УДК 657.6
JEL H29, M42
DOI 10.32782/2617-5940.1.2025.1

Костянтин Безверхий
доктор економічних наук, доцент,
доцент кафедри фінансового аналізу та аудиту,
Державний торговельно-економічний університет
ORCID: https://orcid.org/0000-0001-8785-1147
E-mail: k.bezverkhyi@knute.edu.ua

Ірина Парасій-Вергуненко
доктор економічних наук, професор,
професор кафедри фінансового аналізу та аудиту,
Державний торговельно-економічний університет
ORCID: https://orcid.org/0000-0001-6506-6965
E-mail: i.parasij-vergunenko@knute.edu.ua

Володимир Гордополов
доктор економічних наук, професор,
професор кафедри фінансового аналізу та аудиту,
Державний торговельно-економічний університет
ORCID: https://orcid.org/0000-0002-3151-8035
E-mail: v.hordopolov@knute.edu.ua

РИЗИКИ В МЕЖАХ Е-АУДИТУ ТА НАПРЯМКИ ЇХ МІНІМІЗАЦІЇ

Анотація. Метою статті *є визначення ключових ризиків, які можуть проявитися в процесі реалізації електронного аудиту, а також формулювання напрямків дій для мінімізації їх сили або імовірності виникнення. В роботі використовуються загальнонаукові та спеціальні наукові методи дослідження. До загальнонаукових відноситься дедукція, аналіз, класифікація та інші. В якості спеціальних наукових виділено картографування ризиків, бальну оцінку ризиків, рейтингування та інші.* ***Методика дослідження*** *полягає у роботі з джерелами на першому етапі із виділенням ризиків, що характерні для процесу електронного аудиту при його використанні для цілей податкового контролю. В подальшому застосовується класифікація наявних ризиків, виділення окремих найбільш суттєвих та проведення бальної оцінки у розрізі імовірності настання, потенційної сили впливу, вагомості. По завершенню нормування ваги кожного з ризиків здійснюється рейтингування, а для наочного відображення отриманих результатів побудована сигнальна карта ризиків. Як* ***результат****, сформульовані висновки щодо пріоритетності наявних ризиків та загроз у процесі впровадження та використання електронного аудиту Державної податкової служби України. У роботі досліджено ризики електронного аудиту та шляхи їх мінімізації в умовах цифровізації контрольних процедур. Систематизовано та класифіковано основні види ризиків за різними ознаками: етапами е-аудиту, джерелом виникнення, типом технічних проблем, взаємодією з податковими органами, характером виявлення порушень, результатами е-аудиту, впливом людського фактору та інформаційною безпекою. Виявлено найсуттєвіші ризики, а саме галюцинації штучного інтелекту, хакерське втручання в систему, недостача спеціалістів у сфері програмування, надмірна залежність від постачальників послуг, використання даних у протиправних цілях та несумісність програмного забезпечення. Здійснено оцінку ідентифікованих ризиків за показниками ймовірності та потенційної сили впливу. Запропоновано комплекс заходів для мінімізації кожного з виявлених ризиків, спрямованих на підвищення ефективності та захищеності систем електронного аудиту.* ***Цінність дослідження*** *проявляється як у практичному, так і теоретичному аспекті. Практичний полягає у тому, що отримані результати дозволяють пріоритезувати роботу з ризиками при впровадженні електронного аудиту, а також при подальшому удосконаленні механізму, для максимізації ефективності процесу та мінімізації ймовірності чи сили прояву деструктивних явищ. Теоретична цінність полягає у подальшому розвитку теорії управління ризиками е-аудиту.*

Ключові слова: *електронний аудит, аудиторський консалтинг, ризики е-аудиту, штучний інтелект в аудиті, класифікація ризиків, цифровізація аудиту, податковий контроль, діагностика ризиків.*

Kostiantyn Bezverkhyi
Doctor of Economic Sciences, Docent,
Associate Professor at the Department of Financial Analysis and Audit,
State University of Trade and Economics
ORCID: https://orcid.org/0000-0001-8785-1147
E-mail: k.bezverkhyi@knute.edu.ua

Iryna Parasii-Verhunenko
Doctor of Economic Sciences, Professor,
Professor at the Department of Financial Analysis and Audit,
State University of Trade and Economics
ORCID: https://orcid.org/0000-0001-6506-6965
E-mail: i.parasij-vergunenko@knute.edu.ua

Volodymyr Hordopolov
Doctor of Economic Sciences, Professor,
Professor at the Department of Financial Analysis and Audit,
State University of Trade and Economics
ORCID: https://orcid.org/0000-0002-3151-8035
E-mail: v.hordopolov@knute.edu.ua

