DOI: https://doi.org/10.37634/efp.2024.4.3
УДК 657.1.011.56:004

Наталія Михайлівна ***ЖИДОВСЬКА***
к.е.н., доцент кафедри, Львівський національний університет природокористування
ORCID: https://orcid.org/0000-0002-1883-5992
e-mail: znatalka_2909@ukr.net

Олена Геннадіївна ***ДРОЗДОВА***
к.е.н., доцент кафедри, Одеський національний університет імені І.І. Мечникова
ORCID: https://orcid.org/0009-0006-0906-7983
e-mail: lena_drozdova@ukr.net

Тетяна Петрівна ***ФУРСА***
к.е.н., доцент, Івано-Франківський навчально-науковий інститут менеджменту Західноукраїнського національного університету
ORCID: https://orcid.org/0000-0003-4562-2252
e-mail: t.fursa@wunu.edu.ua

ЗАСТОСУВАННЯ МУЛЬТИФАКТОРНОЇ АУТЕНТИФІКАЦІЇ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ БУХГАЛТЕРСЬКОГО ОБЛІКУ В ЕПОХУ ЦИФРОВОЇ ЕКОНОМІКИ УКРАЇНИ

Статтю присвячено дослідженню особливостей застосування мультифакторної аутентифікації для забезпечення безпеки бухгалтерського обліку в епоху цифрової економіки України. Встановлено, що захист даних бухгалтерського обліку став ключовою проблемою для компаній будь-якого масштабу та сфери діяльності. Застосування мультифакторної аутентифікації є критично важливим для забезпечення безпеки бухгалтерського обліку у цифрову епоху. Цей підхід дає змогу унеможливити процес несанкціонованого доступу шляхом вимагання декількох незалежних методів підтвердження ідентичності користувача.

Ключові слова: *цифрові технології, управління ризиками, кібербезпека, інформаційна система обліку, захист інформації*

ВСТУП

В епоху цифрової економіки, коли технологічні зрушення та інновації відіграють ключову роль у сучасному бізнесі, безпека бухгалтерського обліку стає однією з найважливіших складників успішної діяльності підприємств. Застосування мультифакторної аутентифікації є важливим елементом забезпечення цілісності та конфіденційності фінансових даних.

Мультифакторна аутентифікація забезпечує подвійний, а й часто більш складний рівень захисту, застосовуючи комбінацію різних методів перевірки особистості користувача. Це може включати не лише традиційне введення паролів, але й сканування відбитків пальців, розпізнавання обличчя або навіть й голосову ідентифікацію.

У контексті бухгалтерського обліку, де чутливі фінансові дані мають велике значення, мультифакторна аутентифікація стає необхідним інструментом для запобігання несанкціонованому доступу та зловживанню інформацією. Цей підхід забезпечує високий рівень безпеки, зменшуючи ризик фінансових втрат та порушення конфіденційності даних.

В умовах впровадження мультифакторної антентифікації у бухгалтерському обліку в епоху цифрової економіки України підприємства можуть не лише забезпечити безпеку фінансових процесів, але й підвищити рівень довіри до своїх фінансових операцій як серед клієнтів, так і серед партнерів та інвесторів. Такий підхід відображає прогресивне ставлення до безпеки в умовах постійної цифрової трансформації та сприяє стабільності та успішності українських компаній у глобальному економічному просторі.

Проблеми захисту інформації в бухгалтерському обліку розглядали у своїх дослідженнях С. Бардаш [1], С. Вітер [2], І. Вигівська [7], С. Гаркуша [3], І. Грабчук [1], О. Григоревська [7], К. Ілляшенко [5], С. Легенчук [7], Ю. Попівняк [9], І. Світлишин [2] та ін.

У дослідженні С. Бардаша та І. Грабчук висвітлено актуальні аспекти застосування цифрових технологій у бухгалтерському обліку. Науковці вказують на те, що такі технології сприяють скороченню часу на збір та оброблення інформації, а також розширюють можливості ведення даних. У суті дослідження відзначає і переваги, і ризики впровадження цифрових технологій у сфері бухгалтерського обліку. На думку науковців, хоча вони можуть зробити процес бухгалтерського обліку більш ефективним та зручним, потрібно бути готовими до виникнення нових викликів і ризиків, таких як забезпечення кібербезпеки та правової відповідності [1].

С. Вітер та І. Світлишин також звертають увагу на проблему захисту облікової інформації в контексті кібербезпеки. Автори обґрунтовують актуальність питання організації системи кібербезпеки облікової інформації на підприємствах, зокрема у контексті зростання загроз; визначають принципи і заходи, необхідні для ефективного захисту облікової інформації, а також наводять деякі аспекти організації цього процесу. Стаття важлива для розуміння не лише теоретичних аспектів кібербезпеки облікової інформації, а й для практичного застосування принципів та заходів стосовно її захисту на підприємствах [2].

