УДК 657.6:004.4

ГОРДІЄНКО М.І., к.е.н., доцент, завідувач кафедри економічного контролю та аудиту Сумського НАУ

ДЕГТЯРЕНКО А.В., к.е.н., доцент кафедри економічного контролю та аудиту Сумського НАУ

ОЦІНКА ІНФОРМАЦІЙНОГО РИЗИКУ В АУДИТІ КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Анотація. *В статті описані помилки, які виникають внаслідок використання комп'ютерних інформаційних систем, та новий вид аудиторського ризику, названий інформаційним. Запропонована схема оцінки інформаційного ризику, пов'язаного із можливістю помилок в програмних алгоритмах. Надано рекомендації з оцінки інформаційного ризику, спричиненого функціональними помилками.*

Ключові слова: *аудит, ризик, інформація, оцінка, алгоритм, програма.*

Постановка проблеми у загальному вигляді. З відміною у 2006 році міжнародного стандарту аудиту 401 «Аудит у середовищі комп'ютерних інформаційних систем» весь аудит став розглядатися як комп'ютерний. Всім стало зрозуміло, що комп'ютеризація є невідворотнім шляхом розвитку аудиту як ефективної та незалежної моніторингової системи, створеної для задоволення інформаційних потреб і виконання контрольних функцій. Комп'ютеризація аудиторської діяльності ґрунтується на об'єктивній необхідності повноцінно дослідити усі суттєві аспекти функціонування на підприємстві його комп'ютерної інформаційної системи (далі КІСП) чи комп'ютерної системи бухгалтерського обліку (далі КСБО), якщо автоматизовано лише облік. В таких умовах аудитор стикається не тільки з традиційними аудиторськими ризиками, він вимушений також брати до уваги й кардинально новий вид ризику – інформаційний (технічний).

Аналіз останніх досліджень і публікацій. Питаннями, що стосуються досліджень інформаційних ризиків в комп'ютерному аудиті в українському науковому світі займається небагато вчених. Серед них, слід відмітити Болдуєва М.В. [1], Федоришину Л.І. та Лахман І.С. [6]. Однак, методичний підхід до оцінки інформаційних ризиків в багатьох не систематизовано, в деяких він зовсім відсутній. На цьому тлі, з нашого погляду, тільки в роботах Івахненкова С.В. [3, 4] представлено впорядкованою наукову концепцію щодо оцінки інформаційних ризиків та, загалом, впливу техніки і технологій на здійснення аудиторської перевірки. Саме завдяки науковим дослідженням цього автора вітчизняна

аудиторська наука збагатилася систематизованими і обґрунтованими теоретичними положеннями, врахування яких у практичній діяльності сприяло підвищенню якості аудиту комп'ютерних інформаційних систем. Але певні аспекти, пов'язані із оцінюванням інформаційного ризику, зумовленого ймовірністю виникнення певних видів помилок в Івахненкова С.В. розглянуті поверхнево, тому вони потребують більш деталізованого дослідження, яке представлене нижче.

Мета і завдання досліджень. Метою даного дослідження є аналіз причин помилок, що зумовлюють виникнення інформаційного ризику, а також висвітлення підходів до оцінки такого ризику. Окреслена мета реалізується через виконання наступних завдань:

- класифікувати помилки, притаманні тільки обліку, здійснюваному в КІСП (КСБО);
- виділити причини таких помилок;
- надати характеристику підходів до оцінки інформаційного ризику.

Результати досліджень. Аби надати аудиторові цінний методологічний інструментарій з оцінки інформаційного ризику, а, отже, і для знаходження ефективних способів його зниження звернемося до Міжнародного стандарту аудиту 315 [5], де визначаються джерела ризику в середовищі ІТ, а саме:

- покладання на системи або програми, які неточно обробляють дані, обробляють неточні дані, або і те, й інше;
- неавторизований доступ до даних, що може призвести до знищення даних або їх неналежної зміни, включаючи реєстрацію неавторизованих або неіснуючих операцій, або неточну реєстрацію операцій;
- окремі ризики можуть виникати у разі доступу багатьох користувачів до спільної бази даних;
- можливість отримання ІТ персоналом прав доступу, які перевищують права, необхідні для виконання ними своїх обов'язків, що порушує розподіл обов'язків;
- неавторизоване внесення змін у дані в базових файлах; неавторизоване внесення змін до систем або програм; невнесення необхідних змін до систем або програм; неналежне ручне втручання;
- потенційна втрата даних або неможливість доступу до даних у разі потреби.

