

Електронний журнал «Ефективна економіка» включено до переліку наукових фахових видань України з питань економіки (Категорія «Б», Наказ Міністерства освіти і науки України № 975 від 11.07.2019). Спеціальності – 051, 071, 072, 073, 075, 076, 292.
Ефективна економіка. 2024. № 4.

DOI: <http://doi.org/10.32702/2307-2105.2024.4.9>
УДК 681.3

М. В. Болдуєв,
д. держ. упр., професор, НУ «Запорізька політехніка»
ORCID ID: <https://orcid.org/0000-0002-8889-6555>
О. В. Болдуєва,
д. е. н., доцент, Запорізький національний університет
ORCID ID: <https://orcid.org/0000-0001-5267-1816>
О. Г. Лищенко,
к. е. н., доцент, НУ «Запорізька політехніка»
ORCID ID: <https://orcid.org/0000-0001-9211-9567>

ПОТЕНЦІАЛ І ПРОБЛЕМИ ЗАПРОВАДЖЕННЯ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ В УКРАЇНІ

M. Bolduiev,
Doctor of Sciences in Public Administration, Professor,
National University «Zaporizhzhia Polytechnic»
O. Bolduieva,
Doctor of Economic Sciences, Associate Professor,
Zaporizhzhia National University
O. Lyshchenko,
PhD in Economics, Associate Professor,
National University «Zaporizhzhia Polytechnic»

POTENTIAL AND PROBLEMS OF IMPLEMENTATION OF ELECTRONIC DOCUMENT TRANSFER IN UKRAINE

У статті здійснено узагальнення міжнародного досвіду застосування сучасних технологій електронного документообігу в бухгалтерському обліку, виявлення переваг та загроз його застосування та визначення заходів впровадження в Україні на базі найкращих практик. Встановлено, що основними перевагами технологій електронного документообігу є: швидший обіг документів; зменшення витрат на папір та друк; зручний доступ до інформації; робота в реальному часі; автоматизація бізнес-процесів та гнучкість пристосування до потреб управління; забезпечення безпеки інформації, контролю та захисту від втрати даних; інтеграція з іншими електронно-інформаційними системами.

До недоліків запровадження електронного документообігу в бухгалтерському обліку слід віднести відсутність в країнах які впровадили систему єдиного стандартизованого підходу і законодавчо-нормативного регулювання. Це часто призводить до плутанини та неефективності, оскільки різні країни можуть мати різні стандарти та системи. Проте основною невирішеною проблемою застосування та розвитку електронного документообігу на сьогодні залишаються загрози безпеці зберігання та передачі інформації.

Визначено перспективні заходи впровадження міжнародного досвіду які допоможуть Україні вдосконалити свою систему електронного документообігу та впровадити його з максимальною користю та мінімізацією ризиків.

The article summarizes the international experience of using modern electronic document management technologies in accounting, identifies the advantages and threats of its use, and determines implementation measures in Ukraine based on best practices. It was established that the main advantages of electronic document circulation technologies are: faster circulation of documents; reduction of paper and printing costs; convenient access to information; work in real time; automation of business processes and flexibility of adaptation to management needs; ensuring

information security, control and protection against data loss; integration with other electronic information systems.

Among the shortcomings of the introduction of electronic document flow in accounting should be attributed the absence of a unified standardized approach and legislative regulation in countries that have implemented a system. This often leads to confusion and inefficiency, as different countries may have different standards and systems. However, the main unsolved problem of the application and development of electronic document circulation today remains threats to the security of information storage and transmission.

When implementing electronic document flow in accounting in Ukraine, it is important to take into account international experience and best practices. The main aspects of the implementation of such experience should be considered: the use of international standards to ensure compatibility and interoperability between different systems; implementation of effective cyber protection measures in accordance with international standards and best practices; use of internationally recognized electronic signatures and cryptographic methods to ensure the reliability and legal credibility of documents; taking into account international experience in establishing standards for effective data exchange between organizations and enterprises; implementation of regular monitoring and updating of strategies in accordance with new international standards and technologies.

Ключові слова: електронний документообіг, бухгалтерський облік, міжнародний досвід, інформація, автоматизація

Keywords: electronic document management, accounting, international experience, information, automation

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. У сучасному цифровому світі компанії все частіше звертаються до електронного документообігу, щоб оптимізувати свої процеси та підвищити ефективність. Електронний документообіг – це процес

електронного управління та обміну документами між двома або більше сторонами. З точки зору бухгалтерського обліку електронний документообіг – це система, яка забезпечує можливість зберігати, шукати та здійснювати управління цифровими документами, такими як фінансові записи, рахунки-фактури та інші документи, пов'язані з бухгалтерським обліком. В сучасному світі, де бізнес і технології нерозривно пов'язані, електронний документообіг стає необхідністю для компаній, щоб забезпечити плавність та ефективність інформаційних потоків.

