UDC 657.1
JEL classification: M41
DOI: 10.35774/visnyk2025.01.244

Ірина НАЗАРОВА,
кандидатка економічних наук, доцентка,
доцентка кафедри обліку і оподаткування,
Західноукраїнський національний університет,
вул. Львівська, 11а, м. Тернопіль, 46009, Україна.
Електронна адреса: niyya2016@gmail.com
ORCID ID: 0000-0001-8942-3998

Олександр НАЗАРОВ,
аспірант кафедри обліку і оподаткування,
Західноукраїнський національний університет,
вул. Львівська, 11, м. Тернопіль, 46009, Україна.
Електронна адреса: sasha_nom@ukr.net
ORCID ID: 0009-0006-4711-1973

ОЦІНКА РИЗИКІВ І СИСТЕМИ ЗАХИСТУ ОБЛІКОВОЇ ІНФОРМАЦІЇ В УМОВАХ ЗАСТОСУВАННЯ ІТ

Назарова І., Назаров О. Оцінка ризиків і системи захисту облікової інформації в умовах застосування ІТ. *Вісник економіки*. 2025. Вип. 1. С. 244–255. DOI: 10.35774/visnyk2025.01.244.

Nazarova I., Nazarov O. (2025). Otsinka ryzykiv i systemy zakhystu oblikovoi informatsii v umovakh zastosuvannia IT [Risk assessment and security systems of accounting information in the context of IT application].*Visnyk economiky – Herald of Economics,* 1, 244–255. DOI: 10.35774/visnyk2025.01.244.

Анотація.

Вступ. *Запровадження інформаційних систем і технологій суттєво змінило та прискорило процеси збору, обміну та опрацювання інформації, покращило комунікаційні умови розвитку нових бізнес-технологій. Однак разом зі значними перевагами диджиталізація економічних відносин зумовила нові виклики. Одним із таких є те, що цифровізація бізнесу розвивалася швидшими темпами, ніж система захисту (безпеки) інформації. Це спричинило виникнення нових загроз і ризиків, які необхідно мінімізувати, забезпечивши захист обліково-звітної інформації.*

Метою статті *є дослідження системних і несистемних ризиків та оцінювання дієвих заходів щодо захисту обліково-звітної інформації за умов застосування інформаційно-комунікаційних технологій.*

Методи*. Для досягнення поставленої мети у дослідженні використано системний та аналітичний підходи до узагальнення інформації, методи бібліографічного, концептуального та функціонального аналізу.*

ISSN 2786-4537 (print). Вісник економіки № 1, 2025 р.
ISSN 2786-4545 (online). Herald of Economics № 1, 2025

***Результати**. Розкрито структуру інформаційних ризиків, що є характерними для об'єднань корпоративного типу за умов використання інформаційних технологій. Виокремлено групи ризиків втрати інформації та доступу до неї, фальсифікації даних та втрати легітимності даних, ризики оприлюднення (зливу) або викрадення комерційної чи конфіденційної інформації та інші. Запропоновано багаторівневу систему інформаційної безпеки, яка має формуватися за напрямами фізичного, правового, програмно-технічного та організаційного забезпечення захисту інформації, яку доцільно визначати підприємством чи корпорацією та регламентувати у відповідних документах. Для суб'єктів корпоративного типу, об'єднаних в одну юридичну особу, таку регламентацію захисту облікової інформації можна здійснювати в наказі про облікову політику. У корпоративних групах, об'єднаних на договірних засадах, основним регулювальним документом може бути єдиний внутрішньокорпоративний стандарт політики інформаційної безпеки, де будуть передбачені як внутрішньокорпоративні правила захисту обліково-звітних даних, так і правила взаємодії із зовнішніми інформаційними системами.*

***Перспективи**. Подальші наукові дослідження у цьому напрямі доцільно здійснювати з метою виявлення та мінімізації ризиків й розробки системних методів захисту обліково-звітної інформації.*

***Ключові слова:** облік, звітність, інформація, інформаційні системи, інформаційні технології, інформаційні ризики, захист інформації, стандарти захисту інформації.*

Формули: 0, рис.: 2, табл.: 0, бібл.: 17.

Iryna NAZAROVA,
PhD (Economics), Associate Professor,
Associate Professor of the Department of Accounting and Taxation,
West Ukrainian National University,
11a Lvivska str., Ternopil, 46020, Ukraine.
E-mail: sasha_nom@ukr.net.
ORCID ID: 0000-0001-8942-3998.

Oleksandr NAZAROV,
graduate Student of the Department of Accounting and Taxation,
West Ukrainian National University,
11 Lvivska st., Ternopil, 46020, Ukraine.
E-mail: sasha_nom@ukr.net.
ORCID ID: 0009-0006-4711-1973.