С. Гаркуша у своєму дослідженні вивчає особливості зберігання, архівування та захисту інформації у контексті бухгалтерського обліку. Автор робить акцент на важливості збереження електронних документів на електронних носіях інформації та наголошує на необхідності дотримання встановлених законодавством термінів зберігання. Зокрема, автор підкреслює, що забезпечення безпеки облікової інформації є склад-

ним завданням, яке потребує значних витрат не лише на технічні засоби захисту, але й на розроблення та впровадження відповідних політик і процедур безпеки. Автор наголошує на тому, що облікова інформація є нематеріальною і не наявна окремо, тому потрібно докладати спеціальні зусилля для її збереження та захисту. Це означає, що поряд з технічними заходами необхідно також розвивати і впроваджувати ефективні політики безпеки, залучати кваліфікованих спеціалістів та вдосконалювати процеси управління ризиками [3].

С. Легенчук, І. Вигівська та О. Григоревська акцентують увагу на необхідності захисту інформації, яка формується в системі бухгалтерського обліку, та небезпеках, пов'язаних з її неправомірним використанням. Автори підкреслюють, що безпека цієї інформації є пріоритетом для багатьох компаній, оскільки втрата даних або їх неправильне введення може мати серйозні наслідки. Дослідники наголошують на важливості контролю несанкціонованого доступу до бухгалтерських записів та наводять приклади заходів контролю, таких як політика доступу і паролів, шифрування, блокування дисків тощо. Крім того, науковці обґрунтовують, що захист облікової інформації та уникнення кібератак можливі лише за умови комплексних заходів та спільних дій різних структур, таких як керівництво, бухгалтерія, аудитори та навчальні заклади для підготовки майбутніх фахівців. Ця стаття є важливою для розуміння проблеми захисту інформації в бухгалтерському обліку та пропонує практичні рекомендації для її вирішення [7].

Питання забезпечення кібербезпеки облікової інформації висвітлює також й Ю. Попівняк. Стаття ґрунтується на аналізі статистичних даних та вітчизняних та зарубіжних досліджень: описує ситуацію з кібербезпекою у світі та аналізує ситуацію з кіберзлочинністю в Україні. На основі аналізу автор обґрунтовує систему заходів із забезпечення кібербезпеки бухгалтерської інформації на підприємстві, яка базується на застосуванні загальних та специфічних засобів захисту організаційного, технічного, кадрового та юридичного характеру. Автор закликає до подальших досліджень у напрямі пошуку критеріїв та оцінювання успішності впровадження заходів для забезпечення кібербезпеки бухгалтерської інформації, що є важливим кроком для забезпечення безпеки та надійності облікової інформації [9].

Проте постійні трансформації бізнес-середовища під впливом факторів економічної турбулентності зумовлюють і визначають нові виклики та загрози у сфері кібербезпеки, тому потрібно постійно проводити нові дослідження для розуміння їх впливу на бухгалтерський облік та розробляти стратегії захисту.

МЕТА статті полягає у дослідженні особливостей застосування мультифакторної аутентифікації для забезпечення безпеки бухгалтерського обліку в епоху цифрової економіки України.

РЕЗУЛЬТАТИ

Захист даних бухгалтерського обліку в сучасному бізнес-середовищі став критично важливим питанням для підприємств будь-якого розміру та галузі. Несанкціонований або неправомірний доступ до інформаційної системи бухгалтерського обліку або неспроможність встановлювати та підтримувати внутрішній контроль ускладнюють забезпечення реєстрації, оброблення та подання достовірних і точних транзакцій.

За підрахунками кіберінциденти призводять до серйозних фінансових збитків для багатьох компаній [4, с. 583]. Кібератака, що супроводжується значним порушенням безпеки даних, може не лише негативно вплинути на операційну діяльність компанії, але також спричинити юридичні наслідки для керівництва, яке може стати об'єктом регуляторного або судового розслідування.

Порушення безпеки даних також створює серйозний ризик втрати довіри та репутації, що може призвести до збитків у доходах або зниження ціни акцій публічних компаній [7].

З урахуванням обширного обсягу конфіденційної фінансової інформації, яка зберігається та обробляється в рамках бухгалтерського обліку, необхідність ефективного захисту даних стає не лише проблемою безпеки, а й стратегічним завданням для збереження конфіденційності, точності та інтегритету фінансової інформації. Ця необхідність випливає з низки факторів, серед яких відмітимо:

1. Конфіденційність фінансової інформації. Бухгалтерські дані часто містять конфіденційну інформацію про фінансовий стан підприємства, включаючи прибутки, зобов'язання, активи та інші фінансові показники.

