МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Західноукраїнський національний університет
Навчально-науковий інститут інноватики, природокористування та інфраструктури
Кафедра енергетичних систем та бізнес-аналітики

МИХАНЧУК Наталія Віталіївна

Інформаційна безпека і аудит цифрового облікового середовища / Information Security and Audit of the Digital Accounting Environment

спеціальність: 071 – Облік і оподаткування
освітньо-професійна програма – Бізнес-аналітика та управління інноваційними системами

Кваліфікаційна робота

Виконав студентка групи ОБАм-21
Н. В. Миханчук
_____

Науковий керівник:
к. е. н., доцент І. М. Белова
_____

ТЕРНОПІЛЬ – 2025

АНОТАЦІЯ

Миханчук Н. В. Інформаційна безпека і аудит цифрового облікового середовища. Рукопис.
Дослідження на здобуття освітнього ступеня «магістр» за спеціальністю 071 «Облік і оподаткування», освітньо-професійна програма «Бізнес-аналітика та управління інноваційними системами». Західноукраїнський національний університет, Тернопіль, 2025.
У роботі досліджено теоретичні та прикладні засади забезпечення інформаційної безпеки цифрового облікового середовища підприємства, розкрито особливості ідентифікації цифрових ризиків та оцінено ефективність контрольних процедур у сфері захисту облікової інформації. Проведено аналіз вітчизняного нормативно-правового забезпечення інформаційної безпеки та досліджено стан цифрової облікової інфраструктури ФГ «Волова гора». Розроблено концептуальну модель підвищення рівня інформаційної безпеки підприємства та надано рекомендації щодо удосконалення аудиту цифрових ризиків з урахуванням сучасних підходів, технологій і вимог стандартів.

ANNOTATION

Mykhanchuk N. V. Information Security and Audit of the Digital Accounting Environment. Manuscript.
Master's research for the educational degree "Master" in the specialty 071 "Accounting and Taxation," educational and professional program "Business analytics and management of innovative systems". West Ukrainian National University, Ternopil, 2025.
The thesis examines the theoretical and applied foundations of ensuring information security within an enterprise’s digital accounting environment, reveals the specifics of identifying digital risks, and evaluates the effectiveness of control procedures in the protection of accounting information. The national regulatory framework for information security is analysed, and the state of the digital accounting infrastructure of the farm “Volova hora” is assessed. A conceptual model for strengthening the enterprise’s information security is developed, and recommendations are provided for improving the audit of digital risks, taking into account modern approaches, technologies, and standard requirements.

ЗМІСТ

ВСТУП	4
РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДИЧНІ ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЦИФРОВОГО ОБЛІКОВОГО СЕРЕДОВИЩА	8
1.1. Сутність цифрового облікового середовища та інформаційні ризики в системах бухгалтерського обліку	8
1.2. Методичні підходи до забезпечення інформаційної безпеки та аудиту цифрових облікових систем	16
Висновки до розділу 1	22
РОЗДІЛ 2. ОЦІНЮВАННЯ СТАНУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА АУДИТУ ЦИФРОВОГО ОБЛІКОВОГО СЕРЕДОВИЩА ПІДПРИЄМСТВА	24
2.1. Характеристика цифрової облікової інфраструктури підприємства та ідентифікація інформаційних ризиків	24
2.2. Аналітична оцінка рівня захищеності цифрового облікового середовища та ефективності існуючих контрольних процедур	30
Висновки до розділу 2	37
РОЗДІЛ 3. УДОСКОНАЛЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ АУДИТУ ЦИФРОВОГО ОБЛІКОВОГО СЕРЕДОВИЩА	40
3.1. Концептуальна модель підвищення інформаційної безпеки цифрового облікового середовища підприємства	44
3.2. Розроблення рекомендацій щодо вдосконалення аудиту інформаційної безпеки та оцінки цифрових ризиків	44
Висновки до розділу 3	48
ВИСНОВКИ	50
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	54

ВСТУП

Актуальність вибраної теми. Цифрові зміни, що відбуваються в українській економіці останніми роками, охоплюють не лише оновлення технічних засобів, а й трансформацію самої логіки побудови облікових процесів. На рівні підприємств це спостерігається доволі чітко: господарські операції, які донедавна існували виключно у паперовому вигляді, тепер проходять через електронні сервіси, інтегровані з банківськими системами, податковими платформами чи галузевими інформаційними рішеннями. У результаті бухгалтерська робота все більше нагадує управління потоками даних, що переміщуються між різними цифровими середовищами та вимагають постійної узгодженості.

Перехід до хмарних сервісів і ERP-рішень змінює не тільки технічну сторону обліку, а й підвищує залежність підприємств від стабільності цифрової інфраструктури. Від оперативності доступу до даних, коректності синхронізації та рівня захисту інформації тепер безпосередньо залежить точність управлінських рішень. Тому цифрова трансформація стає не просто модернізацією інструментів, а комплексним управлінським викликом, який потребує переосмислення на методологічному рівні.

Разом із новими можливостями посилюються і ризики. На підприємствах, де внутрішній контроль тривалий час був прив’язаний до паперових процедур, поява електронних сервісів нерідко відкриває нові вразливості: нечіткий розподіл прав доступу, зберігання ключів електронного підпису на звичайних робочих станціях, відсутність системного журналювання подій, залежність від сторонніх сервісів та паралельне існування паперових і цифрових потоків документів. Такі проблеми особливо характерні для малих аграрних господарств, де ресурсні обмеження поєднуються з високою операційною складністю.

У цій ситуації питання безпеки цифрового облікового середовища виходить за межі технічної проблематики й набуває стратегічного значення. Підприємства вимушені переглядати структуру облікових процесів,

формалізовувати політики доступу, впроваджувати внутрішні аудитні процедури та налагоджувати взаємодію між підрозділами на основі нових цифрових регламентів. Динаміка оновлення законодавства України у сфері інформаційної безпеки також створює додаткові виклики: вимоги до цифрового обліку зростають, але далеко не завжди адаптовані до можливостей малого бізнесу.

Отже, дослідження особливостей функціонування цифрового облікового середовища та його захищеності на прикладі малого аграрного підприємства є не лише теоретично значущим. Воно має виразний практичний вимір, оскільки якість облікової системи прямо впливає на достовірність фінансової інформації, стійкість підприємства та здатність адаптуватися до зовнішніх ризиків в умовах економічної турбулентності.

Мета дослідження полягає у теоретичному обґрунтуванні підходів до забезпечення інформаційної безпеки цифрового облікового середовища підприємства, оцінюванні його фактичного стану та розробленні рекомендацій щодо вдосконалення аудиту й управління цифровими ризиками.

Завдання дослідження:

- розкрити теоретико-методичні основи цифрового облікового середовища та інформаційних ризиків;
- дослідити нормативно-правове забезпечення України у сфері інформаційної безпеки цифрових облікових систем;
- узагальнити міжнародні підходи (ISO/NIST/COBIT) до управління інформаційною безпекою;
- охарактеризувати цифрову облікову інфраструктуру ФГ «Волова гора»;
- ідентифікувати основні інформаційні ризики підприємства;
- здійснити аналітичну оцінку рівня захищеності цифрового облікового середовища та ефективності контрольних процедур;
- виконати кількісну оцінку цифрових ризиків;
- розробити рекомендації щодо вдосконалення системи інформаційної безпеки та аудиту на підприємстві;

- сформувати концептуальну модель підвищення ІБ цифрового облікового середовища.

Об’єкт дослідження – цифрове облікове середовище підприємства в умовах сучасної цифровізації економіки.

Предмет дослідження – теоретичні та практичні аспекти забезпечення інформаційної безпеки та аудиту цифрових облікових систем підприємства.

Методи дослідження. У процесі роботи використано:

- системний підхід – для формування комплексної концепції захисту цифрового облікового середовища;
- метод аналізу та синтезу – для узагальнення теоретичних підходів до ІБ;
- порівняльний аналіз – для зіставлення українських і міжнародних стандартів кіберзахисту;
- методи кількісної оцінки ризиків – для визначення інтегрального рівня цифрових загроз;
- структурно-логічне моделювання – для розроблення концептуальної моделі ІБ;
- аналітичні методи — для оцінювання стану інформаційної безпеки ФГ «Волова гора».

Наукова новизна отриманих результатів полягає у розробленні адаптованої моделі інформаційної безпеки цифрового облікового середовища малого аграрного підприємства, створенні кількісної шкали цифрових ризиків та формуванні механізму удосконаленого аудиту ІБ. У роботі запропоновано комплекс рекомендацій, які дозволяють малим підприємствам перейти від фрагментарної практики до системної моделі управління ризиками, що базується на провідних міжнародних стандартах.

Практична значимість дослідження полягає в можливості безпосереднього застосування розроблених рекомендацій ФГ «Волова гора» та іншими малими підприємствами для підвищення стійкості цифрових облікових систем, забезпечення достовірності фінансової інформації, захисту електронних документів і виконання вимог законодавства щодо інформаційної безпеки.

Апробація результатів роботи. Основні положення кваліфікаційної роботи апробовано на практичних матеріалах ФГ «Волова гора» та обговорено на XV Національній науково-практичній конференції «Синергія науки та бізнесу: виклики, трансформації, перспективи», проведеної 29 травня 2025 року в Західноукраїнському національному університеті та II Всеукраїнській науково-практичній конференції ««Інноваційні підходи до розвитку технологій та економіки»», проведеної 6 червня 2025 року в Західноукраїнському національному університеті.

Структура й обсяг роботи. Кваліфікаційна робота складається зі вступу, трьох розділів**,** висновків, списку використаних джерел. Загальний обсяг викладено на 58 сторінках.

РОЗДІЛ 1
ТЕОРЕТИКО-МЕТОДИЧНІ ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЦИФРОВОГО ОБЛІКОВОГО СЕРЕДОВИЩА

1.1. Сутність цифрового облікового середовища та інформаційні ризики в системах бухгалтерського обліку

Розвиток цифрової економіки та масове впровадження інформаційно-комунікаційних технологій зумовлюють глибинну трансформацію системи бухгалтерського обліку. У наукових дослідженнях дедалі частіше використовується термін «цифрове облікове середовище», який відображає перехід від організації обліку як сукупності окремих програм і технічних засобів до інтегрованого інформаційного простору підприємства. Під цифровим обліковим середовищем доцільно розуміти комплекс апаратних засобів, програмного забезпечення, баз даних, мережевої інфраструктури та організаційних регламентів, що забезпечують формування, обробку, зберігання і передачу бухгалтерської інформації в електронній формі та в режимі, максимально наближеному до реального часу. Такий підхід узгоджується з позицією В. Новікова, який трактує цифрове облікове середовище як «результат цілісної цифрової трансформації підприємства, що поєднує автоматизацію процедур, інтеграцію з бізнес-системами, застосування хмарних платформ та впровадження електронного документообігу» [1].

У сучасних умовах цифрове облікове середовище базується не лише на класичних бухгалтерських програмах, а й на розширеному спектрі технологій: хмарних сервісах, мобільних застосунках, системах електронного документообігу, сервісах обміну даними з податковими органами та банками, а також на елементах штучного інтелекту, великих даних і блокчейн-рішень. Дослідження С. Безручук показують, що «цифровізація істотно впливає на якість облікової інформації: з одного боку, підвищується оперативність, доступність та аналітична насиченість даних, з іншого – посилюються вимоги до надійності, зіставності та захищеності інформації, сформованої в облікових системах» [2].

Цифровізація дійсно підвищує оперативність та аналітичну глибину облікових даних, проте одночасно підсилює вимоги до їх надійності та контролю. Це означає, що технічний прогрес супроводжується зростанням навантаження на системи захисту та механізми верифікації інформації. Залишаючись інваріантними за змістом, елементи методу – документація, інвентаризація, оцінка, рахунки, подвійний запис, баланс, звітність – набувають електронної форми реалізації. Підприємства переходять від паперових первинних документів до електронних, від локальних програм до хмарних платформ, від фрагментарних інформаційних рішень до інтегрованих ERP-систем. У працях Ю. Нежид підкреслюється, що «диджиталізація системи обліково-інформаційного забезпечення супроводжується зміщенням акцентів з фіксації фактів господарського життя «заднім числом» до проактивного моніторингу та аналітичної інтерпретації даних у режимі реального часу» [3] .