Аналіз останніх досліджень та публікацій. Питання щодо організування процесу електронного документообігу досліджували такі вчені, як С.Я. Бабінська, Ф.Ф. Бутинець, А.Ю. Герасимчук, Ю. Данькевич, В.П. Завгородній, О.Ю. Закревська, С.В. Івахненко, М.М. Коцупатрий, М.Ф. Кропивко, О.О. Можаяєв, І.Я. Назарова, І.Р. Недошитко, В.С. Політанський, Л. Тарасюк, О.М. Ус, О.В. Шарапова, О.В. Шевченко та ін. Зважаючи на те, що на сьогодні є багато науковців, які досліджували питання формування та організації електронного документообігу на підприємствах, варто зазначити, що проблематика вивчення досвіду впровадження системи електронного документообігу в бухгалтерському обліку на рівні країни, залишається недостатньо дослідженою та потребує подальшого вивчення.

Формулювання цілей статті (постановка завдання). Метою статті є узагальнення міжнародного досвіду застосування сучасних технологій електронного документообігу в бухгалтерському обліку, виявлення переваг та загроз його застосування та визначення заходів впровадження в Україні на базі найкращих практик.

Виклад основного матеріалу дослідження. Електронний документообіг використовує сучасні технології для автоматизації та полегшення обробки документів у компанії.

Однією з головних переваг електронного документообігу є підвищення ефективності інформаційних потоків за рахунок швидкого обігу документів.

Електронні документи можуть бути легко створені, підписані та надіслані. Це створює можливості компаніям швидко обробляти та затверджувати

документи, що покращує загальну продуктивність та сприяє пришвидшенню бізнес-процесів [1].

Можливість створювати, редагувати та формувати документи безпосередньо в електронних системах усуває потребу у фізичних копіях та займає менше часу, порівняно з традиційним методом написання та редагування на папері. Крім того електронні системи надають можливість одночасно працювати з документами декільком особам, забезпечуючи синхронізований доступ до актуальної інформації, а також в реальному часі вносити зміни та співпрацювати над документами.

Системи електронного документообігу можуть генерувати різноманітні звіти та аналітичні дані сприяючи ефективній обробці інформації. Зручний доступ до цих даних забезпечує можливість приймати обґрунтовані рішення на основі актуальної інформації [2]. Сформовані електронні звіти та аналізи не вимагають фізичного друку.

Електронний документообіг забезпечує зручний доступ до інформації завдяки впровадженню сучасних технологій та інновацій в управлінні документами. Завдяки електронним системам, які забезпечують синхронізацію та оновлення в реальному часі, користувачі можуть переглядати завжди актуальні версії документів без необхідності чекати на їхнє фізичне оновлення, швидко знаходити, переглядати та редагувати документи, що сприяє ефективній роботі в умовах розподіленого робочого середовища. Системи електронного документообігу можуть автоматично надсилати повідомлення та нагадування користувачам про важливі терміни, завдання та зміни в документах, які сповіщають користувачів про необхідність дій, таких як підписання, затвердження документів тощо [3].

Застосування в роботі з документами мобільних пристроїв дає можливість отримувати, переглядати та редагувати документи прямо з смартфона чи планшета. Це особливо зручно для бізнесменів та співробітників, які постійно перебувають в русі. Крім того це сприяє розвитку концепції «паперового офісу» і створює умови співробітникам працювати дистанційно, отримуючи доступ до

всіх необхідних документів онлайн зменшуючи необхідність друкування та передачі паперових документів для роботи з ними [4].

Електронний документообіг дозволяє налаштовувати автоматизовані потоки роботи, які автоматично направляють документи на різні стадії рецензування та затвердження. Це забезпечує надсилання документів відразу тим особам, які повинні брати участь у їх обробці. Можливість застосування електронних підписів для підпису та затвердження документів надає можливість здійснювати швидкі та ефективні процеси узгодження без необхідності фізичного підпису та пересилання паперових документів, що зменшує витрати на фізичний обіг документів та поліпшує загальну продуктивність праці [5].

Зберігання документів в електронному форматі економить ресурси та сприяє екологічності бізнесу. Зберігання документів в хмарних системах дозволяє отримувати доступ до них з будь-якого місця за умови підключення до Інтернету. Це робить інформацію доступною в реальному часі, незалежно від місцезнаходження користувача. Потужний інструментарій для ефективного пошуку та фільтрації інформації в електронній системі управління документами дає можливість користувачам легко знаходити необхідні документи за ключовими словами, датами, категоріями тощо. Крім того електронна архівація ефективно зменшує потребу у фізичному зберіганні паперових копій, що також включає в себе витрати на простір для організації архівного господарства.

Регулярне резервне копіювання та захист від втрати даних є необхідним елементом безпеки. Електронний документообіг включає в себе засоби автоматичного збереження копій документів. Він є критично важливим аспектом для забезпечення безпеки, цілісності та доступності інформації в організації [6].