Я. Одовічена та О. Орловський зазначають, що склад і обсяг бухгалтерських даних, які вважаються конфіденційними на підприємстві, а також процедура їх захисту залежать від власника (керівника), який встановлює це відповідно до чинного законодавства, адже саме захист конфіденційної інформації вважається найважливішим аспектом використання таких даних [8].

2. Забезпечення точності та цілісності даних. Бухгалтерська інформація повинна бути захищена від несанкціонованих змін або втручань, щоб гарантувати точність та надійність фінансової звітності.

3. Виконання регулятивних вимог. Багато країн мають регуляторні вимоги до зберігання та захисту бухгалтерської інформації. Їх невиконання може призвести до штрафів, судових справ або навіть втрати ліцензій на ведення діяльності.

4. Збереження конкурентних переваг. Деяка бухгалтерська інформація, така як стратегічні плани, може бути важливою конкурентною перевагою для підприємства. Захист цих даних сприяє запобіганню їх витоку до конкурентів.

Специфіка бухгалтерських даних полягає в тому, що вони нематеріальні й не наявні окремо. Забезпечення безпеки облікової інформації є досить затратною справою не лише через витрати на закупку або установку засобів захисту, але й тому, що важко кваліфіковано визначити межі належної безпеки та гарантувати відповідну безпеку інформаційної системи [3, с. 483].

Проблема забезпечення безпеки під час застосування мережевих продуктів бухгалтерського обліку, якими послуговуються багато користувачів, стоїть дуже гостро. Сформовані в системі бази даних за відсутності адекватних застережних заходів може бути видалено через необережність, зламані або передані зацікавленим особам [2].

Захист облікової інформації визначається рівнем захищеності від випадкових або навмисних впливів,

що можуть завдати шкоди власникам або користувачам цієї інформації.

С. Бардаш та І. Грабчук стверджують, що коли компанії прямо пов'язані з цифровими технологіями, то вплив стає значно більшим, оскільки ці технології тісно пов'язані з роботою персоналу, обробленням інформації та організацією бізнес-процесів. Це означає, що таким компаніям вже притаманний специфічний набір ризиків [1].

Якщо ми говоримо про захист інформації загалом, то маємо на увазі поняття інформаційної безпеки.

Питання інформаційної безпеки у веденні бухгалтерського обліку із застосуванням комп'ютерних технологій доцільно розглядати у двох аспектах (рис. 1).

Превентивні механізми запобігання втратам та перекрученням облікової інформації повинні базуватися на комплексних, взаємопов'язаних методиках і процедурах, серед яких виокремлюють такі [5, с. 181]:

1. Аналіз ризиків:

– проведення систематичного аналізу ризиків для ідентифікації потенційних загроз безпеці обліку;

– оцінювання впливу цих загроз на фінансову інформацію підприємства.

У рамках дослідження варто зазначити, що ризики для бухгалтерської інформації включають будь-які дії або події, спрямовані на незаконний доступ, руйнування, модифікацію або крадіжку фінансових даних, облікових записів, звітності та іншої чутливої інформації, яка застосовується в бухгалтерському обліку. Основні ризики для бухгалтерської інформації згруповано на рис. 2.

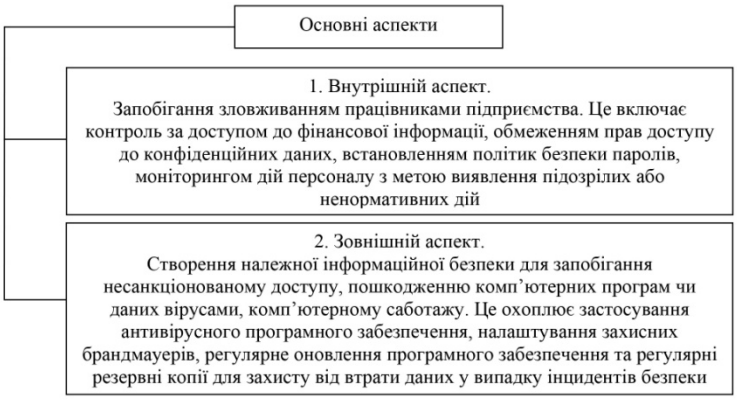

Рис. 1. Основні аспекти інформаційної безпеки під час ведення бухгалтерського обліку [5, с. 181]