В українській практиці цифрове облікове середовище формується на перетині кількох ключових тенденцій. По-перше, це масове використання хмарних облікових рішень, що забезпечують віддалений доступ до інформації, автоматичні оновлення нормативно-довідкової бази та інтеграцію з електронними сервісами держави й банківського сектору. По-друге, це розширення спектра електронних документів – від податкових накладних та звітності до електронних договорів і актів виконаних робіт. По-третє, це поступове впровадження технологій блокчейн, XBRL, штучного інтелекту й роботизованої автоматизації процесів (RPA) для рутинних облікових операцій. Узагальнення результатів досліджень В. Калабіної та співавторів [16] свідчить, що цифровізація бухгалтерського обліку в Україні спрямована на підвищення прозорості, точності та доступності фінансової інформації, але водночас супроводжується появою нових вразливих зон у сфері інформаційної безпеки.

Цифрове облікове середовище вбирає у себе ознаки «відкритої» системи: значна частина облікових даних циркулює в електронному вигляді поза межами виключно внутрішньої інфраструктури підприємства – через хмарні платформи, канали інтернет-з’єднання, інтеграційні шлюзи з державними реєстрами та

сервісами контрагентів. Це розширює можливості обліку, але водночас збільшує поверхню атаки для потенційних загроз. Як слушно зауважує С. Безручук «навіть за підвищення якісних характеристик інформації (оперативності, релевантності, повноти) цифровізація не усуває фундаментальної проблеми – вразливості облікових даних до викривлення, несанкціонованого доступу та зниження довіри з боку користувачів» [1].

У цьому контексті надзвичайно актуальним стає системний аналіз інформаційних ризиків у цифровому обліковому середовищі. Під інформаційним ризиком у системі бухгалтерського обліку доцільно розуміти ймовірність виникнення подій, які призводять до порушення конфіденційності, цілісності або доступності облікової інформації й, як наслідок, до прийняття хибних управлінських рішень, фінансових збитків, санкцій з боку регуляторних органів чи втрати ділової репутації. Така інтерпретація добре узгоджується з класичною тріадою інформаційної безпеки (confidentiality–integrity–availability), що використовується в міжнародних стандартах ISO/IEC 27001, і дозволяє структуровано підходити до оцінки загроз для облікових даних.

Аналіз сучасних публікацій показує, що ризики цифровізації в сфері бухгалтерського обліку мають багатовимірний характер. У роботі І. Грабчук та А. Якубівської виділено низку загроз, пов’язаних із впровадженням цифрових сервісів: від технічних збоїв і уразливостей програмного забезпечення до ризиків помилок користувачів та зловмисного втручання у процеси формування облікової інформації.

Ю. Попівняк, досліджуючи кібербезпеку бухгалтерських даних, наголошує, що саме цифрові канали передачі інформації стають основним середовищем реалізації загроз – через шкідливе програмне забезпечення, фішингові атаки, компрометацію облікових записів користувачів тощо.

Узагальнюючи підходи різних авторів, доцільно виокремити щонайменше п’ять ключових груп інформаційних ризиків у цифровому обліковому середовищі.

По-перше, це організаційні ризики, які пов’язані з недоліками внутрішньої регламентації облікових процесів: відсутністю формалізованої політики інформаційної безпеки, нечітким розподілом повноважень, слабко розробленими процедурами електронного документообігу, відсутністю внутрішніх регламентів використання хмарних сервісів та дистанційного доступу. Дослідження С. Гаркуші демонструють, що «саме організаційні прогалини часто стають тим «слабким місцем», через яке реалізуються технічні й кадрові загрози, навіть за наявності сучасних програмних засобів захисту» [1].

По-друге, технологічні ризики зумовлені вразливістю ІТ-інфраструктури та прикладного програмного забезпечення. Вони охоплюють ризики збоїв у роботі серверів, помилок у програмному коді, відсутності належного резервного копіювання, використання застарілих версій ПЗ та операційних систем, некоректної інтеграції між обліковими системами та зовнішніми сервісами (банківськими застосунками, податковими порталами тощо). У працях, присвячених цифровізації обліку [7; 8], наголошується, що перехід на хмарні рішення одночасно знижує частину інфраструктурних ризиків (пов’язаних із локальним обладнанням) і створює нові – залежність від провайдера послуг, стабільності інтернет-з’єднання, прозорості механізмів зберігання й обробки даних у дата-центрах.

По-третє, правові (комплаєнс) ризики пов’язані з невідповідністю організації цифрового обліку вимогам законодавства щодо захисту інформації та електронних документів. Ідеться, зокрема, про порушення режиму обігу персональних даних, неправомірне використання електронного підпису, недотримання встановлених строків і форматів зберігання електронних документів, відсутність належного підтвердження автентичності й цілісності облікових даних. Порушення таких вимог створює подвійний ризик: з одного боку, підвищується ймовірність технічної або організаційної втрати інформації, з іншого – зростає загроза застосування санкцій з боку контролюючих органів.

По-четверте, кадрові та поведінкові ризики (людський фактор) охоплюють як ненавмисні помилки користувачів, так і потенційні зловживання. Недостатня

обізнаність бухгалтерів та інших працівників щодо правил кібергігієни, використання слабких паролів, передавання облікових записів між співробітниками, нехтування процедурами резервного копіювання, невміння розпізнати фішингові листи – усе це збільшує ймовірність реалізації кіберзагроз. Водночас можливі й умисні дії персоналу: несанкціоноване коригування облікових даних, копіювання й передавання конфіденційної інформації третім особам, маніпулювання доступами до облікової системи. У літературі [18; 19] підкреслюється, що людський фактор залишається одним із найскладніших об’єктів управління в системі інформаційної безпеки.

По-п’яте, зовнішні кіберзагрози пов’язані з діями зловмисників у кіберпросторі: масові вірусні атаки, зокрема із застосуванням програм-вимагачів; цільові хакерські атаки на облікові системи; фішингові кампанії, спрямовані на викрадення облікових даних користувачів; масове сканування мережі на предмет вразливих сервісів з подальшою їх експлуатацією. Ю. Попівняк зазначає, що актуальними стають не лише традиційні вірусні загрози, а й комплексні атаки, орієнтовані на блокування доступу до облікових даних, їх шифрування та подальший шантаж підприємства [5].

Наведені групи ризиків можна звести до узагальнювальної класифікації, яка демонструє взаємозв’язок між джерелами загроз та їх впливом на облікову інформацію.

Узагальнюючи, слід підкреслити, що цифрове облікове середовище, будучи основою сучасної системи бухгалтерського обліку, одночасно виступає й простором підвищеної інформаційної вразливості. З одного боку, цифровізація забезпечує зростання ефективності облікових процесів, оперативності управлінських рішень, можливостей аналітики та прозорості взаємодії з користувачами звітності. З іншого – поява нових форматів даних, каналів їх передачі та режимів доступу суттєво ускладнює завдання забезпечення інформаційної безпеки. Це актуалізує завдання формування практично орієнтованих механізмів управління ризиками, які враховують специфіку цифрових процесів та особливості функціонування бухгалтерських систем.

Таблиця 1.1

Узагальнена класифікація інформаційних ризиків у цифровому обліковому середовищі

Група ризиків	Характеристика	Потенційні наслідки для облікової інформації
Організаційні	Відсутність політик, регламентів, розподілу повноважень	Несистемний захист, хаотичні рішення, зростання вразливості
Технологічні	Збої ПЗ, вразливості ІТ-інфраструктури, помилки інтеграції	Втрата або пошкодження даних, збої у формуванні звітності
Правові (комплаєнс)	Порушення вимог щодо захисту та обігу електронних документів	Санкції регуляторів, недійсність окремих документів
Кадрові та поведінкові	Помилки, недбалість, умисні зловживання персоналу	Фальсифікація або викривлення даних, витік інформації
Зовнішні кіберзагрози	Вірусні атаки, фішинг, зломи облікових систем	Блокування доступу, шифрування даних, несанкціонований доступ

Функціонування цифрового облікового середовища в Україні базується не лише на технологічних інноваціях, але й на розгалуженому нормативно-правовому полі, яке встановлює загальні принципи організації електронного документообігу, вимоги до захисту інформації, правила використання електронних підписів та стандарти забезпечення кібербезпеки. Вітчизняне законодавство формує правові рамки, що визначають обов’язки підприємств у сфері обліку, зберігання даних та захисту електронної інформації.

Ключовим актом, який регламентує використання електронних документів у бухгалтерському обліку, є Закон України «Про електронні документи та електронний документообіг». У ньому визначено правовий статус електронного документа, порядок його створення, обігу, зберігання, а також вимоги до підтвердження цілісності та автентичності інформації. Закон встановлює, що електронний документ є рівнозначним паперовому за умови наявності електронного підпису, що відповідає встановленим стандартам. Саме це

положення створило передумови для широкого запровадження електронних первинних документів і звітності в українському обліку.

Важливу роль у сфері інформаційної безпеки відіграє Закон України «Про захист інформації в інформаційно-комунікаційних системах», який визначає принципи захисту інформації, механізми протидії несанкціонованому доступу та критерії побудови комплексних систем захисту інформації (КСЗІ). Закон встановлює, що власник інформаційної системи зобов'язаний забезпечити конфіденційність, цілісність і доступність інформаційних ресурсів, а також організувати аудит безпеки, адміністрування доступів та використання засобів технічного й криптографічного захисту.

Специфічні вимоги щодо організації електронного підпису та електронної ідентифікації закріплено в Законі України «Про електронні довірчі послуги», який імплементує європейський регламент eIDAS. Цей закон визначає порядок використання кваліфікованих електронних підписів (КЕП), кваліфікованих електронних печаток і часових міток, що забезпечує юридичну значущість електронних документів та їх захищеність у цифровому обліковому середовищі. Для підприємств це означає необхідність впровадження регламентів застосування КЕП, контролю доступу до ключів та процедур управління ними.

Певні аспекти цифровізації обліку також регулюються Законом України «Про бухгалтерський облік та фінансову звітність в Україні», який встановлює вимоги до документування господарських операцій, порядку зберігання документів та формування звітності. У контексті цифрової трансформації актуальним є положення про можливість ведення первинних документів в електронній формі та зберігання їх у ІТ-системах за умови забезпечення захисту від несанкціонованого доступу та забезпечення цілісності інформації. Таким чином, підприємство, що використовує цифрове облікове середовище, зобов'язане гарантувати збереження електронних даних упродовж встановлених строків та мати технічні засоби для підтвердження їх автентичності.

У ширшому контексті діяльність підприємств у цифровому середовищі перебуває під регулюванням законодавства у сфері кібербезпеки. Закон України

«Про основні засади забезпечення кібербезпеки України» визначає державну політику у сфері захисту критичної інформаційної інфраструктури та встановлює загальні вимоги до організації кіберзахисту на суб'єктному рівні. Хоча більшість положень закону адресовано об'єктам критичної інфраструктури, його норми створюють нормативні передумови для впровадження технічних і організаційних заходів захисту в ІТ-системах приватного сектору, у тому числі тих, що забезпечують ведення бухгалтерського обліку.

Окрему роль відіграють нормативні документи системи технічного захисту інформації (НД ТЗІ), зокрема вимоги до комплексних систем захисту інформації в інформаційно-телекомунікаційних системах (ДСТУ 3396.1–96 та пов'язані стандарти). Вони визначають базові принципи побудови безпечних інформаційних систем, що охоплюють і цифрові облікові середовища, та передбачають наявність політик безпеки, розмежування прав доступу, ведення журналів подій, організацію резервного копіювання та регулярний аудит безпеки.

Таким чином, нормативно-правове регулювання цифрового облікового середовища в Україні формує комплексну систему вимог, яка інтегрує норми електронного документообігу, бухгалтерського обліку, кібербезпеки та технічного захисту інформації. У сукупності правові норми визначають обов'язок підприємства забезпечити надійність цифрового облікового середовища, зокрема: гарантувати достовірність електронних документів, організувати їх захист від несанкціонованих дій та зберігати підтвердження цілісності облікових даних протягом установлених строків. Це створює правову платформу для розвитку методів управління інформаційними ризиками та побудови ефективних систем аудиту інформаційної безпеки, що стане предметом детального аналізу в наступному підрозділі.

1.2. Методичні підходи до забезпечення інформаційної безпеки та аудиту цифрових облікових систем

Ефективне функціонування цифрового облікового середовища неможливе без побудови цілісної системи інформаційної безпеки, інтегрованої в загальну систему корпоративного управління. Для бухгалтерського обліку це означає, що захист інформації повинен розглядатися не як сукупність окремих технічних заходів (антивірус, брандмауер тощо), а як система управління інформаційною безпекою, пов'язана з фінансовими, організаційними та контрольними процесами підприємства.

Теоретичним ядром будь-якої системи інформаційної безпеки є класична тріада конфіденційність – цілісність – доступність (CIA). У цифровому обліковому середовищі ці принципи набувають специфічного змісту.