RISK ASSESSMENT AND SECURITY SYSTEMS OF ACCOUNTING INFORMATION IN THE CONTEXT OF IT APPLICATION

Abstract.

***Introduction.** The introduction of information systems and technologies has significantly transformed and accelerated the processes of data collection, exchange, and processing. It has also improved communication conditions for the development of new business technologies. However, alongside its considerable advantages, the implementation of IT in economic relations has introduced new challenges. One of the critical issues is that*

business digitalization has progressed at a faster pace than information security systems. This has led to emerging threats and risks that must be minimized to ensure the protection of accounting and reporting information.

***The purpose** is to study systemic and non-systemic risks and assess effective measures to protect accounting and reporting information in the context of information and communication technology (ICT) implementation.*

***Methods.** To achieve the research objective, the study employs a systematic and analytical approach to information generalization, as well as bibliographic, conceptual, and functional analysis methods.*

***Results.** The study reveals the structure of information risks specific to corporate-type entities using IT. It identifies groups of risks associated with data loss and access restrictions, data falsification and loss of legitimacy, as well as risks of disclosure (leakage) or theft of commercial or confidential information, among others. A multi-level information security system is proposed, which should be developed in four key areas: physical, legal, software-technical, and organizational information protection. The approach to defining and regulating this security system should be determined by the enterprise or corporation and formalized in the relevant internal documents. For corporate entities operating as a single legal entity, such regulations can be outlined in the accounting policy directive. In corporate groups that operate on a contractual basis, the primary regulatory document may be a unified internal corporate standard for information security policy. This document should establish both internal corporate rules for protecting accounting and reporting data and guidelines for interaction with external information systems.*

***Prospects.** Further research in this area should focus on identifying and minimizing risks and developing systematic methods for protecting accounting and reporting information.*

***Keywords:** accounting, reporting, information, information systems, information technologies, information risks, information protection, information security standards.*

Formulas: 0, fig.: 2, tabl.: 1, bibl.: 16.

Постановка проблеми. Інформаційна система бухгалтерського обліку є чи не найбільш вразливою формою економічних відносин, оскільки вона формується на підставі значних масивів, зокрема конфіденційних, даних і є основою для ухвалення управлінських рішень. Нехтування інформаційною безпекою у сфері ведення бухгалтерського обліку та формування звітності збільшує можливість маніпулювання, фальсифікації й зміни бухгалтерських даних або призводить до втрати інформації. І хоча у сфері її захисту уже багато зроблено, проте сьогодні за основними критеріями безпеки, такими як конфіденційність, цілісність та доступність, електронні обліково-інформаційні системи ще поступаються паперовим. Тому питання щодо посилення захисту інформації за умов цифровізації системи бухгалтерського обліку є надзвичайно актуальним та потребує швидкого вирішення.

Аналіз останніх досліджень і публікацій. За дослідженнями Центру Разумкова головними ризиками, пов'язаними з цифровізацією економіки, стали кібератаки, цифрові розриви, невідповідність кваліфікації працівників вимогам цифровізації тощо [1]. Особливо небезпечними були хакерські атаки на сайти Національних інформаційних систем (НАІС) та Міністерства юстиції України та інші економічні

ISSN 2786-4537 (print). Вісник економіки № 1, 2025 р.
ISSN 2786-4545 (online). Herald of Economics № 1, 2025

інституції, за якими стоять російські спецслужби. Остання з таких атак відбулася 19 грудня 2024 р.

Ризики втрати обліково-звітної інформації чи розголошення конфіденційних даних в економічній сфері пов'язані з багатьма чинниками. Зокрема, Євтушевська О. А. [2], Цал-Цалко Ю. С., Мороз Ю. Ю. [3] проводять поділ ризиків, зумовлених впровадженням цифрових технологій у сфері бухгалтерського обліку, за джерелами походження на ті, що викликані зовнішніми загрозами (конкурентами, злочинними угрупованнями, іншими зацікавленими особами) та внутрішніми (адміністрацією й персоналом підприємства).

Реслер М. В. деталізує ризики цифровізації обліку, поділяючи їх на ризики кібербезпеки (злам, витік даних, атаки зловмисного програмного забезпечення); ризики залежності від технологій (технічні збої і програмні помилки); ризики нестачі навичок фахівців (нестача знань з аналітики даних, кібербезпеки та цифрової трансформації); ризики конфіденційності (можливість втрати особистих і фінансових даних працівників й контрагентів); ризики надмірної залежності від автоматизації (втрата навичок критичного мислення, можливостей для аналізу та прийняття стратегічних рішень) [4].

Рожелюк В. М. класифікує інформаційні ризики за часом (короткотермінові, довготривалі, постійні), за ступенем прояву (помірні, середні, повні), за характером прояву (приховані, легкопомітні, відверто агресивні); за наслідками (такі, що не впливають на стан справ; ті, що викликають труднощі й проблеми; такі, що насильно руйнують всю систему); за ймовірністю (малоймовірні, ймовірні, неминучі); за природою походження (зовнішні, внутрішні) [5].