Отже, дамо власну точку зору щодо обґрунтованості впливу певних характеристик комп'ютерної інформаційної системи підприємства на ступінь інформаційного ризику з метою більш об'єктивної його оцінки.

Виходячи з аналізу наданих в МСА джерел, можна стверджувати, що інформаційний ризик в КІСП зумовлений двома причинами. Перша – це недосконалість програмних алгоритмів, процесів обробки і збереження даних (умовно будемо далі такі помилки

називати алгоритмічними). Друга – це недосконаліть організації контрольних функцій, якими наділені працівники – користувачі КІСП (умовно будемо далі такі помилки називати функціональними).

Виникнення алгоритмічних помилок пов'язане із такими характеристиками КІСП як «єдина обробка операцій» [4, с.83] та «відсутність слідів операцій» [4, с.82]. Остання зумовлена незрозумілим перетворенням вхідної інформації (наприклад, даних первинних документів) у вихідну (наприклад, у показники фінансової звітності). Відбувається це через багатоетапність процесів обробки самої інформації, коли на певному етапі (чи декількох етапах) інформація про операцію існує лише у тимчасовій формі й після завершення обробки цей етап випадає із загального ланцюга.

Що ж робити аудиторові, якщо йому доводиться мати справу із такого роду КІСП? Яким чином можна дослідити алгоритм перетворення інформації, якщо цей алгоритм при дослідженні постфактум перерваний? На наш погляд відповідь тут може бути лише одна – за допомогою методу тестових даних. Але, сам же Івахненков С.В. констатує, що даний метод ефективний «при тестуванні логіки обробки даних та засобів контролю з метою підтвердження правильності головних файлів» [4, с. 150]. Зрозуміло, що усі абсолютно вихідні дані (тобто файли з вихідними даними), аудитор за об'єктивних причин дослідити не в змозі. Йому потрібно обирати між тими які він вважає головними і тими, що є, на його думку другорядними.

Аудитор за допомогою стороннього фахівця аналізує технічну документацію, щоб мати цілісну картину про масштаби операцій, сліди від яких відсутні у КІСП. Далі із усього обсягу операцій аудитор виділяє зазначені й оцінює сукупну вартість усіх показників фінансової звітності, які ними сформовані. Виходячи із поставленої межі суттєвості аудитор зараховує до головних операцій тільки ті, які формують найбільш вартісні показники звітності. Інші до уваги не бере, а одразу зараховує їх до ризикових, тобто до таких, які в разі алгоритмічних помилок зумовлять настання інформаційного ризику з низькою оцінкою.

Метод тестових даних полягає у порівнянні фактичних результатів обробки вхідної інформації у програмі із тими, які сформовані аудитором за допомогою спеціального аудиторського програмного забезпечення. Останнє містить вбудований модуль – генератор тестових даних. «Тестові дані — це бухгалтерські документи, операції і проводки, що не відображають реальних фактів господарського життя, а спеціально підготовлені аудитором для перевірки програмних алгоритмів, реалізованих в обліковій системі підприємства-клієнта» [4, с. 148]. Отже, якщо навмисно спотворені тестові дані проходять через алгоритм програми без жодних попереджень щодо помилок, то аудитор вимушений надати найвищу оцінку інформаційному ризику і переходити до надзвичайно працемістких процедур по суті.

Іншими словами, аудитор в цьому разі має формувати чисельні вибірки документів, в яких алгоритм застосованої програми міг пропустити помилку, та робити наскрізну їх перевірку аж до первинних документів – підтверджень.

Слід зазначити, що у сертифікованих та ліцензованих КІСП на початковій стадії впровадження алгоритмічні помилки міститися не можуть (принаймні авторам невідомі такі випадки) через їх багаторазове передпродажне тестування та тривалу апробацію розробниками. Водночас, з часом відбуваються зміни в законодавстві, внутрішній обліковій політиці, організаційній структурі підприємства, на якому впроваджено КІСП, ці зміни іноді не дістають своєчасного відображення через об'єктивні і суб'єктивні обставини, як наслідок виникають помилки в алгоритмах обробки інформації. Отже, аудитору, в разі впевненості у первинній якісності діючої на підприємстві КІСП, з нашої точки зору, доцільно дослідити не наслідки (алгоритмічні помилки), а їх причини. Це слід робити для того, щоб ще більше зменшити кількість головних файлів й максимальну увагу приділити їх тестуванню.