По-перше, конфіденційність означає, що доступ до облікових даних мають лише ті суб'єкти, для яких це необхідно з огляду на посадові обов'язки та повноваження. Йдеться не лише про захист від зовнішніх зловмисників, а й про внутрішнє розмежування доступів: бухгалтер не повинен мати можливості змінювати налаштування системи, а рядовий працівник – переглядати повний масив фінансової звітності. У цифровому середовищі конфіденційність забезпечується комбінацією механізмів автентифікації, авторизації, шифрування та журналізації доступів.

По-друге, цілісність у контексті обліку означає збереження даних у достовірному, повному й незміненому стані протягом усього життєвого циклу – від введення первинної інформації до формування підсумкової звітності та архівування. Будь-які зміни в обліковій інформації мають бути простежуваними, а історія правок – відтворюваною. Втрата цілісності облікових даних означає ризик суттєвих викривлень фінансової звітності та податкових зобов'язань, що має прямі правові та фінансові наслідки.

По-третє, доступність передбачає, що авторизовані користувачі мають можливість своєчасно отримати доступ до потрібної інформації та функцій системи. Для обліку це критично з огляду на жорсткі строки подання звітності,

проведення платежів, закриття періодів. Будь-які тривалі відмови в обслуговуванні (наприклад, через збої в роботі хмарного сервісу або інциденти кібербезпеки) можуть призвести до порушення податкової дисципліни, штрафних санкцій і втрати репутації.

У бухгалтерському середовищі до цієї тріади додаються такі важливі вимоги, як збереження історичних даних (архівів) та безперервність роботи облікової системи. Архіви первинних документів і регістрів обліку мають зберігатися протягом строків, установлених законодавством, із гарантією їх автентичності та непридатності до несанкціонованої модифікації. Безперервність діяльності (business continuity) передбачає, що підприємство має плани аварійного відновлення (disaster recovery) на випадок відмови обладнання, атаки програм-вимагачів, тривалої втрати доступу до хмарних сервісів тощо.

Побудова системи інформаційної безпеки цифрового облікового середовища логічно включає такі взаємопов’язані елементи:

- ідентифікація ризиків і вразливостей, що можуть призвести до порушення конфіденційності, цілісності або доступності облікової інформації;
- формування політики інформаційної безпеки, яка визначає принципи, правила та процедури захисту для всіх підрозділів;
- впровадження комплексу організаційних, технічних і кадрових заходів (регламенти доступу, резервне копіювання, антивірусний захист, навчання персоналу, моніторинг подій тощо);
- планування та тестування процедур реагування на інциденти і відновлення діяльності після збоїв.

Таким чином, система захисту цифрового облікового середовища повинна бути вибудувана так, щоб навіть у разі відмови одного із захисних механізмів доступ до критичних даних залишався контрольованим. Це забезпечує послідовність і стійкість процесів обліку, що є передумовою для формування достовірної фінансової інформації.

Методологічну основу для побудови та аудиту системи інформаційної безпеки цифрового обліку становлять міжнародно визнані стандарти й

фреймворки. Центральне місце серед них посідає стандарт ISO/IEC 27001, який є глобальною базою для створення систем управління інформаційною безпекою (ISMS). Стандарт визначає вимоги до політик, процедур, оцінки ризиків і контролів, спрямованих на захист інформаційних активів організації.

В Україні ISO/IEC 27001 імплементовано як національний стандарт ДСТУ ISO/IEC 27001:2023, що встановлює вимоги до систем управління інформаційною безпекою з урахуванням українського правового поля [11].Це створює нормативне підґрунтя для того, щоб підприємства – включно з тими, що здійснюють бухгалтерський облік у цифровому середовищі, – могли сертифікувати свої системи безпеки та підтверджувати відповідність міжнародним вимогам.

Паралельно важливе місце посідає NIST Cybersecurity Framework (CSF), розроблений Національним інститутом стандартів і технологій США. Фреймворк структурує управління кіберризиками за п’ятьма базовими функціями: Identify, Protect, Detect, Respond, Recover – і пропонує деталізовані категорії та підкатегорії контролів для кожної з них [55]. Для цифрового облікового середовища це дозволяє логічно вибудувати контури захисту: від ідентифікації критичних облікових активів (баз даних, модулів розрахунку зарплати, підсистем податкової звітності) до процедур реагування на інциденти (зокрема, блокування компрометованих облікових записів, відновлення даних із резервних копій, аналізу причин інциденту).

Третім ключовим елементом є фреймворк COBIT (Control Objectives for Information and Related Technologies), розроблений ISACA. COBIT розглядає управління інформаційними технологіями з позицій корпоративного управління: його завданням є забезпечити відповідність IT-цілей стратегічним бізнес-цілям, встановити контрольні цілі та метрики для всіх IT-процесів, у тому числі процесів безпеки. У версії COBIT 2019 описано 40 базових цілей управління й контролю, які охоплюють весь життєвий цикл інформаційних систем [27]. З погляду цифрового обліку це означає можливість оцінювати не лише технічний

стан систем безпеки, а й ступінь їх узгодженості з фінансовою стратегією, внутрішнім контролем та аудиторськими процедурами.

Для зручності порівняння їх змістовних акцентів нижче наведено узагальнену характеристику найбільш поширених міжнародних підходів до управління інформаційною безпекою.

Фреймворк / стандарт	Основний фокус	Застосовність до цифрового обліку
ISO/IEC 27001 / ДСТУ ISO/IEC 27001	Система управління інформаційною безпекою (політики, процеси, контролі)	Побудова формалізованої ISMS для облікових систем, сертифікація відповідності
NIST CSF	Управління кіберризиками, функції «Identify–Protect–Detect–Respond–Recover»	Структурування контролів і процедур захисту облікових IT-активів і каналів обміну даними
COBIT 2019	Корпоративне IT-управління та контроль процесів	Узгодження IT-процесів (у т.ч. облікових) зі стратегією, побудова системи показників і контролів

Зазначені фреймворки знаходяться в тісній взаємодії з українським законодавством. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [12] встановлює принципи захисту інформації, обов’язки власників і розпорядників інформаційно-телекомунікаційних систем щодо забезпечення конфіденційності, цілісності й доступності даних, а також вимоги до побудови комплексних систем захисту інформації (КСЗІ). Закон України «Про основні засади забезпечення кібербезпеки України» [13] визначає державну політику в сфері кібербезпеки, основні принципи захисту об’єктів критичної інформаційної інфраструктури та окреслює загальні підходи до організації кіберзахисту на рівні господарюючих суб’єктів.

Таким чином, застосування ISO/IEC 27001, NIST CSF і COBIT у цифровому обліковому середовищі українських підприємств не є суто «добровільною» адаптацією зарубіжних практик, а логічно доповнює

національне правове поле, яке вимагає наявності дієвих систем захисту інформації, процедур контролю та аудиту.

Сучасна методологія аудиту – як фінансового, так і ІТ-аудиту – базується на ризик-орієнтованому підході. За Міжнародним стандартом аудиту 315 аудитор повинен спочатку отримати розуміння підприємства, його середовища й системи внутрішнього контролю, а вже потім – ідентифікувати та оцінити ризики суттєвого викривлення, у тому числі пов’язані з використанням інформаційних технологій. Цей підхід органічно переноситься на аудит інформаційної безпеки цифрових облікових систем.

У цифровому обліковому середовищі ризик-орієнтований підхід передбачає послідовність:

1. Визначення критичних інформаційних активів – облікових баз даних, модулів обліку заробітної плати, податкових підсистем, каналів обміну з ДПС та банками, архівів електронних документів тощо.
2. Ідентифікація загроз і вразливостей для кожного з цих активів: несанкціонований доступ, шкідливе ПЗ, помилки користувачів, збої хмарного сервісу, втрати резервних копій тощо.
3. Оцінка ризиків через визначення ймовірності реалізації загроз та потенційного впливу (фінансового, правового, репутаційного) на підприємство.
4. Розробка аудиторських процедур, спрямованих насамперед на ті зони, де поєднання ймовірності й наслідків формує високий або неприйнятний рівень ризику.

У практичній площині це означає, що, наприклад, для підприємства, яке критично залежить від хмарної бухгалтерської системи, аудитор приділятиме підвищену увагу питанням безперервності доступу до сервісу, наявності й регулярності резервного копіювання, умовам договору з провайдером, режимам шифрування даних та управлінню обліковими записами. Якщо у цифровому обліковому середовищі активно застосовуються інтеграції з зовнішніми сервісами (CRM, системи складського обліку, банківський клієнт), до зони

підвищеного ризику потрапляють інтерфейси обміну даними, алгоритми узгодження інформації та механізми контролю за цілісністю інтегрованих даних.

Ризик-орієнтований підхід дозволяє поєднати міжнародні стандарти із реальним профілем ризиків конкретного підприємства. Функції NIST CSF “Identify–Protect–Detect–Respond–Recover” фактично задають логіку руху аудитора: від ідентифікації й оцінки ризиків (Identify) – до тестування захисних заходів (Protect, Detect), перевірки процедур реагування й відновлення (Respond, Recover/ Водночас ISO/IEC 27001 забезпечує формальну рамку для документування результатів оцінки ризиків та впровадження відповідних контролів, а COBIT – для оцінки зрілості процесів управління й контролю, пов’язаних з цифровим обліком.

Для цифрового аудиту облікових систем принципово важливо, що об’єктом перевірки є не лише правильність відображення господарських операцій, а й здатність інформаційної системи забезпечити захищене формування й збереження даних. Тому аудиторські процедури включають аналіз:

- організації доступів (хто, до чого і на яких підставах має доступ);
- історії змін у ключових облікових регістрах;
- процедур резервного копіювання й тестування відновлення;
- практик використання електронного підпису;
- відповідності технічних і організаційних заходів вимогам українського законодавства в частині захисту інформації та електронних документів.

Узагальнюючи, методологічні підходи до забезпечення інформаційної безпеки й аудиту цифрових облікових систем формуються на перетині трьох площин: (1) базових принципів інформаційної безпеки (конфіденційність, цілісність, доступність, безперервність), (2) міжнародних рамкових стандартів (ISO/IEC 27001, NIST CSF, COBIT), (3) національного правового поля у сфері захисту інформації й кібербезпеки. Ризик-орієнтований аудит виступає інструментом практичної реалізації цих підходів, дозволяючи фокусувати ресурси на найбільш критичних зонах цифрового облікового середовища та

забезпечуючи належний рівень довіри до облікової інформації в умовах цифрової економіки.

Для подальшого аналізу цифрового облікового середовища в межах цієї кваліфікаційної роботи застосовується інтегрований методичний підхід, що поєднує базові принципи інформаційної безпеки з положеннями ISO/IEC 27001, NIST Cybersecurity Framework та COBIT 2019, адаптованими до реальних умов функціонування українських підприємств. ISO/IEC 27001 використовується як структурна основа побудови системи управління інформаційною безпекою; NIST CSF — як інструментарій формалізації процесів ідентифікації ризиків, захисних заходів, виявлення інцидентів, реагування та відновлення; COBIT 2019 — як рамка оцінювання зрілості IT-процесів та їх узгодженості з цілями обліку й внутрішнього контролю. Додатковим аналітичним орієнтиром виступає ризик-орієнтований підхід, визначений МСА 315, який дає змогу сфокусувати увагу на тих компонентах цифрового облікового середовища, де поєднання ймовірності інцидентів і потенційних наслідків формує підвищений рівень ризику. Сукупність цих методичних засад визначає логіку оцінювання інформаційної безпеки підприємства у розділі 2 та слугує підґрунтям для подальшої розробки практичних рекомендацій у розділі 3.

Висновки до розділу 1

Проведений у розділі 1 теоретико-методичний аналіз дозволив сформувати цілісне уявлення про сутність цифрового облікового середовища, його ключові ризики та методичні засади забезпечення інформаційної безпеки й аудиту. Узагальнення результатів дослідження дає підстави для формування таких висновків.

1. Цифрове облікове середовище є інтегрованим інформаційним простором підприємства, у межах якого здійснюється формування, обробка та передавання бухгалтерської інформації в електронній формі. Його структура охоплює апаратну й програмну інфраструктуру, бази даних, електронні документи, хмарні сервіси, інтеграційні модулі та організаційні регламенти.

Цифровізація обліку докорінно трансформує традиційні елементи методу бухгалтерського обліку, переводячи документацію, регістри, звітність та аналітичні процедури в електронний формат, підвищуючи оперативність і гнучкість облікових процесів.

