УДК 657.6

В.А. Абасов, аспір.
ДВНЗ «Київський національний економічний університет імені Вадима Гетьмана»

АУДИТ ЕФЕКТИВНОСТІ ІТ-СИСТЕМ СТРАТЕГІЧНИХ ОБ'ЄКТІВ ДЕРЖАВНОГО УПРАВЛІННЯ

Хакерські атаки кінця 2016 р. та початку 2017 р. на урядові інформаційно-телекомунікаційні системи, серед яких Міністерство фінансів України, Державна казначейська служба, призвели до масштабних затримок бюджетних виплат. Вони засвідчили вразливість і відкритість урядових установ для кібератак через відсутність контрольованості трьох основних заходів безпеки, таких як: технічне обмеження на програми завантаження, обмежене використання прав локальних адміністраторів, систематичні оновлення програмного забезпечення. Як засвідчує міжнародний досвід, ці заходи безпеки урядових ІТ-систем мають бути предметом аудиту органів державного фінансового контролю.

Базові засади аудиту інформаційних технологій започатковані в дослідженнях І.К. Дрозд, С.В. Івахненкова, М.М. Бенько, Ю.А. Кузьмінського, А.В. Мамишева. Водночас, питання державного аудиту ІТ-систем у теоретичних дослідженнях розглядалися обмежено, оскільки в Україні відсутня практика такого аудиту.

Тому є необхідність вивчення міжнародної практики аудиту ефективності ІТ-систем та світових норм установ сектору державного управління.

Дослідження дозволило запропонувати методологію аудиту ефективності ІТ-систем для державних установ, яка передбачає планування та проведення основних процедур на основі оцінки ризиків загроз безпеки інформаційних систем.

Автором визначено особливості управління ризиками безпеки ІТ-систем шляхом оцінки ризиків складових безпеки ІТ-систем під час аудиту ефективності, запропоновано метод низхідної покрокової деталізації для аудиторської оцінки ефективності управління ризиками ІТ-систем на стратегічних об'єктах сектору державного управління шляхом адаптації норм стандартів ISSAI.

Запропоновано три можливі варіанти рішень керівництва щодо управління ризиками безпеки ІТ-систем на основі інформації про рівні ризику за результатами аудиту ефективності. Для документування результатів аудиту ефективності ІТ-систем розроблено типові форми робочих документів аудитора, а саме: «Повідомлення про уразливість інформації і визначення категорії захисту», «Оцінка наслідків і загроз для діяльності».

Подальші дослідження питання аудиту ефективності ІТ-систем вбачаються у розробці організаційних заходів щодо проведення Рахунковою палатою перевірок безпеки ІТ-систем стратегічних об'єктів сектору державного управління.

Ключові слова: *аудит ефективності; державний аудит; ІТ-системи; методика аудиту ефективності; оцінка ризиків.*

Постановка проблеми. Протягом останніх двох років великі урядові установи зазнали суттєвих втрат інформаційних ресурсів через здійснення кібератак. Перша зареєстрована успішна кібератака на енергетичну систему України з виведенням її з ладу сталася 23 грудня 2015 року. Російським зловмисникам вдалося успішно атакувати комп'ютерні системи управління трьох енергопостачальних компаній.

Кібератака (англ. cyber-attack) – спроба реалізації кіберзагрози, тобто будь-яких обставин або подій, що можуть бути причиною порушення політики безпеки інформації та нанесення збитків автоматизованій системі.

6 грудня 2016 р. була здійснена хакерська атака на урядові інформаційно-телекомунікаційні системи, серед яких Міністерство фінансів України, Державна казначейська служба. Вона призвела до масштабних затримок бюджетних виплат. Відповідно до заяви Казначейства щодо вчинення атаки було проведено розслідування Департаменту кіберполіції Національної поліції України. Керуючись зробленими висновками розслідування даної події, встановлено передумови та причини кібератаки, серед яких є факти використання в органах Казначейства застарілого комп'ютерного обладнання та операційних систем, які не підтримуються вітчизняним виробником, відсутність постійного та відповідного рівня фінансування на оновлення комп'ютерного, серверного обладнання, операційних систем, побудови систем аналізу та виявлення шкідливого програмного забезпечення, систем керування інформаційною безпекою, запровадження технічних рішень щодо створення захищеного інформаційного середовища в органах Казначейства усіх рівнів [1].