Наприклад, припустимо таку ситуацію, коли за весь період від запровадження КІСП на підприємстві відбулася єдина зміна, що мала істотний вплив на бухгалтерський облік, ця зміна полягала у зменшенні касового ліміту. В цій ситуації аудитор мав би тестувати КІСП тільки на предмет перевищення касового ліміту. Звичайно, що описана ситуація є майже ідеальною, і на практиці коло облікових аспектів, які зазнали змін під впливом обставин зовнішнього і внутрішнього характеру, є суттєво більшим, однак, тим не менше, аудиторові раціонально досліджувати тільки такі аспекти, а не всі ділянки господарської діяльності, відображені в КІСП. З цієї позиції логічно буде констатувати, що джерелом інформаційного ризику при цьому будуть виступати ділянки господарської діяльності, які через відсутність впливу змін середовища аудитор не тестував на предмет алгоритмічних помилок. Але через описані вище причини ймовірність помилок при обробці інформації на цих ділянках є мінімальною і аудитор оцінює як низький інформаційний ризик на даних ділянках

З іншої сторони, хоча і рідко, але має місце ситуація, коли в господарському середовищі клієнта аудиту не відбулося жодних внутрішніх і зовнішніх змін, які б спричинили вплив на алгоритми обробки інформації за період від впровадження КІСП або з часу від проведення останнього комп'ютерного аудиту. В цьому випадку аудитор також дає низьку оцінку інформаційному ризику.

Запропонована схема оцінки інформаційного ризику, пов'язаного із можливістю помилок в програмних алгоритмах КІСП, показана на рисунку 1.

Підсумовуючи дослідження інформаційних ризиків, пов'язаних із можливістю алгоритмічних помилок, треба зазначити, що не виявляються вони внаслідок бездіяльності (або некоректних дій) відповідальних технічних спеціалістів в період, що передує технічній

операції системи з генерації чи обробки облікових даних. Тобто їх невиявлення є недоліком системи попереднього контролю. Водночас інший вид помилок – функціональні, на відміну від попередніх, є результатом недосконалості системи оперативного (поточного) контролю, оскільки не виявляються через бездіяльність (або некоректні дії) технічних та облікових працівників під час безпосереднього ініціювання операції системою чи за деякій час після її завершення. Докладніше про останні нижче.