Водночас ефективний захист від втрати даних в електронному документообігу вимагає комплексного підходу, що охоплює технічні, організаційні та людські аспекти безпеки. До методів забезпечення ефективного захисту від втрати даних слід віднести:

- регулярне створення резервних копій – забезпечує можливість зберігати копії важливих даних, що значно полегшує відновлення інформації у випадку

втрати чи пошкодження. Автоматизоване резервне копіювання забезпечує систематичність цього процесу;

- використання хмарових технологій – їх застосування забезпечує зберігання даних в безпечних та надійних хмарових сховищах. Це гарантує доступність інформації з будь-якого місця та захищає від втрати даних через фізичні пошкодження чи збої обладнання [7];

- впровадження систем реєстрації подій та моніторингу – дозволяє вчасно виявляти аномальні ситуації, які можуть призвести до втрати даних, оперативно реагувати й усувати проблеми;

- використання систем інтелектуального виявлення загроз (IDS) та систем захисту від вторгнень (IPS) надає можливість вчасно виявляти та запобігати потенційним загрозам безпеки даних;

- застосування стратегії рековалідації даних – передбачає план дій у випадку втрати інформації. Це може включати відновлення з резервних копій, використання засобів відновлення даних чи інші методи;

- забезпечення фізичної безпеки серверних приміщень та централізованих сховищ даних – є важливим аспектом захисту від природних катастроф, пожеж чи несанкціонованого доступу;

- навчання та свідомість персоналу – ефективний захист від втрати даних також передбачає навчання персоналу та підвищення їхньої свідомості стосовно правил безпеки, відновлення даних та дотримання внутрішніх політик безпеки;

- розробка та проведення тестувань надійності – систематичні тести надійності та відновлення даних забезпечують можливість перевіряти ефективність заходів безпеки та виявляти можливі слабкі місця у системі.

Однією з основоположних вимог до електронного документообігу в умовах сьогодення є реалізація комплексу заходів для забезпечення безпеки та контролю за інформацією, що обробляється в електронній формі [8]. Забезпечення безпеки передачі і зберігання документів, має унеможливити несанкціонований доступ і основним інструментом цього механізму є шифрування. Воно використовується для забезпечення конфіденційності, цілісності та доступності даних. Крім того

шифрування є важливим для відповідності регуляторним вимогам та стандартам безпеки даних, які можуть стосуватися конкретної галузі чи сфери діяльності. Застосування безпечних протоколів передачі даних, таких як SFTP (Secure File Transfer Protocol) або HTTPS, дозволяє забезпечити захищені механізми обміну інформацією між різними сторонами.

В цілому шифрування має вирішувати такі основні завдання:

- захист конфіденційності – шифрування забезпечує зберігання та передачу інформацію так, щоб лише авторизовані особи могли розкодувати і прочитати її. Це важливо для захисту від несанкціонованого доступу із боку третіх осіб;

- захист цілісності даних – шифрування допомагає впевнитися, що дані не були змінені чи підмінені під час передачі або зберігання. Воно забезпечує відсутність будь-яких змін у вмісті даних під час їхнього переміщення.

- захист від кібернетичних атак – шифрування є ефективним способом захисту від різних видів кібератак, таких як перехоплення даних, атаки "посеред людини", введення в обман, злам системи та інші види атак на конфіденційність даних.

Процес шифрування включає в себе використання алгоритму шифрування та ключа шифрування. Інформація шифрується на відправнику і розшифровується на отримувачі за допомогою ключа. Цей процес робить дані непрочитуваними для осіб, які не мають права доступу. Шифрування може використовуватися в різних контекстах, таких як електронна пошта, передача файлів через мережу, зберігання даних на серверах, мобільні додатки, інтернет-банкінг і т.д.

Встановлення конфіденційності на рівні конкретних документів за допомогою шифрування на рівні файлу або застосування прав доступу створює механізм обмеження перегляду або редагування документів з наданням відповідної можливості лише для авторизованих користувачів.

Електронні системи дозволяють налаштовувати права доступу до документів. Це означає, що користувачі отримують доступ тільки до тих документів, до яких у них є відповідні права, забезпечуючи безпеку та конфіденційність інформації. Електронні підписи користувачів системи дають

можливість підтвердження автентичності документів та осіб, які їх підписують. Крім того системи управління ідентифікацією та аутентифікацією (Identity and Access Management, IAM) у електронному документообігу відіграють ключову роль у забезпеченні безпеки, конфіденційності та цілісності інформації. Загальною метою систем IAM є створення ефективної та безпечної ідентифікаційної та аутентифікаційної інфраструктури, що відповідає потребам сучасного електронного документообігу.

До переваг систем IAM слід віднести:

- безпеку – контроль доступу (IAM гарантує, що лише авторизовані користувачі мають доступ до конфіденційної інформації), мінімізацію ризиків (зменшення ризиків несанкціонованого доступу та зловживань за допомогою строгих політик ідентифікації та аутентифікації).

- зручність – забезпечення синхронізації та оновлення даних про користувачів усіма системами, що використовуються.

- ефективність – автоматизація ряду процесів, таких як створення та видалення облікових записів, забезпечує ефективність управління ідентифікацією.

- підтримка політики безпеки – надання можливості налаштовувати деталізовані права доступу для різних користувачів відповідно до політик безпеки.

Забезпечення функціонування систем IAM здійснюється за рахунок застосування таких інструментів:

- багаторівнева аутентифікація – використання двох або більше методів аутентифікації для підвищення рівня безпеки (наприклад, пароль + SMS-код).

