використання блокчейн-технологій у бухгалтерському обліку, зокрема у сільському господарстві та логістиці. При цьому акцентує увагу на забезпеченні прозорості, запобіганні маніпуляціям із фінансовими даними, зниженні ризиків шахрайства та створенні безпечної цифрової архітектури для ризик-менеджменту [5].

А. Алі розкриває практичні аспекти використання блокчейну в транспорті та агробізнесі – від відстеження товару до автоматичного виконання контрактів. Обґрунтовує, як ця технологія забезпечує зниження ризиків втрати інформації, покращення безпеки логістичних операцій та автоматизацію фінансових процедур, що підвищує стійкість підприємств [1].

Т. Бен Хассен, Х. Ель Білалі, Б. Дахер і С. Буркарт досліджують стійкість аграрних систем під впливом криз (зміни клімату, війна, пандемії). Автори наголошують, що цифрові рішення (IoT, платформи контролю поставок, мобільні додатки) суттєво зменшують ризики дестабілізації фінансових потоків і допомагають відновлювати безпеку агрологістичних систем у кризових умовах [2].

Опрацювання вищеназваних та інших наукових праць за означеною тематикою дозволяє не лише окреслити сучасні наукові пріоритети, а і сформувати базис для розробки практичних рекомендацій щодо підвищення фінансової стабільності та стійкості транспортно-логістичних і агровиробничих систем в умовах цифровізації.

Виділення недосліджених частин загальної проблеми. Незважаючи на зростаючий інтерес до цифрової трансформації, комплексне дослідження впливу цифрових технологій саме на фінансовий ризик-менеджмент та безпеку транспортних і аграрних підприємств в українському контексті залишається недостатньо вивченим. Існує потреба в систематизації знань про потенційні ризики та загрози, а також у розробці практичних рекомендацій щодо їхнього ефективного управління та забезпечення безпеки в умовах цифрової економіки, що зумовлює мету обраної теми дослідження.

Метою статті є комплексний аналіз впливу цифрових технологій на фінансовий ризик-менеджмент та безпеку транспортних і аграрних підприємств в Україні.

Виклад основного матеріалу. Досягнення поставленої мети зумовлює доцільність опрацювання теоретичних засад впливу цифрових технологій на фінансовий ризик-менеджмент з огляду на поглиблення розуміння складного та багатогранного впливу цифрових технологій на системи управління фінансовими ризиками та забезпечення безпеки сучасних підприємств, зокрема в транспортному та аграрному секторах, що, по суті, є першим етапом нашого дослідження.

Передусім необхідно чітко визначити, які саме цифрові технології є найбільш релевантними для транспортних та аграрних підприємств і як вони трансформують їхню діяльність. Базуючись на вивчення досвіду використання зазначеними компаніями цифрових новацій, вважаємо, що до ключових цифрових технологій, що мають значний вплив, належать Інтернет речей, Великі дані, штучний інтелект та машинне навчання, блокчейн, хмарні обчислення, а також мобільні технології та додатки.

Інтернет речей (IoT) впливає на моніторинг стану активів, оптимізацію процесів та збір великих обсягів даних. Прикладом застосування даної технології є мережа фізичних об'єктів (транспортних засобів, сільськогосподарської техніки, сенсорів на полях тощо), оснащених датчиками, програмним забезпеченням та іншими технологіями, що дозволяють їм обмінюватися даними.

Технологія *Великих даних (Big Data)* дозволяє збирати, зберігати та аналізувати надвеликі й різноманітні набори даних для виявлення закономірностей, трендів та прийняття обґрунтованих рішень і застосовується у практиці діяльності аграрних та транспортних компаній для прогнозування попиту, оптимізації маршрутів, аналізу врожайності тощо.

Штучний інтелект (AI) та *машинне навчання (ML***)** знаходить застосування в розробці комп'ютерних систем, здатних виконувати завдання, які зазвичай потребують людського інтелекту, наприклад, такі як розпізнавання образів, ухвалення рішень, прогнозування. На сьогодні така технологія використовується в автономних транспортних засобах, системах підтримки ухвалення рішень, діагностиці обладнання та інших процесах.

Технологія *блокчейн*, як децентралізована та розподілена база даних, що забезпечує прозорість, безпеку та незмінність транзакцій, може застосовуватися для управління ланцюгами поставок, відстеження походження продукції, здійснення безпечних фінансових операцій тощо.

Хмарні обчислення передбачають надання обчислювальних ресурсів (серверів, сховищ даних, програмного забезпечення) через інтернет та забезпечують гнучкість, масштабованість та зниження витрат на IT-інфраструктуру компаній.

Мобільні технології та додатки використовуються компаніями через застосування смартфонів та планшетів для доступу до інформації, управління процесами та комунікації між співробітниками.

Зазначимо, що розуміння специфіки застосування кожної з цих технологій у контексті транспортних та аграрних підприємств є критично важливим для подальшого аналізу їхнього складного та багатогранного впливу на системи управління фінансовими ризиками та забезпечення безпеки сучасних підприємств. Отже, більш глибоко це питання буде розкрито в процесі подальших етапів дослідження.

У сучасному економічному ландшафті цифрові технології не просто існують поруч із бізнес-процесами, вони глибоко вплітаються в операційну та фінансову діяльність підприємств, формуючи складну, динамічну мережу взаємозалежностей. Цей взаємозв'язок має подвійний характер: цифровізація одночасно є джерелом нових можливостей для управління ризиками та безпекою і водночас генератором абсолютно нових та посилених ризиків та загроз. Тож, на нашу думку, розуміння цієї динаміки є критично важливим для розробки ефективних стратегій.

Цифровізація не лише породжує нові види фінансових ризиків, але й суттєво трансформує наявні.

Серед *нових* фінансових ризиків, які породжує цифровізація, вважаємо доцільним виділити технологічні інвестиційні ризики, кіберфінансові ризики та ризики, пов'язані з обробкою даних.

Технологічні інвестиційні ризики генеруються значними капітальними витратами на цифрові рішення (наприклад, системи точного землеробства, складні системи управління господарством (FMS), AI-алгоритми), які можуть не принести очікуваної економічної віддачі через значну сукупність причин, як то: швидке застарівання технології, невдалий вибір постачальника, проблеми з інтеграцією, неефективне використання технології через брак кваліфікації персоналу. Такі інвестиції можуть призвести до заморожування капіталу та зниження ліквідності, генеруючи при цьому ще ризики неплатоспроможності, фінансової стійкості, втрати прибутковості та інші.

Кіберфінансові ризики пов'язані з прямими та непрямими фінансовими втратами, спричиненими кіберінцидентами. До прямих витрат можна віднести: викрадення грошових коштів з рахунків, вимогу викупу за зашифровані дані чи розблокування систем, збитки від фішингових атак, шахрайство з використанням фальшивих цифрових транзакцій. Непрямі втрати включають: втрати доходу від простоїв бізнесу, витрати на відновлення систем та даних, юридичні витрати та штрафи за порушення конфіденційності даних, а також значні репутаційні збитки, що призводять до втрати клієнтів та інвесторів тощо.