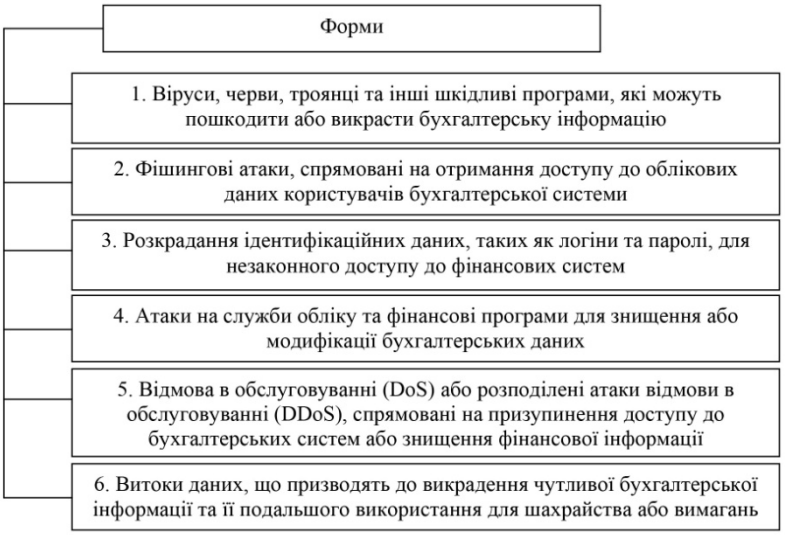

Рис. 2. Ризики для бухгалтерської інформації [власна розробка авторів]

Зауважимо, що такі кіберзагрози можуть призвести до серйозних фінансових проблем, порушення законодавства, втрати довіри клієнтів та інші негативні наслідки для організації. Тому важливо вживати заходів безпеки для захисту бухгалтерської інформації від таких кіберзагроз.

Важливо також окреслити основні передумови виникнення кіберзагроз для бухгалтерської інформації (табл. 1).

Зазначені передумови вказують на широкий спектр факторів, які можуть сприяти виникненню кіберзагроз для бухгалтерської інформації. Для ефективного захисту цієї інформації потрібно вдосконалювати політику кібербезпеки, враховуючи ці передумови, і вживати заходів з мінімізації ризиків.

2. Розроблення політик і процедур:

– розроблення та впровадження політик і процедур забезпечення безпеки, які включають правила доступу, захист паролів, шифрування даних тощо;

– визначення відповідальності за забезпечення безпеки інформації.

3. Впровадження контрольних технологій:

– встановлення системи ідентифікації та аутентифікації, що обмежує доступ до облікової інформації

тільки авторизованим користувачам;

– застосування захисних брандмауерів і систем виявлення вторгнень для моніторингу трафіку та виявлення незвичайних або підозрілих активностей.

4. Технічні заходи безпеки:

– застосування шифрування даних для захисту конфіденційної інформації під час передачі і зберігання;

– регулярне оновлення програмного забезпечення і патчів безпеки для усунення різних недоліків.

5. Навчання персоналу:

– проведення навчання та навчання персоналу з питань безпеки інформації, включаючи правила користування системою, виявлення фішингових атак тощо.

Ці комплексні підходи дають змогу підприємствам ефективно захищати облікову інформацію від загроз і забезпечувати надійність та цілісність їх фінансової звітності.

Сьогодні найбільшу питому вагу в цій групі заходів у системах оброблення обліково-звітної інформації становлять спеціальні пакети програм або окремі програми, які включаються до складу програмного забезпечення з метою реалізації завдань стосовно захисту інформації. Технологічні засоби інформаційної безпеки являють собою комплекс заходів, які вбудовуються в технологічні процеси оброблення даних. Одним із заходів для захисту бухгалтерської інформації підприємства є мультифакторна (багатофакторна) аутентифікація [10].

Н. Коршун, І. Літвінчук, Р. Корчомний та І. Борисов вважають, що мультифакторна аутентифікація – це спосіб підтвердження ідентичності користувача, який вимагає подання двох або більше доказів особистості перед отриманням доступу до облікового запису. Кожен з цих доказів може бути подано у формі номера телефону, адреси електронної пошти або відповіді на секретне питання, доступне лише користувачу. Цей метод забезпечує вищий рівень безпеки, адже для отримання доступу необхідно пройти кілька етапів аутентифікації [6, с 164].

Основні переваги застосування мультифакторної аутентифікації згруповано у табл. 2.

Таблиця 1 – **Передумови виникнення кіберзагроз для бухгалтерської інформації** [9, с. 153–154]