RISKS WITHIN E-AUDIT AND WAYS TO MINIMIZE THEM

Abstract. The purpose *of the article is to identify the key risks that may arise in the process of implementing electronic audit, and also to formulate the areas of action to minimize their strength or probability of occurrence. The article uses general scientific and special scientific research methods. General scientific methods include deduction, analysis, classification, and others. Special scientific methods include risk mapping, risk scoring, rating, and others.* ***The research methodology*** *consists of working with sources at the first stage with the identification of risks that are characteristic of the electronic audit process when used for tax control purposes. The next step is to classify the existing risks, identify the most significant ones, and conduct a scoring assessment in terms of probability of occurrence, potential impact, and weight. Upon completion of the normalization of the weight of each risk, a rating is performed, and a risk signal map is built to visualize the results. As a* ***result****, conclusions are formulated regarding the prioritization of existing risks and threats in the process of implementation and use of electronic audit of the State Tax Service of Ukraine. The paper investigates the risks of electronic audit and ways to minimize them in the context of digitalization of control procedures. The main types of risks are systematized and classified according to various criteria: stages of e-audit, source of occurrence, type of technical problems, interaction with tax authorities, nature of violations detection, e-audit results, human factor impact and information security. The most significant risks have been identified, namely artificial intelligence hallucinations, hacker interference with the system, lack of programming specialists, overdependence on service providers, use of data for illegal purposes, and software incompatibility. The identified risks are assessed in terms of probability and potential impact. The author proposes a set of measures to minimize each of the identified risks aimed at improving the efficiency and security of electronic audit systems.* ***The value of the study*** *is manifested in both practical and theoretical aspects. The practical value lies in the fact that the results obtained allow prioritizing the work with risks when implementing electronic audit, as well as in the further improvement of the mechanism, to maximize the efficiency of the process and minimize the likelihood or severity of destructive phenomena. The theoretical value lies in the further development of the theory of e-audit risk management.*

Keywords: *e-audit, e-audit risks, audit consulting, artificial intelligence in audit, risk classification, digitalization of audit, tax control, risk diagnostics*

Вступ. Спостерігається подальший розвиток технологій, у тому числі базових мовних моделей, фреймворків розробки програмного базезпечення тощо, що дозволяє сформувати новий напрямок аудиту, в межах якого значна частина рутинних інтелектуальних задач вирішується комп'ютерними системами, а не людиною. Як результат, суттєво підвищується результативність такої діяльності, що позитивно відображається на досягнутих результатах. Проте одночасно із розширенням можливостей виконання аналітичної діяльності також спостерігається зростання ризиків, які провокуються саме електронним аудитом. У цьому контексті підвищується актуальність дослідження наявних загроз, які можуть не тільки знизити потенціал електронного аудиту, а й призвести до суттєвого перевищення негативних наслідків від використання такого інструменту над позитивними. Тому важливо чітко ідентифікувати найбільш суттєві ризики електронного аудиту, а також запропонувати напрямки та заходи мінімізації імовірності їх реалізації на практиці або ж пригнічення можливої сили їх впливу. Це дозволить максимально повно розкрити потенціал такого контрольного інструменту.

Метою статті є визначення ключових ризиків, які можуть проявитися в процесі реалізації електронного аудиту, а також формулювання напрямків дій для мінімізації їх сили або імовірності виникнення.

Відповідно, в якості завдань виділено:

– запропонувати класифікаційні ознаки та провести класифікацію ризиків в межах е-аудиту;

– виділити найбільш суттєві ризики в межах процесу е-аудиту;

– провести оцінку та рейтингування ризиків в межах процесу е-аудиту;

– запропонувати напрямки послаблення потенційної сили або імовірності ризиків.

Як результат, проведено класифікацію основних ризиків, здійснено оцінку найбільш суттєвих та вказані напрямки їх послаблення.

Літературний огляд. У дослідженнях ризиків та перспектив електронного аудиту простежуються декілька тематичних напрямків. Топащенко А. А., Артюх О. В. [4], Чвертко Л. А. [8] та Гай О. В. з колегами [2] вивчали особливості електронного фінансового контролю, цифрові платформи взаємодії бізнесу з податковими органами та стан податкового аудиту в умовах цифровізації, акцентуючи увагу на супутніх ризиках та перспективах розвитку. Безверхий К. В., Поддубна Н. М. [1; 7], Аль-Тае С. Х. Х., Флаїх Х. Х. [6] та Закарія Х. [12] вивчали впровадження електронного аудиту, використання інформаційних технологій, штучного інтелекту в аудиті та управління ІТ-ризиками як способу підвищення якості аудиту та мінімізації ризиків. Аль-Салмі М., Ві С., Акбар Ф. [5], Індріянто Е. [10] та Хакім Л. з колегами [9] досліджували вплив електронного аудиту на ефективність роботи організацій, оптимізацію аудиторських процесів та виявлення корупції. Сусанто Х. та співавтори [11] зосередили увагу на впливі незалежності, досвіду та компетентності аудиторів на якість аудиту через призму ефективності електронного аудиту. Група українських авторів К.О. Назарова та інші [3] досліджує аналіз ризиків діяльності компаній на основі нефінансових і фінансових звітів, що може бути використано під час проведення е-аудиту.

Методологія. В роботі використовуються загальнонаукові та спеціальні наукові методи дослідження,

у тому числі робота з джерелами, дедукція, аналіз, класифікація, картографування ризиків, бальна оцінка ризиків, рейтингування та інші. Методика дослідження розпочинається із роботи з джерелами, що присвячені темі ризиків у е-аудиті, для виділення ризиків, що характерні для процесу. Після цього проведено класифікацію наявних ризиків, виділення окремих найбільш суттєвих та застосовано бальну оцінку у розрізі імовірності настання, потенційної сили впливу, вагомості. У кінці застосовуються рейтингування та побудована сигнальна карта ризиків для наочного відображення отриманих результатів. На основі сформульованих висновків запропоновані напрямки зниження сили або імовірності впливу ідентифікованих ризиків для посилення ефективності електронного аудиту, що використовуються у податкових цілях.