Ризики, пов'язані з обробкою даних, є достатньо значними для економічних суб'єктів. Величезні обсяги даних, що генеруються цифровими технологіями, є, з одного боку, цінним активом, а з іншого – джерелом ризику. Наявність недостовірних, неповних, спотворених або скомпрометованих даних є причиною ухвалення помилкових управлінських рішень (наприклад, неточний прогноз врожайності, неоптимальна логістика), що прямо впливає на фінансові показники. Крім того, компрометація конфіденційних даних веде до фінансових штрафів та зниження рівня довіри, що продукує додаткові ризики (наприклад, операційні (зупинка виробництва/надання послуг, нездатність виконувати зобов'язання, підвищення витрат тощо), фінансові, репутаційні, юридичні тощо).

Серед *традиційних* фінансових ризиків, які зазнають суттєвих трансформацій в умовах цифровізації вважаємо доцільним відмітити операційні, ринкові і кредитні.

Природа *операційних* ризиків в умовах цифровізації кардинально змінюється. Зокрема, з одного боку, автоматизація може знизити ризик людських помилок. З іншого боку, залежність від складних програмних та апаратних систем означає, що їхні збої, баги або кібератаки можуть мати значно більші та каскадні фінансові наслідки, ніж традиційні операційні збої. Наприклад, збій у системі управління автопарком може паралізувати сотні одиниць транспорту, спричинивши мільйонні збитки від простою та штрафів.

Великі дані та AI-аналітика можуть покращити прогнозування ринкових цін на паливо, сільськогосподарську продукцію, але водночас залежність від цих прогнозів створює *ринковий* ризик, особливо якщо базові дані скомпрометовані або алгоритми працюють некоректно.

У контексті *кредитних* ризиків зауважимо, що хоча цифровізація може покращити скоринг та оцінку кредитоспроможності, але й залежність від автоматизованих систем може приховати певні нюанси та/або стати мішенню для кібершахрайства, що підвищить рівень цих ризиків.

В умовах цифровізації забезпечення кібербезпеки перестає бути виключно технічною функцією і перетворюється на невід'ємну складову фінансового ризик-менеджменту. Суб'єкти підприємницької діяльності задля запобігання потенційно катастрофічним фінансовим втратам мають інвестувати у створення ефективних систем кіберзахисту (антивіруси, системи виявлення вторгнень, шифрування, резервне копіювання тощо), які мінімізують ризик успішних кібератак, а отже, пов'язаних із ними фінансових втрат. Одночасно фінансові менеджери повинні інтегрувати оцінку кіберризиків у загальну систему управління ризиками, яка, серед іншого, включає кількісну оцінку потенційних збитків від кіберінцидентів (втрачений дохід, витрати на відновлення, штрафи, репутаційні збитки) для адекватного формування бюджетів на кібербезпеку та створення резервів.

У галузях із критичною інфраструктурою, до яких доцільно віднести транспорт та сільське господарство, безпека має прямий вплив на фінансову стійкість, а цифрові технології тільки посилюють цей зв'язок. Зокрема, відмова цифрових систем управління рухом, логістикою, або сільськогосподарською технікою через кібератаку, програмну помилку чи технічний збій призводить до негайної зупинки операцій наслідком чого є втрачений дохід через неможливість надання послуг чи виробництва продукції, штрафи за невиконання контрактних зобов'язань, додаткові витрати на ремонт, відновлення, позапланові закупівлі, а також збитки від псування продукції (наприклад, через збій системи моніторингу в сховищі зерна). Крім того, важливо зазначити, що сучасні транспортні та аграрні підприємства все частіше інтегрують свої інформаційні системи (облік, фінанси, системи управління взаємовідносинами з клієнтами (CRM)) з операційними технологіями (системи управління поїздами, комбайнами, іригацією тощо). Така інтеграція підвищує ефективність, але і створює нові ризики. Наприклад, вразливість в IT-системі може бути використана для компрометації OT-систем, які представлені обладнанням та програмним забезпеченням, яке застосовується для моніторингу та управління фізичними процесами, що має прямі фізичні та фінансові наслідки.

Таким чином, цифрові технології створюють екосистему в якій тісно переплітаються фінансові ризики та безпека. Нехтування питаннями безпеки неминуче призведе до зростання фінансових ризиків, водночас ефективне управління кібер- та операційною безпекою стає фундаментом для фінансової стійкості та сталого розвитку підприємств. Проте така взаємозалежність вимагає від керівництва підприємств комплексного та проактивного підходу до ризик-менеджменту.

Наступний етап нашого дослідження в контексті досягнення поставленої мети передбачає аналіз сучасного стану впровадження цифрових технологій, фінансового ризик-менеджменту та безпеки на транспортних та аграрних підприємствах України. метою цього етапу є виявлення рівня проникнення цифрових технологій, оцінка існуючих практик ризик-менеджменту та безпеки, а також ідентифікація ключових проблем й викликів, що стоять перед зазначеними галузями в умовах стрімких технологічних змін.

Аналіз основних цифрових технологій, що використовуються на транспортних підприємствах. Український транспортний сектор, попри низку викликів, активно впроваджує цифрові рішення для підвищення ефективності, конкурентоздатності та безпеки. Основні напрями використання цифрових технологій включають: системи управління автопарком і логістикою, Великі дані та аналітика, Інтернет речей та сенсори, штучний інтелект та машинне навчання, хмарні обчислення, мобільні додатки та цифрові платформи (табл. 1).

Таблиця 1

Огляд впровадження та впливу цифрових технологій на транспортні підприємства України

Цифрова технологія	**Основні напрямки використання на транспортних підприємствах**	**Поточний стан впровадження в Україні (загальний опис)**	**Позитивний вплив**	**Потенційні виклики та ризики, пов'язані з впровадженням цифрової технології**
1	2	3	4	5
Системи управління автопарком та логістикою (Fleet Management Systems - FMS, Transportation Management Systems - TMS)	GPS-трекінг та моніторинг місцезнаходження; оптимізація маршрутів; контроль витрат пального; моніторинг стилю водіння та стану ТЗ; управління замовленнями та доставками; електронний документообіг.	Широко впроваджені як великими логістичними операторами та вантажними перевізниками, так і багатьма середніми підприємствами. Ступінь інтеграції та функціональності варіюється. Активне використання для підвищення ефективності та контролю.	Оптимізація маршрутів та графіків руху, скорочення часу доставки; значне зниження витрат на паливо та технічне обслуговування; підвищення безпеки водіння та зменшення кількості ДТП; покращення контролю за активами; підвищення прозорості та якості обслуговування клієнтів; швидке реагування на нештатні ситуації.	Залежність від безперебійного зв'язку (GPS, мобільний інтернет); ризики кібератак на системи (зміна маршрутів, викрадення даних, виведення з ладу); потреба у значних початкових інвестиціях та навчанні персоналу; ризики витоку конфіденційної логістичної інформації; складність інтеграції з іншими IT-системами підприємства; збої програмного забезпечення, що можуть паралізувати операції.
Інтернет речей (IoT) та сенсори	GPS-трекінг, моніторинг стану ТЗ/інфраструктури, контроль вантажу (температура, вологість)	Активно впроваджується великими та середніми компаніями, переважно у сфері автотранспорту та логістики.	Оптимізація маршрутів, зниження витрат на паливо, предикативне обслуговування, підвищення безпеки перевезень.	Залежність від безперебійного зв'язку, ризики цілісності даних, вразливості кібербезпеки пристроїв, висока вартість початкових інвестицій.
Великі дані (Big Data) та аналітика	Прогнозування попиту, оптимізація транспортних потоків, аналіз ефективності, предикативне обслуговування.	Використовується переважно великими гравцями. Потенціал реалізується не повною мірою через брак інфраструктури та фахівців.	Підвищення ефективності прийняття рішень, зниження операційних витрат, покращення планування, виявлення прихованих закономірностей.	Ризики конфіденційності даних, потреба у значних інвестиціях в IT-інфраструктуру, брак кваліфікованих аналітиків, складність інтерпретації результатів.