№ з/п	Передумови
1.	Застосування неліцензійного або неперевіреного програмного забезпечення може відкрити доступ для кіберзлочинців через вразливості в програмах.
2.	Застосування слабких інструментів аутентифікації може зробити доступ до бухгалтерської інформації відносно легким для несанкціонованих осіб.
3.	Нехтування правилами захисту робочих комп'ютерів і пристроїв може призвести до інфікування вірусами або зловмисним програмним забезпеченням, що може пошкодити або вкрасти бухгалтерську інформацію.
4.	Застосування робочих пристроїв у неробочих цілях може підвищити ризик втрати або витоку інформації через несанкціонований доступ.
5.	Брак елементарних знань з основ кібербезпеки серед бухгалтерів може призвести до невміння виявити або запобігти кіберзагрозам.
6.	Неправильна розстановка пріоритетів та відсутність підтримки системи менеджменту може призвести до недостатнього фінансування і впровадження заходів з кібербезпеки.
7.	Нехтування правилами збереження бухгалтерських даних і резервування може зробити інформацію вразливою до втрати або пошкодження.
8.	Ігнорування наявних ризиків і негативного досвіду інших учасників ринку може спричинити повторення помилок та збільшення ймовірності кібератак.
9.	Відсутність відповідного спеціаліста із захисту бухгалтерської інформації може призвести до недостатньої уваги до цього аспекту безпеки.
10.	Недостатнє розмежування прав користувачів і довгий перелік осіб, які мають доступ до даних, може створити можливості для несанкціонованого доступу або зловживання правами.
11.	Складне податкове та бізнес-оточення підприємства може створити додаткові виклики для забезпечення безпеки бухгалтерської інформації через різноманітність інтересів та вимог.

Таблиця 2 – **Основні переваги застосування мультифакторної аутентифікації для бухгалтерського обліку [***власна розробка авторів***]**

№ з/п	Перевага	Опис
1.	Захист від несанкціонованого доступу	Мультифакторна аутентифікація дає змогу впевнитися, що лише зареєстровані користувачі мають доступ до бухгалтерських даних і систем. Це може запобігти таким загрозам, як фішинг, перехоплення паролів тощо.
2.	Підвищення рівня безпеки	Пов'язані фактори аутентифікації, такі як пароль та біометричні дані (відбитки пальців, розпізнавання обличчя), створюють більш складний бар'єр для зловмисників, що намагаються отримати доступ до систем бухгалтерського обліку.
3.	Зменшення ризику фінансових втрат	Через застосування мультифакторної аутентифікації, зменшується ризик того, що фінансові дані залишаються захищеними від крадіжок та несанкціонованого доступу, що може призвести до значних фінансових втрат для організації.
4.	Відповідність вимогам законодавства	З урахуванням зростаючого рівня кіберзагроз та змін у законодавстві стосовно захисту даних, застосування мультифакторної аутентифікації може допомогти організаціям відповідати вимогам до забезпечення конфіденційності та цілісності даних.

На нашу думку, мультифакторна аутентифікація є важливим елементом кібербезпеки, що забезпечує додатковий захист для доступу до різноманітних систем, програм та послуг. Зазвичай вона включає в себе комбінацію різних методів перевірки особи, таких як пароль, відбиток пальця або розпізнавання обличчя. Це

дає змогу підвищити безпеку, оскільки збільшується складність для потенційних зловмисників отримати доступ до системи. Виявлення та застосування додаткових факторів автентифікації, крім простого пароля, створює більш міцний бар'єр для несанкціонованого доступу. Мультифакторна аутентифікація зменшує ймовірність успішного злому облікових записів і зберігає конфіденційні дані в безпеці.

Вітчизняні компанії повинні усвідомлювати значення і важливість застосування МФА для забезпечення безпеки фінансових даних. Це допоможе їм зменшити ризик витоку конфіденційної інформації, а також відповісти вимогам регуляторів у сфері безпеки даних.

Розглянемо основні способи застосування мультифакторної аутентифікації для забезпечення безпеки бухгалтерського обліку в Україні:

1. Пароль і біометрія. Комбінація пароля і біометрії є одним з найбільш ефективних способів забезпечення безпеки в електронних системах. Під час введення пароля користувач також надає біометричні дані, такі як відбиток пальця або розпізнавання обличчя, що забезпечує подвійний захист, оскільки ці дані унікальні для кожної особи і неможливо відтворити або підробити.

Паролі можуть бути піддані атакам злому, однак застосування біометричних даних додає більшого захисту даним, оскільки вони вимагають фізичної присутності користувача для підтвердження ідентичності.

Крім того, застосування біометричних даних спрощує процес аутентифікації для користувачів, а отже, вони можуть просто застосовувати свої фізичні характеристики замість запам'ятовування складних паролів.

Все це робить комбінацію пароля та біометрії ефективним і зручним засобом забезпечення безпеки, особливо в контексті бухгалтерського обліку.

2. OTP (Одноразовий пароль) – це ефективний метод забезпечення безпеки, що створює додатковий захист основного пароля. Користувач може отримати одноразовий пароль через різні канали комунікації, такі як SMS, мобільний додаток або електронну пошту. Цей пароль діє лише один раз і надсилається користувачеві під час кожної спроби входу в систему або проведення важливих операцій. Застосування OTP зменшує ризик несанкціонованого доступу, оскільки навіть якщо основний пароль стане відомим зловмисникам, вони все одно не матимуть доступу до системи без одноразового пароля. Цей метод є досить зручним для користувачів.