2. Функціонування цифрового облікового середовища супроводжується виникненням багатовимірних інформаційних ризиків, що охоплюють організаційні, технологічні, правові, кадрові та зовнішні кіберзагрози. Їх спільною рисою є потенційний вплив на конфіденційність, цілісність і доступність облікових даних, що може призвести до спотворення фінансової інформації, порушення вимог законодавства, фінансових втрат і репутаційних збитків. У дослідженні систематизовано основні групи ризиків і виявлено взаємозв'язок між джерелами загроз та їх наслідками для бухгалтерського обліку, що створює основу для подальшої ідентифікації вразливостей у практичній частині роботи.

3. Нормативно-правове поле України визначає комплекс вимог до організації цифрового обліку та інформаційної безпеки, яке включає законодавство про електронні документи, електронні довірчі послуги, захист інформації в інформаційно-комунікаційних системах, бухгалтерський облік та кібербезпеку. Зазначені акти встановлюють обов'язок підприємств забезпечувати достовірність електронних документів, їх юридичну значущість, захист від несанкціонованих дій та збереження протягом установлених строків. Таким чином, правова регламентація виступає фундаментом для побудови ефективної системи захисту цифрових облікових даних.

4. Забезпечення інформаційної безпеки цифрового облікового середовища ґрунтується на поєднанні базових принципів (конфіденційності, цілісності, доступності й безперервності), міжнародних фреймворків (ISO/IEC 27001, NIST CSF, COBIT) та ризик-орієнтованого підходу, закріпленого у МСА 315. Таке інтегроване методичне підґрунтя дозволяє системно оцінювати рівень загроз, обґрунтовувати структуру захисних заходів і вибудовувати аудит цифрових облікових систем з урахуванням найбільш критичних зон ризику.

РОЗДІЛ 2
ОЦІНЮВАННЯ СТАНУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА АУДИТУ ЦИФРОВОГО ОБЛІКОВОГО СЕРЕДОВИЩА ПІДПРИЄМСТВА

2.1. Характеристика цифрової облікової інфраструктури підприємства та ідентифікація інформаційних ризиків

Фермерське господарство «Волова гора» є типовим представником малого аграрного бізнесу, для якого поєднання традиційних виробничих процесів із цифровими інструментами управління стає ключовим чинником підтримання конкурентоспроможності. Господарство здійснює діяльність у сферах рослинництва та тваринництва, працює з істотними обсягами матеріальних ресурсів (насіння, добрива, паливо, корми), біологічних активів, а також із широким спектром основних засобів сільськогосподарського призначення. Окрім цього, підприємство підтримує значний масив розрахункових операцій із контрагентами, бюджетом та працівниками. За таких умов бухгалтерський облік фактично виконує роль ядра інформаційної системи підприємства, а цифрове облікове середовище виступає інфраструктурною основою для оперативного управління та планування.

Матеріали виробничої практики свідчать, що організація облікових процесів у ФГ «Волова гора» побудована на використанні спеціалізованого програмного забезпечення для бухгалтерського й податкового обліку з окремими елементами хмарної архітектури. Функціонал облікової системи охоплює модулі ведення фінансового обліку, обліку виробничих витрат, управління взаєморозрахунками, розрахунку заробітної плати та відображення операцій з персоналом. Паралельно застосовуються програмні засоби електронного документообігу з ДПС — середовище подання звітності, реєстрації податкових накладних — а також клієнт-банкінг для виконання безготівкових платежів. У результаті формується інтегрований цифровий контур, який забезпечує узгодженість основних фінансових, податкових та розрахункових операцій.

Технічна складова цифрового середовища базується на використанні персональних комп’ютерів і ноутбуків бухгалтерії та адміністративного

персоналу, а також мережевого обладнання, що забезпечує доступ до інтернету. Окремі облікові функції — зокрема робота з електронною поштою, обмін первинною інформацією та дистанційний доступ до хмарних сервісів — можуть виконуватися з мобільних пристроїв керівництва. Власного ІТ-підрозділу господарство не має; технічне обслуговування та налаштування програмного забезпечення здійснюється із залученням зовнішніх консультантів. Для малих фермерських підприємств це є типовою практикою, що зменшує витрати на утримання ІТ-персоналу, але водночас формує додаткові ризики, пов’язані з організацією контролю доступів, актуальністю оновлень та безперервністю роботи облікових систем.

Цифровий цикл облікової інформації у ФГ «Волова гора» охоплює трансформацію первинних виробничих даних у фінансові та податкові показники. На початковому етапі формується первинний масив інформації про господарські операції: надходження матеріалів, використання палива, виконання польових робіт, процеси догляду за посівами, збирання врожаю, реалізацію продукції, рух тварин і кормів, нарахування оплати праці. Частина цих даних спочатку фіксується на паперових документах або у відомостях, створених у вигляді електронних таблиць, після чого переноситься до облікової системи. Інша частина надходить у цифровій формі — банківські виписки, електронні податкові накладні, електронні акти від контрагентів. Всі ці операції формують інформаційний потік, який далі перетворюється у регістри бухгалтерського обліку, податкові зобов’язання та фінансову звітність.

На другому етапі первинні дані обробляються в межах програмних модулів системи бухгалтерського обліку: формується бухгалтерське проведення, здійснюється розподіл витрат між культурами та виробничими підрозділами, розраховується собівартість продукції, визначаються фінансові результати діяльності, обчислюються податкові зобов’язання та податковий кредит. На третьому етапі генерується звітна інформація — фінансова звітність, податкові декларації, статистична звітність, а також внутрішні управлінські звіти для керівництва. Реалізація цих процесів у цифровому форматі суттєво скорочує час

обробки даних, мінімізує ручні операції та підвищує оперативність аналітичної інформації для прийняття управлінських рішень.

Інформаційні потоки, що проходять через цифрове облікове середовище, умовно поділяються на кілька взаємопов'язаних сегментів. Перший — виробничий, який охоплює дані про рух матеріальних ресурсів, використання техніки, виробіток, урожайність, зміни в поголів'ї тварин тощо. Другий — фінансовий, який містить інформацію про касові та банківські операції, взаєморозрахунки з контрагентами, податкові платежі, кредитні операції й відсоткові витрати. Третій — кадровий, що забезпечує формування даних щодо чисельності персоналу, нарахування заробітної плати, утримання податків і внесків, обліку відпусток і тимчасової непрацездатності. Четвертий — податково-юридичний сегмент, який включає електронні декларації, реєстр податкових накладних, договори, акти виконаних робіт та інші документи, що циркулюють у цифровому форматі. Збій чи помилка в одному з цих блоків неминуче впливають на достовірність показників інших сегментів.

У структурі цифрового середовища ФГ «Волова гора» можна виокремити низку критично важливих інформаційних активів, від безпечного функціонування яких залежить можливість підприємства підтримувати фінансову стійкість та виконувати свої зобов'язання. До таких активів належать база даних бухгалтерського обліку (у тому числі регістри синтетичного й аналітичного обліку, довідники контрагентів, номенклатура запасів, модуль обліку основних засобів), архів електронних податкових документів, електронні банківські виписки та платіжні доручення, дані щодо розрахунків із персоналом, а також архів резервних копій системи. Втрата або спотворення цих даних створює ризик прямого фінансового збитку, порушення податкових зобов'язань та втрати доказової бази у взаєминах з банками й контрагентами.

Аналіз функціонування цифрової облікової інфраструктури ФГ «Волова гора» виявив низку системних вразливостей. По-перше, відсутність штатного IT-фахівця або окремої відповідальної особи за інформаційну безпеку спричиняє ситуативний характер прийняття рішень у сфері кіберзахисту. Процедури

налаштування прав доступу, резервного копіювання, оновлення програмного забезпечення часто залежать від ініціативності окремих працівників або зовнішніх консультантів, що суперечить принципам формалізованого управління ризиками.

По-друге, використання хмарних рішень для бухгалтерського обліку водночас зменшує навантаження на локальну інфраструктуру та переносить вагому частку відповідальності на провайдера послуг. Реальний рівень інформаційної безпеки залежить від умов договору — зокрема, регламентації резервування даних, політики відновлення після збоїв, механізмів реагування на інциденти та визначення відповідальності у разі витоку інформації. При цьому господарство повинно забезпечити якісний захист на стороні користувача: належне управління доступами, контроль використання облікових записів, шифрування каналів зв’язку, навчання персоналу.

По-третє, у ФГ «Волова гора» зберігається «змішаний» формат формування первинних даних: частина інформації створюється на паперових носіях або в окремих електронних таблицях, а частина — одразу в цифрових модулях. Унаслідок цього виникають ризики втрати даних на етапі перенесення, а також ризики дублювання та неузгодженості між різними джерелами. Якщо процедури збору первинної інформації не формалізовані (не визначено відповідальних, строки, канали передачі), ймовірність помилок істотно зростає.

Окремої уваги потребують ризики, пов’язані з людським фактором. У невеликих фермерських господарствах часто спостерігається концентрація ключових функцій у руках одного бухгалтера, який одночасно відповідає за ведення обліку, податкову звітність, окремі елементи кадрового обліку та розрахунки через банківські сервіси. Будь-яка помилка, перевантаження або тимчасова відсутність цього працівника можуть призвести до збоїв у здійсненні облікових операцій та затримки критичних платежів. Крім того, недостатній рівень кібергігієни (слабкі паролі, необережність у роботі з електронною поштою, передача облікових даних стороннім особам) підвищує вразливість до зовнішніх кіберзагроз.

На основі співставлення теоретичної класифікації інформаційних ризиків із фактичними умовами функціонування ФГ «Волова гора» можна виділити кілька домінантних груп ризиків, що потребують підвищеної уваги з боку керівництва та аудиторів.

Організаційні ризики проявляються у відсутності формалізованої політики інформаційної безпеки, нечіткому розподілі повноважень у сфері доступу до облікових систем, а також у відсутності затверджених процедур резервного копіювання та реагування на інциденти. Така ситуація створює передумови для прийняття ситуативних рішень, що підвищує ймовірність помилок і ускладнює управління ризиками.

Технологічні ризики зумовлені використанням програмного забезпечення без належного контролю за актуальністю оновлень, залежністю від стабільності інтернет-з’єднання при роботі з хмарними сервісами, а також недостатньою увагою до фізичного та логічного відокремлення робочих і резервних копій даних. У сукупності ці чинники посилюють загрозу втрати або пошкодження критичної інформації.

Правові ризики виникають у разі недотримання законодавчих вимог щодо захисту інформації, електронних документів і персональних даних. Некоректне зберігання електронних первинних документів, відсутність підтвердження їх автентичності, використання електронних підписів без належного контролю за ключами можуть поставити під сумнів юридичну силу документів і спровокувати порушення правових норм.

Кадрові ризики пов’язані з тим, що значна частина рішень у сфері інформаційної безпеки ухвалюється працівниками без спеціальної підготовки у сфері кібербезпеки та ІТ-менеджменту. Це стосується як бухгалтерів, так і керівництва, яке може недооцінювати потребу в інвестиціях у захисні технології та підвищення компетентностей персоналу. На цьому тлі зовнішні кіберзагрози — шкідливе ПЗ, фішингові атаки, компрометація облікових записів — стають особливо небезпечними, враховуючи, що малі підприємства часто є «легкими цілями» для зловмисників.

Узагальнюючи, цифрова облікова інфраструктура ФГ «Волова гора» поєднує відносно сучасні програмні рішення та налагоджений електронний документообіг із високою залежністю від людського фактора, зовнішніх сервісів і відсутності формалізованої політики інформаційної безпеки. Це формує вразливе середовище, у якому навіть один інцидент — наприклад, зараження робочої станції програмою-вимагачем або компрометація облікового запису бухгалтера — може мати масштабні наслідки для облікової інформації та фінансових результатів підприємства.

Таблиця 2.1

Домінантні інформаційні ризики у цифровому обліковому середовищі ФГ «Волова гора»

Група ризиків	Конкретні прояви на підприємстві	Потенційні наслідки для облікової інформації
Організаційні	Відсутність формалізованої політики ІБ; нечіткий розподіл повноважень щодо доступу; відсутність регламентів бекапів	Несистемний захист; хаотичні рішення; підвищена ймовірність помилок і несвоєчасного виявлення інцидентів
Технологічні	Залежність від хмарного сервісу; нерегулярне оновлення ПЗ; нестабільність інтернет-з'єднання	Збої в роботі облікової системи; тимчасова втрата доступу до даних; ризик втрати актуальності інформації
Правові (комплаєнс)	Недостатня формалізація роботи з електронними документами та КЕП; відсутність процедур зберігання та автентифікації	Сумніви в юридичній значущості окремих документів; ризик санкцій з боку контролюючих органів
Кадрові та поведінкові	Концентрація функцій в одному бухгалтері; низький рівень обізнаності з кібергігієни; спільне використання акаунтів	Висока залежність результатів обліку від однієї особи; ризик фальсифікації або ненавмисного викривлення даних
Зовнішні кіберзагрози	Потенційна вразливість робочих станцій до вірусів, фішингу, програм-вимагачів	Блокування доступу до облікових даних; шифрування баз; можливий витік конфіденційної інформації

Для систематизації виявлених інформаційних ризиків у цифровому обліковому середовищі ФГ «Волова гора» сформовано узагальнену матрицю, що відображає конкретні прояви загроз та їх потенційні наслідки (табл. 2.1).