Спеціалізовані перевірки захищеності інформаційних ресурсів в Україні здійснює Державна служба спеціального зв'язку та захисту інформації України. Проте цією службою охоплюється лише технічна сторона питання. Управлінська та фінансова складові рішень керівництва щодо забезпечення належного функціонування інформаційних систем, моніторинг та аналіз систем внутрішнього контролю і досі не є об'єктом зовнішніх перевірок з боку органів державного контролю. Події кінця 2016 року засвідчили вразливість і відкритість урядових установ для кібератак через відсутність контрольованості трьох основних заходів безпеки, таких як: технічне обмеження на програми завантаження, обмежене використання прав локальних адміністраторів, систематичні оновлення програмного забезпечення. Ці заходи безпеки ІТ-систем мають бути предметом першочергової уваги під час управління стратегічно важливими установами державного сектору, що актуалізує дослідження з цього питання.

Аналіз останніх досліджень і публікацій. Аудит ефективності ІТ-систем установ державного сектору економіки лише в окремих аспектах теоретичних та практичних розробок досліджувався зарубіжними та вітчизняними вченими. Особливості аудиту інформаційних технологій було започатковано С.В. Івахненковим [2]. Проте він розглядав переважно методику та організацію аудиту в умовах інформаційних систем реального сектору економіки. Це дозволило сформувати у вітчизняній теорії понятійний апарат ІТ-аудиту. Бенько М.М. доповнив теоретичні підходи розкриттям особливостей фінансового аудиту інформаційних систем [3].

Різновидом аудиту в секторі державного управління є аудит ефективності, який досліджувався С.В. Бардашем, І.К. Дрозд, А.В. Мамишевим, В.К. Симоненко, Ю.Л. Слободяник, О.О. Чечуліною та ін. Водночас, питання державного аудиту ІТ-систем у теоретичних дослідженнях не розглядалися, оскільки в Україні відсутня практика такого аудиту.

Виділення не вирішених раніше частин загальної проблеми. Вивчення міжнародної практики аудиту ефективності ІТ-систем та світових норм у частині методичного забезпечення аудиту безпеки ІТ-систем установ сектору державного управління, особливостей оцінки ризиків під час виявлення факторів, що впливають на безпеку функціонування інформаційно-комп'ютерного середовища установ стратегічного значення, є актуальним і потребує нагального вирішення.

Метою статті є поглиблення методичних засад аудиту ефективності ІТ-систем органів державної влади, що виступають стратегічними об'єктами державного управління.

Викладення основного матеріалу. Оцінка ефективності функціонування інформаційних систем органів державної влади та стратегічних об'єктів установ сектору державного управління є предметом аудиторської діяльності вищих органів державного аудиту більшості країн світу. Потреба підтвердити надійність функціонування інформаційних систем, де згенерована та функціонує важлива інформація щодо фінансових, індивідуальних показників фізичних та юридичних осіб, визначила необхідність проведення аудитів ефективності спеціалізованими органами контролю. А опрацювання міжнародного досвіду в цій сфері призвело до розробки членами INTOSAI стандарту ISSAI 5310 «Методика перевірки безпеки інформаційних систем» [4]. Його рекомендовано дотримуватися під час перевірок безпеки функціонування інформаційних систем для забезпечення збору належних доказів їх надійності. Незважаючи на існування серйозних ризиків збою діяльності інформаційних систем органів влади в Україні та фактів несанкціонованого втручання в роботу автоматизованих систем та комп'ютерних мереж, ці об'єкти і досі не зараховані до об'єктів аудитів контрольних органів фінансової сфери. Отже, відсутня практика перевірки надійності інформаційних систем з боку Рахункової палати потребує кардинальної зміни ситуації. Опрацювання наявних у світовому досвіді результатів аудитів ІТ-систем та методологічних вказівок щодо аудиту безпеки ІТ-систем дозволить сприяти адаптації кращих результатів таких перевірок в Україні.