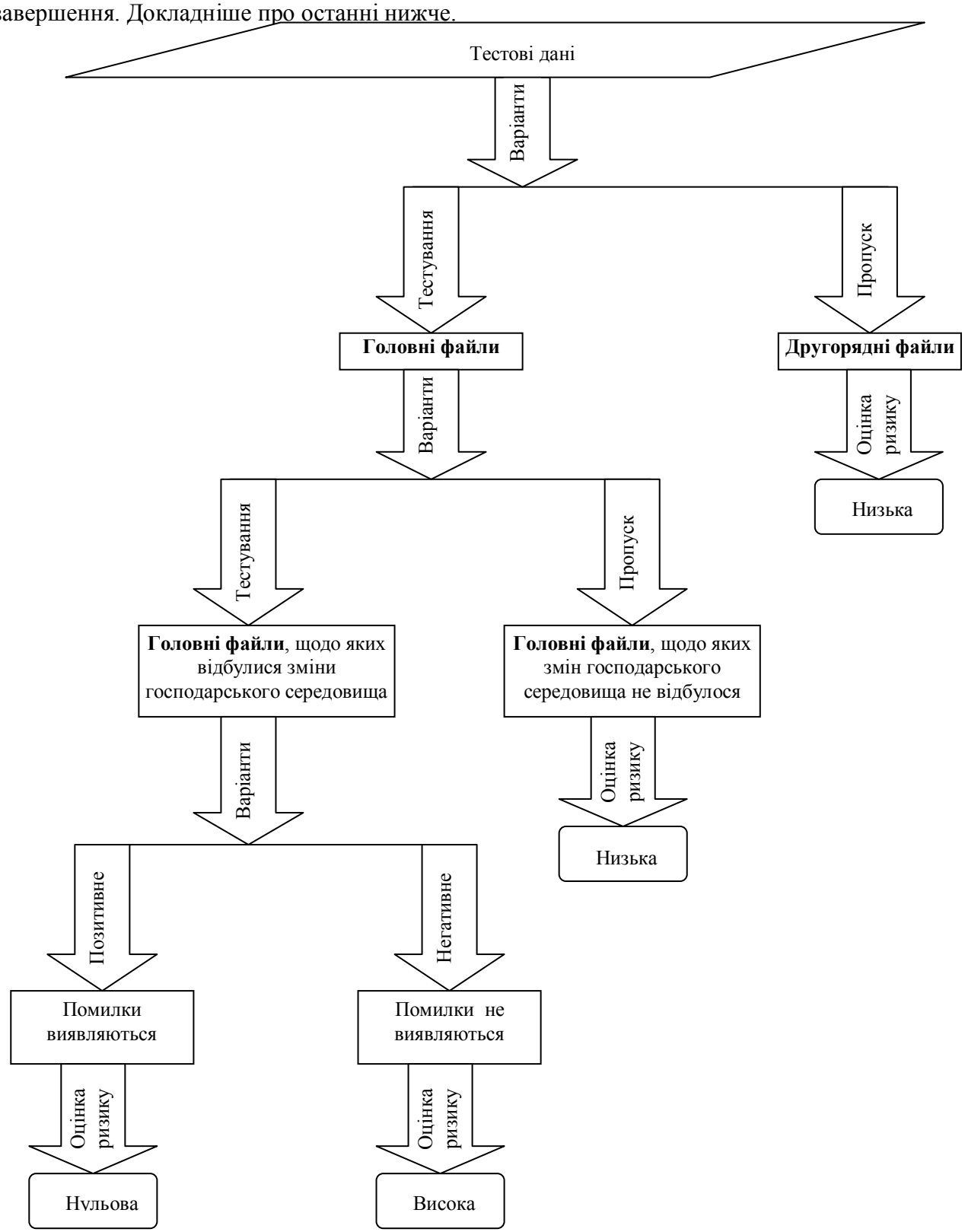

Рис. 1. Схема оцінки інформаційного ризику, пов'язаного із можливістю помилок в програмних алгоритмах КІСП (КСБО)

При практичному застосуванні КІСП іноді можуть виникнути ситуації, коли облікова інформація спотворюється чи навіть знищується внаслідок несанкціонованого втручання певних користувачів у заборонені для них бази даних. Це трапляється тоді, коли на підприємстві існуюча система паролів та розмежування прав доступу є неефективною. Наприклад, паролі відповідальних користувачів не оновлюються системним адміністратором взагалі або тривалий період та з часом стають відомими. Або інший приклад, коли невповноваженому працівникові надане право на редагування чи знищення документів.

Що ж робити аудиторові, якщо в ході попереднього тестування він переконався, що функціональні помилки можливі? По-перше, аудитор має продовжити тестування системи внутрішнього контролю методами, непов'язаними напряму із застосуванням комп'ютерних аудиторських програм та залученням послуг сторонніх фахівців. Ці методи добре нами описані в попередніх дослідженнях [2]. По-друге, якщо ж навіть ці методи підтвердять неефективність підсистеми внутрішнього контролю КІСП, то аудитор має звернутися до комп'ютеризованих процедур по суті, реалізованих в аудиторській програмі. Такі процедури спрямовуються на виявлення наступних категорій електронної інформації:

- електронних записів в КІСП (КСБО), про видалення електронних документів або файлів;

- електронних документів, що редагувалися вже після закриття операційного періоду;

- електронних документів, що створювалися або редагувалися користувачами з неналежними правами.

Тут важливо зазначити, що оцінка аудитором інформаційного ризику обернено залежить від ступеня охоплення перевіркою всіх зазначених вище категорій облікової електронної інформації. Так, якщо програма виявила безліч таких документів і аудитор розуміє, що надалі він не зможе формально й по суті дослідити певну істотну їх частину, то інформаційний ризик в даному випадку повинен бути оцінений як дуже високий. Із збільшенням дослідної вибірки оцінка інформаційного ризику знижується. Врешті решт, коли аудитор впевнений, що він фізично буде в змозі проаналізувати всі такі документи, то інформаційний ризик за даних обставин матиме нульову оцінку.