Закінчення табл. 1

1	2	3	4	5
Штучний інтелект (AI) та машинне навчання (ML)	Автоматизація диспетчерських функцій, оптимізація ресурсів, предикативна аналітика, експерименти з автономними системами.	На початкових етапах впровадження, переважно в пілотних проєктах або для специфічних завдань у великих компаніях.	Автоматизація рутинних операцій, підвищення точності прогнозування, оптимізація логістичних процесів, покращення клієнтського сервісу.	Висока вартість розробки/впровадження, етичні та юридичні питання, ризики "чорного ящика" (непрозорість прийняття рішень), залежність від якості даних.
Блокчейн	Управління ланцюгами поставок, електронний документообіг, відстеження вантажів, безпечні транзакції.	Одиничні пілотні проєкти, низький рівень поширення через складність та відсутність широкої екосистеми.	Підвищення прозорості та довіри, зниження ризиків шахрайства, спрощення документообігу, посилення безпеки транзакцій.	Складність інтеграції з існуючими системами, високі початкові витрати, проблеми масштабованості, регуляторна невизначеність.
Хмарні обчислення	Хостинг IT-систем (FMS, TMS), зберігання даних, доступ до програмного забезпечення як послуги (SaaS).	Широко впроваджується, особливо серед малих та середніх підприємств, завдяки доступності та гнучкості.	Зниження капітальних витрат на IT, гнучкість, масштабованість, доступність з будь-якого місця, покращена співпраця.	Залежність від провайдера хмарних послуг, ризики безпеки даних (для SaaS), необхідність забезпечення надійного інтернет-з'єднання, юридичні питання щодо зберігання даних.
Мобільні технології та цифрові платформи	Мобільні додатки для водіїв/клієнтів, онлайн-платформи для замовлення перевезень, електронний документообіг.	Дуже широке впровадження, є стандартом у багатьох логістичних компаніях та для агрегаторів.	Покращення комунікації, оперативність, підвищення зручності для клієнтів, спрощення взаємодії, оптимізація останньої милі.	Ризики кібербезпеки мобільних пристроїв, залежність від мобільного зв'язку, потреба в постійних оновленнях ПЗ, ризики фішингу.

Джерело: розроблено авторами на основі [1-2, 5, 10-14].

Системи управління автопарком та логістикою (FMS та *TMS*) є найпоширенішими цифровими рішеннями, що дозволяють відстежувати місцезнаходження транспортних засобів у режимі реального часу (GPS-трекінг), оптимізувати маршрути, контролювати витрати пального, моніторити стиль водіння та стан транспортних засобів, що загалом сприяє зниженню операційних витрат і підвищенню ефективності доставки. В Україні такі системи активно впроваджують як великі логістичні компанії, так і малі перевізники.

Великі дані (Big Data) та аналітика використовуються для збору та аналізу величезних обсягів даних із різних джерел (датчики, GPS-трекери, операційні системи, погодні дані) та для прогнозування попиту, оптимізації транспортних потоків, виявлення «вузьких місць» у логістичних ланцюгах, а також для предикативного обслуговування транспортних засобів. Однак повноцінне використання потенціалу Big Data в Україні загалом та в транспортних компаніях зокрема часто обмежене відсутністю необхідної інфраструктури та кваліфікованих кадрів.

Інтернет речей (IoT) та сенсори дозволяють збирати дані про стан обладнання, якість перевезення вантажу (температура, вологість), завантаженість маршрутів. IoT-пристрої, інтегровані в транспортні засоби та інфраструктуру (наприклад, розумні дороги, портові термінали, сприяють підвищенню операційної ефективності та безпеки (наприклад, датчики на залізничних коліях можуть попереджати про знос або деформації колії).

Штучний інтелект (AI) та машинне навчання (ML) застосовуються для складного прогнозування (наприклад, заторів, часу прибуття, попиту на перевезення), автоматизації диспетчерських функцій, розпізнавання об'єктів для безпілотних систем (хоча їхнє повноцінне впровадження в Україні ще на ранніх стадіях) та оптимізації ресурсів. Крім того, сьогодні транспортні компанії активно експериментують з чат-ботами для клієнтської підтримки та використовують системи оптимізації складських запасів.

Хмарні обчислення, зокрема, надання програмного забезпечення та інфраструктури як сервісу (наприклад, SaaS - модель, де програмне забезпечення надається як послуга через інтернет та IaaS - модель, де надається доступ до основної інфраструктури, такої як віртуальні машини та сховища, для запуску власних додатків) дозволяє транспортним підприємствам знижувати капітальні витрати на IT, забезпечувати гнучкість та масштабованість систем. Крам того, багато FMS та TMS працюють на хмарних платформах, що особливо актуально для малих та середніх підприємств, які не мають ресурсів для побудови власної IT-інфраструктури.

Використання *мобільних додатків* для водіїв, диспетчерів та клієнтів, а також інтеграція в цифрові логістичні *платформи* (наприклад, для пошуку вантажів або оптимізації завантаження транспорту) спрощує комунікацію, прискорює обмін документами та підвищує прозорість ланцюгів поставок.

Незважаючи на активне впровадження, ступінь інтеграції та зрілість цих технологій може суттєво відрізнятися між великими державними підприємствами («Укрзалізниця», морські порти) та приватними логістичними компаніями, а також залежить від виду транспорту (автомобільний, залізничний, морський, авіаційний).

Проблеми, ризики і загрози безпеці підприємств транспортної галузі. Проведений авторами аналіз дозволив виділити такі ключові проблеми і виклики з якими стикається транспортна галузь в умовах цифровізації: недостатня інтеграція управління новими ризиками, брак інвестицій та кваліфікованих кадрів, недосконала нормативно-правова база, складність оцінки впливу кібератак або збоїв цифрових систем на потенційні фінансові втрати, взаємозалежність цифрових систем (збій в одній системі може призвести до руйнівних наслідків для всієї інфраструктури), геополітичні і воєнні ризики, недостатня обізнаність персоналу з правилами кібергігієни, низька цифрова грамотність та опір змінам (табл. 2)

Аналіз основних цифрових технологій, що використовуються на аграрних підприємствах. Аграрний сектор України є одним із локомотивів економіки, і його цифрова трансформація є ключовим фактором підвищення конкурентоспроможності та ефективності національної економіки. Впровадження інноваційних технологій дозволяє оптимізувати виробничі процеси, знизити витрати, підвищити врожайність та якість продукції. Однак, як і в транспортній галузі, ця трансформація породжує нові виклики у сфері фінансових ризиків та безпеки.