Бардаш С. В., Грабчук І. Л. виокремлюють інший склад ризиків диджиталізації облікових процесів, акцентуючи увагу на впроваджені нових технологій: ризики застосування інтернету, штучного інтелекту, роботизації, автоматизації (витік комерційної таємниці, скорочення облікового персоналу); ризики використання технології блокчейн (незмінність інформації, неможливість виправлення помилок) та хмарних і розподільних обчислень (складність контролю за роботою хмарного програмного забезпечення та запобігання збоям); ризики стійкості роботи інтернет-зв'язку і наявності кваліфікованих кадрів [6].

Серед вітчизняних науковців найбільш розширену класифікацію ризиків в обліково-інформаційній системі надають Муравський В., Починок Н., Фаріон В., поділяючи їх за значною кількістю критеріїв [7].

Серед зарубіжних джерел щодо структури інформаційних ризиків, пов'язаних з обліковими процесами, варто виокремити праці Дже-Хі Ліма [8] та Мохаммеда Хайджея [9].

Метою статті є дослідження системних і несистемних ризиків та оцінка дієвих заходів щодо захисту обліково-звітної інформації за умов застосування інформаційно-комунікаційних технологій.

Виклад основного матеріалу. Проведене узагальнення напрацювань різних науковців дає змогу запропонувати взаємопов'язану систематизацію ризиків відповідно до основних загроз, що виникають у процесі використання електронних обліково-інформаційних систем (рис. 1).

