https://doi.org/10.31891/2307-5740-2025-342-3(2)-9
УДК 657.6

СОРОКОЛІТ Микола
Західноукраїнський національний університет
https://orcid.org/0009-0005-2024-0727
e-mail: sorokolitmykola@ukr.net

АУДИТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ АВТОМАТИЗАЦІЇ ОБЛІКОВИХ ДАНИХ ВІТЧИЗНЯНИХ ПІДПРИЄМСТВ

У статті досліджено питання аудиту інформаційної безпеки електронних облікових даних підприємств, що є важливим аспектом захисту інформаційних ресурсів організацій. У сучасних умовах автоматизації облікових процесів використання електронних систем значно підвищує ефективність роботи підприємств, мінімізує ризики людських помилок і забезпечує швидкий доступ до необхідних даних. Водночас електронний формат облікової інформації піддається загрозам, таким як кібератаки, технічні збої та несанкціонований доступ, що потребує комплексних заходів захисту. У роботі проаналізовано сучасний стан загроз інформаційній безпеці в Україні, зокрема зростання кількості кібератак, спрямованих на державні установи, підприємства, енергетичний сектор і телекомунікації. Розглянуто найбільш поширені методи атак і помилок, серед яких використання шкідливого програмного забезпечення, фішингові атаки, неправильне зберігання облікових записів і несанкціонований доступ. Зазначено, що метою зловмисників є викрадення конфіденційних даних, порушення роботи інформаційних систем та фінансові махінації. Стаття містить аналіз останніх досліджень у сфері інформаційної безпеки, що висвітлюють різні підходи до оцінки ризиків, методи прогнозування потенційних загроз і стратегії аудиту безпеки інформаційних систем.

Особливу увагу приділено процесу аудиту облікової інформації, що включає оцінку безпеки зберігання даних, управління доступом, політик автентифікації, резервного копіювання та відповідності нормативним вимогам. Запропоновано концептуальний підхід до проведення аудиту, який складається з трьох основних етапів. У статті наголошується на необхідності комплексного підходу до інформаційної безпеки, що включає впровадження багатофакторної аутентифікації, регулярне резервне копіювання даних, контроль за доступом до конфіденційної інформації та моніторинг можливих загроз. Результати дослідження можуть бути використані для розробки стратегій кіберзахисту підприємств і удосконалення політик безпеки. Запропоновані методи аудиту дозволяють вчасно виявляти ризики, знижувати ймовірність втрати даних та підвищувати стійкість організацій до кіберзагроз.

Ключові слова: інформаційна безпека, облікові інформаційні дані, аудит інформаційної безпеки, електронні облікові дані, захист інформації, автоматизація обліку.

SOROKOLIT Mykola
West Ukrainian National University

AUDIT OF INFORMATION SECURITY IN THE CONTEXT OF AUTOMATION OF ACCOUNTING DATA IN DOMESTIC ENTERPRISES

The article examines the issue of auditing the information security of electronic accounting data in enterprises, which is a crucial aspect of protecting an organization's information resources. In the modern era of digitalized accounting processes, the use of electronic systems significantly enhances enterprise efficiency, minimizes the risk of human error, and provides quick access to necessary data. However, the electronic format of accounting information is vulnerable to threats such as cyberattacks, technical failures, and unauthorized access, necessitating comprehensive protection measures. The paper analyzes the current state of information security threats in Ukraine, particularly the increasing number of cyberattacks targeting state institutions, enterprises, the energy sector, and telecommunications. It examines the most common attack methods and security vulnerabilities, including the use of malicious software, phishing attacks, improper account storage, and unauthorized access. The article highlights that attackers primarily aim to steal confidential data, disrupt information systems, and commit financial fraud.

The study also reviews recent research in the field of information security, exploring various approaches to risk assessment, methods for predicting potential threats, and strategies for auditing information systems security. Particular attention is given to the process of auditing accounting information, which includes evaluating data storage security, access management, authentication policies, backup procedures, and compliance with regulatory requirements. A conceptual approach to conducting an audit is proposed, consisting of three main stages. The article emphasizes the importance of a comprehensive approach to information security, which includes implementing multi-factor authentication, regularly backing up data, controlling access to confidential information, and monitoring potential threats. The study's findings can be used to develop enterprise cybersecurity strategies, improve security policies, and ensure compliance with regulatory requirements. The proposed audit methods facilitate the timely identification of risks, reduce the likelihood of data loss, and strengthen organizational resilience against cyber threats.