Українські аграрні підприємства, особливо великі та середні агрохолдинги, активно впроваджують цифрові рішення, що дозволяють перейти до так званого «точного землеробства» та «розумного фермерства». Серед цифрових технологій вважаємо доцільним виділити наступні: системи точного землеробства (GPS-навігація, карти врожайності, диференційоване внесення), дрони та супутниковий моніторинг, Інтернет речей (IoT) та сенсорні мережі, системи управління агробізнесом (ERP), Великі дані та аналітика, хмарні обчислення та мобільні додатки (табл. 3).

Основою цифровізації в агросекторі є *системи точного землеробства (GPS-навігація, карти врожайності, диференційоване внесення),* які дозволяють точно керувати сільськогосподарською технікою, уникати перекриттів та пропусків. Карти врожайності, засновані на супутникових знімках або даних з комбайнів, допомагають оцінювати продуктивність різних ділянок землі. Системи диференційованого внесення дозволяють вносити добрива та засоби захисту рослин саме там і в тій кількості, де це необхідно, оптимізуючи витрати та зменшуючи навантаження на ґрунт.

Світова практика має досвід використання *безпілотних літальних апаратів (БПЛА)* та здійснення *супутникових знімків* для оперативного моніторингу стану посівів, виявлення проблемних ділянок (нестача вологи, шкідники, хвороби), оцінки якості виконання сільськогосподарських робіт, а також для контролю за станом іригаційних систем, що значно підвищує швидкість та точність отримання інформації.

Таблиця 2

Проблеми та виклики у сфері фінансового ризик-менеджменту та безпеки транспортних підприємств України в контексті цифровізації

Категорія проблеми/виклику	Деталізація проблеми / виклику	Вплив на фінансовий ризик-менеджмент	Вплив на безпеку підприємств (кібер- та операційну)
Недостатня інтеграція управління новими ризиками	Існуючі системи ризик-менеджменту не завжди охоплюють технологічні, кібернетичні та дані-пов'язані ризики.	Недооцінка потенційних фінансових втрат, відсутність адекватних резервів, неефективне розподілення капіталу.	Прогалини в захисті, висока вразливість до нових типів загроз, низька спроможність до швидкого реагування на інциденти.
Брак інвестицій та кваліфікованих кадрів	Обмежені фінансові ресурси для ІТ та кібербезпеки; дефіцит фахівців.	Збільшення ймовірності фінансових втрат від кібератак, низька ефективність впровадження нових технологій, втрата конкурентоспроможності.	Низький рівень кіберзахисту, неможливість повноцінного впровадження сучасних систем безпеки, підвищена вразливість до атак, людський фактор як джерело ризиків.
Недосконала нормативно-правова база	Чинне законодавство не відповідає темпам розвитку цифрових технологій та кіберзагроз.	Ризики штрафів за недотримання нових стандартів (наприклад, GDPR-подібних), юридична невизначеність щодо відповідальності за кіберінциденти.	Відсутність чітких вимог до кіберзахисту, складнощі в розслідуванні кіберзлочинів, відсутність механізмів обміну інформацією про загрози.
Складність кількісної оцінки впливу	Важко оцінити потенційні фінансові втрати від непередбачуваних кібератак чи збоїв цифрових систем.	Неможливість адекватного планування бюджетів на кібербезпеку, труднощі у розрахунку страхових покриттів, проблеми з обґрунтуванням інвестицій у захист.	Нечітке розуміння критичності різних систем, відсутність метрик ефективності заходів безпеки, складність розробки ефективних планів реагування.
Взаємозалежність систем	Висока інтеграція цифрових систем робить підприємства вразливими до каскадних відмов.	Значні фінансові втрати через зупинку операцій (простій, штрафи, втрата доходу), репутаційні ризики, зростання витрат на відновлення.	Широке розповсюдження збоїв або атак, ускладнення локалізації інцидентів, підвищений ризик системних відмов, ускладнення управління кризовими ситуаціями.
Людський фактор	Недостатня обізнаність персоналу з кібергігієною, низька цифрова грамотність, опір змінам.	Фінансові втрати через внутрішні загрози (наприклад, витік даних, дії інсайдерів), штрафи за порушення регуляторних норм, пов'язані з даними.	Збільшення кількості кіберінцидентів через помилки користувачів (фішинг, несанкціоноване використання ПЗ), труднощі з впровадженням нових політик безпеки.
Геополітичні та воєнні ризики	Транспортна інфраструктура є пріоритетною ціллю в умовах війни і посилення кіберзагроз	Прямі фінансові втрати від руйнувань, зростання витрат на підвищення стійкості, складнощі в залученні інвестицій, підвищені страхові премії.	Зростання інтенсивності та складності кібератак, підвищена потреба в постійному моніторингу та швидкому реагуванні, ризики фізичного знищення об'єктів інфраструктури.

Джерело: розроблено авторами на основі [1-2, 5, 10-14].

Таблиця 3

Огляд впровадження та впливу цифрових технологій на аграрних підприємствах України

Цифрова технологія	**Основні напрямки використання на аграрних підприємствах**	**Поточний стан впровадження в Україні (загальний опис)**	**Позитивний вплив**	**Потенційні виклики та ризики, пов'язані з впровадженням**
1	2	3	4	5
Системи точного землеробства (GPS, карти врожайності, диференційоване внесення)	Точне керування технікою, оптимізація посівів та обробки, внесення ресурсів за потребою.	Широко впроваджується великими та середніми агрохолдингами, у меншому ступені – малими фермерськими господарствами.	Оптимізація витрат на паливо, насіння, добрива, ЗЗР; підвищення врожайності; зниження екологічного навантаження.	Висока вартість обладнання, потреба у кваліфікованих кадрах, залежність від GPS-сигналу та супутникових даних, ризики помилок у даних.
Дрони та супутниковий моніторинг	Моніторинг стану посівів, виявлення проблемних ділянок (шкідники, хвороби), контроль за виконанням робіт.	Активно використовується для оперативного контролю та аналізу на середніх та великих підприємствах.	Оперативне виявлення проблем, швидке реагування, економія ресурсів на обробку, збір великих обсягів просторових даних.	Висока вартість дронів/сервісів, потреба у спеціальному ПЗ та навичках, ризики конфіденційності даних, вразливості кібербезпеки, залежність від погодних умов.
Інтернет речей (IoT) та сенсорні мережі	Датчики вологості ґрунту, температури повітря, моніторинг тварин, розумні сховища.	Розвивається, але ще не має повсюдного поширення. Найбільш активне впровадження в іригації та тваринництві.	Оптимізація використання води та добрив, покращення умов утримання тварин, зниження втрат врожаю при зберіганні, підвищення точності рішень.	Складність встановлення та обслуговування, висока вартість сенсорів, ризики відмов обладнання, вразливості мереж та пристроїв, потреба у надійному зв'язку.