Виявлені особливості цифрової інфраструктури та спектр інформаційних ризиків у ФГ «Волова гора» створюють підґрунтя для подальшої аналітичної оцінки фактичного рівня захищеності облікового середовища та дієвості наявних контрольних процедур, що буде детально розглянуто у підрозділі 2.2.

2.2. Аналітична оцінка рівня захищеності цифрового облікового середовища та ефективності існуючих контрольних процедур

Аналітична оцінка стану інформаційної безпеки у ФГ «Волова гора» потребує комплексного підходу, що поєднує вивчення фактичних технічних та організаційних практик, моделювання інформаційних ризиків і визначення рівня відповідності чинним нормативним вимогам та усталеним міжнародним моделям кіберзахисту. У процесі дослідження цифрової облікової інфраструктури враховано особливості, притаманні малим аграрним підприємствам, зокрема залежність від зовнішніх IT-сервісів, відсутність штатного IT-персоналу, змішаний формат первинних даних та обмежені ресурси для впровадження комплексних систем аудиту. Оцінювання здійснювалося за ключовими напрямами: організація контролю доступу, наявність і зміст політик безпеки, функціонування системи журналізації подій, стан резервного копіювання, порядок роботи з електронними документами, рівень кібергігієни користувачів, а також відповідність сукупності технічних, організаційних і правових механізмів установленим вимогам.

Контроль доступу є базовим елементом захисту облікової інформації, адже визначає обсяг операцій, які користувач може виконувати відповідно до своїх повноважень. У ФГ «Волова гора» застосовується персоніфікована модель доступу для працівників бухгалтерії та керівництва, проте її реалізація залишається недостатньо формалізованою. Аналіз засвідчує, що конфігурація доступів не завжди відповідає принципу мінімальних привілеїв, а низка операцій

виконується за допомогою спільних облікових записів або з використанням загальних робочих станцій. За відсутності детальної журналізації таких дій виникають труднощі з ідентифікацією відповідальних осіб, що ускладнює внутрішній аудит і реагування на інциденти.

Додаткові ризики пов’язані з тим, що політика паролів фактично не регламентована: вони можуть використовуватися тривалий час без зміни, не відповідають вимогам до складності, не перевіряються на повтори й не доповнюються механізмами двофакторної автентифікації. Такі практики підвищують імовірність компрометації облікових записів через brute-force атаки, фішингові повідомлення чи несанкціоноване використання даних доступу.

Оцінювання рівня ризиків здійснюється із застосуванням формалізованої шкали ймовірності та впливу, адаптованої до специфіки діяльності фермерського господарства. Діапазони характеристик ризиків подано у табл. 2.2.

Таблиця 2.2

Умовна шкала оцінювання ймовірності та впливу інформаційних ризиків

Показник	Рівень	Опис
Ймовірність (P)	0,2	Низька – подія малоймовірна, поодинокі випадки
Ймовірність (P)	0,5	Середня – подія може реалізуватися періодично
Ймовірність (P)	0,8	Висока – подія має тенденцію до регулярної реалізації
Вплив (I)	1	Низький – незначні відхилення в облікових даних, локальні наслідки
Вплив (I)	2	Середній – суттєві відхилення, що потребують коригування, можливі штрафи
Вплив (I)	3	Високий – істотні викривлення звітності, значні фінансові та репутаційні втрати

Кількісна оцінка ризику за шкалою ймовірності (низький — 0,2; середній — 0,5; високий — 0,8) та впливу (низький — 1; середній — 2; високий — 3) показує, що:

- ймовірність компрометації облікового запису оцінюється на рівні 0,6,
- потенційний вплив на облікову інформацію — 3,

- що формує інтегральний ризик R = 1,8 (високий).

Застосування наведеної шкали дозволило здійснити кількісну оцінку одного з ключових ризиків — компрометації облікового запису користувача. Результати розрахунку наведено у табл. 2.3.

Таблиця 2.3

Приклад кількісної оцінки ризику компрометації облікового запису у ФГ «Волова гора»

Інформаційний ризик	Ймовірність (P)	Вплив (I)	Інтегральний ризик R = P × I	Рівень ризику
Компрометація облікового запису користувача	0,6	3	1,8	Високий

Таким чином, система контролю доступу у ФГ «Волова гора» потребує суттєвого вдосконалення, зокрема шляхом запровадження персоніфікованих облікових записів, політики складності та регулярного оновлення паролів, механізмів журналізації входів і виходів, а також переходу до використання двофакторної автентифікації. Це дасть можливість обмежити необґрунтований доступ до облікової інформації та забезпечити належну простежуваність користувацьких дій.

У межах господарства відсутні письмово затверджені політики інформаційної безпеки, які б регламентували правила зберігання даних, порядок доступу, процедури підтвердження надійності електронних документів, а також вимоги щодо обробки персональних даних працівників і контрагентів. Для малого бізнесу така практика є поширеною, однак саме відсутність формалізованих правил спричиняє хаотичність рішень і підвищує вразливість інформаційної інфраструктури, навіть за умов достатнього технічного оснащення.

Відповідно до норм Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» і Закону України «Про електронні документи та електронний документообіг», підприємство зобов’язане забезпечити захист інформації від несанкціонованих дій, гарантувати її

цілісність і доступність, а також визначити відповідальних за підтримку безпечної роботи системи. На підприємстві такі відповідальні особи формально не призначені, що створює додаткові правові ризики — зокрема у випадку перевірок, втрати даних або інцидентів, пов’язаних із компрометацією інформації.

За моделлю зрілості політик інформаційної безпеки (рівні 0–5) ФГ «Волова гора» може бути віднесене до рівня 1 (Initial/Ad-hoc), тобто такого, де політики існують лише на рівні індивідуальних практик окремих працівників, не документуються та не охоплюють усі ключові процеси цифрового облікового середовища.

Механізми журналізації подій є критичним інструментом аудиту, оскільки забезпечують можливість відстеження дій користувачів у системі — доступу до файлів, створення та зміни документів, коригування довідників і регістрів обліку. У ФГ «Волова гора» журналізація реалізована переважно за рахунок базового функціоналу хмарного облікового сервісу, однак її практичне застосування є обмеженим:

- аналіз журналів не проводиться регулярно;
- відповідальні за моніторинг подій не визначені;
- не сформовано перелік «тривожних подій», які мають активувати негайну реакцію (масові зміни даних, нетипові входи, видалення документів тощо).

Відсутність системного підходу до журналізації та реагування на аномальні події створює ризик несвоєчасного виявлення інцидентів і ускладнює подальше розслідування причин та обставин порушень.

Стан організації реагування на інциденти інформаційної безпеки у ФГ «Волова гора» можна оцінити за умовною шкалою оперативності, поданою в таблиці 2.4.

Таблиця 2.4

Умовна шкала оцінювання оперативності реагування на інциденти інформаційної безпеки

Рівень	Характеристика
0	Відсутнє реагування – інциденти не фіксуються, формальні процедури не визначені.
1	Низька – реагування здійснюється епізодично, без стандартизованих процедур.
2	Середня – існують базові процедури, але вони виконуються нерегулярно, без системного аналізу та документування.
3	Висока – формалізовані процедури реагування, регулярний аналіз причин інцидентів, ведення журналів та запровадження коригувальних заходів.

З позицій цифрового аудиту це означає низьку здатність підприємства до виявлення інцидентів на ранній стадії. Використовуючи умовну 4-рівневу шкалу оперативності реагування (0 — відсутня; 3 — висока), рівень можна оцінити як 1 (низький).

Резервне копіювання у ФГ «Волова гора» здійснюється нерегулярно, переважно у вигляді ручного копіювання важливих документів та файлів на зовнішні носії. Водночас хмарний провайдер облікової системи забезпечує власні процедури резервування, але їх обсяг і деталізація не повністю відомі користувачеві. Така ситуація створює ризики подвійної залежності:

1. Залежність від добросовісності та технічної ефективності хмарного провайдера.

2. Вразливість локальних копій до фізичних ризиків (втрата, пошкодження).

За результатами аналізу резервне копіювання як процес можна віднести до рівня «мінімально функціонального», але такого, що не забезпечує гарантій безперервності діяльності у разі серйозного інциденту (кібератаки, збій обладнання, криптовірус).

Інтегральний ризик втрати даних за моделлю «ймовірність × вплив» оцінюється:

- ймовірність – 0,5**,**
- вплив – 3**,**
- результат – 1,5 (середньо-високий ризик)**.**

Електронний документообіг у господарстві залежить від кількох зовнішніх сервісів: порталів податкової служби, системи клієнт-банкінгу, електронного підпису. Аналіз показує, що:

- ключі підпису зберігаються на робочих станціях без додаткового шифрування,
- доступ до ключів має обмежене коло працівників, але без формалізованих правил,
- не фіксуються факти доступу до ключів або спроби їх копіювання.

Це є критичною вразливістю, оскільки компрометація ключа може призвести до несанкціонованої подачі документів, зміни фінансових показників або отримання доступу до конфіденційної інформації.

У структурі цифрового облікового середовища людський фактор залишається найвразливішою ланкою. Персонал не проходить регулярного навчання з кібербезпеки, а рівень навичок використання засобів захисту визначається здебільшого практичним досвідом. Це підтверджується такими спостереженнями:

- часте використання одного облікового запису кількома працівниками,
- відкриття електронних листів із підозрілих адрес,
- зберігання паролів у відкритому вигляді або у браузері,
- відсутність практики блокування комп’ютерів під час відсутності працівників.

Рівень управління людським фактором проаналізовано за стандартною моделлю зрілості, що включає п’ять рівнів розвитку практик кібергігієни (табл. 2.5).

Таблиця 2.5

Умовна шкала оцінювання зрілості управління людським фактором в інформаційній безпеці

Рівень	Характеристика
0 — Вразливий	Відсутнє навчання, інструктажі, політики щодо користувачів; високий рівень імпровізації.
1 — Початковий	Проводяться поодинокі інструктажі; відсутня системність; знання фрагментарні; реагування на інциденти хаотичне.
2 — Базовий	Проводяться періодичні навчання; існують мінімальні внутрішні регламенти; рівень технічної грамотності середній.
3 — Керований	Систематичні тренінги, контроль дотримання політик, регулярне оновлення знань; наявний визначений відповідальний за ІБ.
4 — Оптимізований	Культура безпеки інтегрована в щоденну діяльність; персонал володіє навичками кібергігієни; проводиться постійне вдосконалення практик.

За 5-рівневою шкалою зрілості людського фактору (від 0 — «вразливий» до 4 — «керований») господарство відповідає рівню **1 («початковий»)».

Для оцінювання системи захисту в контексті міжнародних стандартів застосовано адаптовану модель відповідності вимогам ISO/IEC 27001, COBIT 5 та NIST CSF із використанням якісно-кількісної шкали.

Узагальнення результатів оцінювання відповідності вимогам міжнародних стандартів інформаційної безпеки подано в табл. 2.6, яка відображає рівень зрілості ключових контрольних компонентів.

Узагальнена оцінка (середнє значення 1,5 бала) свідчить, що система інформаційної безпеки ФГ «Волова гора» перебуває на рівні зрілості «Initial/Repeatable», характерному для малих підприємств із низьким ступенем формалізації процесів кіберзахисту (див. табл. 2.2).

Проведений аналіз показує, що цифрове облікове середовище ФГ «Волова гора» перебуває на початкових етапах становлення системи інформаційної безпеки. Використовувані технічні засоби є достатніми для ведення оперативного обліку, проте не формують повноцінного середовища для захисту критичних даних і забезпечення безперервності діяльності.