Основна частина. У процесі реалізації електронного аудиту може проявитись ряд проблем. Перш за все, мова йде про недостатню кваліфікацію персоналу суб'єкта, який реалізує аудит, а також самого об'єкту аудиту [7, с. 87]. На поточний момент ризик останнього мінімізується шляхом поетапного впровадження відповідної системи у практику українських податкових органів. На початковому етапі мова йде лише про формування відповідних структурованих форм інформації, що подається до Державної податкової служби України, великими компаніями, які володіють достатніми ресурсами для відповідного інформаційно-аналітичного задоволення потреб перевіряючих органів. Що ж до проблем кваліфікації персоналу Державної податкової служби України, що використовує електронний аудит для забезпечення контролю повноти виконання податкових зобов'язань підприємств, то такий ризик є суттєвим.

На подібну проблему звертають увагу і Гай О., Кононенко Л., Черновол О., які вказують, що впровадження електронного адміністрування податків потребує певної підтримки (технічної, кваліфікаційної), яку мають не всі платники податків (особливо малі та географічно віддалені) [2, с. 57].

Також може проявлятися нестача людських ресурсів для аудиторів [9, с. 2]. У цьому випадку мова йде не про недостатню загальну кількість кадрів, а про структуру, недостатню кількість спеціалістів, що володіють навиками, корисними у контексті подальшого розвитку електронного аудиту, автоматизації відповідних аудиторських процедур, обробки інформації, отриманої із різнорівневих баз даних для виявлення фактів маніпуляції податковими зобов'язаннями конкретного підприємства.

Ще однією проблемою є інформаційна безпека [6, с. 99], яка проявляється у багатьох вимірах. На поточний момент наявний значний перелік випадків хакерського втручання у діяльність державних органів України, в основному зі сторони російської федерації. Відповідні дані підприємств щодо їх господарського становища можуть становити цінність для ворога, адже демонструють динаміку розвитку економіки, ділянки, які постраждали від відповідних дій ворога, показувати економічних суб'єктів, які створюють найбільшу додану вартість. Як результат, така інформація може використовуватись для пріоритезації подальших бомбардувань цивільної інфраструктури.

Крім цього, проблема інформаційної безпеки може також стосуватися дій конкретних аудиторів, що працюють на Державну податкову службу України. Конкуренти, в межах бізнес-розвитку, можуть зацікавитись відповідними даними і у випадку наявності корумпованої особи в державних органах придбати її. Відповідно, у конкурентній боротьбі буде перемагати не той суб'єкт, який здатен сформувати найкраще співвідношення якісних характеристик товару та його ціни, а той, хто використовує наявний адміністративний ресурс, корупційні зв'язки для посилення свого господарського становища.

Ще один автор звертає увагу на той факт, що через автоматизацію перевірок якість аудиту може знижуватись, адже відсутнє скептичне та обережне вивчення даних під час проведення таких перевірок [11, с. 349]. Тобто, на думку автора, така система забезпечує виявлення тих помилок, які знаходяться на поверхні, проте є недостатньою для ідентифікації продуманих спроб маніпулювання податковими зобов'язаннями. Все ж вважаємо, що таке твердження є суперечливим. Електронний аудит дозволяє охопити значно більший обсяг інформації відповідними процедурами перевірки. Звичайно, сам по собі конкретний алгоритм вивчення даних не забезпечує якісного проведення відповідних контрольних процедур. Він дозволить виявити невідповідності у відображених господарських операціях, арифметичні помилки, найбільш типові порушення податкового законодавства. Проте це лише один із інструментів, який знаходиться в арсеналі контролюючого органу. Звичайно, важлива також участь професіонала, який розуміє особливості побудови господарських систем компаній, здатен осмислено ідентифікувати ризики наявності порушень та забезпечити високий рівень впевненості у тому, що вони відсутні. Тобто електронний аудит забезпечує вищу продуктивність, як інструмент, що здійснює інтенсивне застосування сучасних технологій, проте не заміняє податкового контролера, який повинен приймати першочергову участь у такому процесі. Тобто у цьому контексті ситуація не міняється кардинально, але лише спостерігається подальший еволюційний розвиток аудиторського процесу.

Зарубіжний вчений, Закарія Хешам, звертає увагу на технологію штучного інтелекту [12, с. 341]. В основному автор зосереджений на тих позитивних сторонах, які асоціюються із застосуванням штучного інтелекту, у тому числі і в межах електронного аудиту, націленого на перевірку податкових зобов'язань великих підприємств. Проте така нова технологія тісно асоціюється із рядом ризиків. Перш за все, мова йде про так звані галюцинації. Будь-який штучний інтелект, наприклад, велика мовна модель, представляє собою статистичну модель, яка прогнозує та обирає наступний токен у певному ряді попередніх токенів. Тобто на основі запропонованої штучному інтелекту числової інформації можна очікувати, що у великій кількості випадків буде сформовано правильний висновок про адекватність певних господарських операцій та повне відображення наявних податкових зобов'язань. Проте залишається невелика імовірність, що буде допущено помилку і сформований висновок не відповідатиме завантаженим даним. Відповідно, розглядаючи кожну операцію окремо на великому масиві даних імовірним є отримання результату, який в цілому призведе до недостатньої впевненості ауди-

тора у тому, що проведений автоматичний аналіз, його заключення, відображають реальне становище у контексті податкових зобов'язань. Тому система повинна бути спроектована таким чином, щоб мінімізувати імовірність виникнення відповідної ситуації.