Закінчення табл. 3

1	2	3	4	5
Системи управління агробізнесом (ERP)	Бухгалтерський облік, управління складом, логістикою, персоналом, виробниче планування.	Впроваджені переважно у великих агрохолдингах; малі та середні підприємства використовують спрощені рішення.	Комплексна автоматизація процесів, інтеграція даних, підвищення прозорості та контролю, покращення управлінських рішень, оптимізація ресурсів.	Висока вартість впровадження та підтримки, складність інтеграції, потреба в перенавчанні персоналу, ризики витоку або втрати критичних даних, залежність від розробника.
Великі дані (Big Data) та аналітика	Прогнозування врожайності, оптимізація стратегій продажів, аналіз ринкових цін, моделювання кліматичних ризиків.	На початковому етапі розвитку, використовується переважно великими агрохолдингами для стратегічного планування.	Зниження ризиків від волатильності ринків та кліматичних змін, підвищення точності прогнозів, виявлення прихованих закономірностей, оптимізація бізнес-моделей.	Потреба у значних інвестиціях в інфраструктуру та фахівців, ризики конфіденційності даних, складність верифікації та інтерпретації великих обсягів даних.
Хмарні обчислення та мобільні додатки	Доступ до даних та платформ, управління технікою, комунікація, електронний документообіг.	Широко впроваджується як доступний та гнучкий інструмент для різних рівнів підприємств.	Гнучкість та масштабованість, зниження капітальних витрат на IT, доступність інформації з будь-якої точки, покращена співпраця та оперативність.	Залежність від провайдера хмарних послуг, ризики безпеки даних у хмарі, необхідність стабільного інтернет-з'єднання, ризики фішингу та злому мобільних пристроїв.

Джерело: розроблено авторами на основі [1, 3-5, 7-14].

Технологія *IoT та сенсорні мережі* реалізуються у датчиках вологості ґрунту, температури повітря, інтенсивності сонячного світла, рівня pH, стану здоров'я тварин (у тваринництві) дозволяють збирати дані в реальному часі, що серед іншого дозволяє оптимізувати полив, внесення добрив, годівлі тварин, моніторинг мікроклімату в теплицях тощо.

Системи управління агробізнесом (ERP) дозволяють автоматизувати бухгалтерський облік, управління персоналом, складом, логістикою, виробничим плануванням та звітністю. Крім того, вони дають можливість консолідувати дані з різних підрозділів підприємства та покращити управлінські рішення.

Big Data аналітика дозволяє аграрним підприємствам прогнозувати врожайність, оптимізувати стратегії продажів, мінімізувати ризики, пов'язані з кліматичними змінами, та приймати більш виважені інвестиційні рішення.

Хмарні обчислення та мобільні додатки на сьогодні широко використовуються для доступу до даних та аналітичних платформ з будь-якої точки, а також для роботи з мобільними додатками для управління технікою, контролю робіт, оперативного зв'язку з агрономами та механізаторами, що забезпечує гнучкість та оперативність в управлінні.

Зауважимо, що впровадження цих технологій є нерівномірним: великі агрохолдинги демонструють високий рівень цифровізації, тоді як малі та середні фермерські господарства часто стикаються з фінансовими та технічними обмеженнями, що негативно позначається на результативності їх діяльності і породжує додаткові ризики і загрози економічній безпеці.

Проблеми, ризики і загрози безпеці підприємств аграрної галузі. До основних викликів і загроз безпеці вважаємо доцільним віднести: недостатнє усвідомлення та оцінка нових ризиків, дефіцит фінансових ресурсів та інфраструктури, нестача кваліфікованих IT-фахівців, агрономів, які володіють цифровими компетенціями, та спеціалістів з кібербезпеки, проблеми з інтеграцією різних цифрових систем від різних постачальників, правові та регуляторні прогалини, вплив воєнних дій, надійність даних та систем (табл. 4).

У таблицях 2 і 4 узагальнено вплив проблем і викликів, які відчувають транспортні та аграрні підприємства в умовах цифровізації та встановлено як цифрова трансформація впливає на кібербезпеку та операційну безпеку транспортних та аграрних підприємств України. Це дає підстави проаналізувати нові види загроз безпеці, пов’язаних з цифровою трансформацією, оцінити вплив цифрових технологій на операційну безпеку підприємства та визначити фактори, що впливають на рівень безпеки підприємств.

Впровадження IoT, AI, Big Data, хмарних обчислень та інших цифрових рішень породжує абсолютно нові види загроз, які раніше були нерелевантними або менш значущими, у тому числі: кібератаки на критичну інфраструктуру, витік та компрометація даних, несанкціонований доступ до систем управління, ризики, пов’язані із ланцюгом постачання програмного забезпечення та послуг, соціальна інженерія та фішинг.

Таблиця 4

Проблеми та виклики у сфері фінансового ризик-менеджменту та безпеки аграрних підприємств України в контексті цифровізації

Категорія проблеми/виклику	**Деталізація проблеми / виклику**	**Вплив на фінансовий ризик-менеджмент**	**Вплив на безпеку підприємств (кібер- та операційну)**
1	2	3	4
Недостатнє усвідомлення та оцінка нових ризиків	Фокус на традиційних агроризиках, недооцінка кібернетичних та технологічних фінансових ризиків.	Неадекватне планування бюджетів на безпеку, відсутність резервів для компенсації втрат від нових ризиків, неефективний розподіл капіталу.	Прогалини у стратегії безпеки, зростання вразливості до неочікуваних загроз, відсутність превентивних заходів, низька готовність до кризових ситуацій.
Дефіцит фінансових ресурсів та інфраструктури	Висока вартість цифрових рішень та необхідність модернізації IT-інфраструктури.	Обмеження в інвестиціях у передові технології, що знижує конкурентоспроможність; зростання операційних витрат через застарілі системи, підвищені ризики збитків від збоїв.	Неможливість впровадження сучасних систем кіберзахисту; використання застарілих систем з відомими вразливостями; низька стійкість до зовнішніх і внутрішніх загроз.
Кадровий голод	Нестача кваліфікованих IT-фахівців, агрономів з цифровими навичками, спеціалістів з кібербезпеки.	Неефективне використання інвестицій у технології, помилки в управлінні даними, що можуть призвести до фінансових втрат, труднощі з аналізом ринкових даних.	Людський фактор як основна вразливість (фішинг, несанкціоновані дії), неефективне впровадження політик безпеки, проблеми з технічною підтримкою систем, зниження операційної надійності.
Складність інтеграції та сумісності	Проблеми інтеграції різнорідних цифрових систем, "інформаційні силоси".	Неповний облік даних для фінансового аналізу, дублювання інформації, що призводить до неефективних рішень та фінансових втрат, труднощі у впровадженні комплексних систем ризик-менеджменту.	Створення нових точок вразливості на стиках систем, складність централізованого моніторингу безпеки, труднощі в забезпеченні цілісності та узгодженості даних, ускладнення реагування на інциденти.

Закінчення табл. 4

1	2	3	4
Правові та регуляторні прогалини	Відсутність чітких нормативних актів щодо захисту аграрних даних, відповідальності за кіберінциденти.	Ризики судових позовів та штрафів через неврегульовані питання, юридична невизначеність щодо власності та використання даних, що може впливати на вартість активів.	Нечіткі вимоги до кіберзахисту критичної агроінфраструктури, труднощі у співпраці з правоохоронними органами при розслідуванні кіберзлочинів, відсутність стимулів для впровадження високих стандартів безпеки.
Вплив воєнних дій	Зростання інтенсивності та складності кібератак, націлених на критичну агроінфраструктуру; фізичні руйнування.	Прямі та непрямі фінансові втрати від кібератак (викуп, простій), втрати врожаю та активів через фізичні руйнування, зростання витрат на забезпечення безпеки та відновлення.	Збільшення ризиків порушення цілісності та доступності даних та систем, загроза саботажу та диверсій через кіберпростір, підвищена потреба у стійкості та планах безперервності бізнесу.
Надійність даних та систем	Забезпечення цілісності, доступності та конфіденційності аграрних даних.	Фінансові втрати від неправильних агрономічних рішень через невірні дані, збитки від зупинки виробництва через збій систем управління, втрата конкурентних переваг через витік даних.	Ризик компрометації критично важливих даних, що впливає на прийняття рішень та репутацію; загроза операційним збоям, якщо системи управління залежать від ненадійних даних або програм.

