

УПРАВЛІННЯ РИЗИКОМ ДЛЯ ЦІЛЕЙ ОБЛІКУ В СУЧАСНИХ УМОВАХ ЦИФРОВІЗАЦІЇ

*А. А. Макурін д. е. н., професор, Національного технічного університету
«Дніпровська політехніка», makurin.A.A@ntu.one, <https://orcid.org/0000-0001-8093-736X>,
Н. Л. Шишкова, к. е. н., доцент, Національного технічного університету
«Дніпровська політехніка», shyshkova.n.l@ntu.one, <https://orcid.org/0000-0002-6675-8223>*

Методологія дослідження. Дослідження базується на використанні таких загальнонаукових методів, як: абстракція – при визначенні сутності цифрового ризику, що у подальшому впливає на формування інформації на підприємстві. Метод групування застосовувався під час надання характеристик різним видам ризику та формування їхнього ранжування з метою визначення напрямів управління їхнім впливом на господарюючих суб'єктів.

Результати дослідження. У статті проаналізовано вплив цифровізації на інформаційне забезпечення обліку. Встановлено, що в рамках комунікації бухгалтер повинен вміти використовувати сучасні технології, нові платформи та сервіси у процесі взаємодії із внутрішніми та зовнішніми користувачами інформації, дотримуючись при цьому правил етикету та поведінки, що існують в рамках даного формату взаємодії. Зазначено, що управління ризиком для цілей обліку в умовах цифровізації набуває особливої актуальності через зростаючу складність інформаційних систем і впровадження новітніх технологій, що впливають на ведення фінансового обліку та управлінські процеси. Виокремлено основні види ризиків при цифровій трансформації обліку, які включають: технологічні, кіберризики, ризики баз даних, операційні, правові, стратегічні, фінансові. Розглянуто загрози та особливості цифрового середовища формування інформації в обліку, які можуть викривити фінансову звітність підприємства або вплинути на прийняття управлінських рішень через недостатній рівень захищеності даних.

Новизна. Наукова новизна результатів дослідження полягає у виокремленні ризиків, які притаманні сучасному підприємству в умовах цифровізації, що в подальшому дозволяє їх ідентифікувати, вимірювати, управляти та контролювати.

Практична значущість. Результати дослідження розкривають змінність інформаційної площини бухгалтерського обліку на підприємстві, яка виконує функцію доведення інформації до структурних підрозділів з метою створення підґрунтя для подальшого прийняття управлінських рішень. Оскільки цифровізація передбачає вирішення великого кола питань, пов'язаного зі збором, обробкою і аналізом інформації та застосування професійного судження бухгалтера, то результати даного дослідження набувають великого значення для ефективної діяльності підприємства.

Ключові слова: цифровізація суспільства, управління ризиком та його інформаційне забезпечення, бухгалтерський облік, функціонування підприємства, зовнішній та внутрішній ризик.

Постановка проблеми. Цифрова трансформація суспільства спонукає до змін в усіх сферах суспільно-економічного життя людства. В свою чергу, це відзначається на господарській діяльності суб'єктів господа-

рювання, в тому числі й на їх обліковій практиці. Відбувається значна переорієнтація траєкторії розвитку бізнеса на різних рівнях (мікро, регіональний, глобальний). Віртуалізація бізнес-процесів вимагає змін організа-

ційного та методичного забезпечення обліку. Також цифровізацією викликані зміни в частині формування компетенцій фахівців, необхідних в сучасних умовах господарювання, які повинні навчитись ідентифікувати та управляти ризиками на підприємстві.

Перед фахівцями різних галузей постають нові завдання які вимагають оперативного втручання та отримання інформації з різних структурних підрозділів підприємства для прийняття рішень щодо стратегічного розвитку підприємства, що в свою чергу неможливо без інформації про ризики та стан діяльності суб'єкта господарювання. Оскільки управління ризиком це система прийняття управлінських рішень та реалізація заходів, спрямованих на його контроль, зменшення рівня чи усунення. Під час впровадження інформаційних систем та технологій перелік зовнішніх ризиків впливає на внутрішнє середовище підприємства. Тому необхідним є дослідження не тільки зовнішніх, а й внутрішніх ризиків на підприємстві. Враховуючи умови цифровізації та управління в сучасних умовах підприємством суттєво змінює традиційні підходи в обліковій практиці. Свою особливість має зберігання, обіг та захист інформації на підприємстві з подальшим інноваційним процесом обробки. Все це сприяє оптимізації роботи та оброблення інформації, проте разом із додатковими можливостями виникають і додаткові ризики, пов'язані з впровадженням інформаційних систем та технологій у діяльність суб'єкта господарювання.