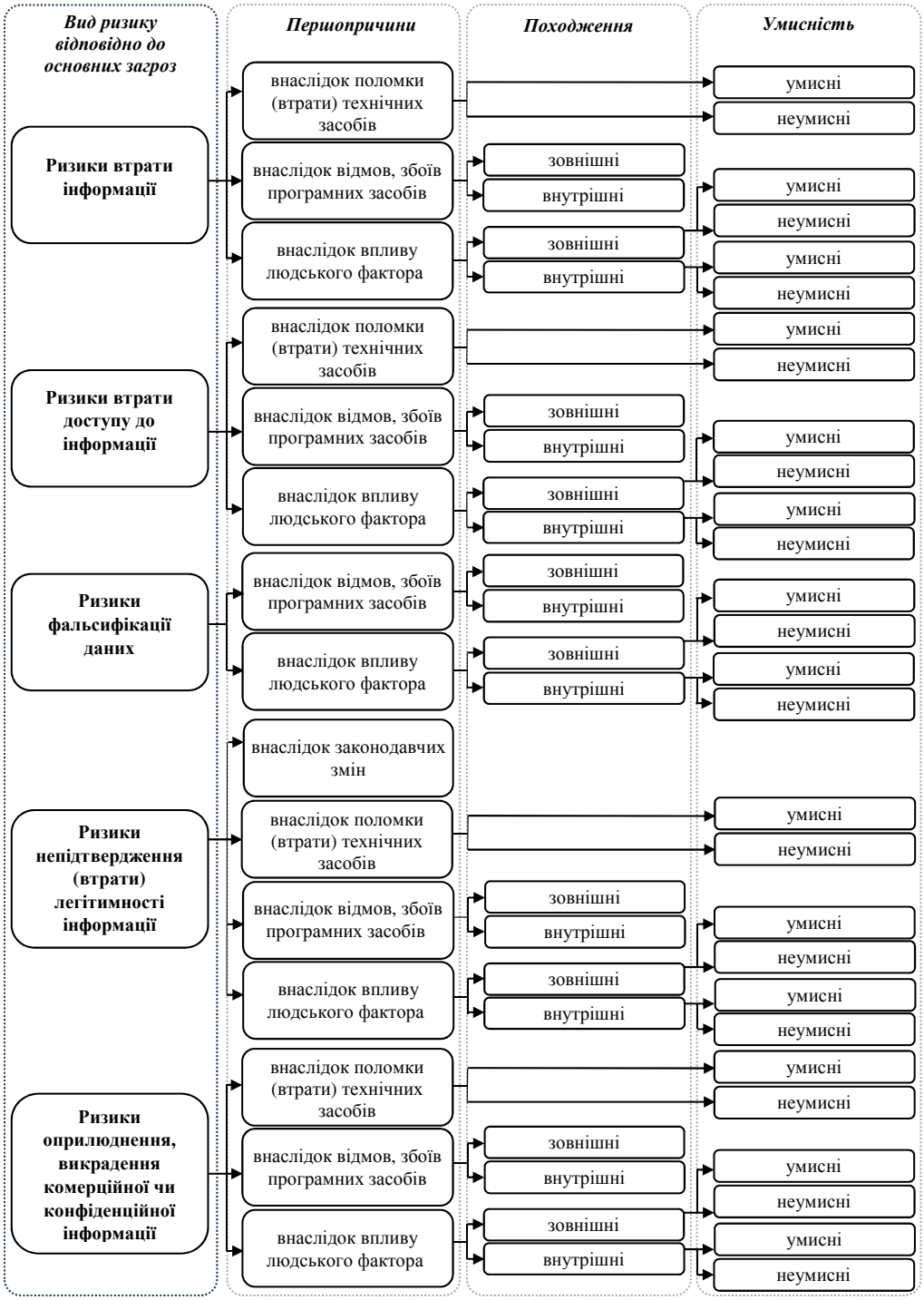

Рис. 1. Види ризиків втрати інформації відповідно до основних загроз
Джерело: розроблено авторами.

1. Ризики втрати інформації: внаслідок поломок (втрат) технічних засобів – умисних (пошкоджень, крадіжок), неумисних (поломок); відмов, збоїв програмних засобів – зовнішніх (через хакерські атаки, вірусні програми, заборони використання програмних продуктів), внутрішніх (через системні збої, програмні помилки); внаслідок впливу людського фактора – зовнішніх користувачів (зломлювачів, хакерів, програмістів, системних адміністраторів обслуговувальних фірм, аудиторів, тощо), внутрішніх користувачів (власників, персоналу) (умисного, неумисного).

2. Ризики втрати доступу до інформації: внаслідок поломок (втрат) технічних засобів – умисних (пошкоджень, крадіжок), неумисних (поломок); внаслідок збоїв програмних засобів – зовнішніх (через хакерські атаки, вірусні програми, заборони використання програмних продуктів), внутрішніх (через системні збої, програмні помилки); внаслідок впливу людського фактора – зовнішніх користувачів (зломлювачів, хакерів, програмістів, системних адміністраторів фірм, аудиторів, тощо), внутрішніх користувачів (власників, персоналу) (умисного, неумисного).

3. Ризики фальсифікації даних: внаслідок збоїв програмних засобів – зовнішніх (через хакерські атаки, вірусні програми, заборони використання програмних продуктів), внутрішніх (через системні збої, програмні помилки); внаслідок впливу людського фактора – зовнішніх користувачів (зломлювачів, хакерів, програмістів, системних адміністраторів обслуговуючих фірм, аудиторів тощо), внутрішніх користувачів (власників, персоналу підприємства) (умисного, неумисного).

4. Ризики непідтвердження (втрати) легітимності інформації: внаслідок законодавчих змін; технічних збоїв, поломок (втрат) технічних засобів – умисних (пошкоджень, крадіжок), неумисних (поломок); внаслідок збою програмних засобів – зовнішніх (через хакерські атаки, вірусні програми, заборони використання програмних продуктів); внутрішніх (через системні збої, програмні помилки); внаслідок впливу людського фактора – зовнішніх користувачів (зломлювачів, хакерів, програмістів, системних адміністраторів обслуговуючих фірм, аудиторів тощо), внутрішніх користувачів (власників, персоналу підприємства) (умисного, неумисного).

5. Ризики оприлюднення (зливу), викрадення комерційної чи конфіденційної інформації: внаслідок поломок (втрат) технічних засобів – умисних (пошкоджень, крадіжок), неумисних (поломок); внаслідок збоїв програмних засобів (зовнішніх (через хакерські атаки, вірусні програми, заборони використання програмних продуктів); внутрішніх (через системні збої, програмні помилки)); внаслідок впливу людського фактора – зовнішніх користувачів (зломщиків, хакерів; програмістів, системних адміністраторів обслуговуючих фірм, аудиторів, тощо), внутрішніх користувачів (власників, персоналу підприємства) (умисного, неумисного).

Найбільш поширеною загрозою, на нашу думку, є витік (оприлюднення) закритої інформації. Це також підтверджується статистичними даними. Зокрема, кількість витоків інформації за останні 10 років збільшилася більш ніж у 10 разів, а у 2023 р., якщо порівняти з 2022 р., – більш ніж на 60%. Водночас у понад 90% випадків це було зумовлено викраденням даних через інтернет-мережу зовнішніми користувачами [10].

Якщо розглядати витоки інформації за типами даних, то в Україні й у світі у 2023 р. найбільша частка належить викраденню конфіденційних персональних даних (понад

60%), а друге місце займає витік комерційної інформації підприємств (11,0% в Україні та 33,1% у світі) (рис. 2).