- силові паролі та політики паролів – запровадження політик, що вимагають використання складних паролів, зменшує ймовірність взлому електронної системи.

- сертифікати і застосування жетонів. Використання сертифікатів здійснюється для ідентифікації та підтвердження вірності користувача. Використання жетонів доступу для застосовують для забезпечення безпеки під час обміну інформацією.

- централізоване управління обліковими записами та їх привілеями для спрощення адміністрування.

- шифрування інформації використовується для захисту збережених та передаваних даних.

- моніторинг та звітність застосовують для виявлення підозрілих або несанкціонованих дій.

- адаптивний доступ – використання аналітики для виявлення аномальної поведінки користувачів та вжиття відповідних заходів безпеки.

В свою чергу журналювання та аудит у електронному документообігу є необхідними компонентами для ефективного управління інформацією та забезпечення безпеки інформації в сучасних підприємствах. Сучасна система електронного документообігу в обов'язковому порядку веде журнали та аудит дій користувачів. Це не лише забезпечує відстеження, хто і коли здійснював доступ чи зміни в документах, але й надає можливість швидко виявляти та реагувати на потенційні загрози.

Журналювання та аудит у електронному документообігу спрямовані на вирішення таких завдань:

- відстеження та аналіз дій користувачів інформації – журналювання створює механізми відстеження усі дії користувачів в системі, включаючи перегляд, редагування, видалення документів та інші операції. Аудит дозволяє аналізувати ці журнали для виявлення тенденцій, несправностей або потенційних загроз;

- забезпечення безпеки та захисту від зловживань – виявлення незвичайних або підозрілих дій, що можуть бути ознакою зловживань або несанкціонованого доступу. Це сприяє попередженню можливих загроз безпеці;

- відновлення даних та відновлення системи – журнали подій можуть використовуватися для відновлення даних у випадку їх втрати чи пошкодження. Також, вони допомагають відновити систему до попереднього стану після інциденту;

- забезпечення відповідності законодавчо-нормативним вимогам, що вимагають збереження історії дій, особливо в чутливих галузях, наприклад, в фінансовому секторі;

- зменшення ризику помилок та фінансових втрат – відстеження кожного етапу роботи з документами забезпечує можливість виявлення та виправлення помилок, а також запобігання можливим фінансовим втратам підприємства через неправильні рішення;

- інформаційне забезпечення аналітики та оптимізація процесів – дані з журналів подій можуть використовуватися для аналізу ефективності та оптимізації бізнес-процесів в організації, спрямовуючи увагу на найбільш вдалі практики та виявлення можливих покращень;

- забезпечення довіри та легальності дій та рішень – аудит та журналювання надають переконливі докази щодо легальності дій та рішень, що може бути важливим у випадках конфліктів, перевірок чи судових справ;

- співставлення прав доступу та фактичного використання – даними аудиту можна порівнювати надані права доступу та фактичне їх використання, що дає можливість виявляти можливі відхилення від установлених норм та правил;

- ефективне управління ризиками – збір та аналіз журналів подій дозволяє ефективно виявляти та управляти потенційними ризиками, зменшуючи ймовірність виникнення проблем.

Метою автоматизованих систем попередження та виявлення загроз є забезпечення високого рівня безпеки та надійності електронного документообігу, а також швидкого реагування на нові та такі, що постійно розвиваються загрози. Автоматизовані системи попередження та виявлення загроз (Automated Threat Prevention and Detection Systems) в електронному документообігу відіграють критичну роль у забезпеченні безпеки та цілісності інформації.

Перевагами такої системи слід вважати:

- реагування в реальному часі і миттєве виявлення загроз забезпечуючи можливість негайно реагувати на потенційні атаки.

- мінімізація витрат на час та ресурсів – застосування алгоритмів та технологій штучного інтелекту для швидкого та ефективного аналізу великих обсягів даних, що, в свою чергу, забезпечує можливість мінімізувати витрати часу та ресурсів.

- синхронізація з базами даних загроз шляхом постійного оновлення сигнатур – автоматизовані системи мають можливість постійно оновлювати бази даних сигнатур та аномалій для виявлення нових та еволюціонуючих загроз.

- можливість попереднього попередження перед настанням загроз – системи можуть працювати у режимі попередження, виявляючи потенційні загрози перед тим, як вони встигнуть завдати шкоди.

- контроль заходів безпеки – системи здатні аналізувати ефективність застосованих заходів безпеки та рекомендувати вдосконалення.

Реалізація автоматизованих систем попередження та виявлення загроз досягається за рахунок застосування таких методів: використання моделей машинного навчання для виявлення патернів та аномалій у поведінці користувачів та систем; постійний моніторинг журналів подій та інцидентів для виявлення підозрілих дій; використання систем, що реагують на несподівані зміни у звичайних патернах роботи системи; виявлення вже відомих сигнатур загроз та атак; моніторинг та виявлення незвичайних або неординарних переміщень в мережі; застосування штучного інтелекту для аналізу та розпізнавання патернів у поведінці користувачів [9].