Keywords: information security, accounting information data, information security audit, electronic accounting data, information protection.

Стаття надійшла до редакції / Received 01.04.2025
Прийнята до друку / Accepted 27.04.2025

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

У сучасних умовах уся облікова інформація зберігається в електронному вигляді, що значно спрощує її обробку, аналіз та управління. Використання автоматизованих систем обліку дозволяє підвищити

ефективність роботи підприємств, мінімізувати ризики людських помилок і забезпечити зручний доступ до даних. Проте електронний формат облікової інформації потребує належного рівня захисту, оскільки вона може стати об'єктом кібератак, втрат через технічні збої або несанкціонований доступ. Тому важливими аспектами її збереження є резервне копіювання, шифрування, багатофакторна аутентифікація та контроль доступу. Використання електронних систем також сприяє автоматизації облікових процесів, інтеграції з іншими цифровими платформами та дотриманню нормативних вимог щодо ведення бухгалтерської та фінансової документації. У 2024 році урядова команда CERT-UA, що діє при Держспецзв'язку, зафіксувала 4315 кіберінцидентів, що на 69,8% більше, ніж у 2023 році (2541 випадок). Основними цілями атак залишаються місцеві органи влади, урядові установи, сектор безпеки й оборони, енергетика, бізнес і телекомунікації, промислові підприємства. Зловмисники найчастіше використовують шкідливе програмне забезпечення, несанкціоновані підключення та компрометацію облікових записів. Головна мета – викрадення конфіденційних даних, знищення інформації та порушення роботи систем [1]. Інформаційною безпекою підприємства є сукупність заходів, стратегій та технологій, спрямованих на захист інформаційних активів організації від несанкціонованого доступу, втрати, зміни, розголошення чи знищення. Аудит інформаційної безпеки облікових даних на підприємствах України є критично важливим процесом, оскільки витоки даних, кібератаки та внутрішні загрози можуть призвести до значних фінансових втрат, штрафів та репутаційних ризиків. Цей аудит спрямований на перевірку захищеності облікових записів, систем управління доступом, політик паролів та автентифікації.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Зростання кількості та складності кібератак на об'єкти автоматизації за останні роки свідчить про те, що, попри всі зусилля із впровадження дедалі досконаліших апаратно-програмних рішень для кіберзахисту, проблема оцінки поточного та прогнозування майбутнього рівня інформаційної безпеки залишається актуальною. Колектив вітчизняних науковців Я. В. Рой, П. М. Складанний і Н. П. Мазур виокремили загальні чотири етапи аудиту інформаційної безпеки та перелік вихідних даних, необхідних для перевірки. Науковці виділяють дві основні групи методів оцінки ризиків інформаційної безпеки. Перша група спрямована на визначення рівня ризику через оцінку відповідності встановленим вимогам у сфері кібербезпеки. Джерелами таких вимог можуть бути нормативно-правові документи підприємства (політики безпеки, накази), чинне законодавство України, міжнародні стандарти, а також рекомендації виробників програмного та апаратного забезпечення. Друга група методів ґрунтується на аналізі ймовірності реалізації атак та оцінці можливих збитків від них. Цей підхід дозволяє більш точно визначити потенційні загрози та розробити заходи для їх мінімізації [10]. Інший науковець В. Д. Хох досліджував автоматизовану систему проведення аудиту інформаційної безпеки комп'ютерних систем та мереж. У науковій праці розроблено програмну систему тестування способів управління інформаційною безпекою на основі експертного дослідження з використанням знань та методів нечіткої логіки [11].

С. В. Любарський та П. В. Шаціло провели дослідження архітектури системи оперативного аудиту подій безпеки інформаційної системи. Автори розглядають два підходи до оцінки інформаційної безпеки інформаційних систем, а саме формальний і неформальний (класифікаційний) підходи [5]. Інший вітчизняний науковець О. В. Мельниченко досліджував питання інформаційної безпеки в банківській системі, а саме при роботі з електронними грошима [6]. О. В. Криворучко, О. М. Сунічук, А. М. Десятко досліджували процес моделювання інформаційної системи проведення незалежного аудиту інформаційної безпеки. Авторами розроблено декомпозицію концептуальної моделі системи аудиту інформаційної безпеки [2].