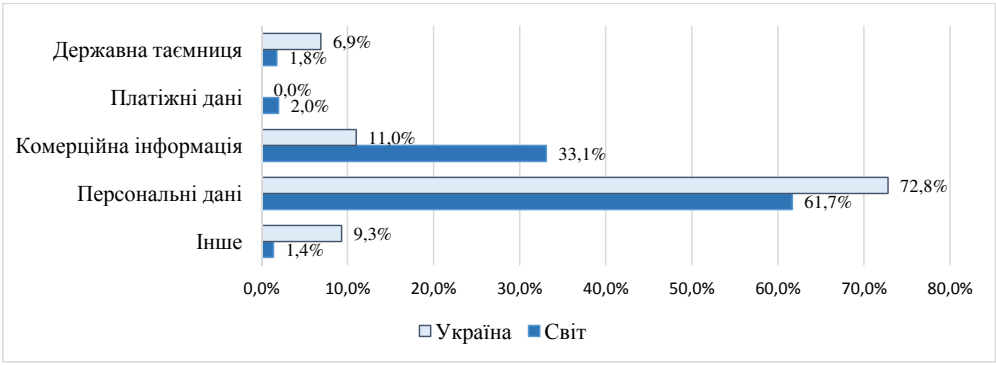

Рис. 2. Витоки інформації за типами даних в Україні і світі
Джерело: розроблено авторами з використанням [10].

Згідно з рис. 2, крадіжки комерційних даних у світовому просторі займають суттєву частку, причому їхня кількість постійно збільшується. Так, якщо порівняти із 2022 р., у 2023 р. вони зросли майже у три рази (з 12% до 33%) і більшість таких крадіжок здійснювалась у сегментах великих (понад 28%) і середніх (понад 35%) підприємств, до яких переважно належать суб'єкти корпоративного типу [10].

Зазначені вище дані підтверджують, що корпоративні групи мають чи не найбільші загрози щодо виникнення ризикових операцій. Це, нашу думку, пов'язано з низкою факторів, а саме: розпорошеністю підрозділів об'єднань (у різних регіонах або навіть країнах), використанням віддалених серверів або хмарних технологій для консолідації та зберігання даних, більшими обсягами й цінністю консолідованої інформації, ніж у невеликих підприємствах тощо. Тому такі суб'єкти господарювання мають більше уваги приділяти попередженню порушення інформаційної безпеки та забезпеченню захисту інформації, зокрема облікової.

З огляду на велику кількість інформаційно-комунікаційних зв'язків у корпоративних групах та складність обліково-інформаційної системи вони потребують побудови багаторівневої системи інформаційної безпеки. Водночас для забезпечення найкращих умов збереження даних необхідне здійснення безперервного контролю та миттєвого реагування на загрози в режимі реального часу. Побудова такої системи можлива лише за умови комплексного підходу, що передбачає використання різних напрямів забезпечення захисту інформації.

Погляди науковців щодо складових системи інформаційної безпеки дещо різняться. Так, Євтушевська О. А. виокремлює фізичні, апаратні, програмні й криптографічні напрями побудови такої системи [2, с. 160]. Схожими є пропозиції Вітер С. А., Світлишин І. І. [11], що виокремлюють організаційні, технічні, кадрові елементи, і Дикого А. П., що вирізняє організаційно-технічні, організаційно-режимні, кадрові елементи системи безпеки [12, с. 211]. Такі автори, як Шпак В. А. [13] та Муравський В. В. [14, с. 99], вважають, що систему захисту облікової інформації слід будувати на правових, технічних, програмних та організаційних засадах. Водночас Попівняк

ISSN 2786-4537 (print). Вісник економіки № 1, 2025 р.
ISSN 2786-4545 (online). Herald of Economics № 1, 2025

Ю. М. виокремлює юридичні, кадрові, технічні й організаційні напрями [15, с. 156]. Дещо відрізняється щодо цього питання думка Грабчук І. Л., яка вважає, що системи інформаційної безпеки мають ґрунтуватися на заходах логічної та фізичної безпеки [16, с. 23].

На нашу думку, багаторівнева система інформаційної безпеки має розбудовуватись за напрямами фізичного, а також правових, програмно-технічних та організаційних напрямах забезпечення захисту інформації.

Напрям фізичного захисту технічного забезпечення, передбачає обмеження допуску (доступу) до приміщень, де знаходяться основні носії інформації та комунікаційні засоби, а також використання систем протипожежного та протиандального захисту.

Програмно-технічний напрям ґрунтується на використанні інформаційно-комунікаційного комплексу забезпечення захисту даних, що охоплює різноманітні електронно-цифрові пристрої захисту, засоби захисту комунікаційного зв'язку та спеціальні програми, що виконують функції захисту.

Організаційний напрям окреслює заходи, що охоплюють сукупність обов'язкових процедур, які учасники повинні виконувати у процесі роботи електронної обліково-інформаційної системи для забезпечення захисту даних. Загалом організаційні заходи передбачають призначення відповідальних осіб за управлінням інформаційної безпекою на підприємстві; інформаційно-навчальну роботу з персоналом щодо застосовуваних на підприємстві способів та заходів захисту інформації; інформаційно-аналітичну діяльність з оцінювання ризиків інформаційної безпеки; проведення інформаційного аудиту тощо.