Однією з переваг електронного аудиту є те, що він може автоматично повторювати процес аудиту та зберігати аудиторські сліди в інформаційних системах [5, с. 4129]. Тому для забезпечення більш-менш однакових результатів важливо застосовувати більш прямолінійні методи, наприклад, звичайні алгоритми, що дозволяють адекватно перевіряти числові дані, кожен раз з ідентичним результатом, зіставляти різні господарські операції, а не залежати суттєво від штучного інтелекту та його порівняно непередбачуваних відповідей.

Вагомою ділянкою, в якій також проявляються ризики, є системна безпека [4, с.345], тобто та, яка пов'язана із використанням певного програмного забезпечення. Мова може йти про помилки, наприклад, які призведуть до втрати відповідних даних, тимчасової зупинки аналітичного процесу, інших втрат. Відповідно, важливо формувати єдину цілісну екосистему, яка дозволить використовувати різноманітні модулі, плагіни, функції в залежності від того, яке конкретне аудиторське завдання виконується, які саме цілі перевірки сформовані на етапі планування.

Таким чином, враховуючи розглянуті роботи, а також вивчаючи інші види ризиків у практиці реалізації електронного аудиту, можна запропонувати їх класифікацію. В якості ознак виділено такі, як інформаційна безпека, вплив людського фактору, етап електронного аудиту, результати аудиту, характер виявлених порушень, особливості взаємодії з податковими органами, тип технічних проблем, джерело виникнення тощо (табл. 1).

За етапами електронного аудиту можна говорити, як і у випадку з іншими видами аудиту, про ризики допущення помилок, обрання невідповідної методології, формування інших параметрів, що недостатньо відповідають конкретному аудиторському завданню. Це ті ризики, які реалізуються на етапі планування. Також мова може йти про ризики відбору об'єктів аудиту, ризики збору електронних даних, безпосередньої аналітичної обробки даних, ризики на етапі формування висновків тощо. За джерелами виникнення мова може йти про методологічні, технічні, часові, правові, організаційні ризики електронного аудиту.

Взаємодія з податковими органами породжує комунікаційні ризики, пов'язані з неефективним обміном інформацією між платниками податків та контролюючими органами. Інтерпретаційні ризики виникають через неоднозначне тлумачення нормативно-правових актів різними сторонами процесу, що може призвести до суперечностей. Процедурні ризики обумовлені недосконалістю механізмів проведення електронних перевірок та недостатньою регламентацією окремих етапів. Неузгодженість дій між різними підрозділами контролюючих органів часто стає причиною адміністративних затримок та ускладнень.

Характер виявлення порушень визначає наявність хибнопозитивних результатів, коли система помилково ідентифікує правомірні операції як порушення. Хибнонегативні результати представляють протилежну проблему – невиявлення реальних порушень автоматизованими системами. Ризики неоднозначної інтерпретації виникають, коли програмне забезпечення не може остаточно класифікувати операцію через недостатність даних або складність транзакції.

Наслідки е-аудиту формують окрему групу ризиків, серед яких найвагомішими є ризики донарахування податків через виявлені розбіжності в обліку. Фінансові санкції у вигляді штрафів становлять відчутну загрозу для суб'єктів господарювання при встановленні порушень. Судові спори часто виникають внаслідок незгоди платників податків з результатами електронних перевірок, що вимагає виділення обмежених ресурсів від усіх сторін конфлікту. Додаткові перевірки можуть бути призначені за результатами первинного е-аудиту, що збільшує адміністративне навантаження на конкретний бізнес.

Таблиця 1

Класифікація ризиків в межах е-аудиту

Класифікаційна ознака	Види ризиків
За етапами е-аудиту	Ризики планування аудиту, ризики відбору об'єктів аудиту, ризики збору електронних даних, ризики аналізу даних, ризики формування висновків
За джерелом виникнення	Методологічні, технічні, організаційні, правові, часові
За типом технічних проблем	Ризики несумісності форматів даних, ризики втрати даних, ризики цілісності даних, ризики неповноти даних, ризики помилок при передачі даних
За взаємодією з податковими органами	Ризики комунікаційні, ризики інтерпретаційні, ризики процедурні, ризики неузгодженості дій
За характером виявлення порушень	Ризики хибнопозитивних результатів, ризики хибнонегативних результатів, ризики неоднозначної інтерпретації
За результатами е-аудиту	Ризики донарахування податків, ризики накладення штрафів, ризики судових спорів, ризики додаткових перевірок
За впливом людського фактору	Ризики некомпетентності аудиторів, ризики суб'єктивності оцінки, ризики недобросовісності
За інформаційною безпекою	Ризики витоку даних, ризики несанкціонованого доступу, ризики порушення конфіденційності
За дотриманням процедур	Ризики порушення термінів, ризики недотримання законодавства, ризики порушення послідовності процедур

Джерело: складено авторами

Відповідно до такої класифікаційної ознаки, як тип технічної проблеми, мова може йти про ризики помилок при передачі даних, ризики цілісності даних, ризик неповноти даних, втрати даних, несумісності форматів даних тощо. У цьому контексті важливим є впровадження стандартизованих форм, наприклад, SAF-T [1, с. 97], які акумулюють інформацію чітко визначеним чином відповідно до потреб податкових органів. Що ж до інших періодичних технічних проблем, то вони повинні вирішуватись на рівні самої Державної податкової служби України.