ВИДІЛЕННЯ НЕВИРІШЕНИХ РАНІШЕ ЧАСТИН ЗАГАЛЬНОЇ ПРОБЛЕМИ, КОТРИМ ПРИСВЯЧУЄТЬСЯ СТАТТЯ

Проте питання інформаційної безпеки саме облікових даних та особливостей їх зберігання протягом тривалого періоду часу залишається відкритим та актуальним. Зростання кількості та складності кібератак на об'єкти інформатизації за останні роки свідчить про те, що, попри всі зусилля із впровадження дедалі досконаліших апаратно-програмних рішень для кіберзахисту, проблема оцінки поточного та прогнозування майбутнього рівня інформаційної безпеки залишається актуальною, особливо в контексті облікової інформації.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Мета статті полягає в дослідженні можливостей і шляхів удосконалення аудиту інформаційної безпеки електронних облікових даних вітчизняних підприємств. Зважаючи на мету дослідження важливим є виокремити основні цілі аудиту облікових даних та сформувати концептуальний підхід до етапів аудиту електронних облікових інформаційних ресурсів.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Сучасний стан електронного ведення обліку на підприємствах характеризується активним впровадженням цифрових технологій для автоматизації фінансових, бухгалтерських і управлінських

процесів. Використання спеціалізованих програмних рішень дозволяє підприємствам підвищувати ефективність роботи, зменшувати ризики людських помилок і забезпечувати швидкий доступ до необхідних даних. Водночас, рівень впровадження електронного обліку суттєво варіюється залежно від розміру підприємства, сфери діяльності та рівня цифровізації.

Термін зберігання електронних документів на електронних носіях має відповідати строкам, визначеним законодавством для аналогічних паперових документів. Це встановлено статтею 13 розділу I Закону України «Про електронні документи та електронний документообіг» [9]. Водночас, згідно зі статтею 8 Закону України «Про бухгалтерський облік та фінансову звітність в Україні» [8], власник підприємства або уповноважена особа, відповідальна за його управління, зобов'язані забезпечити ведення бухгалтерського обліку, фіксацію всіх господарських операцій у первинних документах, а також зберігання оброблених документів, регістрів і звітності протягом визначеного періоду, але не менше трьох років.

Згідно Переліку типових документів, що створюються під час діяльності державних органів та органів місцевого самоврядування, інших юридичних осіб, із зазначенням строків зберігання документів [7] визначено терміни зберігання окремих документів, а їх максимальне збереження досягає навіть 75 років. Перебої в постачанні електроенергії можуть мати серйозний вплив на зберігання облікової інформації, особливо якщо відсутні резервні джерела живлення та заходи захисту. Раптові відключення електроенергії можуть призвести до втрати або пошкодження даних, збоїв у роботі серверів, а також порушення роботи баз даних і систем управління обліковою інформацією. Також протягом останніх років хакерські атаки значно зросли як за кількістю, так і за складністю. Кіберзлочинці дедалі частіше використовують удосконалені методи атак, спрямовані на державні установи, фінансові організації, підприємства різних галузей та навіть окремих користувачів.

Особливо поширеними стали фішингові атаки, спрямовані на викрадення облікових даних через підроблені електронні листи та сайти. Програмне забезпечення-вимагач також набуло великої популярності, блокуючи доступ до файлів і вимагаючи викуп за їх відновлення. Зростає кількість атак, що спричиняють перевантаження серверів і тимчасове виведення з ладу критичних онлайн-сервісів. Не менш небезпечною тенденцією є цільові атаки на підприємства, у яких зловмисники тривалий час залишаються в системі, викрадаючи важливі дані. Кіберзлочинці активно використовують витоки корпоративних облікових даних, які потрапляють у відкритий доступ через слабкі паролі або злами сервісів. У зв'язку з цими загрозами компаніям та організаціям необхідно посилювати кібербезпеку, запроваджувати багатофакторну аутентифікацію, регулярно оновлювати системи безпеки та проводити навчання персоналу з виявлення потенційних атак.