Проведення аудиту ефективності ІТ-систем розпочинається з планування, як невід'ємної складової організації перевірок вищих органів аудиту, відповідно до чинних документів та міжнародних норм [5]. Планування має охоплювати такі основні елементи:

• знання клієнта і середовища;

• межі проведення перевірки: ідентифікація інформаційних систем, структура та обсяги установи, що перевіряється, у т.ч. в географічному аспекті;

• доступні ресурси: кваліфікований персонал або консультанти, бюджет, терміни;

• наявність надійних статистичних даних про загрози і показники вартості, характерні для умов і обставин об'єкту перевірки;

• вимоги до звітності: користувачі звіту, обставини перевірки (щорічний звіт, спеціальний звіт, внутрішній, зовнішній тощо), тип необхідних рекомендацій;

• метод перевірки: метод низхідної покрокової деталізації, детальний аналіз або використання обох методів.

Згідно з ISSAI 5310 «Методика перевірки безпеки інформаційних систем», під час аудиту ефективності ІТ-систем застосовують дворівневий підхід: низхідний метод перевірки забезпечення безпеки інформації та метод деталізації забезпечення безпеки інформаційних систем [4]. Другий з цих двох методів є менш поширеним, адже він потребує ґрунтовної автоматизованої бази для оцінок безпеки

інформаційних систем і може застосовуватися лише у тих країнах, де вже є велика практика таких аудитів. Складність цього методу зумовлена також необхідністю виконання складних автоматичних розрахунків ризиків порушення безпеки інформації.

Метод низхідної покрокової деталізації більш простий у застосуванні, не потребує автоматизованої перевірки інформаційних систем, працює в разі обмежених ресурсів, тому методологію і організацію його проведення розглянемо детальніше.

Даний метод застосовується до будь-якого інформаційного середовища (комп'ютерної або локальної мережі мікрокомп'ютерів).

Головне завдання методики аудиту ефективності ІТ-систем – допомогти вищим органам аудиту, які володіють необхідними повноваженнями, в перевірці програм забезпечення безпеки інформаційних систем, використовуваних різними державними установами. Вищі органи аудиту також можуть використовувати методику для налаштування комплексних і економічно ефективних програм забезпечення безпеки, що охоплюють ключові інформаційні системи у власному офісі. Нашим завданням було описати методологічно структурований підхід до оцінки і управління ризиками в інформаційних системах державних установ.

Відповідно до сутності поняття «безпека інформаційних систем», аудиторам варто встановити наявність програми забезпечення безпеки інформаційних систем, яка призначена для захисту інформації установи шляхом зниження ризику втрати конфіденційності, цілісності та доступності цієї інформації до прийнятного рівня. Належна програма забезпечення безпеки інформації має враховувати два основних елементи: аналіз ризиків і управління ризиками.

Основи наукових підходів до застосування ризик-орієнтованого підходу щодо контролю сформувалися в працях І.К. Дрозд, В.О. Шевчука, які розглядали ефективність системи контролю через ефективність окремих її складових, у т.ч. і контрольних дій [6, С. 115–116]. А задля досягнення ефективності контрольних дій, на думку зазначених вчених, варто було застосовувати нові методики, засновані на оцінці ризиків [7].

Серед практиків контролю також поширювалися ідеї західних методик здійснення контролю і аудиту, які використовували оцінку ризиків для обґрунтування залучення до планових перевірок об'єктів з високим ступенем загального ризику [8, С. 29].

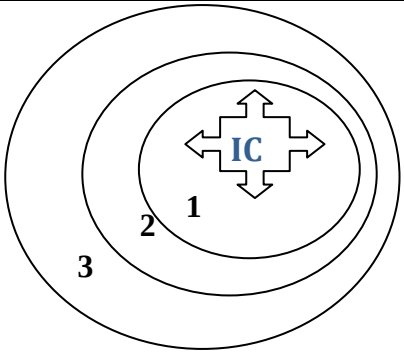
Власне, методика оцінки аудиторського ризику, що застосовувалася аудиторами в реальному секторі економіки, почала поширюватися і на бюджетну сферу та державний аудит. Любенко А.М. у своїх наукових роботах, а згодом й у докторській дисертації обґрунтував необхідність ризик-орієнтованого підходу до планування [9]. Це сприяло вдосконаленню методологічної бази діяльності органів державного аудиту, зокрема, залученню Концепції ризик-орієнтованого відбору об'єктів контролю до Плану контрольно-ревізійної роботи Держфінінспекції України та її територіальних органів [10].