Правовий напрям полягає в затвердженні на корпоративному рівні зорієнтованих на вітчизняну та міжнародну нормативно-правову базу правил і заходів, що забезпечують інформаційну безпеку, у формі внутрішніх регулювальних документів. Більшість вітчизняних та зарубіжних науковців вважають, що основні положення інформаційної безпеки мають бути прописані в наказі про облікову політику чи додатках до нього. Проте такий підхід неможливо застосувати в корпоративних групах, об'єднаних на договірних засадах, оскільки для них форми такого єдиного наказу не передбачено.

Тому, на нашу думку, основним регулювальним документом має бути єдиний внутрішньокорпоративний стандарт політики інформаційної безпеки, де будуть передбачені як внутрішньокорпоративні правила користування електронною обліково-інформаційною системою, так і правила взаємодії із зовнішніми інформаційними системами.

Внутрішньокорпоративний стандарт політики інформаційної безпеки може бути окремим регулювальним документом корпоративної групи або частиною (окремим додатком) до корпоративного договору. Щодо його структури, то він може виступати єдиним документом у формі політики інформаційної безпеки або містити інші внутрішні нормативні документи щодо організації інформаційного захисту.

Незалежно, в якій формі буде розроблено внутрішньокорпоративний стандарт політики інформаційної безпеки, у ньому доцільно виокремити основні домінантні умови мінімізації ризиків, пов'язаних з використанням електронної обліково-звітної інформації, зокрема: базову політику, політику можливих загроз, політику контролю тощо.

Базова політика інформаційної безпеки визначає основні правила роботи в інформаційній системі щодо порядку і способів обробки інформації у корпорації, перелік осіб та умови отримання доступу до даних, дозволені та заборонені дії в електронній обліково-інформаційній системі. Серед них акцентується увага на необхідності гарантування інформаційної безпеки законодавчим нормам, дотриманні правил користувацької інформаційної безпеки (доступу для внутрішніх та зовнішніх користувачів до технічних засобів та електронної обліково-інформаційної системи корпорації, правил користування нею).

Окремо у стандарті має бути прописана політика можливих загроз інформаційній безпеці, що полягає у визначенні основних із них та алгоритмів дій для стримування або зменшення впливу таких загроз.

Політика контролю інформаційної безпеки полягає у визначенні параметрів та умов поточного контролю інформаційної безпеки, інформування про оновлення політики безпеки, проведення аудиту інформаційної безпеки.

На завершення у розробленому внутрішньому стандарті мають бути наведені спеціальні заходи політики інформаційної безпеки, які визначають особливі умови посилення захисту даних та унеможливлення фальсифікації інформації: політика багаторівневої системи захисту; ідентифікації, автентифікації й авторизації; підтвердження достовірності та легітимності електронних документів; безпечного видалення й коригування даних; резервного копіювання, архівування та відновлення даних; політика взаємодії з персоналом, контрагентами, що полягає у погодженні умов дотримання конфіденційності інформації та захисту даних, про що укладається договір з кожним працівником,контрагентом.

Висновки і перспективи подальших досліджень. Захист обліково-звітної інформації за умов застосування ІТ-технологій обумовлений значними системними й несистемними ризиками, пов'язаними із втратою такої інформації чи обмеженням доступу до неї, викраденням та розголошенням конфіденційної інформації, іншими фактами втрати чи фальсифікації облікових даних. Такий захист має бути багаторівневим з використанням фізичного, правового, програмно-технічного й організаційного способів забезпечення захисту інформації. Для суб'єктів корпоративного типу, об'єднаних в одну юридичну особу, регламентацію захисту облікової інформації можна здійснювати в наказі про облікову політику. У корпоративних групах, об'єднаних на договірних засадах, основним регулювальним документом може бути єдиний внутрішньокорпоративний стандарт політики інформаційної безпеки, де будуть передбачені як внутрішньокорпоративні правила захисту обліково-звітних даних, так і правила взаємодії із зовнішніми інформаційними системами.

Подальші наукові дослідження у цьому напрямі доцільно здійснювати для виявлення та мінімізації ризиків, вдосконалення системних методів захисту обліково-звітної інформації.

Література

1. Цифрова економіка: тренди, ризики та соціальні детермінанти ; за заг. ред. О. Пищуліної, Центр Разумкова. Київ : Заповіт, 2020. 274 с.