Таким чином, необхідно розробити вимоги до інформаційного забезпечення ризику на підприємства для облікових цілей в розрізі ведення фінансового та управлінського обліку з подальшим виокремленням внутрішніх та зовнішніх ризиків.

Аналіз останніх досліджень і публікацій. Вплив цифровізації на інформаційне забезпечення обліку на підприємстві досліджували різні науковці. Більшість наукових досліджень стосовно даної теми мають фрагментарний характер та спрямовані на формування теоретико-методичного підґрунтя нової цифрової парадигми в розрізі інформаційного забезпечення. Серед науковців, які досліджували цю тему, слід відзначити такі праці, зокрема: Абрамова А. С. в

своїй статті розглянула основні тенденції діяльності підприємств в сучасних глобалізаційних умовах господарювання [3]. В дослідженні авторка розглянула механізм управління ризиками цифровізації. Лише правильний підхід та підбір елементів та інструментів управління ризиками в майбутньому може забезпечити стабільність та ефективність функціонування. Руденко С. В., Погрібняк Д. С. в своєму дослідженні наголошують увагу на тому, що трансформаційні зміни в суспільно-економічному житті світу значно вплинули і на господарську діяльність суб'єктів, що вимагає змін у обліковій практиці також [4]. Охарактеризували коло перешкод, які гальмують розвиток цифрових трансформацій в Україні: інституційні, інфраструктурні, екосистемні.

Наведено хронологію розвитку практики обліку у розрізі промислових революцій та визначено в їх контексті основні управлінські цілі та завдання обліку, що виникають. Довели необхідність формування нової методичної основи для ідентифікації, оцінювання та обліку нових об'єктів, що виникають в умовах цифровізації. Відзначено зростання ролі облікової-інформації для менеджменту підприємств в сучасних умовах. Осадча О. О., Павленко О. В. розглядали проблеми впровадження електронних технологій фінансової звітності в Україні, виокремили фактори які гальмують розвиток цифровізації на підприємствах [5]. Запропонували шляхи удосконалення технологій побудови звітності та управління інформаційними потоками на підприємстві.

Power M. стверджує, що аналіз фінансової звітності сприймається як найбільший внесок в управління ризиками. Як зазначає автор, функція управлінського обліку була значною мірою залучена до управління ризиками організації [7]. Бюджетний контроль, бюджетування та стратегічне планування відіграють важливу роль в управлінні ризиками. Van der Poll H., Mthiyane Z. Z. F. автори наголошують, що цінності корпоративного управління та управління ризиками, які недостатньо встановлені та порушені, можуть призвести до гальмування потенціалу зростання підприємства [8]. Основною метою дослідження було перевірити взаємозалежність управління ризиками, корпоратив-

ного управління та управлінського обліку в найефективніших публічних компаніях. Для проведення дослідження використовували огляд літератури, структуровану анкету та огляд документів. Емпіричні результати дослідження демонструють, що існує взаємозалежність управління ризиками, корпоративного управління та управлінського обліку. Науковці зазначили, що майбутні дослідження повинні охоплювати управління ризиками шахрайства, управління зацікавленими сторонами та сфери управління інфраструктурою. Селезньова Г. О. у дослідженні розглядала питання щодо вияву загроз і ризиків для економічної безпеки підприємств в умовах цифровізації і глобалізації економіки та управління ними [9]. Автор зазначила основні ризики економічної безпеки в умовах цифровізації бізнесу, навела принципи управління ризиками, а також результативність системи управління ризиками з метою підвищення економічної безпеки. Зазначено, що необхідно своєчасно здійснювати моніторинг економічної безпеки на основі ризикорієнтованого підходу, а також моделювання організаційного підходу для стейкхолдерів підприємства в умовах змін та достовірності фінансової звітності на основі виявлених ризиків, які встановлено на підприємстві.

Формулювання мети статті. Метою статті є ідентифікація вимог до інформаційного супроводу та управління ризиком в сучасних умовах цифровізації на підприємстві.