Джерело: розроблено авторами на основі [1, 3-5, 7-14].

354

Транспортні (залізничні системи, портові термінали, аеропорти, системи управління дорожнім рухом) та аграрні (великі агрохолдинги, іригаційні системи, елеватори) об'єкти все частіше класифікуються як критична інфраструктура, що робить їх привабливими мішенями для цілеспрямованих кібератак з боку хакерів та / або терористичних груп. Метою таких атак може бути різною (саботаж, шпигунство, дестабілізація), однак такі дії можуть спричинити суттєві негативні фінансові, репутаційні та інші наслідки

Великі обсяги даних, що збираються та обробляються (інформація про маршрути, вантажі, клієнтів, постачальників, фінансові показники, дані про ґрунти, посіви, тварин), стають надзвичайно цінними, а їх втрата та або компрометація – є джерелом збитків і можливої втрати прибутку / доходу / капіталу, як у коротко-, так і в середньо- і довгостроковій перспективі.

При цьому несанкціонований доступ до цих даних може призвести до розголошення комерційної таємниці, персональних даних, що тягне за собою репутаційні збитки, штрафи та втрату довіри клієнтів, а у песимістичному сценарії – може паралізувати роботу підприємств.

В умовах цифровізації підприємства всіх видів діяльності все більше залежать від зовнішніх постачальників програмного забезпечення, хмарних сервісів, IoT-пристроїв. Вразливість у програмному забезпеченні або системі безпеки постачальника створити «каскадні» ризики, що позначиться на діяльності всіх залежних від такого постачальника підприємств.

Зловмисники використовують цифрові канали (електронна пошта, месенджери, соціальні мережі) для маніпулювання персоналом з метою отримання конфіденційної інформації або доступу до систем управління, а складність цифрових систем та швидкий потік інформації створюють нові можливості для таких атак. З огляду на це ризики пов'язані із соціальною інженерією і фішінгом посилені цифровізацією, потребують особливої уваги.

Цифрові технології кардинально змінюють операційні процеси, що має як позитивний, так і негативний вплив на операційну безпеку.

Позитивний вплив (посилення операційної безпеки) проявляється у:

– підвищенні точності та зниження впливу людського фактора (автоматизовані системи (автопілоти, точне землеробство) зменшують імовірність помилок, спричинених втомою або неуважністю персоналу);

– ранньому виявленні несправностей (предикативному обслуговуванні) (зокрема, IoT-сенсори та аналітика дозволяють моніторити стан обладнання в реальному часі, прогнозувати поломки та проводити обслуговування до виникнення критичної ситуації, що зменшує ризик аварій, простоїв та підвищує надійність);

– оптимізації та контролі процесів, котрі забезпечують прозорість та можливість швидкого реагування на відхилення, що знижує операційні ризики;

– покращенні умов праці та безпеки персоналу за рахунок автоматизації небезпечних робіт (наприклад, використання дронів замість обходу полів), моніторинг стану водіїв/операторів знижує ризик травматизму та нещасних випадків).

Негативний вплив (створення нових операційних ризиків) знаходить відображення у:

– залежності від технологій та їхній складності (чим складніша система, тим важче ідентифікувати причину збою та відновити роботу);

– неправильних або спотворених даних з сенсорів чи інших джерел, які можуть призвести до хибних рішень автоматизованих систем, що матиме прямі негативні наслідки для операцій (наприклад, неправильне внесення добрив, хибне перемикання стрілок залізничних колій тощо).

– збільшення кількості точок входу для атак, оскільки кожен новий IoT-пристрій, сенсор або елемент цифрової інфраструктури стає потенційною точкою входу для кібератаки, яка, у свою чергу, може спричинити операційний збій;

– недостатній підготовці персоналу до роботи з новими технологіями, ігноруванні правил безпеки, помилках при налаштуванні або експлуатації цифрових систем, що може стати причиною серйозних операційних інцидентів;

– взаємопов’язаності цифрових систем, яка означає, що збій в одній підсистемі може спровокувати ланцюгову реакцію та призвести до відмови всієї операційної системи.

Рівень безпеки транспортних та аграрних підприємств в умовах цифрової трансформації визначається комплексом взаємопов’язаних факторів, до яких вважаємо доцільним віднести наступні:

– рівень інвестицій у кібербезпеку (системи захисту, навчання персоналу, регулярні аудити та оновлення інфраструктури);

– якість та зрілість системи управління кібербезпекою (CSMS), що передбачає наявність чітких політик, процедур, стандартів (наприклад, ISO 27001), а також регулярних оцінок ризиків, планів реагування на інциденти та відновлення після них.

– рівень знань працівників щодо загроз кібербезпеки, правил безпечної роботи з цифровими системами, вміння розпізнавати підозрілі дії (фішинг, соціальна інженерія);

– складність та інтегрованість IT-інфраструктури та її здатність до забезпечення цілісного захисту;

– наявність планів безперервності бізнесу та відновлення після катастроф;.

– наявність чітких законодавчих вимог до кібербезпеки критичної інфраструктури, механізмів обміну інформацією про загрози, програм підтримки підприємств у сфері кіберзахисту;

– зростання кількості та складності кібератак, пов'язаних з війною, спрямованих на стратегічні галузі, що вимагає підвищеної пильності та інвестицій у захист;

– перевірка безпеки та надійності сторонніх компаній, які надають програмне забезпечення, апаратне забезпечення або хмарні сервіси.

На нашу думку, вплив зазначених факторів визначає загальний рівень кіберстійкості та операційної надійності підприємства в умовах динамічного цифрового середовища.

Висновки та перспективи подальших досліджень. Проведене дослідження дозволило визначити в комплексно проаналізувати вплив цифрових технологій на фінансовий ризик-менеджмент та безпеку транспортних і аграрних підприємств України.

Доведено, що впровадження цифрових технологій (IoT, Big Data, AI, хмарні обчислення) є стратегічною необхідністю для підвищення ефективності та конкурентоспроможності підприємств. Незважаючи на безумовні переваги, цей процес генерує значні нові виклики для фінансового ризик-менеджменту та безпеки.

Досліджено специфічні цифрові ризики: інвестиційні у технології, кіберфінансові (прямі втрати від атак, простої, штрафи, репутаційні збитки), ризики даних (втрата, компрометація, спотворення інформації), а також операційні ризики (збої систем, програмні помилки, що паралізують процеси та спричиняють фінансові та інші втрати підприємств транспорту та аграрного сектору.

Встановлено, що основними перешкодами є дефіцит інвестицій та кваліфікованих кадрів, застаріла нормативно-правова база, низька обізнаність персоналу (людський фактор), складність інтеграції різнорідних систем, а також посилений вплив воєнних дій, що робить питання безпеки критично важливим.