Навіть при стандартному представленні даних SAF-T під час передачі та аналізу інформації, що використовується для створення кожного звіту, може виникнути кілька проблем. Тоді як структурну перевірку можна легко виконати (використовуючи відповідну XML-схему), цілісність даних може бути складно підтримувати через помилки при введенні даних, зміни в даних з часом або програмні помилки, які важко виявити під час генерації та перетворення великих обсягів даних [8, с. 128]. З таким твердженням можна погодитися.

Вплив людського фактору залишається суттєвим навіть у цифровому середовищі аудиту. Некомпетентність аудиторів у роботі з програмними комплексами може призводити до невірних висновків. Суб'єктивність оцінки виникає при аналізі нестандартних ситуацій, які вимагають експертного судження. Проблеми недобросовісності окремих перевіряючих створюють передумови для зловживань та корупційних проявів.

Інформаційна безпека набуває критичного значення в умовах е-аудиту через обробку великих масивів конфіденційної інформації. Витік даних може завдати репутаційної шкоди та призвести до фінансових збитків. Несанкціонований доступ до податкових баз даних становить загрозу для всієї системи електронного адміністрування. Порушення конфіденційності комерційної інформації платників податків підриває довіру до системи е-аудиту в цілому.

Дотримання процедур е-аудиту супроводжується ризиками порушення термінів проведення перевірок та надання відповідної документації. Недотримання законодавства з боку контролюючих органів може призвести до скасування результатів перевірки. Порушення послідовності процедур перевірки створює передумови для оскарження її результатів та визнання їх недійсними.

Говорячи про конкретні ризики, вважаємо, що на поточний момент найбільш суттєвими є галюцинації штучного інтелекту, використання працівниками аудитора даних компаній у протиправних цілях, хакерське втручання в систему, недостача спеціалістів у сфері програмування серед власних співробітників для забезпечення автоматизації процесу перевірки, втрати через надмірну залежність від постачальника послуг, технічні збої та втрата даних під час обробки, несумісність різних елементів програмного забезпечення (табл. 2).

Таким чином, усі перелічені ризики є суттєвими і вагомими, окрім ризику технічного збою та втрати

Таблиця 2

Суттєві ризики в межах процесу е-аудиту

Ризик	**Фактор ризику**	**Імовірність (1 – низька, 5 – висока)**	**Потенційна сила впливу (1 – низька, 5 – висока)**	**Вагомість (Імовірність х потенційна сила)**	**Нормування вагомості**	**Ранг**
Галюцинації штучного інтелекту	Фундаментальні особливості ШІ-моделей	5	4	20	0,194	1
Використання працівниками аудитора даних компаній у протиправних цілях	Недостатній контроль доступу до даних, відсутність моніторингу дій працівників, низька корпоративна етика	3	4	12	0,117	5
Хакерське втручання в систему	Вразливості в системі безпеки, слабкі паролі, відсутність двофакторної автентифікації, застаріле програмне забезпечення	4	5	20	0,194	1
Недостача спеціалістів у сфері програмування серед власних співробітників для забезпечення автоматизації процесу перевірки	Низька конкурентність зарплат, недостатні інвестиції в розвиток персоналу, висока плинність ІТ-кадрів, зміна структури потреб від трудового колективу	4	4	16	0,155	3
Втрати через надмірну залежність від постачальника послуг	Відсутність диверсифікації постачальників, недосконалі договірні умови, монопольне становище постачальника на ринку	3	5	15	0,146	4
Технічні збої та втрата даних під час обробки	Недостатнє резервне копіювання, апаратні несправності, перебої електроживлення, програмні помилки	2	4	8	0,078	7
Несумісність різних елементів програмного забезпечення	Відсутність стандартизації форматів даних, використання несумісних технологій, недостатнє тестування інтеграції систем	3	4	12	0,117	5
Всього	–	–	–	103	1,000	

Джерело: складено авторами

даних під час обробки. Він характеризується відносно низьким значенням нормованої ваги. Усі інші продемонстрували відносно високий рівень, що пов'язано або із надзвичайно високою імовірністю реалізації такого ризику на практиці, або ж із надзвичайно високою потенційною деструктивною силою, що може вплинути на якість електронного аудиту. Така ситуація помітна на сигнальній карті, де технічний збій та втрата даних під час обробки знаходиться в середині жовтої лінії, в той час як усі інші ризики знаходяться вже у червоній області (Рис. 1).

Найбільш висока імовірність характерна для галюцинації штучного інтелекту. Фактором такого ризику є фундаментальна особливість такої технології. Що ж до потенційної сили впливу, то найбільш високою вона є у випадку із хакерським втручанням у роботу системи, а також із втратою через надмірну залежність від постачальників послуг тощо.