Виклад основного матеріалу дослідження. Розвиток цифрових трансформацій в нашій країні гальмується певним колом перешкод, до яких належить інституційне коло, інфраструктурне та екосистемне. Інституційне коло пов'язано з державним впливом, тобто як нормативна база країни встигає регулювати питання цифровізації та цифрової трансформації. Інфраструктурне полягає в формуванні цифрової культури, рівних умов доступу до інформації різних верст населення до цифрових технологій та необхідний перелік інфраструктур які притаманні розвиненим цифровим країнам. Екосистема полягає з площиною інноваційних аспектів, відсутність належних умов для формування сприятливого інвестиційного

клімату, впровадження та залучення ринку капіталу інвестицій в країні та на підприємстві в ІТ-сферу. Залучення кваліфікованих фахівців в процес цифрової трансформації суспільства.

Цифрова трансформація суспільства вимагає набуття відповідних знань в цій галузі різними фахівцями, в тому числі й бухгалтерами. Так бухгалтер при сучасних умовах цифровізації повинен набутися значної кількості навичок, які дещо виходять за звичні рамки кваліфікації даної професії, а саме: вміти орієнтуватися у процесах фільтрування та відбору даних серед масивів інформації в цифровому контенті, використовувати нейронні мережі, ідентифікувати бізнес-процеси та використовувати сучасні інформаційні технології в роботі з обліковою інформацією. Розуміти специфіку цифрового аудиту тощо. В рамках комунікації та взаємодії бухгалтер повинен вміти використовувати сучасні технології, нові платформи та сервіси у процесі взаємодії із внутрішніми та зовнішніми користувачами інформації, дотримуючись при цьому правил етикету та поведінки, що існують в рамках даного формату взаємодії. Важливим умінням є створення, зміни та удосконалення цифрового контенту, що передбачає також знання нормативно-законодавчих аспектів щодо авторських прав, політики рецензування; вміння використовувати імітаційне моделювання та адаптувати бухгалтерські програми до існуючих вимог. Перед бухгалтером стоїть завдання збереження та захисту цифрової інформації, яка в рамках використання цифрових технологій може стати доступною для шахраїв, конкурентів сторонніх осіб, адже виток інформації, особливо тієї, що належить до комерційної таємниці, негативно вплине на господарську діяльність суб'єкта господарювання.

Таким чином, цифровізація передбачає виникнення значного кола технічних проблем, які бухгалтер також повинен вміти вирішувати у процесі своєї професійної діяльності, тому креативний підхід до адаптації цифрових технологій під власні потреби з метою вирішення облікових проблем є досить важливою здатністю, оскільки виникнення ризиків в такій системі є неминучим процесом. Креативність по відношенню

до обліку як «інтелектуалізація інформаційних систем бухгалтерського обліку» є досить влучним положенням, який заслуговує, на нашу думку, стати частиною нової цифрової облікової парадигми.

Управління ризиком для цілей обліку в умовах цифровізації набуває особливої актуальності через зростаючу складність інформаційних систем і впровадження новітніх технологій, що впливають на ведення фінансового обліку та управлінські процес. Серед основних аспектів варто зазначити:

1. Автоматизація облікових процесів. Цифровізація дає можливість автоматизувати безліч рутинних облікових операцій, таких як обробка первинних документів, ведення реєстрів, складання звітів. Однак це створює нові ризики, пов'язані з: помилки програмного забезпечення; неправильні чи некоректні конфігурації автоматизованих систем; втрата контролю над коректністю введених даних.

2. Кібербезпека та захист інформації У сучасних умовах кіберзагрози є одним з ключових ризиків для облікових даних. Можливі загрози включають: кіберзлочинність (крадіжка даних, маніпуляція фінансовими звітами); хакерські атаки на облікову систему; незахищені канали передачі даних та недостатня захищеність інформаційних систем.

3. Доступ до даних і управління доступами з ідентифікації користувачів. Підвищення прозорості та швидкості доступу до фінансових даних, які забезпечують цифрові рішення, також несе ризики. Потрібно належно керувати правами доступу до інформаційних систем: контроль рівнів доступу до різних категорій даних; відстеження активності користувачів для запобігання несанкціонованому доступу; аудит логінів та контроль за змінами в облікових даних.