Основними цілями інформаційної безпеки є конфіденційність, цілісність та доступність даних, що забезпечують їхній захист від загроз та несанкціонованого доступу протягом тривалого часу зберігання облікової інформації. Конфіденційність означає, що доступ до інформації мають лише авторизовані користувачі. Для цього застосовуються механізми захисту, такі як шифрування, багатофакторна аутентифікація та сувора політика управління доступом. Це допомагає запобігти витоку конфіденційних даних та захистити їх від стороннього втручання. Цілісність передбачає захист інформації від випадкових або навмисних змін, що можуть спотворити її зміст. Для цього використовуються цифрові підписи, контрольні суми та резервне копіювання, які дозволяють виявляти й запобігати несанкціонованим модифікаціям даних. Доступність гарантує, що інформація та системи залишаються доступними для користувачів у потрібний момент. Це досягається за рахунок впровадження резервного копіювання, використання систем та засобів захисту, а саме антивірусні програми. Досягнення цих трьох цілей є основою ефективної інформаційної безпеки, яка забезпечує надійний захист даних та підтримує стабільну роботу підприємства.

Під час аудиту інформаційної безпеки підприємств часто виявляються критичні проблеми, які можуть призвести до компрометації даних та несанкціонованого доступу. Однією з найбільш поширених загроз є використання слабких або однакових паролів у різних системах, що значно полегшує роботу зловмисників у разі витоку даних. Ситуацію ускладнює відсутність багатофакторної аутентифікації, яка могла б додатково захистити корпоративні способи доступу. Ще одним серйозним ризиком є наявність активних акаунтів колишніх співробітників, що створює потенційну можливість несанкціонованого доступу до систем. До цього ж переліку проблем можна віднести використання адміністративних облікових записів для повсякденних задач, що підвищує ймовірність компрометації критично важливих ресурсів.

Особливістю облікових ресурсів є їх тривалий термін зберігання. Тому використовуючи програмне забезпечення особливої актуальності набуває збереження інформації протягом періоду встановленого чинним законодавством з метою уникнення порушень та штрафів. Не менш небезпечною проблемою є витоки корпоративних облікових даних у публічний доступ, що може стати причиною кібератак або фінансових втрат. Усі ці ризики вимагають системного підходу до безпеки, регулярного аудиту та впровадження ефективних заходів захисту. Узагальнюючи цю інформацію, в таблиці 1 подано основні напрями і завдання аудиту інформаційної безпеки облікових даних вітчизняних підприємств.

Таблиця 1

Основні цілі аудиту облікових даних

№ з/п	Напрями перевірки	Основні завдання
1.	Перевірка способів зберігання інформації	Оцінка облікових програм та способів і збереження інформації
2.	Аналіз носіїв збереження інформації і їх резервних копій	Оцінка матеріальних ресурсів та хмарних технологій для збереження інформації і їх резервного копіювання
3.	Перевірка безпеки облікових записів співробітників	Оцінка ризиків, пов'язаних із несанкціонованим доступом
4.	Аналіз управління паролями та політик автентифікації	Оцінка надійності паролів та використання багатофакторної аутентифікації
5.	Виявлення критичних місць у системах управління доступом	Аналіз розподілу прав та привілеїв у корпоративних системах
6.	Оцінка відповідності законодавчим вимогам України	Відповідність стандартам захисту персональних даних (Закон України «Про захист персональних даних», «Про електронні документи та електронний документообіг», «Про бухгалтерський облік та фінансову звітність в Україні» та ін.)
7.	Виявлення витоків облікових даних	Перевірка, чи не були паролі або дані доступу скомпрометовані

Інформаційна безпека є критично важливою для захисту комерційної та конфіденційної інформації, запобігання кібератакам, збереження репутації компанії та дотримання законодавчих вимог. Інформаційна безпека підприємства є багаторівневим процесом, що включає організаційні, технічні та фізичні заходи. Впровадження комплексних систем безпеки, дотримання міжнародних стандартів, навчання персоналу та регулярний аудит допомагають мінімізувати ризики та забезпечити стабільну роботу компанії. Аудит інформаційної безпеки включає кілька ключових етапів, а саме підготовчий, основний та заключний, які допомагають оцінити рівень захисту автоматизованих систем обліку, виявити ризики та запропонувати рекомендації щодо їх усунення.