Удосконалення такого підходу здійснила Ю.П. Кравченко. Нею було критично оцінено недосконаліть методики оцінки ризиків Держфінінспекції, яка «дає змогу оцінити лише ризики, пов'язані зі здійснюваними установами операціями і, взагалі, не враховує ризики порушень» [11]. Науковцем було доповнено зазначену методику ризиками, оцінка яких залежатиме не від вартісних оцінок здійснюваних операцій, а від кількості зареєстрованих правопорушень, що пов'язані з вчиненням працівниками установи корупційних вчинків чи використанням даної бюджетної установи у схемах відмивання «брудних» грошей. Отже, теорія і практика використання ризик-орієнтованого підходу під час контролю дозволяє розглядати методику аудиту ІТ-систем з точки зору оцінки ризиків та управління ними.

На етапі аналізу ризиків аудиторами до уваги береться реєстр усіх інформаційних систем. Визначається цінність кожної системи для установи і ступінь ризику, якому вона підлягає. З іншого боку, управління ризиками враховує вибір засобів контролю та заходів безпеки, які знижують схильність установи до прийнятного рівня ризику. Щоб заходи зниження ризику були ефективними, результативними та відображали здоровий глузд, вони мають прийматися в межах інфраструктури безпеки, де заходи загальної безпеки доповнюються заходами комп'ютерної, адміністративної, кадрової, фізичної безпеки (рис 1).

Управління ризиками має стати проблемою для вищого керівництва, яка потребує негайного вирішення. При управлінні ризиками необхідно досягти балансу між важливістю інформації для установи, з одного боку, та вартістю кадрових, адміністративних і технічних заходів забезпечення безпеки, з іншого боку. Витрати на вживані заходи забезпечення безпеки мають бути менші, ніж потенційний збиток внаслідок втрати конфіденційності, цілісності та доступності інформації.

Багато методик аналізу ризиків, що відомі в науці та використовуються на практиці, вимагають технічної експертизи в області інформаційних технологій і релевантних засобів контролю, а також наявності точних відомостей про прояви загроз, тому не завжди можуть бути використаними аудиторами. Отже, завдання полягає в накопиченні необхідної експертизи та ресурсів.



Довідка: складено автором

Рис. 1. Інфраструктура захисту інформації
ІС – інформаційні системи;
Додаткові рівні захисту інформації: 1 – апаратні засоби/програмне забезпечення;
2 –адміністративний; 3 –кадровий

Захист інформації є єдиним важливим елементом інфраструктури захисту. Отже, це і є єдиний об'єкт аудиторського дослідження, який оцінюється з точки зору ефективності управління ризиками. В установі має бути система стратегій безпеки, що охоплює всі аспекти фізичної, кадрової та інформаційної безпеки. Мають бути чітко визначені повноваження та обов'язки користувачів, співробітників служби безпеки і керівництва з інформаційними системами. Програма забезпечення безпеки інформації має враховувати всі сторони уразливості корпоративної інформації за критеріями конфіденційності, цілісності та доступності.

Згідно з рисунком, безпека інформації являє собою комплекс заходів, що вживаються на фізичному, кадровому, адміністративному, комп'ютерному рівнях та на рівні інформаційних систем. Заходи мають працювати всі разом. Безпека інформації являє собою ефективний адміністративний контроль, причому відсутність такого контролю на будь-якому рівні може загрожувати безпеці на інших рівнях.

Метод низхідної покрокової деталізації простий, але в той же час характеризується детальністю. З його допомогою вищі органи аудиту можуть зробити висновки щодо ризиків порушення безпеки інформаційних систем, що розглядаються під час перевірки. Метод використовує спадний принцип забезпечення безпеки інформації, оскільки в його основі лежить точка зору вищого керівництва щодо визначення того, яка інформація є цінною для установи, які ризики і наслідки порушення безпеки та які рекомендації мають бути виконані. Такий підхід дозволяє аудиторам сфокусувати свою увагу на ключових інформаційних системах, зокрема, на тих, які мають особливе значення при забезпеченні безпеки ІТ.