Першими за рангом є галюцинації штучного інтелекту та хакерські втручання в систему, при цьому нормована вага обох ризиків є однаковою. Тобто вони розділять між собою перше та друге місце без визначення, який із ризиків конкретно на якому місці знаходиться. Недостача спеціалістів у сфері програмування серед власних співробітників для забезпечення автоматизації процесу перевірки знаходиться на третьому місці, а втрати через надмірну залежність від постачальника послуг на четвертому. Також нормована вага більше 0,1 характерна для ризиків використання працівниками аудитора даних компаній у протиправних цілях, а також несумісності різних елементів програмного забезпечення.

Відповідно, доцільно запропонувати заходи, які дозволять мінімізувати або силу, або імовірність реалізації відповідних ризиків е-аудиту на практиці (табл. 3).

Перш за все, суттєвою проблемою є виникнення галюцинації в процесі застосування штучного інтелекту в межах електронного аудиту. У цьому контексті доцільно використовувати такі два підходи, як кількаразове застосування штучного інтелекту для повторного отримання відповіді на те ж запитання з подальшим співставленням таких результатів, а також застосування декількох штучних інтелектів для отримання відповіді на те ж запитання з подальшою перевіркою отриманих результатів. Також доцільно реалізувати додаткові процедури для верифікації результатів, отриманих із застосуванням штучного інтелекту. Таким чином, як і будь-яка технологія, ця також володіє своїми слабкими сторонами та обмеженнями, проте виважене застосування дозволить їх нівелювати.

Що ж до контексту використання працівниками Державної податкової служби даних компаній у протиправних цілях, наприклад, у зв'язку із корупційними діями, то для обґрунтування можливості мінімізації ризику слід звернути увагу на пропозиції у інших наукових роботах. Важливість контролю доступу в аудиті посилюється інформаційно-технологічними системами, які можуть забезпечити максимальний захист аудиторських даних. Завдяки суворому контролю доступу система гарантує, що тільки уповноважені особи мають права доступу до конфіденційної інформації в процесі аудиту. Таким чином, ризик витоку даних можна значно мінімізувати, зберігаючи конфіденційність аудиторської інформації та цілісність всього процесу [10, с. 1444]. Окрім цього, слід впровадити сучасні політики конфіденційності, здійснювати логування, тобто постійно фіксувати у системі дії співробітників, дані, які ними отримані. Крім цього, слід підписувати угоду про нерозголошення відповідної інформації, хоча такий тип договору ще до кінця не врегульований в українському законодавстві.

Хакерське втручання в систему є однією з найбільш критичних загроз, що вимагає впровадження багаторівневої системи захисту. Регулярне оновлення критичних компонентів безпеки забезпечує відповідність актуальним стандартам інформаційної захищеності. Шифрування унеможливлює несанкціонований доступ до конфіденційної інформації. Також доцільним є проведення тестів на проникнення, що дозволяє своєчасно виявляти вразливості системи. Відповідно, розробка плану реагування на інциденти безпеки гарантує швидке відновлення функціональності в разі успішної атаки.

Суттєву перешкоду для забезпечення автоматизації процесу перевірки становить недостатня кількість кваліфікованих спеціалістів у сфері програмування серед власних співробітників. Підвищення кваліфікації наявного персоналу через спеціалізовані навчальні

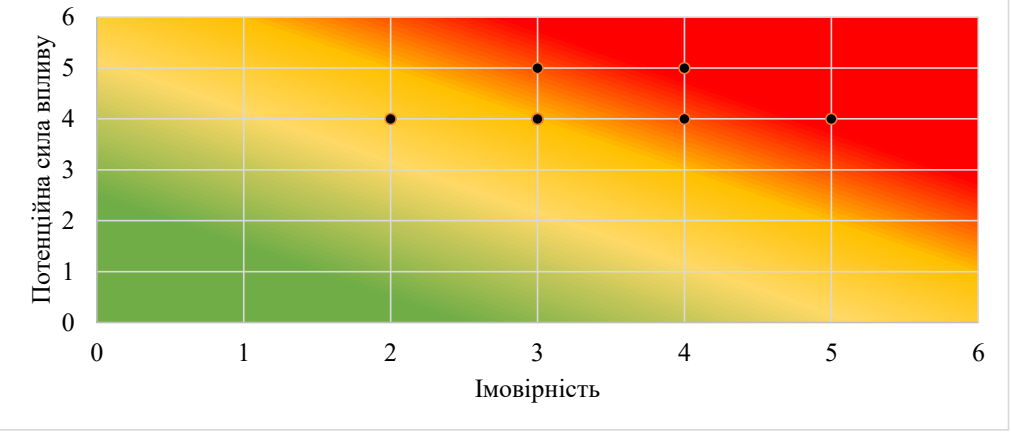

Рис. 1. Сигнальна карта ризиків в межах процесу е-аудиту на поточному етапі його розвитку