4. Точність і достовірність даних Автоматизовані системи спрощують процес обробки великої кількості даних, але водночас збільшується ймовірність механічних помилок або неправильного налаштування алгоритмів. Тому управління ризиками має включати: перевірку та валідацію даних на різних етапах обробки; Використання технологій штучного інтелекту для виявлення аномалій у даних. Резервне копіювання кри-

тичних даних і своєчасне оновлення систем.

5. Регулювання і нормативне середовище З розвитком цифрових технологій зростає потреба адаптації бухгалтерського обліку до змін у нормативно-правовій базі. Важливо стежити за: новими стандартами, що регулюють цифрові облікові системи; впровадженням вимог щодо захисту персональних даних. Відповідністю міжнародним стандартам фінансової звітності.

6. Впровадження штучного інтелекту та аналітики даних. Використання аналітичних інструментів на базі штучного інтелекту дозволяє покращити управління ризиками в обліку через: виявлення потенційних шахрайств; прогнозування ризиків на основі історичних даних; Оптимізацію проведення аудиту та здійснення контролю.

7. Ризики людського фактору. Незважаючи на автоматизацію, людський фактор залишається суттєвим ризиком у системі обліку. Це може включати: помилки при введенні даних або налаштуванні систем; несвоєчасне оновлення програмного забезпечення; ненавмисне створення вразливостей через неправильне поводження з технікою або програмними продуктами. Використання не захищених Wi-Fi мереж, тощо [10].

Управління ризиками в умовах цифровізації вимагає інтегрованого підходу, який включає не тільки технічні засоби захисту, але й удосконалення процесів управління, підвищення рівня обізнаності персоналу та створення нових нормативних основ для захисту облікових даних. При цифровій трансформації обліку виникають нові ризики, які можуть суттєво вплинути на фінансову інформацію, процеси та безпеку даних, які формуються на підприємстві. Основні види ризиків при цифровій трансформації обліку включають: технологічні, кіберризики, ризики баз даних, операційні, правові, стратегічні, фінансові.

Цифрова система може бути неготова до майбутніх змін в облікових стандартах або законодавстві. Управління всіма цими ризиками вимагає комплексного підходу, який включає постійний моніторинг, оцінку та адаптацію до змін. Ідентифікація всіх цих ризиків допомагає в подальшому управляти ними та контролювати їх. В першу чергу

варто розподілити ризики на категорії та надати їм відповідну характеристику. Так, пропонується розподіляти ризики на такі категорії як, внутрішні, зовнішні, стратегічні. Відповідно до категорії необхідно виокремити особливості та причини їх виникнення.

В обліковій практиці варто зазначити внутрішні ризики – які пов'язані з безпосереднім досягненням мети, цілей та завдань обліку на підприємстві. Необхідно врахувати особливості галузі, підприємства та об'єкту обліку. Крім того, на ризики цієї групи будь-яке підприємство має вплив та може їх контролювати. До основних причин виникнення належать: шахрайство, використання неналежного програмного забезпечення, відвідування небажаних веб-ресурсів, втрата електронно-цифрового підпису, плинність кадрів.

Категорія зовнішніх ризиків полягає з досягненням мети та місії підприємства. Саме ці ризики пов'язані з зовнішнім впливом на підприємство. Основна проблема полягає у визначенні, яка саме подія чи загроза призведе до негативних наслідків на підприємстві. Розглядаються можливості як зробити установу більш стійкою до їх впливу. До них належать природні явища та катастрофи, кібератаки (фішинг), форс-мажори.

До категорії стратегічних ризиків за міжнародною практикою управління ними прийнято виділяти наступні: ідентифікація – визначаються потенційні ризики та їх можливий вплив шляхом використання «сценарного планування» [10].

Враховуючи особливості цифрового середовища та формування інформації в обліку існують наступні загрози, які можуть викривити фінансову звітність підприємства або вплинути на прийняття управлінських рішень через недостатній рівень захищеності даних. Так, наприклад,

Ботнет – комп'ютерна мережа що складається з великої кількості хостів і запущеними ботами, які працюють автономно. Найчастіше вони прикріплені до звичайного програмного продукту та як тільки користувач встановлює його на свій пристрій, бот автоматично встановлюється. Такий комп'ютер вже є інфікований. Хакер зможе

викрасти інформацію про користувача, здійснити розсилку від його імені, перебрати паролі від гаманців та отримати доступ до кредитних карток чи розрахункових рахунків установи.