Метод низхідної покрокової деталізації ґрунтується на якісних оцінках ризику можливих загроз і ступеня їх наслідків. Увага фокусується на оцінці важливості інформації або даних, що передаються через інформаційні системи, для керівництва, а не лише на важливості власне технології. Саме це відрізняє аудиторську перевірку від подібних перевірок технічних аспектів спеціалізованих органів. Для кожної інформаційної системи спочатку індивідуально оцінюються важливість інформації для установи, загрози та можливі наслідки, а потім у цілому визначається ступінь небезпеки. Такі оцінки є суб'єктивними і, зазвичай, виражаються в термінах: високий, середній та низький рівень ризику.

Відповідно до цих оцінок керівництво отримує від аудиторів рекомендації про подальші дії або про тип певних засобів контролю та заходів забезпечення безпеки, які варто реалізувати. Дані рекомендації, що узагальнено представлені в таблиці, є частиною управління ризиками.

Таблиця

Ризик-орієнтований підхід до управління безпекою ІТ систем за результатами аудиту ефективності

Рівень ризику порушення безпеки	Рішення щодо забезпечення безпеки	Рекомендований захід
Високий (9,8,7)	Контроль ризику	Впровадити додаткові стратегії і вжити заходів (стандарти, процедури, інструменти)
Середній (6,5,4)	Контроль ризику	Уникнення ризику Впровадити додаткові стратегії і вжити заходів Змінити / поліпшити послідовність операцій
Низький (3,2,1)	Уникнення ризику Обмеження ризику Прийняття ризику	Змінити / поліпшити послідовність операцій Отримати страхове покриття Жодних змін / продовжувати роботу згідно з планом

Аудитори, оцінюючи ступінь ризику ІТ-систем, виявляють дії управлінського персоналу щодо реагування на ці ризики. Метод низхідної покрокової деталізації при такому підході має ряд переваг. Він простий і недорогий. Він не механізований і може бути застосований будь-яким вищим органом аудиту, в штаті якого є співробітники, обізнані в питаннях засобів контролю управління, інформаційних і комп'ютерних систем в цілому. Внутрішніх кадрових ресурсів може виявитися достатньо. Немає необхідності в установці складних пакетів програмного забезпечення для збору даних про перевірені інформаційні системи, для отримання оновлених і відповідних статистичних даних та для виконання дуже складних аналізів і складання звітів. Електронні таблиці можуть допомогти у складанні підсумкових таблиць. Для отримання більшої кількості переваг під час аудиту можна використовувати програмні пакети, що забезпечують функціональність баз даних для збору інформації та подальше складання звітів за результатами аналізу.

У дворівневому підході до перевірки забезпечення безпеки інформаційних систем, пропонованому стандартом ISSAI 5310 «Методика перевірки безпеки інформаційних систем», метод низхідної покрокової деталізації розглядається як точка прийняття рішення щодо методу в цілому. Залежно від обставин перевірки вищі органи аудиту можуть бути задоволені результатами перевірки або можуть прийняти рішення про виконання перевірки із застосуванням більш складних процедур в областях особливого значення або там, де може знадобитися для керівництва привести обґрунтування введення спеціальних або дорогих заходів забезпечення безпеки.

Для документування результатів аудиту ефективності ІТ-систем доцільно використати типові форми, серед яких найважливіші «Повідомлення про уразливість інформації і визначення категорії захисту», «Оцінка наслідків і загроз для діяльності». Заповнені форми стають невід'ємною частиною робочої та звітної документації аудиту безпеки даних систем.

Висновок. Аналіз практики аудиту ефективності ІТ-систем у країнах світу дозволив з'ясувати необхідність застосування методології аудиту, заснованої на оцінці ризиків безпеки ІТ та виявленні впливів на безпеку діяльності установи і, перш за все, таких, що здійснюють стратегічне управління в державному секторі.

Дослідження показало необхідність дотримуватися під час аудиту послідовності дій, що призводять до рекомендацій для вищого керівництва щодо контролю ризику безпеки ІТ-систем. Запропоновано три можливі варіанти рішень керівництва щодо управління ризиками безпеки ІТ-систем на основі інформації про рівні ризику за результатами аудиту ефективності.