Створення інформаційно безпечних зон (DMZ – Demilitarized Zone) або застосування віртуальних приватних мереж дає можливість відокремлювати області обміну даними від загальної мережі, забезпечуючи додатковий рівень захисту.

Механізми блокування та захисту від зловживань призначений для виявлення надмірного використання ресурсів, великої кількості запитань чи недозволеного обміну, які можуть свідчити про потенційні загрози та відповідно запровадження в дію автоматичного протоколу забезпечення безпеки.

Проте сучасний стан електронного документообігу у міжнародній практиці бухгалтерського обліку далекий від ідеального. Впровадження електронного документообігу для бухгалтерського обліку та інших бізнес-процесів здійснюється з метою полегшення роботи підприємств, зменшення бюрократії та впровадження сучасних технологій. Естонія вважається однією з передових країн у використанні електронних технологій у сфері бізнесу та управління. Ця країна використовує електронний документообіг для подання звітів, оплати податків, реєстрації підприємств та багатьох інших операцій. Фінляндія впроваджує електронні бізнес-процеси для спрощення облікових операцій та обміну інформацією між підприємствами та органами влади. Нідерланди активно впроваджують електронні технології у сфері бухгалтерського обліку для покращення ефективності та зменшення витрат. Сінгапур використовує електронні платіжні системи та електронний документообіг для сприяння бізнес-процесам та полегшення взаємодії з урядовими органами. У США багато штатів та підприємств впроваджують електронний документообіг для оптимізації бухгалтерських процесів [10]. Китай активно розвиває електронні технології у сфері бізнесу, включаючи електронний документообіг для обліку та обміну документами.

Водночас багато країн ще не прийняли систему електронного документообігу, а ті, які прийняли, здійснюють це поступово. Впровадження електронного документообігу може залежати від законодавства, технічної готовності та інших факторів у кожній конкретній країні. Країни постійно розвивають свої інформаційні технології для полегшення бізнес-процесів та підтримки цифрової трансформації.

Сьогодні в сфері електронної обробки даних відсутній загальносвітовий стандарт чи узгоджені правила, які б визначали, як системи обробки даних мають виглядати та взаємодіяти між собою. В різних країнах можуть застосовуватися різні технічні рішення та стандарти, що ускладнює обмін інформацією між цими системами. Це призводить до відсутності одноманітності та послідовності в тому, як реалізовано електронний документообіг в різних країнах, а також до плутанини

та неефективності, оскільки різні країни можуть мати різні стандарти та системи [11]. Без стандартів комп'ютерної взаємодії може виникати ситуація, коли системи не можуть правильно інтерпретувати та обробляти інформацію одна від одної, що може викликати затримки та неефективність в процесі обліку.

Загалом слід зазначити, що стандарти та системи електронного документообігу в бухгалтерському обліку є ключовими компонентами цифрової трансформації та автоматизації бухгалтерських процесів.

Стандарти електронного документообігу – це узагальнені правила, норми або специфікації, які встановлюють загальні вимоги та формати для створення, обміну та зберігання електронних документів. Стандарти визначають, як має виглядати структура та зміст електронного документа забезпечуючи єдність та сумісність між різними системами та допомагають в уніфікації процесів обміну електронною інформацією в галузі бухгалтерського обліку [12].

Сьогодні в міжнародній практиці бухгалтерського обліку існує кілька стандартів електронних документів, які визначають формати та структури для обміну інформацією між різними системами та учасниками бізнес-процесів:

- UBL (Universal Business Language) є мовою для опису бізнес-документів, таких як рахунки, накладні, замовлення, тощо. Цей стандарт створений для сприяння глобальному обміну інформацією між підприємствами різних галузей та країн;

- EDIFACT (Electronic Data Interchange for Administration, Commerce, and Transport) – міжнародний стандарт для електронного обміну структурованою інформацією між компаніями. EDIFACT використовується в різних галузях, включаючи логістику, фінанси та бухгалтерію;

- IFRS (International Financial Reporting Standards) – визначає стандарти фінансової звітності для компаній та організацій. Вони визначають правила та принципи формування фінансових звітів. Застосовується для складання фінансових звітів, звітів про прибутки, баланси;

- ISO 20022 – визначає універсальні формати обміну інформацією для фінансових служб. Він застосовується у банківській та фінансовій сфері.

Врегулює порядок здійснення і оформлення платежів, повідомлень про платежі, банківські транзакції тощо;

- ISO/IEC 27001 – міжнародний стандарт для систем управління інформаційною безпекою. Хоча не є прямим стандартом для електронних документів, він визначає вимоги до забезпечення безпеки інформації, включаючи електронні дані. Регулює порядок захисту електронної інформації, включаючи бухгалтерські дані.