Підготовчий етап є ключовим для успішного проведення аудиту, оскільки на цьому етапі визначаються його цілі, масштаби та методи. Основне завдання полягає в тому, щоб чітко окреслити, які аспекти діяльності підлягатимуть перевірці, хто відповідатиме за аудит і які методи будуть використовуватися для аналізу. Першочергово визначаються цілі аудиту, які можуть включати оцінку відповідності встановленим стандартам, виявлення можливих вразливостей або оцінку ефективності існуючих заходів безпеки. Після цього відбувається вибір об'єктів аудиту, серед яких можуть бути програмні продукти, сервери, комп’ютерні мережі, бази даних, політики інформаційної безпеки та інші важливі елементи інфраструктури. Наступним кроком є формування команди аудиторів. Це можуть бути як внутрішні фахівці компанії, так і незалежні зовнішні експерти, залежно від потреб підприємства та складності аудиту. Важливо сформувати команду з спеціалістів, які володіють інформацією про особливості інформаційних систем та мають необхідні технічні знання й володіють інформацією про законодавчі норми стосовно особливостей організації обліку й документообігу на вітчизняних підприємствах. Остаточним етапом підготовки є узгодження з керівництвом плану аудиту, включаючи затвердження методів, графіка проведення перевірки та рівнів доступу до даних. Це дозволяє забезпечити ефективне проведення аудиту та уникнути можливих конфліктів під час його реалізації.

Основний етап є найбільшим та передбачає безпосереднє проведення перевірки. На цьому етапі аудитори здійснюють детальне вивчення документації компанії, щоб отримати повне розуміння про існуючі політики та механізми захисту облікової інформації. Найпершим етапом є тестування ряду працівників для визначення критичних точок. Аналіз документації дозволяє оцінити, наскільки ефективно впроваджені заходи інформаційної безпеки та чи відповідають вони встановленим стандартам і нормативним вимогам. Перш за все, проводиться аналіз політики інформаційної безпеки, що включає вивчення процедур управління ризиками, а також механізмів контролю доступу та захисту даних. Вітчизняні науковці М. Р. Лучко та М. Я. Остап’юк зазначають, що створюючи автоматизоване робоче місце для бухгалтера необхідно врахувати доступність інформації для різних користувачів з метою попередження несанкціонованого внесення або знищення даних [Лучко, с. 17]. Важливим аспектом є оцінка політик резервного копіювання, яка дозволяє визначити, чи забезпечує компанія надійне збереження критично важливої інформації та чи має ефективний план відновлення після збоїв.

Крім того, аудитори перевіряють регламент реагування на інциденти. Це дає змогу оцінити готовність компанії до потенційних атак, збоїв або витоку даних, а також ефективність заходів, що вживаються для мінімізації наслідків таких інцидентів. Загалом цей етап дає змогу отримати об’єктивне уявлення про рівень інформаційної безпеки підприємства та виявити можливі слабкі місця, які потребують подальшого вдосконалення. Також аудитори аналізують технічні аспекти безпеки інформаційних систем, щоб визначити їхню стійкість до загроз. Основна увага приділяється аналізу побудови автоматизованого програмного забезпечення, перевірці ефективності антивірусних систем та механізмів автентифікації й авторизації. Також здійснюється аналіз журналів безпеки, що дозволяє виявити потенційні вразливості та сліди можливих порушень безпеки.

На цьому етапі аудитори аналізують, наскільки облікова інформаційна інфраструктура та системи зберігання відповідають встановленим стандартам чинного законодавства. Особлива увага приділяється

технічним характеристикам фактичних накопичувачів даних та їх здатності зберігати інформацію, адже електронні носії мають властивості втрачати характеристики з плином часу. Виходячи з цієї інформації аудитор перевіряє наявність внутрішньофірмових стандартів стосовно копіювання даних та регулярності її здійснення. Також проводиться оцінка відповідності національному законодавству, що дозволяє виявити потенційні порушення та мінімізувати ризики штрафів або санкцій з боку контролюючих органів. Результати цієї перевірки допомагають компанії забезпечити відповідність усім необхідним нормам та покращити управління інформаційною безпекою.

На кожному підприємстві для належної роботи всіх підрозділів систематично здійснюється документообіг. Здійснюючи перевірку системи електронного документообігу дослідження спрямоване на оцінку захисту даних під час їх зберігання та передачі. Аудитори перевіряють механізми шифрування, аналізують системи контролю доступу до конфіденційної інформації та виявляють можливі витоки даних. Особлива увага приділяється рівню захисту персональної інформації, щоб гарантувати відповідність політик компанії сучасним вимогам безпеки.