Таблиця 2.6

Оцінка зрілості системи інформаційної безпеки ФГ «Волова гора»

(адаптовано до вимог ISO/IEC 27001, COBIT, NIST CSF)

Критерій відповідності	Рівень (0–5)	Характеристика
Політики ІБ	1	Несформовані, відсутні регламенти
Контроль доступу	2	Базові механізми без чіткого розмежування ролей
Управління активами	2	Відсутній реєстр інформаційних активів
Журналізація та аудит	1	Нерегулярний аналіз, обмежена деталізація
Резервне копіювання	2	Змішана система, низька частота копій
Захист від шкідливого ПЗ	3	Базові антивірусні рішення без політики
Кадрова безпека	1	Відсутність навчання й інструктажів
Управління інцидентами	0	Процес не визначений

Основні проблеми пов’язані з:

- фрагментарністю заходів кіберзахисту;
- відсутністю політики та процедур ІБ;
- недостатньо ефективним контролем доступу;
- низьким рівнем журналізації та моніторингу подій;
- недостатньою організацією резервного копіювання;
- ризиками, спричиненими людським фактором;
- невідповідністю вимогам законодавства щодо захисту електронних документів та персональних даних.

Виявлений стан системи інформаційної безпеки не є критичним для поточної діяльності господарства, проте створює суттєві ризики у разі масштабування діяльності, введення нових цифрових сервісів або виникнення кібератаки. Отримані результати формують підґрунтя для розроблення практичних рекомендацій з підвищення рівня кіберзахисту та впровадження аудиторських процедур, що буде розглянуто у розділі 3.

Висновки до розділу 2

1. Цифрова облікова інфраструктура ФГ «Волова гора» забезпечує інтеграцію фінансових, податкових, виробничих та кадрових потоків інформації, але характеризується низьким рівнем формалізації процесів та надмірною залежністю від людського фактору. Поєднання хмарного програмного забезпечення, локальних робочих станцій, електронного документообігу та клієнт-банкінгу створює необхідний мінімум для ведення обліку, проте відсутність системної IT-політики, внутрішніх регламентів, визначених відповідальних осіб за інформаційну безпеку та контролю за життєвим циклом даних формує вразливе середовище, де навіть незначний інцидент може призвести до суттєвих порушень цілісності та доступності інформації.
2. Ідентифіковано домінантні групи інформаційних ризиків, які мають значний вплив на облікові процеси підприємства. Організаційні ризики зумовлені відсутністю політик ІБ та процедур резервного копіювання; технологічні — залежністю від хмарного сервісу та несистемним оновленням ПЗ; правові — нечітким дотриманням вимог щодо електронних документів і персональних даних; кадрові — концентрацією критичних функцій у одного бухгалтера та слабкими навичками кібергігієни; зовнішні — зростаючими кіберзагрозами, характерними для малих бізнесів. Формалізована оцінка (P•I) засвідчила високий рівень ризику компрометації облікових записів (R = 1,8) та середньо-високий ризик втрати даних через недостатню організацію резервного копіювання (R = 1,5).
3. Аналітична оцінка контрольних процедур показала фрагментарність та низький рівень зрілості механізмів інформаційної безпеки. Контроль доступу здійснюється без принципу мінімальних привілеїв і без журналізації дій користувачів; резервне копіювання відбувається нерегулярно та не забезпечує гарантій відновлення; електронні ключі підпису зберігаються без шифрування; реагування на інциденти не структуроване. За моделлю відповідності ISO/IEC 27001, COBIT та NIST CSF сформовано середній рівень зрілості 1,5 бала, що відповідає стадії Initial/Repeatable — початкові практики

існують, але не підтримані політиками, регламентами та системним моніторингом.

4. Наявний рівень інформаційної безпеки є достатнім для базового функціонування, але не забезпечує стійкості до сучасних цифрових загроз та не відповідає вимогам масштабування діяльності. Для підвищення зрілості системи необхідні системні зміни: формалізація політик ІБ, впровадження контрольних механізмів, підвищення рівня цифрових компетентностей персоналу та адаптація підприємства до міжнародних підходів аудиту й управління інформаційною безпекою. Це визначає логічні передумови для формування рекомендацій, представлених у розділі 3.

РОЗДІЛ 3
УДОСКОНАЛЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ АУДИТУ ЦИФРОВОГО ОБЛІКОВОГО СЕРЕДОВИЩА

3.1. Концептуальна модель підвищення інформаційної безпеки цифрового облікового середовища підприємства

Побудова ефективної системи інформаційної безпеки цифрового облікового середовища на підприємстві потребує цілісної моделі, яка охоплює організаційні, технологічні та процесні елементи. На основі проведеного оцінювання ФГ «Волова гора» встановлено, що підприємство перебуває на початковому рівні інформаційної зрілості: відсутня політика інформаційної безпеки, процедури доступу не формалізовано, резервне копіювання здійснюється епізодично, а аудит ІБ не є системним. Це вимагає розроблення моделі, що формує взаємозв'язок між управлінням ризиками, контролем доступу, цифровою інфраструктурою та циклом аудиту.

Запропонована модель складається з трьох взаємопов'язаних блоків: організаційного**,** технологічного та процесного, які разом формують каркас системи управління інформаційною безпекою цифрового облікового середовища підприємства (рис. 3.1).

Структурно-логічна модель складається з трьох взаємопов'язаних блоків:

- організаційного**,** який формує нормативну та управлінську основу забезпечення безпеки (політика, ролі, навчання);
- технологічного**,** що охоплює інфраструктурні механізми (Zero Trust, сегментація, резервування);
- процесного**,** який створює цикл безперервного аудиту та управління ризиками.

Їх інтеграція формує єдину систему, яка забезпечує стійке та контрольоване цифрове облікове середовище підприємства.

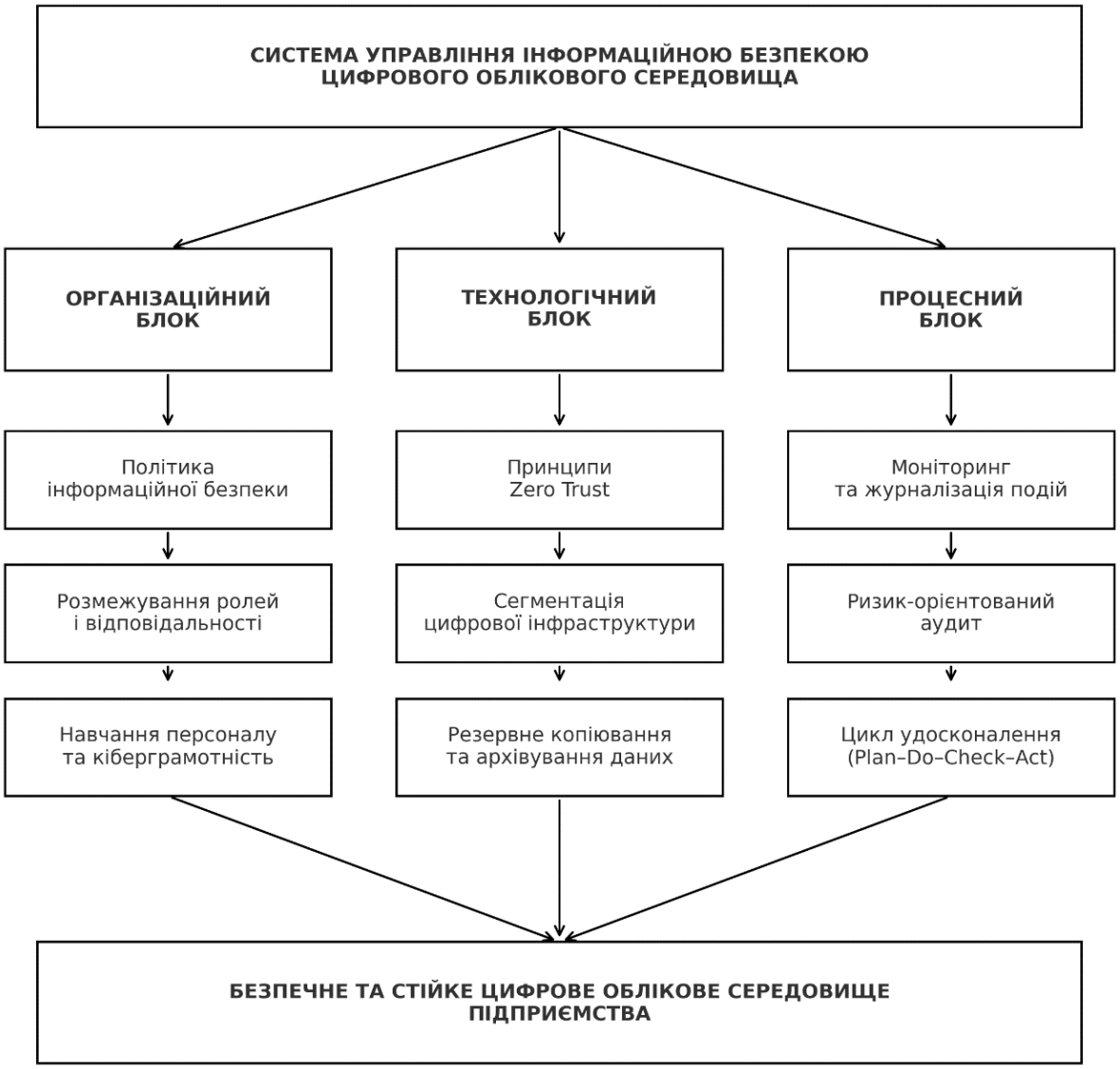

Рис. 3.1. Структурно-логічна модель підвищення інформаційної безпеки цифрового облікового середовища підприємства

Організаційна складова є визначальною, оскільки саме вона забезпечує керованість та передбачуваність роботи з інформацією. Для ФГ «Волова гора» ключовою проблемою є відсутність єдиної нормативної рамки. Тому першим елементом моделі є впровадження комплексної політики інформаційної безпеки**,** що регламентує:

- правила доступу до цифрової облікової системи;
- порядок створення, блокування та архівування облікових записів;
- правила використання КЕП та носіїв ключів;
- принципи обробки персональних й фінансових даних відповідно до Закону

України «Про захист інформації в ІКС»;

- вимоги до резервного копіювання та зберігання архівів;
- процедури реагування на інциденти.

Розроблення політики ІБ дозволяє підприємству здійснити перехід від інтуїтивних дій до керованої системи з чітко визначеними правами, обов'язками та зонами відповідальності.

Суттєвий вплив на рівень безпеки має формалізація ролей. У контексті діяльності підприємства доцільно виокремити такі ролі: відповідальний за інформаційні активи, адміністратор доступу, користувач облікової системи, відповідальний за інциденти. Запропонована система розмежування ролей (таблиця 3.1) забезпечує прозорість управління та створює основу для внутрішнього контролю.

Окремої уваги потребує розвиток цифрової грамотності персоналу, який у малих господарствах часто є критично низьким. Запровадження коротких регламентованих інструктажів — щодо безпечної роботи з електронними документами, ознак фішингу, правил створення паролів — може підвищити загальний рівень інформаційної зрілості підприємства з рівня 1 (початковий) до рівня 2–3 (керований) протягом року.

Таблиця 3.1

Розподіл функцій та відповідальності у системі інформаційної безпеки ФГ «Волова гора»

Роль	Основні функції	Значення для ІБ
Власник інформації	затвердження політики, розподіл прав	стратегічний контроль
Адміністратор доступу	створення та блокування доступів, моніторинг	захист від внутрішніх загроз
Користувач	робота з даними, дотримання регламентів	цілісність інформації
Відповідальний за інциденти	реагування, звітування, відновлення	безперервність роботи

Технологічна основа моделі спрямована на мінімізацію технічних ризиків та забезпечення контролю над усіма каналами обробки облікових даних.

Ключовим елементом є впровадження принципів Zero Trust Architecture, яка передбачає відмову від апріорної довіри до будь-якого користувача чи пристрою. Для ФГ «Волова гора» це означає застосування двофакторної автентифікації для доступу до облікової системи, перевірку пристроїв, обмеження доступу за мережевими параметрами та контроль усіх сесій користувачів.

Іншим важливим елементом є сегментація цифрового середовища, коли критичні елементи облікової інфраструктури відокремлені від загальної офісної мережі. Така сегментація зменшує ймовірність несанкціонованого поширення шкідливого коду та унеможливлює неконтрольований доступ до бухгалтерських ресурсів.

Суттєвим технічним напрямом є підвищення надійності зберігання даних. Для підприємства запропоновано комбіновану модель резервного копіювання (таблиця 3.2), яка поєднує хмарні копії для оперативного доступу та локальні копії для захисту від зовнішніх інцидентів.