Подальші дослідження питання аудиту ефективності ІТ-систем вбачаються у розробці організаційних заходів щодо проведення Рахунковою палатою перевірок безпеки ІТ-систем стратегічних об'єктів сектору державного управління.

Список використаної літератури:

1. Матеріали Колегії Казначейства : Редакція від 17 лютого 2017 року // Офіційний сайт Державної казначейської служби України [Електронний ресурс]. – Режим доступу : http://www.treasury.gov.ua/main/uk/publish/article/352513.
2. *Ivakhnenkov S.V.* Ukrainian Businesses' Characteristics and the Use of Information Technology: Introduction to Exploratory Studies / *S.V. Ivakhnenkov, A.Heorhiadi* // Наукові записки НаУКМА. – 2013. – Т. 146. – С. 39–44.
3. *Бенько М.М.* Можливості здійснення фінансового аудиту у середовищі інформаційних технологій / *М.М. Бенько* // Вісник ЖДТУ. Серія : Економічні науки. – 2013. – № 2 (64). – С. 3–7.
4. ISSAI 5310 «Методика перевірки безпеки інформаційних систем» // Офіційний сайт Міжнародної організації вищих органів фінансового контролю [Електронний ресурс]. – Режим доступу : http://www.intosai.org/issai-executive-summaries/view/article/issai-5310-information-system-security-review-methodology.html.
5. ISSAI 1300 – Planning an Audit of Financial Statements // Офіційний сайт Міжнародної організації вищих органів фінансового контролю [Електронний ресурс]. – Режим доступу : http://www.issai.org/en_us/site-issai/issai-framework/4-auditing-guidelines.htm.
6. *Дрозд І.К.* Державний фінансовий контроль : навч. посібник / *І.К. Дрозд, В.О. Шевчук.* – К. : ТОВ «Імекс-ЛТД», 2007. – 304 с.
7. *Дрозд І.К.* Сучасні підходи до системи фінансового контролю / *І.К. Дрозд* // Галицький економічний вісник. – 2009. – № 1 (22). – С. 164–168.
8. Внутрішній контроль та аудит у секторі державного управління України та європейський досвід : навч. посібник / *П.П. Андрєєв, Л.В. Гізатуліна, І.К. Дрозд та інші*. – К. : Кафедра, 2011. – 130 с.
9. *Любенко А.М.* Трансформація контролю діяльності суб'єктів державного сектору економіки до міжнародних стандартів : автореф. дис. … д-ра екон. наук : 08.00.09 – бух. облік, аналіз та аудит (за видами екон. діяльн.) / А.М. Любенко. – Тернопіль : ТНЕУ, 2016. – 36 с.
10. Концепція ризик-орієнтованого відбору об'єктів контролю до Плану контрольно-ревізійної роботи Держфінінспекції України та її територіальних органів : схвалена протоколом засідання Методологічної ради Держфінінспекції України : від 23.04.2012. – № 7 [Електронний ресурс]. – Режим доступу :

http://cons.parus.ua/map/doc/08DKX521BE/Protokol--7-zasidannya-Metodologichnoyi-radi-schodo-kontseptsiyi-rizikoriientovanogo-vidboru-obiektiv-kontrolyu-do-planu-kontrolnoreviziinoyi-roboti-Derzhfininspektsiyi-U.html.

11. *Кравченко Ю.П.* Розвиток методології контролю діяльності бюджетних установ на основі оцінки ризиків // Модернізація фінансової системи України в процесі євроінтеграції : у 2 т. / *Т.І. Єфименко, С.С. Гасанов, П.М. Леоненко та ін.* ; за ред. *О.В. Шлапака, Т.І. Єфименко* ; ДННУ «Акад. фін. управління». – К., 2014. – Т. 2. – 2014. – 784 с. – С. 270–279.