На завершальному етапі процесу аудиту відбувається формування звіту та рекомендацій. Аудитори систематизують та аналізують усі отримані дані, щоб створити структурований документ, який відображає стан інформаційної безпеки облікових даних підприємства. Звіт про аудит інформаційної безпеки містить ключові висновки та рекомендації, що допомагають компанії усунути виявлені проблеми та покращити захист своїх даних. Одним із головних розділів є виявлені помилки, неточності та їх критичність. У цьому розділі описуються слабкі місця в системах безпеки, які можуть бути використані зловмисниками або відбуватися внаслідок неналежної організації зберігання даних. Аудитори оцінюють потенційний вплив цих вразливостей на бізнес-процеси та визначають ступінь загрози для підприємства. Далі у звіті надаються рекомендації щодо усунення ризиків. Це перелік конкретних заходів, спрямованих на ліквідацію або мінімізацію виявлених загроз, з урахуванням їхньої складності та ефективності. Звіт є ключовим документом, який допомагає керівництву організації зрозуміти поточний стан безпеки облікової інформації та визначити стратегію подальшого вдосконалення кіберзахисту. Він також слугує основою для планування ресурсів та впровадження необхідних змін.

Проведення аудиту інформаційної безпеки облікової інформації приносить організаціям значні переваги, сприяючи надійному захисту даних та дотриманню вимог контролюючих органів. Однією з ключових переваг є виявлення та усунення помилок. Аудит дозволяє знайти слабкі місця в системах захисту, такі як недоліки в налаштуваннях програмного забезпечення, відсутність оновлень або помилки в управлінні доступом. Це допомагає запобігти потенційним кібератакам або витоку конфіденційних даних, забезпечуючи стабільність і безпеку бізнес-процесів. Аудит допомагає переконатися, що облікова інформація захищена від несанкціонованих змін, втрати або знищення, що є критично важливим для фінансової звітності.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Аудит інформаційної безпеки електронних облікових даних є критично важливим процесом для забезпечення надійного захисту інформації на підприємствах. Зважаючи на зростаючі загрози кібератак, витоків даних та технічних збоїв, підприємствам необхідно впроваджувати ефективні заходи безпеки, що включають резервне копіювання, шифрування, багатофакторну аутентифікацію та контроль доступу. Проведення перевірки способів зберігання облікової інформації, аналіз носіїв збереження інформації, їх резервних копій і термінів зберігання, безпеки облікових записів співробітників, управління паролями та політик автентифікації, оцінка відповідності законодавчим вимогам України і виявлення критичних місць у системах управління доступом дозволить сформувати надійну систему автоматизованих інформаційних ресурсів. Крім того, під час аудиту часто виявляються проблеми, пов'язані з недостатньою обізнаністю персоналу щодо правил інформаційної безпеки. Це дає змогу провести навчання та підвищити рівень кіберкультури серед співробітників.

Література

1. CERT-UA минулого року опрацювала 4315 кіберінцидентів. URL: https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv (дата звернення 10.03.2025 р.).

2. Криворучко О. В., Десятко А. М., Сунічук О. М. Моделювання інформаційної системи проведення незалежного аудиту інформаційної безпеки. *Управління розвитком складних систем*. 2020. Вип. 43. С. 67–75

3. Лахно В., Блозва А., Часновський Є., Криворучко О., Десятко А. Аудит інформаційної безпеки на основі застосування нейро-нечіткої системи. *Технічні науки та технології*. 2021. № 3. С. 125–137.

4. Лучко М. Р., Остап'юк М. Я. Основи побудови АРМ бухгалтера: Навчальний посібник. Київ: ІСДО, 1993. 60 с.

5. Любарський С. В., Шаціло П. В. Дослідження архітектури системи оперативного аудиту подій безпеки інформаційної системи. *Information Technology and Security*. 2012. № 2. С. 45–53

6. Мельниченко О. В. Аудит інформаційної безпеки банку при роботі з електронними грошима. *Проблеми економіки*. 2013. № 4. С. 341–347

7. Перелік типових документів, що створюються під час діяльності державних органів та органів місцевого самоврядування, інших юридичних осіб, із зазначенням строків зберігання документів: Наказ Міністерства юстиції України від 12.04.2012 р. № 578/5. URL: https://ips.ligazakon.net/document/RE20884?an=18719 (дата звернення 11.03.2025 р.).