3. Токен аутентифікації є ефективним засобом забезпечення безпеки в епоху цифрової економіки. Це може бути фізичний пристрій, наприклад ключ-карта, USB-токен або віртуальний пристрій, що генерує одноразові паролі або коди доступу. Користувач отримує цей токен і використовує його для аутентифікації під час входу в систему або підтвердження важливих операцій. Одноразові паролі або коди доступу генеруються на токені і зазвичай мають обмежений час дії, зменшуючи ризик несанкціонованого доступу. Застосування такого методу забезпечує високий рівень безпеки, оскільки потрібно мати фізичний доступ до токена або відповідних віртуальних пристроїв для отримання доступу до системи. Токен аутентифікації є важливим елементом забезпечення безпеки бухгалтерського обліку в умовах цифрової економіки України, де інформаційні загрози є серйозними.

4. Двоетапна або багатоетапна аутентифікація є досить ефективним методом забезпечення безпеки в епоху цифрової економіки. Її суть полягає в тому, що користувач повинен пройти кілька етапів підтвердження своєї ідентичності. Наприклад, спочатку він вводить основний пароль, а потім має ввести OTP, який надсилається на його мобільний пристрій або іншим каналом зв'язку.

Крім того, в деяких випадках потрібно буде додаткове підтвердження через біометричні дані, такі як відбиток пальця або розпізнавання обличчя. Багатоетапна аутентифікація є важливим елементом забезпечення безпеки бухгалтерського обліку, оскільки допомагає уникнути несанкціонованого доступу та захищає конфіденційні дані користувачів.

5. Аутентифікація на основі місцезнаходження або IP-адреси є ще одним важливим аспектом забезпечення безпеки в епоху цифрової економіки. Система може перевіряти географічне місцезнаходження користувача або IP-адресу його пристрою як додаткове підтвердження його ідентичності. Наприклад, якщо зазвичай користувач входить у систему з певного місця або за допомогою IP-адреси, а згодом спроба входу відбувається з іншої локації, система може вимагати додаткової перевірки, такої як введення OTP-коду або пароля або навіть заблокувати доступ до облікового запису до подальшого підтвердження. Цей підхід допомагає уникнути несанкціонованого доступу до системи, особливо в разі, якщо обліковий запис користувача викрадено.

6. Строгий контроль доступу є критичним аспектом забезпечення безпеки в бухгалтерському обліку в епоху цифрової економіки. Це означає, що кожен працівник, який має доступ до бухгалтерської системи, повинен мати чітко визначені ролі та обмежений доступ до відповідних функцій згідно з його обов'язками та повноваженнями. Такий підхід дає змогу зменшити ризик несанкціонованого доступу до конфіденційної інформації та запобігає можливим внутрішнім загрозам безпеці.

Кожному користувачеві надаються лише ті права доступу, які необхідні для виконання його конкретних завдань, і ці права регулярно переглядаються та оновлюються відповідно до змін у ролі або функціях працівника. Такий підхід допомагає попереджати можливі порушення безпеки та забезпечує високий рівень захисту конфіденційної інформації в бухгалтерському обліку.

7. Моніторинг та аналіз поведінки користувачів є ключовим компонентом забезпечення безпеки в епоху цифрової економіки. Ця практика передбачає постійне спостереження за звичайними діями користувачів у межах бухгалтерської системи з метою виявлення будь-яких аномальних чи незвичайних активностей.

Система проводить аналіз великого обсягу даних, щоб виявити відхилення в поведінці, такі як незвичайні часи входу в систему, несподівані операції чи доступ до неавторизованих ресурсів. Ці аномалії можуть свідчити про можливі загрози безпеці, такі як несанкціонований доступ або компрометація облікових записів. Після виявлення підозрілих дій система може автоматично виконати певні заходи, такі як блокування облікового запису або повідомлення адмініс-

тратора системи для подальшого аналізу та реагування. Моніторинг та аналіз поведінки користувачів допомагають вчасно виявляти та впроваджувати заходи з виявлення потенційних загроз безпеці, ство-рюючи високий рівень захисту в бухгалтерському обліку.

Отже, загальний принцип мультифакторної антентифікації полягає в тому, щоб ускладнити процес несанкціонованого доступу до бухгалтерської інформації шляхом вимагання декількох незалежних способів підтвердження ідентичності користувача. Застосування мультифакторної аутентифікації допоможе забезпечити високий рівень безпеки бухгалтерського обліку в умовах цифрової економіки.

ВИСНОВКИ

Отже, застосування мультифакторної аутентифікації є критично важливим для забезпечення безпеки бухгалтерського обліку в епоху цифрової економіки України. Цей підхід дає змогу ускладнити процес несанкціонованого доступу шляхом вимагання декількох незалежних методів підтвердження ідентичності користувача.