References:

1. Derzhavna kaznachejs'ka sluzhba Ukrai'ny (2017), «Materialy Kolegii' Kaznachejstva», *Oficijnyj sajt Derzhavnoi' kaznachejs'koi' sluzhby Ukrai'ny*, Redakcija vid 17 ljutogo, available at: http://www.treasury.gov.ua/main/uk/publish/article/352513
2. Ivakhnenkov, S.V. and Heorhiadi, A. (2013), «Ukrainian Businesses' Characteristics and the Use of Information Technology: Introduction to Exploratory Studies», *Наукові записки НаУКМА*, Vol. 146, pp. 39–44.
3. Ben'ko, M.M. (2013), «Mozhlyvosti zdijsnennja finansovogo audytu u seredovyshhi informacijnyh tehnologij», *Visnyk ZhDTU*, Serija *Ekonomichni nauky*, No. 2 (64), pp. 3–7.
4. Mizhnarodna organizacia vyshhyh organiv finansovogo kontrolju, ISSAI 5310 «Metodyka perevirky bezpeky informacijnyh system», *Oficijnyj sajt Mizhnarodnoi' organizacii' vyshhyh organiv finansovogo kontrolju*, available at: http://www.intosai.org/issai-executive-summaries/view/article/issai-5310-information-system-security-review-methodology.html
5. Mizhnarodna organizacia vyshhyh organiv finansovogo kontrolju, ISSAI 1300 «Planning an Audit of Financial Statements», *Oficijnyj sajt Mizhnarodnoi' organizacii' vyshhyh organiv finansovogo kontrolju*, available at: http://www.issai.org/en_us/site-issai/issai-framework/4-auditing-guidelines.htm
6. Дрозд, І.К. and Шевчук, В.О. (2007), *Державний фінансовий контроль*, ТОВ «Імекс-ЛТД», Kyi'v, 304 p.
7. Drozd, I.K. (2009), «Suchasni pidhody do systemy finansovogo kontrolju», *Galyc'kyj ekonomichnyj visnyk*, No. 1 (22), pp. 164–168.
8. Andrjejev, P.P., Gizatulina, L.V. and Drozd, I.K. (2011), *Vnutrishnij kontrol' ta audyt u sektori derzhavnogo upravlinnja Ukrai'ny ta jevropejs'kyj dosvid*, Kafedra, Kyi'v, 130 p.
9. Ljubenko, A.M. (2016), *Transformacija kontrolju dijal'nosti sub'jektiv derzhavnogo sektoru ekonomiky do mizhnarodnyh standartiv*, avtoref. dys. … d-ra ekon. nauk: 08.00.09, buh. oblik, analiz ta audyt za vydamy ekon. dijal'n., TNEU, Ternopil', 36 p.
10. Derzhfininspekcija Ukrai'ny (2012), «Koncepcija ryzyk-orijentovanogo vidboru ob'jektiv kontrolju do Planu kontrol'no-revizijnoi' roboty Derzhfininspekcii' Ukrai'ny ta i'i' terytorial'nyh organiv», shvalena protokolom zasidannja Metodologichnoi' rady Derzhfininspekcii' Ukrai'ny, vid 23 kvitnja, N 7, available at: http://cons.parus.ua/map/doc/08DKX521BE/Protokol--7-zasidannya-Metodologichnoyi-radi-schodo-kontseptsiyi-rizikoriientovanogo-vidboru-obiektiv-kontrolyu-do-planu-kontrolnoreviziinoyi-roboti-Derzhfininspektsiyi-U.html
11. Kravchenko, Ju.P., Jefymenko, T.I., Gasanov, S.S. and Leonenko, P.M. (2014), «Rozvytok metodologii' kontrolju dijal'nosti bjudzhetnyh ustanov na osnovi ocinky ryzykiv», *Modernizacija finansovoi' systemy Ukrai'ny v procesi jevrointegracii'*, in 2 parts, in Shlapak, O.V. and Jefymenko, T.I. (ed.), *DNNU «Akad. fin. upravlinnja»*, Vol. 2, Kyi'v, 784 p., pp. 270–279.

АБАСОВ Віталій Акімович – аспірант ДВНЗ «Київський національний економічний університет імені Вадима Гетьмана».

Наукові інтереси:

– державний аудит: методологія, організація, стандартизація.

Тел.: (067) 520–25–11.

E-mail: zentr_ipo@ukr.net.

Стаття надійшла до редакції 18.04.2017.