8. Про бухгалтерський облік та фінансову звітність в Україні: Закон України від 16.07.1999 р. № 996-XIV в редакції від 03.09.2024 р. URL: https://zakon.rada.gov.ua/laws/show/996-14#Text (дата звернення 12.03.2025 р.).

9. Про електронні документи та електронний документообіг: Закон України від 22.05.2003 р. № 851-IV в редакції від 31.12.2023 р. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text (дата звернення 14.03.2025 р.).

10. Рой Я. В., Мазур Н. П., Складанний П. М. Аудит інформаційної безпеки – основа ефективного захисту підприємства. *Кібербезпека: освіта, наука, техніка*. 2018. № 1. С. 86–93.

11. Хох В. Д. Автоматизована система проведення аудиту інформаційної безпеки комп'ютерних систем та мереж. *Збірник наукових праць Кіровоградського національного технічного університету. Техніка в сільськогосподарському виробництві, галузеве машинобудування, автоматизація*. 2018. Вип. 31. С. 174–181.

References

1. CERT-UA processed 4,315 cyber incidents last year (2025), available at: https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv (accessed March 10, 2025).

2. Kryvoruchko O. V., Desiatko A. M., Sunichuk O. M. (2020) Modeliuvannia informatsiinoi systemy provedennia nezalezhnoho audytu informatsiinoi bezpeky [Modeling of an information system for conducting an independent information security audit]. *Upravlinnia rozvytkom skladnykh system*, no. 43, pp. 67–75.

3. Lakhno V., Blozva A., Chasnovskyi Ye., Kryvoruchko O., Desiatko A. (2021) Audyt informatsiinoi bezpeky na osnovi zastosuvannia neiro-nechitkoi systemy [Information security audit based on the use of a neuro-fuzzy system]. *Tekhnichni nauky ta tekhnolohii*, no. 3, pp. 125-137.

4. Luchko M. R., Ostapiuk M. Ya. (1993) Osnovy pobudovy ARM bukhhaltera: Navchalnyi posibnyk [Basics of building an accountant's workstation: Training manual]. Kyiv: ISDO, 60 p.

5. Liubarskyi S. V., Shatsilo P. V. (2012) Doslidzhennia arkhitektury systemy operatyvnoho audytu podii bezpeky informatsiinoi systemy [Research on the architecture of the information system security event operational audit system]. *Information Technology and Security*, no. 2, pp. 45–53.

6. Melnychenko O. V. (2013) Audyt informatsiinoi bezpeky banku pry roboti z elektronnymy hroshyma [Audit of bank information security when working with electronic money]. *Problemy ekonomiky*, no. 4, pp. 341–347.

7. Order of the Ministry of Justice of Ukraine "List of standard documents created during the activities of state bodies and local self-government bodies, other legal entities, indicating the storage periods of documents" dated April 12, 2012 No. 578/5, available at: https://ips.ligazakon.net/document/RE20884?an=18719 (accessed March 11, 2025).

8. Law of Ukraine "On accounting and financial reporting in Ukraine" dated July 16, 1999 No. 996-XIV as amended on September 3, 2024, available at: URL: https://zakon.rada.gov.ua/laws/show/996-14#Text (accessed March 12, 2025).

9. Law of Ukraine "On electronic documents and electronic document flow" dated May 22, 2003 No. 851-IV as amended on December 31, 2023, available at: https://zakon.rada.gov.ua/laws/show/851-15#Text (accessed March 14, 2025)

10. Roi Ya. V., Mazur N. P., Skladannyi P. M. (2018) Audyt informatsiinoi bezpeky – osnova efektyvnoho zakhystu pidpryiemstva [Information security audit is the basis for effective enterprise protection]. *Kiberbezpeka: osvita, nauka, tekhnika*, no. 1, pp. 86–93.

11. Khokh V. D. (2018) Avtomatyzovana systema provedennia audytu informatsiinoi bezpeky kompiuternykh system ta merezh [Automated system for auditing information security of computer systems and networks]. *Zbirnyk naukovykh prats Kirovohradskoho natsionalnoho tekhnichnoho universytetu. Tekhnika v silskohospodarskomu vyrobnytstvi, haluzeve mashynobuduvannia, avtomatyzatsiia*, no. 31, pp. 174–181.