Системами електронного документообігу є програмні продукти або платформи, які надають інфраструктуру для створення, обміну, підписання та зберігання електронних документів. Системи надають інтерфейси для користувачів та автоматизовані механізми для обробки документів. Існує багато систем електронного документообігу в бухгалтерському обліку, які надають різноманітні функції для ефективного управління документами та обліком [13]. До найбільш розповсюджених слід віднести такі:

- Docu Ware – це система електронного документообігу та управління документами, яка дозволяє зберігати, організовувати та обробляти електронні документи. Включає в себе електронний документообіг, потокову обробку документів, інтеграцію з іншими системами, електронні підписи тощо;

- Microsoft Share Point – це платформа для спільної роботи та обміну документами, розроблена корпорацією Microsoft. Включає управління версіями документів, можливість створення спільних робочих просторів для колективної роботи, потокову обробку тощо;

- EpicorECM є системою електронного документообігу, яка дозволяє організаціям автоматизувати обробку та зберігання документів. Забезпечує електронний документообіг, потокову обробку документів, інтеграцію з іншими додатками та системами;

- SAP S/4HANA призначена для обробки фінансових документів, інтеграції з іншими модулями платформи, аналітики тощо. Включає рішення для управління фінансами та обліком, у тому числі можливості електронного документообігу;

- Oracle Content and Experience Cloud – хмарне рішення для зберігання та управління контентом, включаючи електронні документи. Призначена для зберігання та обробки документів, колективної роботи над документами, доступу до контенту з будь-якого пристрою тощо;

- M-Files – система управління документами, яка дозволяє класифікувати та знаходити документи за їхнім змістом. Призначена для забезпечення електронного документообігу, автоматизації процесів, інтеграції з різними системами тощо.

Ці системи надають різноманітні можливості для управління електронними документами та оптимізації бухгалтерських процесів в організаціях. Системи електронного документообігу можуть використовувати стандарти для забезпечення сумісності та обміну інформацією між різними платформами.

Здебільшого, країни, які впроваджують електронний документообіг в бухгалтерському обліку, спираються на використання стандартів для того, щоб забезпечити стандартизацію та сумісність між різними системами та організаціями. Такий підхід сприяє ефективній інтеграції та обміну інформацією в електронному форматі в межах країни та міжнародних відносин.

Запровадження загальноприйнятого стандарту для електроерозійної обробки даних полегшило б взаємодію між різними системами та забезпечило більш ефективний обмін інформацією в глобальному масштабі.

Проте основною невирішеною проблемою застосування та розвитку електронного документообігу на сьогодні залишається загрози безпеці зберігання та передачі інформації. Як свідчить практика системи електронного документообігу вразливі до кібератак, і це може призвести до втрати конфіденційної фінансової інформації. Несанкціонований доступ до електронних документів може мати серйозні наслідки для бізнесу, оскільки втрата інформації може стати причиною фінансових втрат і репутаційної шкоди [14].

Основні аспекти проблем безпеки електронного документообігу включають:

- зберігання інформації – інформація, яка зберігається в електронному вигляді піддається загрозам безпеки, таким як хакерські атаки або несанкціонований доступ до систем зберігання даних;

- передача інформації – процес передачі електронних документів може бути вразливим до кібератак та перехоплення даних під час передачі по мережі;

- кібератаки – системи електронного документообігу можуть стати метою кібератак, де хакери намагаються отримати несанкціонований доступ до інформації чи завдати шкоду системі;

- втрати конфіденційності – якщо інформація у електронних документах стосується фінансових даних чи інших конфіденційних даних, несанкціонований доступ може викликати втрату конфіденційності;

- фінансові та репутаційні втрати – якщо несанкціонований доступ до електронних документів призводить до втрати конфіденційної інформації, це може викликати фінансові втрати для компанії, а також завдати шкоду її репутації.

Як зазначають міжнародні організації такі як Internet Crime Project, Cybersecurity Ventures, які вивчають кібербезпеку та мають доступ до актуальних статистичних даних, кіберзлочинність у 2021 році завдала глобальних збитків на загальну суму 6 трильйонів доларів США. За даними Cybersecurity Ventures, очікується, що глобальні витрати на кіберзлочинність зростатимуть на 15% щороку і до кінця 2025 року досягнуть 10,5 трильйонів доларів США на рік, порівняно з 3 трильйонами доларів США у 2015 році.

Дослідники зазначають, що це приклад найбільшого перерозподілу коштів в історії. Кіберзагрози ставлять нівелюють стимули для інновацій та інвестицій. Крім того, завданні хакерами збитки значно перевищують збитки від стихійних лих протягом відповідного терміну часу. Кіберзлочинність становиться більш прибутковою, ніж глобальна торгівля всіма наркотиками разом узятими [15].

Втрати, пов'язані з кіберзлочинністю, включають пошкодження та знищення даних, викрадені гроші, втрату продуктивності, крадіжку інтелектуальної власності, крадіжку особистих і фінансових даних, розкрадання,

шахрайство, порушення роботи бізнесу після атаки, судове розслідування, відновлення та видалення скомпрометованих даних і систем, а також шкоду репутації.