Наприклад, використання мережі WiFi в готелі не є безпечним, оскільки на пристрої може з'явитись прохання оновити програмне забезпечення чи ще якийсь його компонент, що автоматично дає можливість встановити Backdoor, який виступає віддаленим керуванням гаджету. Вся інформація з пристрою доступна не тільки його власнику, а й зловмиснику.

Фішинг – вид шахрайства, метою якого є отримання прибутку чи конфіденційної інформації. Приклад фішингу – SMS повідомлення та дзвінки від незнайомих осіб, а також відправлення листів електронною поштою від імені певних користувачів яким довіряє особа.

Малвертайзинг – поширення небажаного програмного забезпечення через онлайн ресурси, закриття реклами на певній сторінці активує код і вся інформація з пристрою передається хакеру.

Кардинг – рід шахрайства який здійснюється через використання платіжних карток та їх реквізитів, що не ініційовано власником такої картки. Реквізити платіжних карток, як правило, беруть зі зламаних серверів інтернет-магазинів, платіжних і розрахункових систем, а також з персональних комп'ютерів.

Враховуючи вище наведені особливості пропонується виділити та надати можливість ідентифікувати як зовнішні так і внутрішні ризики на підприємстві, а саме:

1. Технологічні ризики, пов'язані з використанням нових технологій, програмного забезпечення і систем обробки даних: Збої в роботі систем виникають внаслідок помилок програмного забезпечення, відмови систем, технічних збоїв. Має місце неправильна інтеграція: труднощі з поєднанням нових цифрових рішень зі старими обліковими системами. Швидкий розвиток технологій може призвести до того, що впроваджені рішення не будуть відповідати сучасним вимогам.

2. Ризики, пов'язані з даними, можуть бути викликані помилками при автоматич-

ній обробці, що призводить до перекручення фінансової інформації. Неналежне збереження резервних копій або ненадійні системи можуть призвести до втрати важливих даних. Порушення конфіденційності фінансової або персональної інформації може виникнути через незахищений доступ до даних.

3. Операційні ризики пов'язані з перебоями або помилками в процесах, що виникають через цифрові інструменти. Це можуть бути помилки автоматизації (неправильні налаштування алгоритмів або автоматизованих систем обліку, що тягнуть масові помилки), залежність від технічної інфраструктури: будь-який збій в ІТ-інфраструктурі може паралізувати роботу бухгалтерії. Також надмірна довіра до автоматизованих рішень без належного контролю може призвести до ігнорування важливих аспектів обліку.

4. Правові ризики. Використання цифрових інструментів може супроводжуватися юридичними проблемами, до яких належать невідповідність нормативним вимогам (технологічні зміни можуть випереджати зміни у законодавстві та стандартах бухгалтерського обліку), а також порушеннями вимог щодо захисту персональних даних (недотримання законодавчих норм, наприклад, GDPR). Присутні і ліцензійні ризики: використання програм з порушенням прав інтелектуальної власності.

5. Ризики людського фактору. Незважаючи на автоматизацію процесів, люди продовжують бути важливим фактором функціонування підприємства. Тому можуть виникати помилки, які є наслідком недостатньої цифрової кваліфікації співробітників. Можуть мати місце навмисні шахрайські дії співробітників, пов'язані з маніпуляцією цифровими даними або їхнє небажання адаптуватися до нових технологій.

6. Фінансові ризики. Впровадження цифрових технологій часто вимагає значних фінансових ресурсів, що може призвести до фінансових втрат. Цифрові рішення можуть не виправдати очікувань і не принести необхідної фінансової вигоди. Мають місце також і зміни в обліковій політиці: цифровізація може вимагати перегляду облікової політики підприємства, що може вплинути на

його фінансові результати.

7. Стратегічні ризики. Вони пов'язані з вибором невідповідних або застарілих стратегій цифрової трансформації: рішення про впровадження конкретної технології може виявитися неефективним або несумісним із бізнес-процесами, а цифрова система може бути неготовою до майбутніх змін в облікових стандартах або законодавстві. Управління усіма цими ризиками вимагає комплексного підходу, який включає постійний моніторинг, оцінку та адаптацію до змін.