Комп'ютеризовані процедури по суті дають тільки формальні відповіді на питання, що стосуються невідображення у фінансовій звітності видалених документів, відображення у фінансовій звітності змін внаслідок редагування документів або виправлення показників фінансової звітності наступних періодів через редагування документів, здійснене після закінчення операційного періоду. Водночас, комп'ютеризованих методів, що стосуються

підтвердження правомірності санкціонування електронних облікових записів із зазначених категорій не існує. Тобто, щоб з'ясувати чи є такі записи несанкціонованими, а, отже, і помилковими в принципі, аудиторові треба вручну вишукувати належним чином оформлені паперові підтвердження – службові записки, письмові пояснення персоналу, лікарняні листи, накази керівництва, які стосуються кожного конкретного випадку. Цим, власне, і пояснюються великі витрати часу і високій ступінь інформаційного ризику, при значних кількостях таких електронних записів.

Висновки. В теперішніх умовах стрімкого розвитку технологій аудитори все більше стикаються із ризиками, що спостерігаються виключно у комп'ютерному середовищі суб'єктів господарювання і за умов паперової обробки інформації не можуть виникнути в принципі. Саме аналізу таких ризиків і присвячена дана публікація. Особливий наголос був зроблений на розмежуванні помилок, внаслідок яких виникає інформаційний ризик. Схематично показаний процес оцінки інформаційного ризику, зумовленого алгоритмічними помилками, який дає узагальнене сприйняття процесу відбору і аналізу найважливішої електронної інформації, необхідної для вироблення конкретної стратегії проведення аудиторської перевірки. Досліджено також і сутність функціональних помилок, як носіїв інформаційного ризику, які виникають здебільшого із суб'єктивних причин.

Бібліографія

1. Болдуєв М.В. Оцінювання аудиторських ризиків в умовах автоматизованої обробки інформації / М.В. Болдуєв // Держава та регіони: Серія: Економіка та підприємництво: науково-виробничий журнал Класичного приватного університету. - Запоріжжя., 2011. – Вип.1. – С. 54–57.

2. Дегтяренко А.В. Тести контролю в аудиті: прикладний інструментарій і переваги від застосування / А.В. Дегтяренко // Вісник Сумського НАУ: Серія: Фінанси і кредит. - Суми, 2011. – Вип.1(30). - С. 118-123.

3. Івахненков С.В. Інформаційні технології в організації бухгалтерського обліку та аудиту: Навч. посібн. - 4-те вид., випр. і доп. / С.В. Івіхненков. - К.: Знання, 2008. - 343 с.

4. Івахненков, С.В. Комп'ютерний аудит: контрольні методики і технології : наукове видання / С.В. Івахненков. - К. : Знання, 2005. -286 с.

5. Міжнародні стандарти контролю якості, аудиту, огляду, іншого надання впевненості та супутніх послуг: видання 2010 року, частина 1 / Пер. з англ.: Ольховікова О.Л., Селезньов О.В., Зєніна О.О., Гик О.В., Біндер С.Г. – К.: Фенікс, 2011. – 842 с.

6. Федоришина Л.І. Аудит в умовах автоматизованої обробки інформації / Л.І. Федоришина, І.С. Лахман // Інноваційна економіка: науковий журнал Тернопільського інституту агропромислового виробництва НААН України. – Тернопіль., 2012. – Вип.2. - С. 143 - 146.

Аннотация. *В статье описаны ошибки, которые возникают в результате использования компьютерных информационных систем, и новый вид аудиторского риска, названный информационным. Предложенная схема оценки информационного риска, связанного с возможностью ошибок в программных алгоритмах. Даны рекомендации по оценке информационного риска, вызванного функциональными ошибками.*

Summary. *The article describes the errors arising from the use of computer information systems, and a new type of audit risk, called informational. The scheme of informational risk assessment associated with the possibility of errors in software algorithms is offered. The recommendations of the assessment of information risk caused by functional errors are given.*

Гордієнко Микола Іванович
м. Суми, вул. Кірова, б.160, кім. 129 е
тел. м. 050-726-55-30
E – mail: migsumy@mail.ru

Дегтяренко Андрій В’ячеславович
м. Суми, вул. Кірова, б.160, кім. 129 е
тел. м.