Кіберзлочинність настільки сильно вдарила по США, що в 2018 році спеціальний агент ФБР, який розслідує кіберзлами, заявив The Wall Street Journal, що кожен американський громадянин повинен очікувати, що всі його дані (особиста інформація) були викрадені та знаходяться в дарквебі (частина глибинної мережі, яка навмисно прихована та використовується для приховування та сприяння злочинній діяльності). За деякими оцінками, розмір глибинної мережі (яка не індексується та не доступна пошуковими системами) у 5000 разів більший ніж поверхнева мережа, і зростає зі швидкістю, яка не піддається кількісному оцінюванню.

Організовані кіберзлочинні організації об'єднують зусилля, і, згідно зі Звітом про глобальні ризики Всесвітнього економічного форуму за 2020 рік, ймовірність їх виявлення та судового переслідування становить лише 0,05% у США.

Висновки та перспективи подальших розвідок у даному напрямі. Досліджені параметри були покладені в основу авторського розуміння змісту міжнародного досвіду електронного документообігу в бухгалтерському обліку та стали основою пропозицій спрямованих на встановлення перспектив його впровадження і удосконалення в Україні з метою забезпечення максимальної користі та мінімізації ризиків. Основними аспектами впровадження такого досвіду слід вважати: використання міжнародних стандартів, таких як Universal Business Language (UBL), для забезпечення сумісності та інтероперабельності між різними системами; впровадження ефективних заходів кіберзахисту відповідно до міжнародних стандартів та найкращих практик; використання міжнародно визнаних електронних підписів та криптографічних методів для забезпечення надійності та юридичної вірогідності документів; врахування міжнародного досвіду у встановленні стандартів для ефективного обміну даними між організаціями та підприємствами; застосування моніторингу найкращих практик у

розробці та удосконаленні нормативно-правової бази для визнання та легалізації електронних документів; вивчення міжнародного досвіду електронного обміну даними з податковими органами для спрощення звітності та підтримки податкової декларації; використання досвіду управління проектами з впровадження електронного документообігу в інших країнах для уникнення можливих помилок та забезпечення успішного запуску системи; врахування інтернаціональних підходів до навчання персоналу та користувачів щодо нових електронних технологій та систем; вивчення методів взаємодії та залучення різних стейкхолдерів, включаючи бізнес, уряд та громадянське суспільство; здійснення регулярного моніторингу та оновлення стратегій відповідно до нових міжнародних стандартів та технологій.

В подальших дослідженнях увагу доцільно приділити розробленню практичних механізмів адаптування законодавчо-нормативного регулювання та техніко-технологічного забезпечення функціонування електронного документообігу в бухгалтерському обліку України.

Література

1. Бабінська С.Я. Електронний документообіг у процесі ведення бухгалтерського обліку в сучасних умовах. *Наукові записки Національного університету "Острозька академія". Серія : Економіка*. 2023. № 30. С. 70-74.
2. Назарова І. Електронний документ у контексті міжнародних економіко-правових відносин. *Журнал європейської економіки*. 2023. Т. 22, № 1. С. 33-48.
3. Закревська О. Ю. Електронний документообіг в системі управління підприємством *Інвестиції: практика та досвід*. 2023. № 9. С. 71-74.
4. Недошитко І.Р., Патряк О.Т. Електронний документообіг та його цінність для бізнесу. *Цифрова платформа: інформаційні технології в соціокультурній сфері*. 2022. Т. 5, № 2. С. 368-379.
5. Герасимчук А.Ю. Використання цифрових підписів, цифрових та електронних документів. досвід іноземних держав. *Нотатки сучасної науки*. 2023. № 6. С. 25-26.

6. Ус О.М. Досвід архівного зберігання електронних документів та електронних інформаційних ресурсів у Вільній федеральній землі Баварія (ФРН). *Архіви України*. 2011. № 5. С. 196-202.

7. Ясінська А.І. Проблеми та перспективи електронного документообігу в умовах цифрової трансформації. *Молодий вчений*. 2022. № 11. С. 128-134.

8. Шевченко О.В., Спрінсян В. Г. Електронні документи в складі цифрової спадщини сучасного суспільства. *Бібліотекознавство. Документознавство. Інформологія*. 2022. № 3. С. 49-55.

9. Можасєв О.О., Сухина Ф.Ф. Метод виявлення втручання в комп'ютерні системи електронного обігу документів. *Системи управління, навігації та зв'язку*. 2023. Вип. 1. С. 122-126.

10. Шарапова О.В., Зленко О.О. Розвиток електронного документообігу в Сполучених Штатах Америки *Молодий вчений*. 2021. № 6(1). С. 79-82.

11. Назарова І.Я. Можливості та функції електронного документообігу *Економічний простір*. 2020. № 159. С. 166-170.

12. Політанський В. С. Теоретико правові засади системи електронного документообігу в Україні *Право і суспільство*. 2021. № 1. С. 22-27.

13. Тарасюк Л., Герасимюк Л., Ліщина В. Перспективи впровадження електронного документообігу на сучасних підприємствах. *Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія : Філологія. Журналістика*. 2021. Т. 32(71), № 5(2). С. 177-181.

14. Данькевич Ю., Гуйда О., Головченко М. Безпечна передача інформації через сучасні електронні документи. *Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія : Філологія. Журналістика*. 2021. Т. 32(71), № 6(3). С. 231-236.