З метою ранжування та управління ризиками пропонується наступна їх градація. Низький рівень впливу має цифрове значення 1. Ймовірність виникнення ризику та його вплив на підприємство малий або незначний. Якщо ризик має високу ймовірність, то його можна віднести до середнього рівня впливу. Проте ця група вже має показник 2. та ті ж види ймовірності. Високий рівень впливу – група має показник 3. та характеризується значним впливом на діяльність підприємства, отримання перекурен у його фінансовій звітності чи викривлення даних або технічні особливості, що значно впливають на нормальну діяльність.

У міжнародній практиці встановлення різних видів ризиків, визначення їхнього рівня, ймовірності настання та впливу відбувається у різний спосіб і має неоднакові механізми подолання. Найпоширенішим способом боротьби з різними видами ризику є такі методи, як: вартості, контролю поточного рівня, історичного рівня, аналізу показників діяльності підприємства, стрес-тестування, експертної думки фахівця, комбінований метод. Використання будь-якого з них на практиці потребує додаткових досліджень.

Висновки. В умовах розвитку інформаційного суспільства та цифрової економіки виникає величезна кількість передумов для формування нової парадигми з ведення бухгалтерського обліку, формування інформаційних потоків на підприємстві, захисту інформації. Моніторинг – з метою своєчасного реагування на можливі ризики здійснюється постійний моніторинг зовнішнього середовища (наприклад, аналізується інформація у засобах масової інформації, статистичні дані, відомості про можливі

зміни у законодавстві. Способи реагування - визначаються заходи контролю на ідентифіковані ризики з метою запобігання їх виникненню або мінімізації впливу.

Перспективами подальшого дослідження є розроблення наукового підходу до формування моделі ведення обліку в цифровій площині з виокремленням відповідних ризиків та використання методів їх контролю, аналізу та впливу на їх рівень. З метою покращення інформаційної функції обліку.

Література

1. An endurance course surviving and thriving through 10 major risks over the next decade. Tenth annual EY. [Electronic resource] Accessed mode: [https://www.ey.com/Publication/vwLUAssets/ey-global-risk-survey2019/\\$FILE/ey-globalrisk-survey-2019.pdf](https://www.ey.com/Publication/vwLUAssets/ey-global-risk-survey2019/$FILE/ey-globalrisk-survey-2019.pdf)
2. Івлєва М.І. Тенденція цифровізації банківської галузі. *Молодий вчений*. 2020. №2(292). С. 268-270. Режим доступу: <https://moluch.ru/archive/292/66194>.
3. Абрамова А. Система ризиків діяльності комерційних банків в умовах цифровізації. *Проблеми і перспективи економіки та управління*. 2021. №4(28). С. 186-193. URL: <http://ppeu.stu.cn.ua/article/view/262944>
4. Руденко С.В., Погрібняк Д.С. Бухгалтерський облік в умовах цифровізації *Вісник Хмельницького нац-го ун-ту (Економічні науки)*. 2021. №1.
5. Осадча О.О., Павленко О.В. Розвиток обліково-аналітичної системи в умовах цифровізації економіки України. *Bulletin National University of Water and Environmental Engineering*. 2021. №94. С. 162-174.
6. Подання фінансової звітності у новому форматі iXBRL. Національна комісія з цінних паперів та фондового ринку. 2019. Режим доступу: https://nfp.gov.ua/files/tacsonomia/NSSMC_Financial%20Reporting%20System%20XBRL.pdf
7. Pover, M. (2019). The risk management of everything. *Journal of Risk Finance*. Vol. 5. No. 3. pp. 58-65. <https://doi.org/10.1108/eb023001>
8. Van der Poll H., Mthiyane Z. Z. F. The interdependence of risk management, corporate governance and management accounting. *Southern African Business Review*. 2018. T. 22. №1.
9. Селезнєва Г.О. Сучасні ризики забезпечення економічної безпеки підприємств за умов циф-

ровізації. *Український журнал прикладної економіки та техніки*. 2023. № 4. С. 167-173.