Процесний елемент моделі забезпечує її динамічність та адаптивність. На основі ризик-орієнтованого підходу формується цикл безперервного аудиту**,** який складається з п’яти етапів:

1. ідентифікація ризиків у цифровому обліковому середовищі;
2. оцінювання ймовірності та впливу;
3. тестування ефективності контрольних процедур;
4. впровадження коригувальних заходів;
5. повторний аудит.

Таблиця 3.2

Пропонована модель резервного копіювання для ФГ «Волова гора»

Тип копії	Періодичність	Місце зберігання	Призначення
Оперативна хмарна	щоденно	сервери провайдера	швидке відновлення
Контрольна локальна	щотижнево	ізольований носій	захист від атак/збоїв
Архівна	щомісяця	зовнішній носій	довгострокове зберігання

У підсумку формується замкнена система удосконалення: результати аудиту переходять у плани змін, які потім підлягають повторній перевірці. Це забезпечує сталий розвиток системи ІБ та дозволяє підприємству просуватися від реактивної поведінки до превентивного управління ризиками.

Узагальнена концептуальна модель ґрунтується на поєднанні організаційних, технологічних та процесних механізмів та враховує специфіку малого аграрного підприємства. Для ФГ «Волова гора» її впровадження забезпечить підвищення зрілості інформаційної безпеки з рівня 1 (початковий) до рівня 3 (керований), зменшить ризики втрати й спотворення облікових даних та підвищить стійкість цифрового середовища до внутрішніх та зовнішніх загроз.

3.2. Розроблення рекомендацій щодо вдосконалення аудиту інформаційної безпеки та оцінки цифрових ризиків

Ефективне вдосконалення аудиту інформаційної безпеки в цифровому обліковому середовищі мікро- та малих підприємств потребує переходу від фрагментарних, епізодичних перевірок до цілісної, методологічно обґрунтованої системи контролю. У випадку ФГ «Волова гора» специфіка функціонування цифрового середовища характеризується низкою організаційних і технологічних вразливостей, які зумовлюють необхідність розроблення методичних рекомендацій, здатних забезпечити підвищення передбачуваності, прозорості та керованості процесів цифрової безпеки.

Для досягнення цієї мети доцільно інтегрувати ризик-орієнтований підхід, сучасні стандарти оцінювання інформаційної безпеки та елементи внутрішнього аудиту, адаптовані до масштабу та ресурсу підприємства. Аудит інформаційної безпеки перестає бути технічною процедурою та перетворюється на інструмент управління стійкістю цифрового середовища.

Першим етапом розбудови надійної системи аудиту є перегляд самого принципу його виконання. Замість фіксації окремих недоліків необхідно формувати структуроване бачення того, як інформаційні потоки, електронні документи, облікові записи та інші цифрові активи взаємодіють між собою. Саме

це й визначає концептуальну основу аудиту — розуміння, що цифрова інформація є не просто окремими файлами, а елементами єдиного інформаційного циклу, вразливість будь-якої його частини може створити загрози для всієї облікової системи підприємства.

Така логіка вимагає переходу до чотириетапної аудиторської моделі:

1. встановлення критичних активів;
2. виявлення зон ризику;
3. аналіз стану наявних контрольних процедур;
4. визначення пріоритетів удосконалення.

Ці етапи взаємопов’язані та формують методичний контур, який можна представити як циклічну систему оцінювання (рис. 3.3). У графічному вигляді така схема демонструє, що аудит не є разовою дією, а розвивається як неперервний процес, де завершення одного циклу створює підґрунтя для наступного.

Рис. 3.3. Логічна модель удосконаленого аудиту інформаційної безпеки

Удосконалений аудит потребує розширення інструментарію шляхом впровадження кількісних методів оцінювання ризиків. Для малого підприємства доцільно застосувати спрощену, але достатньо інформативну модель, яка дозволяє вимірювати цифровий ризик як добуток ймовірності інциденту та масштабу потенційної шкоди. Такий підхід забезпечує систематизацію ризиків і

можливість порівнювати їх між собою, що важливо для визначення пріоритетних напрямів удосконалення.

На основі отриманих даних ФГ «Волова гора» сформовано кількісний профіль ризиків, поданий у табл. 3.3. Він свідчить, що найуразливішими зонами є зберігання ключів КЕП, доступ до хмарної бази даних та помилки персоналу, які зумовлюють найбільший інтегральний рівень ризику. Менш критичними, але теж значущими залишаються ризики, пов’язані з вірусними атаками та надійністю локальних архівів.

Для підвищення точності оцінювання доцільно використовувати уніфіковану шкалу ризиковості (рис. 3.4), яка дозволяє класифікувати ризики на низькі, середні, підвищені та критичні. Така шкала є не лише інструментом аналізу, а й механізмом комунікації між керівництвом і виконавцями, оскільки вона перетворює складні цифрові характеристики на зрозумілі категорії управлінських рішень.

Таблиця 3.3

Оцінка цифрових ризиків ФГ «Волова гора» за кількісною моделлю

Загроза	Ймовірність (0–10)	Вплив (0–10)	Інтегральний ризик R	Інтерпретація
Компрометація ключа КЕП	7	9	63	критичний
Втрата доступу до хмарної бази	6	8	48	високий
Помилки персоналу при введенні даних	8	5	40	підвищений
Вірусні атаки	5	6	30	середній
Несанкціонований доступ	4	7	28	середній
Втрата локальних копій	3	6	18	низький

0–20 21–40 41–60 61–100

низький середній підвищений критичний

Рис. 3.4. Шкала рівнів цифрових ризиків підприємства

Поглиблений аналіз діяльності підприємства свідчить, що внутрішній аудит ІБ потребує суттєвої перебудови. На сьогодні він має епізодичний

характер, не охоплює повного циклу безпеки та фактично не забезпечує зворотного зв’язку між виявленими проблемами та запровадженими змінами. Рекомендованим є формування так званого «вбудованого аудиту», коли функції перевірки інтегруються у повсякденні управлінські рішення.

Такий підхід передбачає, що контроль доступів має здійснюватися не лише за фактом створення нового облікового запису, а й шляхом регулярної (наприклад, щоквартальної) ревізії відповідності доступів фактичним трудовим функціям працівників. Аналогічно, перевірка резервних копій повинна відбуватися не формально, а через тестове відновлення даних. Журнали подій мають аналізуватися не ситуативно, а з визначеною періодичністю, що дозволить виявляти аномалії у поведінці користувачів або у функціонуванні системи.

Удосконалений внутрішній аудит повинен завершуватися формуванням «карти цифрових ризиків» підприємства, яка містить дані щодо загроз, їхнього рівня та відповідальних осіб за мінімізацію ризиків. Це створює замкнену систему управління, де кожен аудиторський цикл веде до конкретних змін і покращень.

Удосконалення аудиту цифрової безпеки передбачає також розширення зовнішнього аудиту. Для ФГ «Волова гора» доцільним є залучення незалежних спеціалістів не лише для формальної перевірки хмарної бухгалтерії, а й для оцінювання політик, процедур та практик інформаційної безпеки. Такий аудит повинен базуватися на комбінованому підході, що включає чеклісти ISO/IEC 27001, оцінювальні карти COBIT та елементи NIST CSF.

Особливо важливим є тестування здатності підприємства до відновлення після інцидентів — так звані Disaster Recovery Drill, які проводяться щорічно. Вони дозволяють перевірити не лише технічні можливості, а й організаційну готовність підприємства діяти у кризових ситуаціях.

Розроблені рекомендації демонструють, що удосконалення аудиту інформаційної безпеки не може бути обмежене суто технічними діями. Воно потребує переходу до методично структурованого підходу, який поєднує кількісне оцінювання ризиків, побудову шкали ризиковості, регулярний

внутрішній аудит, створення карти ризиків, а також періодичне залучення зовнішніх фахівців. Така система дозволяє ФГ «Волова гора» перейти від реактивного до превентивного управління цифровою безпекою, підвищуючи інтегральну стійкість облікового середовища та забезпечуючи захист критичних даних у довгостроковій перспективі.

Висновки до розділу 3

У третьому розділі сформовано цілісну концепцію підвищення інформаційної безпеки та вдосконалення аудиту цифрового облікового середовища, яка поєднує організаційні, технологічні та процесні елементи. На основі проведеного аналізу та розроблених рекомендацій сформульовано такі узагальнені висновки:

1. Розроблена структурно-логічна модель інформаційної безпеки забезпечує перехід підприємства від фрагментарних, ситуаційних дій до системного управління ризиками. Запропонована трикомпонентна архітектура (організаційна, технологічна та процесна) формує цілісну рамку для підвищення стійкості цифрового облікового середовища. Центральним елементом є запровадження політики інформаційної безпеки, формалізація ролей і розмежування відповідальності, що дає змогу підвищити керованість інформаційних потоків та зменшити залежність від людського фактора. В умовах малого підприємства це створює основу для переходу до вищого рівня інформаційної зрілості та забезпечує відповідність законодавчим вимогам щодо захисту електронних даних.

2. Технологічні рекомендації спрямовані на мінімізацію ключових технічних ризиків та забезпечення безперервності роботи облікового середовища. Впровадження принципів Zero Trust, сегментація облікової інфраструктури, двофакторна автентифікація, підсилені механізми моніторингу та журналізації подій формують технічну основу захищеного середовища. Запропонована комбінована модель резервного копіювання — з поєднанням

оперативних хмарних, локальних контрольних та архівних копій — підвищує стійкість до кіберінцидентів і збоїв та є економічно доцільною для мікробізнесу.

3. Удосконалений аудит інформаційної безпеки орієнтований на оцінку реальних ризиків та формування циклу безперервного вдосконалення.

Запропонована чотириетапна модель аудиту (ідентифікація активів, виявлення ризиків, оцінка контрольних процедур, визначення пріоритетів удосконалення) у поєднанні з кількісною оцінкою цифрових ризиків дозволяє підприємству вимірювати рівень загроз та оптимізувати розподіл ресурсів. Використання інтегрального показника ризику, шкали ризиковості та формування карти цифрових ризиків надає керівництву інструменти для прийняття обґрунтованих управлінських рішень. Важливо, що аудит перестає виконуватися епізодично і трансформується у превентивну систему контролю.

4. Реалізація запропонованої моделі та рекомендацій забезпечує підвищення рівня інформаційної безпеки з початкового стану до керованого.

Інтеграція організаційних, технологічних і процесних заходів дозволить ФГ «Волова гора» суттєво знизити ризики компрометації ключових даних, втрати доступу до хмарних ресурсів чи помилок персоналу. Комплексність моделі забезпечує підсилення внутрішнього та зовнішнього аудиту, підвищення рівня цифрової грамотності працівників та формування культури інформаційної безпеки. У результаті підприємство отримує стійке, кероване та прогнозоване цифрове середовище, здатне адаптуватися до зовнішніх та внутрішніх загроз і підтримувати безперервність бухгалтерського та управлінського обліку.

ВИСНОВКИ

1. Дослідження засвідчило, що цифрова трансформація облікового середовища малого аграрного підприємства вимагає комплексного підходу до організації інформаційних потоків і побудови системи їхнього захисту. У процесі аналізу було визначено, що цифрова облікова інфраструктура ФГ «Волова гора» є структурно сформованою, але недостатньо формалізованою щодо безпеки та контролю операцій. Облікові дані циркулюють між кількома програмними модулями (фінансовий, виробничий, податковий облік, електронний документообіг, клієнт-банк), що забезпечує певний рівень автоматизації, однак одночасно підвищує залежність від зовнішніх сервісів та людського фактору. Встановлено, що облікова система функціонує ефективно для щоденних операцій, але не відповідає сучасним вимогам цифрової безпеки, що підтверджує актуальність вибраної тематики та визначеної проблематики.
2. Теоретичний аналіз сучасних підходів до організації інформаційної безпеки у цифровому обліковому середовищі засвідчив, що законодавча база України перебуває в процесі розвитку та не забезпечує повного методичного інструментарію для захисту даних у бухгалтерському обліку. Попри наявність законів України «Про електронні документи», «Про захист інформації в ІКС», «Про захист персональних даних», практична реалізація вимог залишається складною для малих підприємств. Водночас міжнародні стандарти (ISO/IEC 27001, ISO/IEC 27002, ISO 22301, COBIT, NIST CSF) пропонують чіткі моделі управління ризиками та побудови захисних заходів, які відзначаються системністю та універсальністю. Визначено, що інтеграція їх елементів у діяльність малих підприємств можлива за умови адаптації до їх ресурсного потенціалу та управлінських можливостей.
3. Проведений аналіз цифрової інфраструктури ФГ «Волова гора» дозволив визначити її сильні та слабкі сторони. До сильних сторін належать: використання хмарного ПЗ, оперативність доступу до даних, інтеграція податкового та фінансового документообігу, можливість оперативного формування звітності. Водночас встановлено низку критичних вразливостей:

відсутність формалізованої політики інформаційної безпеки, недостатня диференціація прав доступу, зберігання ключів КЕП на робочих станціях, епізодичне резервне копіювання, використання спільних облікових записів, наявність змішаних паперово-цифрових потоків первинних документів. Саме ці фактори визначають підвищену вразливість цифрового середовища та формують підґрунтя для кількісної оцінки ризиків.