Джерело: складено авторами

Таблиця 3

Суттєві ризики в межах процесу е-аудиту

Ризик	Напрямки та засоби їх мінімізації
Галюцинації штучного інтелекту	Кількаразове застосування ШІ для отримання відповіді на теж запитання та співставлення отриманих результатів Застосування декількох ШІ для отримання відповіді на теж запитання та співставлення отриманих результатів Створення додаткових процедур для верифікації результатів, отриманих від ШІ Навчання персоналу щодо обмежень ШІ
Використання працівниками аудитора даних компаній у протиправних цілях	Впровадження політик конфіденційності Обмеження доступу до даних за принципом необхідності Моніторинг дій співробітників у системі (логування) Підписання угод про нерозголошення
Хакерське втручання в систему	Впровадження багаторівневої системи захисту Регулярне оновлення критичних компонентів систем безпеки Шифрування даних Проведення регулярних тестів на проникнення Розробка плану реагування на інциденти безпеки
Недостача спеціалістів у сфері програмування серед власних співробітників для забезпечення автоматизації процесу перевірки	Підвищення кваліфікації поточних співробітників Залучення зовнішніх консультантів Партнерство з ІТ-компаніями Формування крос-функціональних команд Розробка довгострокової стратегії найму ІТ-спеціалістів
Втрати через надмірну залежність від постачальника послуг	Створення екосистеми власних рішень Диверсифікація постачальників Детальне опрацювання контрактних умов Забезпечення доступу до коду та даних
Несумісність різних елементів програмного забезпечення	Проведення детального аналізу сумісності перед впровадженням Використання відкритих стандартів та API Розробка інтеграційних рішень Документування системної архітектури та залежностей

Джерело: складено авторами

програми дозволяє частково компенсувати цей дефіцит. Також слід проаналізувати можливість залучення зовнішніх консультантів, що забезпечує доступ до актуальних знань та досвіду в галузі. Стратегічне партнерство з ІТ-компаніями надає можливість використання передових технологічних рішень. Ще одним заходом є формування крос-функціональних команд, що сприяє ефективному обміну знаннями між аудиторами та технічними фахівцями. Загалом довгострокова стратегія найму ІТ-спеціалістів має бути спрямована на створення стабільного внутрішнього потенціалу.

Економічні та технологічні втрати через надмірну залежність від постачальника послуг потребують створення екосистеми власних рішень, що забезпечують автономність функціонування системи е-аудиту. Диверсифікація постачальників технологій зменшує вплив окремих розробників на загальну стабільність системи. Ще одним заходом є детальне опрацювання контрактних умов щодо формування чітких процедур передачі технологій та знань. Забезпечення доступу до програмного коду та даних гарантує можливість подальшого розвитку системи незалежно від зовнішніх факторів.

В якості ще одного суттєвого ризику була відмічена несумісність різних елементів програмного забезпечення. Це створює технічні бар'єри для інтеграції компонентів е-аудиту, а тому необхідне проведення детального аналізу сумісності перед впровадженням нових елементів, що дозволяє уникнути значних витрат на подальшу інтеграцію. Використання відкритих стандартів та інтерфейсів прикладного програмування забезпечує гнучкість архітектури системи. Крім цього, подальша розробка спеціалізованих інтеграційних рішень усуває технологічні розриви між компонентами різних виробників.

Висновки. Підводячи підсумок, зазначимо, що для розділення ризиків процесу е-аудиту на види запропоновані такі класифікаційні ознаки, як етап е-аудиту, джерело виникнення ризику, тип технічних проблем, особливості взаємодії з податковими органами, характер виявлення порушень, результати е-аудиту, вплив людського фактору, інформаційна безпека та дотримання процедур. Виділено такі ключові ризики, як галюцинації штучного інтелекту, використання працівниками аудитора даних компаній у протиправних цілях, хакерське втручання в систему, недостача спеціалістів у сфері програмування серед власних співробітників для забезпечення автоматизації процесу перевірки, втрати через надмірну залежність від постачальника послуг, несумісність різних елементів програмного забезпечення. Запропоновані такі заходи мінімізації їх сили та імовірності, як кількаразове застосування ШІ для отримання відповіді на теж запитання та співставлення отриманих результатів, моніторинг дій співробітників у системі (логування), шифрування даних, залучення зовнішніх консультантів, диверсифікація постачальників послуг розробки, використання відкритих стандартів та інші.

Список використаних джерел:

1. Безверхий К., Поддубна Н. Prerequisites for the implementation of e-audit in Ukraine. *Scientia fructuosa*. 2023. № 2. С. 92–104. DOI: https://doi.org/10.31617/1.2023(148)09
2. Гай О., Кононенко Л., Черновол О. Tax audit in the conditions of digitalization: current state, problems, perspectives. *Економіка та суспільство.* 2023. № 54. С. 54–62. DOI: https://doi.org/10.32782/2023-54-16
3. Назарова К., Безверхий К., Гордополов В., Мельник Т., Поддубна Н. Аналіз ризиків діяльності компаній на основі нефінансових і фінансових звітів. *Agricultural and Resource Economics: International Scientific E-Journal.* 2021. Вип. 7. № 4. С. 180–199. DOI: https://doi.org/10.51599/are.2021.07.04.10.
4. Топащенко А. А., Артюх О. В. Електронний фінансовий контроль: можливості та ризики. *Стратегія розвитку України: фінансово-економічний та гуманітарний аспекти: матеріали X Міжнародної науково-практичної конференції.* 2023. С. 344–346.
5. Al-Salmi M., Wee S., Akbar F. Impact of E-Audit on Public Organization's Performance in Oman. *3rd Asia Pacific International Conference on Industrial Engineering and Operations Management.* 2022. P. 4127–4135. DOI: https://doi.org/10.46254/AP03.20220681
6. Al-Taee S.H.H., Flayyih H.H. Impact of the electronic internal auditing based on IT governance to reduce auditing risk. C*orporate Governance and Organizational Behavior Review*. Vol. 7. № 1. 2023. P. 94–100. DOI: https://doi.org/10.22495/cgobrv7i1p9
7. Bezverkhyi K., Poddubna N. Audit in the digital economy. *Foreign trade: economics, finance, law.* Vol. 123. № 4. 2022. P. 81–90. DOI: https://doi.org/10.31617/3.2022(123)07
8. Chvertko L. Challenges of digital platforms implementation for cooperation of business and tax authorities. *Economic Security in the Context of Systemic Transformations. International Conference.* 2024. P. 127–130. DOI: https://doi.org/10.53486/escst2023.15
9. Hakim L., Pardomuan R., Tantri M. Electronic Audit (E-Audit), Audit Judgement, Corruption Detection And Audit Quality: BPK RI. *IJHCM: International Journal Of Human Capital Management.* 2023. Vol. 7. № 1. P. 1–27. DOI: https://doi.org/10.21009/IJHCM.07.01.1
10. Indriyanto E. The role of information technology in increasing audit process efficiency. *Jurnal Ekonomi.* Vol. 7. № 2. 2023. P. 1441–1446.
11. Susanto H., et al. The Influence of Independence, Experience, and Competence on Audit Quality Mediated by the Effectiveness of E-Audit. *Research Horizon.* Vol. 3. №1. 2023. P. 348–361.
12. Zakaria, Hesham. The use of artificial intelligence in e-accounting audit. *The fourth industrial revolution: Implementation of artificial intelligence for growing business success.* 2021. P. 341–356. DOI: https://doi.org/10.1007/978-3-030-62796-6_20