15. 10 guards. Якщо уявити кіберзлочинність як країну це була б третя економіка світу. Cybersecurity Ventures. URL: <https://10guards.com/ua/articles/cybercrime-as-empire-would-be-the-worlds-third-largest-economy/#:~:text=%D0%AF%D0%BA%D1%89%D0%BE%20%D0%BE%D1%86%>

D1%96%D0%BD%D1%8E%D0%B2%D0%B0%D1%82%D0%B8%20%D1%97%D1%97%20%D1%8F%D0%BA%20%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D1%83,%D1%81%D0%B2%D1%96%D1%82%D1%83%20%D0%BF%D1%96%D1%81%D0%BB%D1%8F%20%D0%A1%D0%A8%D0%90%20%D1%82%D0%B0%20%D0%9A%D0%B8%D1%82%D0%B0%D1%8E

References.

1. Babins'ka, S. Ya. (2023), "Electronic document flow in the process of accounting in modern conditions", Naukovi zapysky Natsional'noho universytetu "Ostroz'ka akademiia". Serii: Ekonomika, vol. 30, pp. 70-74.
2. Nazarova, I. (2023), "Electronic document in the context of international economic and legal relations", Zhurnal ievropejs'koi ekonomiky, vol. 22, no. 1, pp. 33-48.
3. Zakrevs'ka, O. Yu. (2023), "Electronic document management in the enterprise management system", Investytsii: praktyka ta dosvid, vol. 9, pp. 71-74.
4. Nedoshytko, I. R. and Patriak, O. T. (2022), "Electronic document flow and its value for business", Tsyfrova platforma: informatsijni tekhnolohii v sotsiokul'turnij sferi, vol. 5, no. 2, pp. 368-379.
5. Herasymchuk, A. Yu. (2023), "Use of digital signatures, digital and electronic documents. experience of foreign countries", Notatky suchasnoi nauky, vol. 6, pp. 25-26.
6. Us, O. M. (2011), "Experience of archival storage of electronic documents and electronic information resources in the Free Federal Land of Bavaria (Germany) (FRN)", Arkhivy Ukrainy, vol. 5, pp. 196-202.
7. Yasins'ka, A. I. (2022), "Problems and prospects of electronic document management in conditions of digital transformation", Molodyj vchenyj, vol. 11, pp. 128-134.
8. Shevchenko, O. V. and Sprinsian, V. H. (2022), "Electronic documents as part of the digital heritage of modern society", Bibliotekoznavstvo.Dokumentoznavstvo. Informolohiia, vol. 3, pp. 49-55.

9. Mozhaiev, O. O., Sukhyna, F.F. and Bashylov, S.V. (2023), “The method of detecting interference in computer systems of electronic circulation of documents”, *Systemy upravlinnia, navihatsii ta zv'iazku*, vol. 1, pp. 122-126.

10. Sharapova, O. V. and Zlenko, O. O. (2021), “Development of electronic document management in the United States of America”, *Molodyj vchenyj*, vol. 6(1), pp. 79-82.

11. Nazarova, I. Ya.(2020), “Possibilities and functions of electronic document management”, *Ekonomichnyj prostir*, vol. 159, pp. 166-170.

12. Polits'kyj, V. S. (2021), “Theoretically legal principles of the system of electronic document circulation in Ukraine”, *Pravo i suspil'stvo*, vol. 1, pp. 22-27.

13. Tarasiuk, L., Herasymiuk, L. and Lischyna V. (2021), “Prospects for the introduction of electronic document management at modern enterprises”, *Vcheni zapysky Tavrijs'koho natsional'noho universytetu imeni V. I. Vernads'koho. Seriiia : Filolohiia. Zhurnalistyka*, vol. 32(71), no. 5(2), pp. 177-181.

14. Dan'kevych, Yu., Hujda, O. and Holovchenko, M. (2021), “Safe transmission of information through modern electronic documents”, *Vcheni zapysky Tavrijs'koho natsional'noho universytetu imeni V. I. Vernads'koho. Seriiia : Filolohiia. Zhurnalistyka*, vol. 32(71), no. 6(3), pp. 231-236.

15. 10 guards (2022), “If you imagine Cybercrime as a country, it would be the world's third economy”, available at: <https://10guards.com/ua/articles/cybercrime-as-empire-would-be-the-worlds-third-largest-economy/#:~:text=%D0%AF%D0%BA%D1%89%D0%BE%20%D0%BE%D1%86%D1%96%D0%BD%D1%8E%D0%B2%D0%B0%D1%82%D0%B8%20%D1%97%D1%97%20%D1%8F%D0%BA%20%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D1%83,%D1%81%D0%B2%D1%96%D1%82%D1%83%20%D0%BF%D1%96%D1%81%D0%BB%D1%8F%20%D0%A1%D0%A8%D0%90%20%D1%82%D0%B0%20%D0%9A%D0%B8%D1%82%D0%B0%D1%8E> (Accessed 14 Nov 2023).

Стаття надійшла до редакції 21.03.2024 р.