4. Ідентифікація інформаційних ризиків у цифровому обліковому середовищі показала, що підприємство має низку технологічних, організаційних, кадрових, правових та зовнішніх цифрових загроз. Найбільш небезпечними є: компрометація облікових записів та ключів КЕП, втрата доступу до хмарних сервісів, вірусні атаки, некоректні або несвоєчасні оновлення програмного забезпечення, людські помилки при введенні даних, відсутність контролю журналів подій, а також недотримання вимог щодо електронного документообігу. У роботі встановлено, що сукупність цих ризиків здатна спричинити прямі фінансові втрати, спотворення звітності, порушення зобов’язань перед бюджетом та контрагентами, а також репутаційні наслідки.
5. Результати кількісної оцінки ризиків, виконаної за моделлю $R = P \times I$, продемонстрували, що підприємство має декілька зон з критично високим та високим рівнем небезпеки. Так, компрометація ключа КЕП отримала інтегральний показник 63 (критичний рівень), помилки персоналу — 40 (підвищений), а ризики, пов’язані з вірусними атаками та втратою локальних копій, хоч і мають нижчі значення, проте не можуть бути проігноровані. Визначено, що відсутність регулярного аналізу ризиків та їх документування суттєво знижує стійкість облікової системи до внутрішніх та зовнішніх факторів.
6. За результатами оцінювання відповідності міжнародним стандартам встановлено, що рівень зрілості інформаційної безпеки ФГ «Волова гора» перебуває в межах 1–1,5 балів із 5 можливих. Найнижчі оцінки отримали такі компоненти: журналізація, управління інцидентами, політики ІБ, кадрова безпека. Середні значення мають контроль доступу та захист від шкідливого

ПЗ. Системність у сфері захисту інформаційних активів поки що не сформована, а функції безпеки реалізуються в реактивному форматі, що характерно для більшості малих аграрних підприємств.

7. Запропонована у роботі концептуальна модель інформаційної безпеки цифрового облікового середовища на основі організаційного, технологічного та процесного блоків створює системну платформу для підвищення рівня захисту інформації. Модель забезпечує логічну взаємодію політик, технологій та аудиту, формує механізми розмежування ролей, встановлює процеси управління активами та ризиками, а також закладає фундамент для створення культури інформаційної безпеки. Визначено, що впровадження моделі дозволяє мінімізувати критичні ризики та сформувати керовану архітектуру цифрових процесів.
8. Комплекс рекомендацій, розроблений у роботі, охоплює вдосконалення аудиту інформаційної безпеки, формування карти цифрових ризиків, застосування кількісних методів оцінювання, удосконалення механізмів резервного копіювання та підвищення рівня кіберграмотності персоналу. Особливу увагу приділено практичним інструментам: періодичному тестуванню відновлення даних, регулярному аналізу журналів, ревізії доступів, застосуванню двофакторної автентифікації для входу в облікову систему, а також впровадженню щорічних Disaster Recovery Drill. Дослідження довело, що такі заходи здатні суттєво підвищити стійкість облікової системи навіть за умов обмежених ресурсів підприємства.
9. Наукова новизна роботи полягає у адаптації та практичному застосуванні методології ризик-орієнтованого аудиту та міжнародних стандартів ІБ до умов малого аграрного підприємства. У роботі запропоновано комплексну методику оцінювання цифрових ризиків, побудовано шкалу ризиковості, розроблено карту цифрових загроз, а також запропоновано концептуальну модель підвищення інформаційної безпеки, що враховує специфіку діяльності ФГ «Волова гора». Практична значущість роботи підтверджується

можливістю безпосереднього впровадження запропонованих заходів у діяльність аналогічних підприємств аграрної сфери.

10. Загальний висновок підтверджує, що підвищення рівня інформаційної безпеки цифрового облікового середовища є ключовою передумовою фінансової стійкості, достовірності звітності та ефективності управління підприємством. Аналіз практичних даних ФГ «Волова гора» показав, що впровадження запропонованої моделі організаційних, технологічних і процесних заходів здатне забезпечити підвищення інформаційної зрілості щонайменше до рівня 3 (керований), суттєво знизити інтегральні цифрові ризики та мінімізувати ймовірність втрати або спотворення облікових даних. Узгоджена система політик, контрольних процедур та технологічних рішень формує передумови для стійкого функціонування цифрової інфраструктури й підвищення надійності облікового процесу в умовах зовнішніх та внутрішніх загроз. Отже, результати дослідження створюють практичне та теоретичне підґрунтя для подальшого зміцнення інформаційної безпеки й розвитку цифрового аудиту в аграрному секторі, демонструючи реальну застосовність підходів на прикладі діяльності ФГ «Волова гора».

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Аналітичні матеріали з нормативного регулювання інформаційної безпеки. URL: https://consultant.net.ua.
2. Белова І. М., Ярощук О. В. Сучасна парадигма цифрової економіки та її методологія. У: Розвиток цифровізації обліку, оподаткування, аналізу і контролю в управлінні підприємствами : монографія / Р. Ф. Бруханський, П. Р. Пуцентейло [та ін.]. Тернопіль : ВПЦ «Університетська думка», 2021. С. 24–53.
3. Белова І., Гомотюк А., Ярощук О. Цифрова трансформація управлінських та бізнес-процесів в Україні під час воєнного стану. Економічний аналіз. 2024. Том 34. № 1. С. 42–52.
4. Белова І., Ярощук О., Гомотюк А. Розвиток процесів цифровізації в Європейському Союзі: перспективний досвід для України. Економічний аналіз. 2023. Том 33. № 1. С. 180–191.
5. Бруханський Р. Ф. Блокчейн vs розподілений реєстр. У: Цифрова економіка: тренди та перспективи : матеріали Міжнародної науково-практичної конференції (Тернопіль, 25 жовтня 2018 р.). Тернопіль : ФОП Осадца Ю. В., 2018. С. 51–53.
6. Бруханський Р. Ф. Методологія наукових досліджень і викладання облікових дисциплін : навчально-методичний посібник. Тернопіль : ТНЕУ, 2019. 174 с.
7. Бруханський Р. Ф. Методологія наукових досліджень. Тернопіль : Осадца Ю. В., 2022. 208 с.
8. Бруханський Р. Ф., Спільник І. В. Цифровий облік: поняття, витоки та актуальний дискурс. Інститут бухгалтерського обліку, контроль та аналіз в умовах глобалізації. 2020. Вип. 3–4. С. 7–20.
9. Бруханський Р., Спільник І. Бізнес-аналітика vs. бізнес-аналіз: сучасний дискурс, модель професійної компетенції ініціатора позитивних змін. Інститут бухгалтерського обліку, контроль та аналіз в умовах глобалізації. 2022. Вип. 1–2. С. 7–21.

10. ДСТУ ISO/IEC 27001:2015. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги.
11. ДСТУ ISO/IEC 27001:2023. Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги (ISO/IEC 27001:2022, IDT). Національний стандарт України. Київ : ДП «УкрНДНЦ», 2023. 28 с. URL: https://zakon.isu.net.ua/sites/default/files/normdocs/dstu_iso_iec_27001_2023.pdf (дата звернення: 21.11.2025).
12. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах». URL: https://zakon.rada.gov.ua/laws/show/80/94-вр.
13. Закон України «Про основні засади забезпечення кібербезпеки України». URL: https://zakon.rada.gov.ua/laws/show/2163-19.
14. Інформаційно-довідковий ресурс про цифрову безпеку. URL: https://diegobittencourt.org.
15. Кастельс М. Інформаційна епоха: економіка, суспільство і культура. Київ : Видавництво «Основи», 2014.
16. Матеріали з питань кібербезпеки освітніх закладів. URL: https://csecurity.kubg.edu.ua.
17. Матеріали конференції «Цифрова трансформація і безпека інформаційних систем». URL: https://scispace.com.
18. Матеріали щодо оцінювання ризиків та методів аудиту IT-середовищ. URL: https://repo.btu.kharkiv.ua.
19. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР. База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/80/94-вр (дата звернення: 21.11.2025).
20. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2163-19 (дата звернення: 21.11.2025).

21. Пуцентейло П. Р., Гуменюк О. О. Цифрова економіка як новітній вектор реконструкції традиційної економіки. Інноваційна економіка. 2018. № 5–6 (75). С. 131–143.
22. Сайт консалтингової компанії «ICR Group» про стандарти ISO 27001. URL: https://icr-cert.com.ua.
23. Accenture. Technology Vision 2022: We, the Post-Digital People. Accenture, 2022.
24. Accenture. Unlocking Value in Data with AI (Accenture Strategy). Accenture, 2021.
25. Brynjolfsson E., McAfee A. The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies. W.W. Norton & Company, 2014.
26. Bughin J., Manyika J., Woetzel J. How Digital Reinventors Are Shaping the Next-Generation Business. McKinsey Global Institute, 2017.
27. COBIT 2019 Framework. ISACA. URL: https://www.isaca.org/resources/cobit.
28. COBIT® | Control Objectives for Information Technologies® : resource. Rolling Meadows : ISACA, [без дати]. URL: https://www.isaca.org/resources/cobit.
29. Davenport T. H. Big Data at Work: Dispelling the Myths, Uncovering the Opportunities. Harvard Business Review Press, 2014.
30. Davenport T. H., Harris J. Competing on Analytics: The New Science of Winning. Harvard Business Review Press, 2007.
31. Drucker P. The Effective Executive: The Definitive Guide to Getting the Right Things Done. HarperCollins, 2006.
32. EY. How Artificial Intelligence Is Transforming the World of Business. EY Global, 2020.
33. Gartner. Augmented Analytics: The Future of Data and Analytics. Gartner, 2020.
34. Gartner. Top 10 Strategic Technology Trends. Gartner, 2021.
35. General Electric. The Industrial Internet of Things: Pushing the Boundaries of Minds and Machines. GE Reports, 2018.
36. Huang M., Rust R. T., Maksimovic V. Artificial Intelligence in Service. Journal of Service Research, 2019.

37. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. International Organization for Standardization.
38. Kaplan R. S., Norton D. P. The Balanced Scorecard: Translating Strategy into Action. Harvard Business Review Press, 1996.
39. Kotler P., Keller K. L. Marketing Management. 15th ed. Pearson Education Limited, 2016.
40. Loshin D. Business Intelligence: The Savvy Manager's Guide. Morgan Kaufmann, 2012.
41. McKinsey & Company. The Next Normal: The Recovery Will Be Digital. McKinsey Global Institute, 2020.
42. Mitchell T. M. Machine Learning. McGraw-Hill, 1997.
43. Morabito V. Big Data and Analytics: Strategic and Organizational Impacts. Springer, 2015.
44. NIST Cybersecurity Framework (CSF). URL: https://www.nist.gov/cyberframework.
45. OECD. Digital Economy Outlook 2020. OECD Publishing, 2020.
46. Osterwalder A., Pigneur Y. Business Model Generation: A Handbook for Visionaries, Game Changers, and Challengers. Wiley, 2010.
47. Portal of security and risk management. URL: https://tecnovy.com.
48. Porter M. Competitive Advantage: Creating and Sustaining Superior Performance. Free Press, 1985.
49. PwC. Global Data and Analytics Survey: Big Decisions 2020. PwC, 2020.
50. PwC. The Global Artificial Intelligence Study: Exploiting the AI Revolution. PwC, 2021.
51. Rouse M. Enterprise Resource Planning (ERP). TechTarget, 2019.
52. SAS Institute. Artificial Intelligence and Machine Learning: Concepts and Applications. SAS Institute, 2019.
53. Schwab K. The Fourth Industrial Revolution. Crown Business, 2017.

54. Sullivan D., Williams P. Big Data in Business and Industry. Wiley Publishing, 2018.
55. The CSF 1.1 Five Functions : learning module. Gaithersburg : NIST, 2018. URL: https://www.nist.gov/cyberframework/getting-started/online-learning/five-functions.
56. Westerman G., Bonnet D., McAfee A. Leading Digital: Turning Technology into Business Transformation. Harvard Business Review Press, 2014.