Більшість українських підприємств транспортного й аграрного сектору демонструють неготовність до ефективного управління цими новими фінансовими ризиками та загрозами безпеки. Системні підходи до їх ідентифікації, оцінки та пом’якшення часто відсутні, що потребує проведення детальних теоретико-прикладних досліджень.

Для забезпечення сталого розвитку та безпеки підприємств в умовах цифрової трансформації необхідний інтегрований підхід до управління фінансовими ризиками та безпеки, що відкриває перспективи подальших наукових досліджень.

Список використаних джерел

1. Ali A. Advancements and transformative applications of blockchain technology [Electronic resource] / A. Ali // Journal of Engineering and Computational Intelligence Research. – 2025. – Accessed mode: https://jecir.com/index.php/jecir/article/download/8/9.

2. Ben Hassen T. Sustainable and resilient food systems in times of crises [Electronic resource] / T. Ben Hassen, H. El Bilali, B. Daher, S. Burkart // Frontiers in Nutrition. – 2025. – № 8. – 1564950. – Accessed mode: https://www.frontiersin.org/articles/10.3389/fnut.2025.1564950/full.

3. Deshmukh S. S. Challenges and opportunities for agri-tech startups in developing economies [Electronic resource] / Deshmukh, S. S., & Bethi, S. K. // International Journal of Agriculture and Sustainability. – 2023. – Issue 15(9). – Pp. 12661-12666. – Accessed mode: https://www.researchgate.net/publication/375696436.

4. Melesse T. Y. Analyzing the implementation of digital twins in the agri-food supply chain / T. Y. Melesse, C. Franciosi, V. Di Pasquale, S. Riemma // Logistics. – 2023. – Vol. 7(2). – P. 33. DOI: https://doi.org/10.3390/logistics7020033.

5. Zhou L. The application and challenges of blockchain technology in accounting and financial information systems [Electronic resource] / L. Zhou // ICAID 2024 Conference Proceedings. – 2024. – Accessed mode: https://www.atlantis-press.com/article/126002627.pdf.

6. Богданюк І. В. Стратегічне управління безпекою підприємства в умовах глобальної конкуренції [Електронний ресурс] / І. В. Богданюк, С. М. Мандич // Регіональна економіка. – 2024. – № 3. – С. 149-156. – Режим доступу: https://re.gov.ua/re202403/re202403_149_BohdanyukIV,MandychSM.pdf.

7. Горобець Н. М. Перспективи використання цифрових технологій в діяльності аграрних підприємств [Електронний ресурс] / Н. М. Горобець, Д. О. Хомякова, Д. Стариковська // Ефективна економіка. – 2021. – № 1. DOI: 10.32702/2307-2105-2021.1.90.

8. Ковтун В. А. Роль інтелектуальних технологічних рішень для ефективного використання ресурсів сільського господарства [Електронний ресурс] / В. А. Ковтун // Економіка та управління підприємствами. – 2019. – Вип. 1(18). – С. 132-138. – Режим доступу: http://dspace.ksaeu.kherson.ua/bitstream/handle/123456789/2244/23.pdf?sequence=1.

9. Коляденко С. В. Формування смарт-промисловості в аграрному секторі економіки на основі цифрового розвитку [Електронний ресурс] / С. В. Коляденко, Д. П. Саулко, В. В. Мазур // Міжнародний науковий журнал «Інтернаука». Серія: «Економічні науки». – 2024. – № 2(82), т. 1. – С. 94-102. DOI: 10.25313/2520-2294-2024-2-9653.

10. Орел А. М. Виклики та перешкоди впровадження цифрової бізнес-моделі банку в Україні [Електронний ресурс] / А. М. Орел, В. В. Дяченко // Інвестиції: практика та досвід. – 2024. – № 5. – С. 54-59. – Режим доступу: https://dspace.chmnu.edu.ua/jspui/bitstream/123456789/2563/1/%D0%86%D0%BD%D0%B2%D0%B5%D1%81%D1%82%D0%B8%D1%86%D1%96%D1%97_%D0%BF%D1%80%D0%B0%D0%BA%D1%82%D0%B8%D0%BA%D0%B0%20%D1%82%D0%B0%20%D0%B4%D0%BE%D1%81%D0%B2%D1%96%D0%B4,%202024.%20%E2%84%96%205.pdf#page=55.

11. Попова Ю. Логістика та повоєнне відновлення економіки України: Напрацювання стратегій сумісно з іноземними партнерами [Електронний ресурс] / Ю. Попова, О. Чуприна // Економіка та суспільство. – 2025. – Вип. 73(56).– Режим доступу: https://economyandsociety.in.ua/index.php/journal/article/download/5839/5780.

12. Тарасенко А. Управління ризиками в контексті забезпечення фінансово-економічної безпеки транспортних і промислових компаній / А. Тарасенко, Т. Бойчук, А. Даньков // Науковий вісник Полісся. – 2023. – № 2(27). – С. 143–160. DOI: https://doi.org/10.25140/2410-9576-2023-2(27)-143-160.

13. Шишкіна О. В. Механізм управління фінансовими ризиками промислових підприємств: теорія, методологія, практика : монографія / О. В. Шишкіна. – Чернігів : ЧНТУ, 2020. – 318 с.

14. Юрчук Н. П. Розвиток технологій Big data в умовах цифрових трансформацій [Електронний ресурс] / Н. П. Юрчук, С. С. Кіпоренко // Агросвіт. – 2021. – № 9–10. – С. 60–68. DOI: 10.32702/2306&6792.2021.9-10.60.

References

1. Ali, A. (2025). Advancements and transformative applications of blockchain technology. *Journal of Engineering and Computational Intelligence Research*. https://jecir.com/index.php/jecir/article/download/8/9.

2. Ben Hassen, T., El Bilali, H., Daher, B., & Burkart, S. (2025). Sustainable and resilient food systems in times of crises. *Frontiers in Nutrition, 8*, 1564950. https://doi.org/10.3389/fnut.2025.1564950.

3. Deshmukh, S. S., & Bethi, S. K. (2023). Challenges and opportunities for agri-tech startups in developing economies. *International Journal of Agriculture and Sustainability*, *15*(9), 12661-12666. https://www.researchgate.net/publication/375696436.

4. Melesse, T. Y., Franciosi, C., Di Pasquale, V., & Riemma, S. (2023). Analyzing the implementation of digital twins in the agri-food supply chain. *Logistics*, *7*(2), 33. https://doi.org/10.3390/logistics7020033.

5. Zhou, L. (2024). The application and challenges of blockchain technology in accounting and financial information systems. In *ICAID 2024 Conference Proceedings*. Atlantis Press. https://www.atlantis-press.com/article/126002627.pdf.

6. Bohdaniuk, I. V., & Mandych, S. M. (2024). Stratehichne upravlinnia bezpekoiu pidpryiemstva v umovakh globalnoi konkurentsii [Strategic management of enterprise security in the context of global competition]. *Rehionalna ekonomika – Regional economy*, (3), 149–156. https://re.gov.ua/re202403/re202403_149_BohdanyukIV,MandychSM.pdf.

7. Horobets, N. M., Khomiakova, D. O., & Starykovska, D. O. (2021). Perspektyvy vykorystannia tsyfrovykh tekhnolohii v diialnosti ahrarnykh pidpryiemstv [Prospects for the use of digital technologies in the activities of agricultural enterprises]. *Efektyvna ekonomika – Effective Economy*, (1). https://doi.org/10.32702/2307-2105-2021.1.90.