ISSN 2786-4537 (print). Вісник економіки № 1, 2025 р.
ISSN 2786-4545 (online). Herald of Economics № 1, 2025

2. Євтушевська О. А. Інформаційна безпека як елемент підвищення ефективності комплексного контролю підприємств водного транспорту. Зовнішня торгівля: економіка, фінанси, право. 2015. № 5-6. С. 157–162.
3. Цал-Цалко Ю. С., Мороз Ю. Ю. Облікова політика підприємства та її кібербезпека. Облік, аналіз і контроль в умовах сучасних концепцій управління економічним потенціалом і ринковою вартістю підприємства *:* зб. наук. праць. Т. І, ч. І. Житомир : ПП «Рута», 2017. С. 8–11.
4. Реслер М. Вплив цифрової економіки на обліково-аналітичну систему. *Acta Academiae Beregsasiensis. Economics*. 2024. № 5. С. 441–450. DOI: https://doi.org/10.58423/2786-6742/2024-5-441-450
5. Рожелюк В. М. Заходи забезпечення захисту облікової інформації. Бухгалтерський облік, аналіз та аудит: проблеми теорії, методології, організації : зб. наук. праць Національної акад. статистики, обліку та аудиту. 2013. № 2 (12). С. 335–340.
6. Бардаш С. В., Грабчук І. Л. Цифрові технології в сфері бухгалтерського обліку: основні можливості та ризики. Ефективна економіка. 2021. № 9. DOI: 10.32702/2307-2105-2021.9.18.
7. Муравський В., Починок Н., Фаріон В. Класифікація кіберризиків у бухгалтерському обліку. Вісник Економіки. 2021. Вип. 2. С. 129–144. DOI:https://doi.org/10.35774/ visnyk2021.02.129.
8. Lim Jae-Hee. A Study on the Effects of Accounting Information System Characteristics on Accounting Information System Performance. *Korea International Accounting Review.* 2010. 34. P. 129–146. DOI: 10.21073/kiar.2010..34.006.
9. Haija Mohammed. The Impact of Computerized Accounting Information Systems Risks on the Quality of Accounting Information. *International Journal of Business and Management.* 2021. 16(7). P. 91–103. DOI: 10.5539/ijbm.v16n7p91.
10. Назарова І. Я. Модернізація електронних обліково-інформаційних систем в корпоративних об'єднаннях : дис. ... д-ра екон. наук: 08.00.09 – бухгалтерський облік, аналіз та аудит (за видами економічної діяльності). Тернопіль, 2024. 578 с.
11. Вітер С. А., Світлишин І. І. Захист облікової інформації та кібербезпека підприємства. Економіка і суспільство. 2017. Вип. 11. С. 497–502.
12. Дикий А. П. Порядок забезпечення безпеки бухгалтерської інформації в умовах застосування сучасних комп'ютерних технологій. Проблеми теорії та методології бухгалтерського обліку, контролю і аналізу. 2008. № 3. С. 208–214.
13. Шпак В. А. Організація захисту облікової інформації. Бухгалтерський облік, аналіз та аудит: проблеми теорії, методології, організації. 2015. № 2. С. 181–187.
14. Муравський В. В. Комп'ютерно-комунікаційна форма обліку : моногр. Тернопіль : ТНЕУ, 2018. 486 с.
15. Попівняк Ю. М. Кібербезпека та захист бухгалтерських даних в умовах застосування новітніх інформаційних технологій. Бізнес Інформ. 2019. № 8. С.150–157. DOI: 10.32983/2222-4459-2019-8-150-157.

16. Грабчук І. Л. Організація захисту облікової інформації в умовах гібридної війни. Проблеми теорії та методології бухгалтерського обліку, контролю і аналізу. 2018. Вип. 3. С. 20–24.