10. Україна 2030Е – країна з розвинутою цифровою економікою. – Режим доступу: <https://strategy.uifuture.org/kraina-z-rozvinutoyu-cifrovoyu-ekonomikoyu.html>

References

1. An endurance course surviving and thriving through 10 major risks over the next decade (2019). Tenth annual EY. Retrieved from [https://www.ey.com/Publication/vwLUAssets/ey-global-risk-survey2019/\\$FILE/ey-globalrisk-survey-2019.pdf](https://www.ey.com/Publication/vwLUAssets/ey-global-risk-survey2019/$FILE/ey-globalrisk-survey-2019.pdf)
2. Ivlieva, M.I. (2020). Tendentsia tsyfrovizatsii bankivskoi haluzi. *Molodyi vchenyi*, 2(292), 268-270. Retrieved from <https://moluch.ru/archive/292/66194>.
3. Abramova, A. (2021). Systema ryzykiv diialnosti komertsiiynkh bankiv v umovakh tsyfrovizatsii. *Problemy i perspektyvy ekonomiky ta upravlinnia*, 4(28), 186-193. DOI: 10.25140/2411-5215-2021-4(28)-186-193
4. Rudenko, S.V., & Pohribniak, D.S. (2021). Bukhhalterskyi oblik v umovakh tsyfrovizatsii. *Visnyk Khmelnytskoho nats-ho un-tu (Ekonomichni nauky)*, (1).
5. Osadcha, O.O., & Pavlenko, O.V. (2021). Rozvytok oblikovo-analitychnoi systemy v umovakh tsyfrovizatsii ekonomiky Ukrainy. *Bulletin National University of Water and Environmental Engineering*, (94), 162-174. <https://doi.org/10.31713/ve2202115>
6. Podannia finansovoi zvitnosti u novomu formati iXBRL. (3019). Natsionalna komisiiia z tsinnykh paperiv ta fondovoho rynku. Retrieved from https://nfp.gov.ua/files/tacsonomia/NSSMC_Financial%20Reporting%20System%20XBRL.pdf
7. Pover, M. (2019). The risk management of everything. *Journal of Risk Finance*, Vol. 5, (3), 58-65. <https://doi.org/10.1108/eb023001>
8. Van der Poll H., & Mthiyane, Z. Z. F. (2018). The interdependence of risk management, corporate governance and management accounting. *Southern African Business Review*, (1). <https://doi.org/10.25159/1998-8125/4344>
9. Seleznova, H.O. (2023). Suchasni ryzyky zabezpechennia ekonomichnoi bezpeky pidpriemstv za umov tsyfrovizatsii. *Ukrainskyi zhurnal prykladnoi ekonomiky ta tekhniky*, (4), 167-173. <https://doi.org/10.36887/2415-8453-2023-4-26>
10. Ukraina 2030E – kraina z rozvynutoiu tsyfrovoiu ekonomikoiu. Retrieved from <https://strategy.uifuture.org/kraina-z-rozvinutoyu-cifrovoyu-ekonomikoyu.html>

RISC MANAGEMENT FOR ACCOUNTING PURPOSES IN THE MODERN CONDITIONS OF DIGITALIZATION

A. A. Makurin, D.E., Professor, N. L. Shishkova, Ph. D (Econ.), Associate Professor, Dnipro University of Technology

Methods. The study is based on the use of such general scientific methods as: abstraction – when determining the essence of digital risk, which subsequently affects the formation of

information at the enterprise. The grouping method was used when characterizing various types of risk and forming their ranking in order to determine the directions of managing their impact on business entities.

Results. The article analyzes the impact of digitalization on the information support of accounting. It was established that in the framework of communication and interaction, the accountant must be able to use modern technologies, new platforms and services in the process of interaction with internal and external users of information, while observing the rules of etiquette and behavior that exist within this format of interaction. It is noted that risk management for accounting purposes in the context of digitalization is gaining special relevance due to the growing complexity of information systems and the introduction of the latest technologies that affect financial accounting and management processes. The main types of risks in the digital transformation of accounting are given, which include technological, cyber risks, database risks, operational, legal, strategic, financial. There are considered threats and features of the digital environment for the formation of information in accounting which can distort the financial reporting of the enterprise or affect management decisions due to an insufficient level of data security.

Novelty. The scientific novelty of the research results lies in the identification of risks that are inherent in a modern enterprise in conditions of digitalization. Which in turn allows them to be identified, measured, managed and controlled.

Practical value. The results of the study reveal the variability of the information plane of accounting at the enterprise, which performs the main function related to the informativeness of structural divisions for further decision-making in its management. Since digitalization involves solving a wide range of issues related to the collection, processing and analysis of information and the application of the accountant's professional judgment then the results of this study are of great importance for the effective operation of the enterprise.

Keywords: digitalization of society, risk management and its information support, accounting, enterprise functioning, external and internal risk.

Надійшла до редакції 30.01.25 р.