8. Kovtun, V. A. (2019). Rol intelektualnykh tekhnolohichnykh rishen dlia efektyvnoho vykorystannia resursiv silskoho hospodarstva [The role of intelligent technological solutions for the effective use of agricultural resources]. *Ekonomika ta upravlinnia pidpryiemstvamy – Economics and enterprise management*, *1*(18), 132–138. http://dspace.ksaeu.kherson.ua/bitstream/handle/123456789/2244/23.pdf?sequence=1.

9. Koliadenko, S. V., Saulko, D. P., & Mazur, V. V. (2024). Formuvannia smart-promyslovosti v ahrarnomu sektori ekonomiky na osnovi tsyfrovoho rozvytku [Formation of smart industry in the agricultural sector of the economy based on digital development]. *Mizhnarodnyi naukovyi zhurnal "Internauka", Seriia: Ekonomichni nauky – International scientific journal "Internauka". Series: Economic Sciences*, *82*(2), 94–102. https://doi.org/10.25313/2520-2294-2024-2-9653.

10. Orel, A. M., & Diachenko, V. V. (2024). Vyklyky ta pereshkody vprovadzhennia tsyfrovoi biznes-modeli banku v Ukraini [Challenges and obstacles to implementing a digital business model for a bank in Ukraine]. *Investytsii: praktyka ta dosvid – Investments: practice and experience*, (5), 54–59. https://dspace.chmnu.edu.ua/jspui/bitstream/123456789/2563/1/%D0%86%D0%BD%D0%B2%D0%B5%D1%81%D1%82%D0%B8%D1%86%D1%96%D1%97_%D0%BF%D1%80%D0%B0%D0%BA%D1%82%D0%B8%D0%BA%D0%B0%20%D1%82%D0%B0%20%D0%B4%D0%BE%D1%81%D0%B2%D1%96%D0%B4,%202024.%20%E2%84%96%205.pdf#page=55.

11. Popova, Yu., & Chupryna, O. (2025). Lohistyka ta povoienne vidnovlennia ekonomiky Ukrainy: Napratsiuvannia stratehii sumisno z inozemnymy partneramy [Logistics and post-war recovery of the Ukrainian economy: Development of strategies jointly with foreign partners]. *Ekonomika ta suspilstvo – Economy and Society*, (73). https://economyandsociety.in.ua/index.php/journal/article/download/5839/5780.

12. Tarasenko, A., Boichuk, T., & Dankov, A. (2023). Upravlinnia ryzykamy v konteksti zabezpechennia finansovo-ekonomichnoi bezpeky transportnykh i promyslovykh kompanii [Risk management in the context of ensuring the financial and economic security of transport and industrial companies]. *Naukovyi visnyk Polissia – Scientific Bulletin of Polissya*, *27*(2), 143–160. https://doi.org/10.25140/2410-9576-2023-2(27)-143-160.

13. Shyshkina O.V. (2020). *Mekhanizm upravlinnia finansovymy ryzykamy promyslovykh pidpryiemstv: teoriia, metodolohiia, praktyka [The mechanism of financial risk management of industrial enterprises: theory, methodology, practice].* ChNTU.

14. Yurchuk, N. P., & Kiporenko, S. S. (2021). Rozvytok tekhnolohii Big data v umovakh tsyfrovykh transformatsii [Development of Big data technologies in the context of digital transformations]. *Ahrosvit*, (9–10), 60–68. https://doi.org/10.32702/2306-6792.2021.9-10.60.

Отримано 28.04.2025

UDC 004.056:330.131.7:658.155:338.47:338.48

Olena Shyshkina
Doctor of Economic Sciences, Professor,
Professor of the Department of Finance, Banking and Insurance,
Chernihiv Polytechnic National University (Chernihiv, Ukraine)
E-mail: shyshkina.olena.v@gmail.com. **ORCID:** http://orcid.org/0000-0002-8946-1027
ResearcherID: F-3208-2014. **Scopus Author ID:** 58995081900

Taras Boichuk
PhD student of the Department of Finance, Banking and Insurance
Chernihiv Polytechnic National University (Chernihiv, Ukraine)
E-mail: taras.boychuk.cv@ukr.net. **ORCID:** https://orcid.org/0009-0000-9073-8620

Dmytro Yevchuk
PhD student of the Department of Finance, Banking and Insurance
Chernihiv Polytechnic National University (Chernihiv, Ukraine)
E-mail: dimon.evchuk@gmail.com. **ORCID:** https://orcid.org/0009-0006-9585-638X

THE IMPACT OF DIGITAL TECHNOLOGIES ON FINANCIAL RISK MANAGEMENT AND SECURITY OF TRANSPORT AND AGRICULTURAL ENTERPRISES

The article examines the impact of digital technologies on financial risk management systems and the overall level of security of strategically important transport and agricultural enterprises in Ukraine. The author analyzes the key digital technologies that are being actively implemented in these sectors, including the Internet of Things (IoT) for asset monitoring, Big Data and predictive analytics for process optimization, artificial intelligence (AI) for decision automation, as well as cloud computing and integrated management systems (TMS, FMS, ERP) as the basis for a new digital infrastructure.

It is found that digital technologies are not only a tool for increasing efficiency, but also a catalyst for new risks that were previously not inherent in the industry, and at the same time are a powerful modifier of traditional risks. The new financial risks include: significant technological investment risks associated with the high cost and rapid obsolescence of digital solutions; cyberfinancial risks, which include direct losses from attacks (theft of funds, ransom for data) and indirect losses from downtime and reputational damage; and risks associated with data processing, where compromise or distortion of information leads to incorrect management decisions with direct financial consequences.

The impact of digitalization on the security of enterprises that are critical infrastructure is studied in detail. New types of threats are identified: targeted cyberattacks on traffic or agricultural machinery control systems, massive data leakage and compromise, unauthorized access to control systems through vulnerabilities, and risks spreading through the software supply chain from third-party contractors. It is emphasized that the level of cybersecurity in both industries is often insufficient and does not correspond to the scale of threats due to chronic underinvestment, acute shortage of qualified personnel, use of outdated infrastructure, and low awareness of cyber hygiene rules among staff.

The author summarizes the systemic problems that impede the effective management of new risks, which include the following: insufficient integration of digital risks into existing corporate risk management systems, financial and human resources shortages, a significant backlog of the regulatory framework, difficulty in quantifying the potential impact of cyber incidents on financial performance, high interdependence of systems, which creates the risk of cascading failures, and a significant increase in threats in wartime. Based on the analysis, the author formulates the urgent need to develop and implement a comprehensive, proactive and integrated approach to financial risk management that would consider technological, operational and cyber risks as a single system.

Keywords*: digital technologies; financial risk management; digitalization; transport enterprises; agricultural enterprises; cyber risks; security; cybersecurity.*

Табл.: 4. Бібл.: 14.

Шишкіна О. В., Бойчук Т. Т., Євчук Д. В. Вплив цифрових технологій на фінансовий ризик-менеджмент та безпеку транспортних і аграрних підприємств. *Проблеми і перспективи економіки та управління.* 2025. № 2(42). С. 337-360. DOI: https://doi.org/10.25140/2411-5215-2025-2(42)-337-360.