Розглянуті методи, такі як комбінація пароля та біометрії, застосування одноразових паролів, токенів аутентифікації, а також моніторинг та аналіз поведінки користувачів, сприяють зменшенню ризику кіберзагроз і забезпечують високий рівень захисту конфіденційної інформації. Ці підходи демонструють ефективність у боротьбі з різноманітними загрозами безпеці та допомагають уникнути можливих порушень безпеки.

Реалізація мультифакторної аутентифікації є важливим кроком для підвищення захищеності бухгалтерської інформації в умовах постійно зростаючої кількості кіберзагроз та загроз безпеці в цифровій економіці.

Подальші дослідження можуть спрямовуватися на пошук нових, більш інноваційних методів, що дадуть змогу підвищити ефективність заходів безпеки. Наприклад, вивчення можливості інтеграції штучного інтелекту та машинного навчання для автоматизації процесів аналізу поведінки користувачів та виявлення аномальних активностей.

Список використаних джерел

1. Бардаш С.В., Грабчук І.Л. Цифрові технології в сфері бухгалтерського обліку: основні можливості та ризики. *Ефективна економіка*. 2021. № 9. URL: https://doi.org/10.32702/2307-2105-2021.9.18

2. Вітер С.А., Світлишин І. І. Захист облікової інформації та кібербезпека підприємства. *Економіка та суспільство*. 2017. № 11. С. 497–502. URL: http://ir.znau.edu.ua/handle/123456789/9969

3. Гаркуша С.А. Особливості зберігання, архівування та захисту інформації в процесі організації бухгалтерського обліку. *Інфраструктура ринку*. 2019. № 30. С. 478–485. URL: http://www.market-infr.od.ua/journals/2019/30_2019_ukr/75.pdf

4. Григоревська О.О. Захист облікової інформації в умовах забезпечення кібербезпеки підприємства. *Achievements and prospects of modern scientific research*: abstracts of the I International scientific and practical conference (Buenos Aires, Argentina, 6–8 December 2020). Buenos Aires, Argentina : Editorial EDULCP, 2020. P. 582–584. URL: https://er.knutd.edu.ua/handle/123456789/17377

5. Ілляшенко К. Інформаційна безпека сучасного бухгалтерського обліку. *Науковий вісник Міжнародного гуманітарного університету*. 2019. № 40. С. 179–184. URL: https://doi.org/10.32841/2413-2675/2019-40-23

6. Коршун Н.В., Літвінчук І.С., Корчомний Р.О., Борисов І.В. Розробка рекомендацій щодо мінімізації ризиків зломів облікових записів на основі аналізу найпоширеніших методів злому. *Кібербезпека: освіта, наука, техніка*. 2021. № 4 (12). С. 163–171. URL: https://elibrary.kubg.edu.ua/id/eprint/38750

7. Легенчук С.Ф., Вигівська І.М., Григоревська О.О. Захист облікової інформації в умовах забезпечення кібербезпеки. *Проблеми теорії та методології бухгалтерського обліку, контролю і аналізу*. 2022. № 2 (52). С. 40–46. URL: https://doi.org/10.26642/pbo-2022-2(52)-40-46

8. Одовічена Я.А., Орловський О.Я. Комерційна таємниця. Як роботодавцю захистити секрети? *Науковий вісник Ужгородського національного університету. Серія Право*. 2023. № 80, Ч. 1. С. 312–318. URL: https://doi.org/10.24144/2307-3322.2023.80.1.44

9. Попівняк Ю.М. Кібербезпека та захист бухгалтерських даних в умовах застосування новітніх інформаційних технологій. *Бізнес Інформ*. 2019. № 8. С.150–157. URL: https://doi.org/10.32983/2222-4459-2019-8-150-157

10. Шевчук І.Б., Депутат Б.Я., Тарасенко О.Є. Цифровізація та її вплив на економіку України: переваги, виклики, загрози й ризики. *Причорноморські економічні студії.* 2019. № 47–2. С. 173–177. URL: https://doi.org/10.32843/bses.47-66

References

1. Bardash S.V., Hrabchuk I. L. Digital technologies in the field of accounting: main opportunities and risks. *Efektyvna ekonomika*. 2021. No. 9. URL: https://doi.org/10.32702/2307-2105-2021.9.18 *(in Ukrainian)*.

2. Viter S.A., Svitlishin I.I. Protection of accounting information and cyber security of the enterprise. *Economy and Society*. 2017. No. 11. pp. 497–502. URL: http://ir.znau.edu.ua/handle/123456789/9969 *(in Ukrainian)*.

3. Harkusha S.A. Features of storage, archiving and protection of information at the accounting organization. *Market Infrastructure*. 2019. No. 30. pp. 478–485. URL: http://www.market-infr.od.ua/journals/2019/30_2019_ukr/75.pdf *(in Ukrainian)*.