References:

1. Bezverkhyi K., Poddubna N. (2023) Peredumovy vprovadzhennia elektronnoho audytu v Ukraini [Prerequisites for the implementation of e-audit in Ukraine]. *Scientia fructuosa,* no. 2, pp. 92–104. DOI: https://doi.org/10.31617/1.2023(148)09
2. Hai O., Kononenko L., Chernovol O. (2023) Podatkovyi audyt v umovakh didzhytalizatsii: suchasnyi stan, problemy, perspektyvy [Tax audit in the conditions of digitalization: current state, problems, perspectives]. *Ekonomika ta suspilstvo – Economy and Society,* no. 54, pp. 54–62. DOI: https://doi.org/10.32782/2023-54-16
3. Nazarova K., Bezverkhyi K., Hordopolov V., Melnyk T., Poddubna N. (2021) Analiz ryzykiv diialnosti kompanii na osnovi nefinansovykh i finansovykh zvitiv [Risk analysis of companies' activities on the basis of non-financial and financial statements]. *Agricultural and Resource Economics: International Scientific E-Journal,* vol. 7, no. 4, pp. 180–199. DOI: https://doi.org/10.51599/are.2021.07.04.10
4. Topashchenko A. A., Artiukh O. V. (2023) Elektronnyi finansovyi kontrol: mozhlyvosti ta ryzyky [Electronic financial control: opportunities and risks]. *Stratehiia rozvytku Ukrainy: finansovo-ekonomichnyi ta humanitarnyi aspekty:* materialy X Mizhnarodnoi naukovo-praktychnoi konferentsii – Ukraine's Development Strategy: Financial-Economic and Humanitarian Aspects: Proceedings of the X International Scientific-Practical Conference, pp. 344–346.
5. Al-Salmi M., Wee S., Akbar F. (2022) Impact of E-Audit on Public Organization's Performance in Oman. *3rd Asia Pacific International Conference on Industrial Engineering and Operations Management,* pp. 4127–4135. DOI: https://doi.org/10.46254/AP03.20220681
6. Al-Taee S.H.H., Flayyih H.H. (2023) Impact of the electronic internal auditing based on IT governance to reduce auditing risk. *Corporate Governance and Organizational Behavior Review,* vol. 7, no. 1, pp. 94–100. DOI: https://doi.org/10.22495/cgobrv7i1p9
7. Bezverkhyi K., Poddubna N. (2022) Audit in the digital economy. *Foreign trade: economics, finance, law,* vol. 123, no. 4, pp. 81–90. DOI: https://doi.org/10.31617/3.2022(123)07
8. Chvertko L. (2024) Challenges of digital platforms implementation for cooperation of business and tax authorities. *Economic Security in the Context of Systemic Transformations. International Conference,* pp. 127–130. DOI: https://doi.org/10.53486/escst2023.15
9. Hakim L., Pardomuan R., Tantri M. (2023) Electronic Audit (E-Audit), Audit Judgement, Corruption Detection And Audit Quality: BPK RI. *IJHCM: International Journal Of Human Capital Management,* vol. 7, no. 1, pp. 1–27. DOI: https://doi.org/10.21009/IJHCM.07.01.1
10. Indriyanto E. (2023) The role of information technology in increasing audit process efficiency. *Jurnal Ekonomi,* vol. 7, no. 2, pp. 1441–1446.
11. Susanto H., et al. (2023) The Influence of Independence, Experience, and Competence on Audit Quality Mediated by the Effectiveness of E-Audit. *Research Horizon,* vol. 3, no. 1, pp. 348–361.
12. Zakaria H. (2021) The use of artificial intelligence in e-accounting audit. *The fourth industrial revolution: Implementation of artificial intelligence for growing business success,* pp. 341–356. DOI: https://doi.org/10.1007/978-3-030-62796-6_20

Стаття надійшла до редакції 28.04.2025