References

1. Tsyfrova ekonomika: trendy, ryzyky ta sotsialni determinanty (2020). [Digital economy: trends, risks, and social determinants] Za zah. red. O. Pyshchulinoi. Tsentr Razumkova. Kyiv: Zapovit, 2020. 274 p. [in Ukrainian].
2. Yevtushevska, O. A. (2015). Informatsiina bezpeka yak element pidvyshchennia efektyvnosti kompleksnoho kontroliu pidpryiemstv vodnoho transportu [Information security as an element of increasing the efficiency of comprehensive control of water transport enterprises]. *Zovnishnia torhivlia: ekonomika, finansy, pravo – Foreign trade: economics, finance,* 5-6, 157–162. [in Ukrainian].
3. Tsal-Tsalko, Yu. S., Moroz, Yu. Yu. (2017). Oblikova polityka pidpryiemstva ta yii kiberbezpeka [Accounting policy of the enterprise and its cybersecurity]. *Oblik, analiz i kontrol v umovakh suchasnykh kontseptsii upravlinnia ekonomichnym potentsialom i rynkovoiu vartistiu pidpryiemstva:* zb. nauk. prats, t. I, ch. I, Zhytomyr: PP «Ruta». P. 8–11. [in Ukrainian].
4. Resler, M. (2024). Vplyv tsyfrovoi ekonomiky na oblikovo-analitychnu system [The impact of the digital economy on the accounting and analytical system]. *Acta Academiae Beregsasiensis. Economics*, 5, 441-450. DOI: https://doi.org/10.58423/2786-6742/2024-5-441-450. [in Ukrainian].
5. Rozheliuk, V. M. (2013). Zakhody zabezpechennia zakhystu oblikovoi informatsii [Measures to ensure the protection of accounting information]. *Bukhhalterskyi oblik, analiz ta audyt: problemy teorii, metodolohii, orhanizatsii:* zb. nauk. prats Natsionalnoi akad. statystyky, obliku ta audytu, 2 (12), 335–340. [in Ukrainian].
6. Bardash, S. V., Hrabchuk, I. L. (2021). Tsyfrovi tekhnolohii v sferi bukhhalterskoho obliku: osnovni mozhlyvosti ta ryzyky [Digital technologies in the field of accounting: main opportunities and risks]. *Efektyvna ekonomika - Effective economy*, 9. DOI: 10.32702/2307-2105-2021.9.18. [in Ukrainian].
7. Muravskyi, V., Pochynok, N., Farion, V. (2021). Klasyfikatsiia kiberryzykiv u bukhhalterskomu obliku [Classification of cyber risks in accounting]. *Visnyk Ekonomiky - Herald of Economics*, 2, 129–144. DOI: https://doi.org/10.35774/visnyk2021.02.129. [in Ukrainian].
8. Lim, Jae-Hee. (2010). A Study on the Effects of Accounting Information System Characteristics on Accounting Information System Performance. *Korea International Accounting Review*, (34), 129–146. DOI: 10.21073/kiar.2010..34.006. [in English].
9. Haija, Mohammed. (2021). The Impact of Computerized Accounting Information Systems Risks on the Quality of Accounting Information. *International Journal of Business and Management*, 16(7), 91–103. DOI: 10.5539/ijbm.v16n7p91. [in English].
10. Nazarova, I. Y. (2024). Modernizatsiia elektronnykh oblikovo-informatsiinykh system v korporatyvnykh obiednanniakh]: dys. ... d-ra ekon. nauk: 08.00.09 – bukhhalterskyi oblik, analiz ta audyt (za vydamy ekonomichnoi diialnosti)

[Modernization of electronic accounting and information systems in corporations: Thesis ... Dr. Econ. Sciences: 08.00.09 – accounting, analysis and audit (according to information on economic activity)]. Ternopil, 2024. 578 p. [in Ukrainian].
11. Viter, S. A., Svitlyshyn, I. I. (2017). Zakhyst oblikovoi informatsii ta kiberbezpeka pidpryiemstva [Accounting information protection and cybersecurity of the enterprise]. *Ekonomika i suspilstvo – Economy and society*, 11, 497–502. [in Ukrainian].
12. Dykyi, A. P. (2008). Poriadok zabezpechennia bezpeky bukhhalterskoi informatsii v umovakh zastosuvannia suchasnykh kompiuternykh tekhnolohii [Procedure for ensuring the security of accounting information in the conditions of using modern computer technologies.]. *Problemy teorii ta metodolohii bukhhalterskoho obliku, kontroliu i analizu – Problems of theory and methodology of accounting, control and analysis*, 3, 208-214. [in Ukrainian].
13. Shpak, V. A. (2015). Orhanizatsiia zakhystu oblikovoi informatsii [Organization of accounting information protection.]. *Bukhhalterskyi oblik, analiz ta audyt: problemy teorii, metodolohii, orhanizatsii – Accounting, analysis and audit: problems of theory, methodology, organization,* 2, 181–187. [in Ukrainian].
14. Muravskyi, V. V. (2018). Kompiuterno-komunikatsiina forma obliku: monohr. [Computer-communication form of accounting: monogr.]. Ternopil, TNEU, 486 p. [in Ukrainian].
15. Popivniak, Yu. M. (2019). Kiberbezpeka ta zakhyst bukhhalterskykh danykh v umovakh zastosuvannia novitnikh informatsiinykh tekhnolohii [Cybersecurity and protection of accounting data under conditions of modern information technology]. *Biznes Inform – Business Inform,* 8, 150–157. DOI: 10.32983/2222-4459-2019-8-150-157. [in Ukrainian].
16. Hrabchuk, I. L. (2018). Orhanizatsiia zakhystu oblikovoi informatsii v umovakh hibrydnoi viiny [Organization of accounting information protection in the context of hybrid war]. *Problemy teorii ta metodolohii bukhhalterskoho obliku, kontroliu i analizu – Problems of theory and methodology of accounting, control and analysis,* 3, 20–24. [in Ukrainian].

Статтю отримано 9 січня 2025 р.
Article received January 9, 2025.