4. Hryhorevska O.O. Protection of accounting information in the conditions of ensuring cyber security of the enterprise. *Achievements and prospects of modern scientific research* : abstracts of the I International scientific and practical conference (Buenos Aires, Argentina, 6–8 December 2020). Buenos Aires, Argentina : Editorial EDULCP, 2020. pp. 582–584. URL: https://er.knutd.edu.ua/handle/123456789/17377 *(in Ukrainian)*.

5. Illiashenko K. Informacijna bezpeka suchasnogo buhgalterskogo obliku. *Scientific Herald of International Humanitarian University*. 2019. No. 40. P. 179–184. URL: https://doi.org/10.32841/2413-2675/2019-40-23 *(in Ukrainian)*.

6. Korshun N.V., Litvinchuk I.S., Korchomnyi R.O., Borysov I.V. Development of recommendations for minimizing the risks of account hacking on the basis of analysis of the most common hacking methods. *Cybersecurity: Education, Science, Technique*. 2021. No. 4 (12). pp. 163–171. URL: https://elibrary.kubg.edu.ua/id/eprint/38750 *(in Ukrainian)*.

7. Legenchuk S.F., Vyhivska I.M., Hryhorevska O.O. Protection of accounting information in the conditions of cyber security.

Problems of Theory and Methodology of Accounting, Control and Analysis. 2022. No. 2 (52). pp. 40–46. URL: https://doi.org/10.26642/pbo-2022-2(52)-40-46 *(in Ukrainian)*.

8. Odovichena Y.A., Orlovskyi O.Y. A commercial secret. How can employer protect his secrets? *Uzhhorod National University Herald. Series: Law*. 2023. Vol. 80. No. 1. pp. 312–318. URL: https://doi.org/10.24144/2307-3322.2023.80.1.44 *(in Ukrainian)*.

9. Popivnyak Y.M. Cybersecurity and protection of accounting data under conditions of modern information technology. *Business Inform*. 2019. No. 8. pp. 150–157. URL: https://doi.org/10.32983/2222-4459-2019-8-150-157 *(in Ukrainian)*.

10. Shevchuk I.B., Deputat B.Ya., Tarasenko O.Y. Digitalization and its impact on Ukraine's economy: advantages, challenges, threats and risks. *Black Sea Economic Studies*. 2019. No. 47–2. pp. 173–177. URL: https://doi.org/10.32843/bses.47-66 *(in Ukrainian)*.

Nataliia ZHYDOVSKA
PhD in Economics, Associate Professor of department, Lviv National Environmental University
ORCID: https://orcid.org/0000-0002-1883-5992
e-mail: znatalka_2909@ukr.net

Olena DROZDOVA
PhD in Economics, Associate Professor of department, Odesa I.I. Mechnikov National University
ORCID: https://orcid.org/0009-0006-0906-7983
e-mail: lena_drozdova@ukr.net

Tetiana FURSA
PhD in Economics, Associate Professor, Ivano-Frankivsk Educational and Scientific Institute of Management of West Ukrainian National University
ORCID: https://orcid.org/0000-0003-4562-2252
e-mail: t.fursa@wunu.edu.ua

THE USE OF MULTI-FACTOR AUTHENTICATION TO ENSURE THE SECURITY OF ACCOUNTING IN THE ERA OF THE DIGITAL ECONOMY OF UKRAINE

This paper is devoted to the study of the features of the application of multifactor authentication to ensure the security of accounting in the era of the digital economy of Ukraine. The research uses scientific and empirical methods, including the collection and comparison of information, as well as complex methods of analysis, synthesis and generalization. The informational basis of the paper is the scientific works of domestic and foreign scientists, which highlight the issue of using multifactor authentication to ensure the security of accounting. It is noted that nowadays, the protection of accounting data has become a key problem for companies of any scale and field of activity. Unauthorized access to the accounting system, as well as the failure to establish and maintain internal controls, can make it difficult to record, process and present reliable and accurate transactions. It is noted that cyber threats to accounting information include any actions or events aimed at illegal access, destruction, modification or theft of financial data, accounts, reports and other sensitive information used in accounting. The conclusion noted that the use of multi-factor authentication is critically important for ensuring the security of accounting in the era of Ukraine's digital economy. This approach makes it possible to complicate the unauthorized access process by requiring multiple independent methods of verifying the user's identity. The considered methods, such as a combination of password and biometrics, use of one-time passwords, authentication tokens, as well as monitoring and analysis of user behavior, contribute to reducing the risk of cyber threats and provide a high level of protection of confidential information. These approaches demonstrate effectiveness in combating a variety of security threats and help avoid possible security breaches.

Keywords: *digital technologies, risk management, cyber security, accounting information system, information protection*