УДК 657.631:338.432 (075.8)

Сметанко О.В.

УДОСКОНАЛЕННЯ ПРОЦЕСУ ВНУТРІШНЬОГО АУДИТУ ПРОТИДІЇ КІБЕРШАХРАЙСТВУ В СИСТЕМІ КОРПОРАТИВНОГО УПРАВЛІННЯ ТОВАРИСТВОМ

У статі розкриваються питання, пов'язані з особливостями застосування комп'ютерних методів та процедур, що використовуються внутрішніми аудиторами у процесі профілактики та протидії шахрайству в комп'ютерному середовищі.

Розглядається модель процесу внутрішнього аудиту в умовах комп'ютерної обробки даних з урахуванням особливостей алгоритмів обробки облікової інформації і процедур контролю за введенням та коригуванням даних в комп'ютерній інформаційній системі.

Визначено контрольні процедури, які доцільно застосовувати внутрішнім аудиторам у процесі попередження кібершахрайства в системі корпоративного управління товариством.

Ключові слова: *внутрішній аудит шахрайства, процедури внутрішнього аудиту, протидія шахрайству, методи внутрішнього аудиту, інформаційна безпека.*

Постановка проблеми. В умовах розвитку і широкого використання комп'ютерних систем та технологій зростає кількість шахраїв, що користуються недосконалістю наявних в акціонерному товаристві систем протидії комп'ютерному шахрайству і привласнюють активи товариства або маніпулюють комп'ютерними даними, що призводить до викривлення фінансової звітності з метою навмисного покращення або погіршення фінансових показників товариства.

Такі обставини потребують проведення додаткових досліджень у сфері протидії комп'ютерному шахрайству в акціонерних товариствах, де ключовим елементом в системі профілактики та протидії комп'ютерному шахрайству є внутрішній аудит.

Внутрішній аудит кібершахрайства дозволить керівництву акціонерного товариства визначити слабкі місця в системі захисту облікової інформації, а також розробити превентивні заходи, спрямовані на профілактику та попередження шахрайства з урахуванням чинників внутрішнього та зовнішнього середовища.

Складність процесу ідентифікації ознак шахрайства в комп'ютерних інформаційних системах (КІС) вимагає від керівників служби внутрішнього аудиту (СВА) та внутрішніх аудиторів визначення та запровадження в систему корпоративного управління дієвих методів протидії кібершахрайству як серед персоналу акціонерного товариства, так і від зовнішніх агентів загроз шахрайства.

Зазначені обставини з урахуванням змін, що відбуваються під впливом стрімкого розвитку КІС потребують від науковців та практиків проведення додаткових досліджень щодо визначення найбільш ефективних методів і процедур профілактики та протидії кібершахрайству в корпоративному секторі економіки.

Аналіз останніх досліджень і публікацій вітчизняних, російських та закордонних науковців з питань шахрайства, зокрема роботи Г.С. Артемьевой [1], А. М. Єлінсона [2], С. В. Єлисеева [3], Дж. Л. Ковасича [4, с. 139-142], Н. В. Ковтуна [5], О. С. Пантелеєва [6], Д.В. Слабінського [7], Дж. Т. Уэллса [8], О. Н. Филатової [9] вказують на те, що як серед практикуючих аудиторів так і в наукових колах залишаються дискусійними питання щодо визначення методів, підходів і засобів профілактики та протидії кібершахрайству в корпоративному секторі економіки.

Незважаючи на численні наукові публікації, в яких досліджуються питання боротьби з комп'ютерним шахрайством (кібершахрайством) на сьогодні залишаються відкритими і не повною міріою досліджені питання щодо визначення методів та процедур, що доцільно застосовувати внутрішнім аудиторам у процесі виявлення ознак шахрайства у комп'ютерному середовищі та протидії (профілактики) йому.

Формулювання цілей статті. Метою дослідження є визначення і розкриття особливостей застосування внутрішніми аудиторами програмних методів та процедур комп'ютерного тестування, аналізу, контролю та підтримки рішень, що дозволяють нівелювати ризики комп'ютерного шахрайства з акціонерним капіталом (активами) товариства.

Виклад основного матеріалу дослідження. Різноманітність методів та процедур, що можуть застосовуватись у процесі проведення внутрішнього аудиту кібершахрайства в системі корпоративного управління насамперед обумовлено складністю побудови алгоритмів обробки та захисту даних в КІС.

Необхідно зазначити, що для ефективної протидії комп'ютерному шахрайству в акціонерному товаристві керівнику СВА необхідно:

- визначити найбільш вразливі місця в системі КОД, що дозволяють шахраям проводити незаконні операції з активами та зобов'язаннями товариства;

- розробити алгоритм тестування спеціалізованих комп'ютерних програм: бухгалтерських, складських, банківських, систем підтримки рішень та стороннього програмного забезпечення, що використовується управлінським персоналом у межах єдиного інформаційно-аналітичного простору системи корпоративного управління товариства;

- ініціювати перед керівництвом АТ пропозицію щодо обов'язкового інтегрування в КІС товариства, необхідні програмні модулі для ефективної реалізації ключових функцій внутрішнього аудиту.

Необхідність інтеграції програмних модулів в комп'ютерну інформаційну систему управління акціонерним товариством є пріоритетним напрямом у створенні інтерактивної системи моніторингу та контролю

© Сметанко Олександр Васильович, кандидат економічних наук, доцент, докторант кафедри аудиту, ДВНЗ «Київський національний економічний університет імені Вадима Гетьмана», Київ, e-mail: smetanko@mail.ru

за ключовими показниками ефективної діяльності товариства з метою виявлення нетипових операцій або закономірностей у процесі роботи управлінського персоналу в КІС.

Керівнику СВА у процесі розробки програми протидії шахрайству в КІС, необхідно враховувати, що найбільш ефективними методами виявлення (ідентифікації) ознак шахрайства та протидії йому є прості комп'ютерні програмні методи тестування – порівняльний метод тестування.

Застосування програмного методу тестування дозволяє:

- визначати ступінь захищеності системи від несанкціонованого введення та модифікації даних до інформаційної системи товариства;

- здійснити експрес-перевірку правильності введення до КІС бухгалтерських записів і формування форм первинних облікових документів та звітності товариства;

- виявити нетипові відхилення або незвичайні взаємозалежності між окремо взятими показниками та даними, що введено в КІС товариства.

Слід зазначити, що використання комп'ютерних методів у процесі внутрішнього аудиту в комп'ютерному середовищі потребує від внутрішніх аудиторів застосування додаткових аудиторських процедур, спрямованих на перевірку алгоритмів комп'ютерної обробки облікової інформації та процесу контролю за введенням і коригуванням даних в КІС.

Для вирішення цього питання у статті наведено модель внутрішнього аудиту в умовах комп'ютерної обробки даних (рис. 1), у якій визначено критерії складності як самої корпоративної інформаційної системи, так і процесу комп'ютерної обробки даних з урахуванням завдань, що стоять перед внутрішніми аудиторами:

1) система має складні запити (SQL), пов'язані з обробкою даних і формуванням документів, регістрів та звітів – внутрішньому аудитору необхідно дослідити та дати оцінку можливості маніпулювання даними у процесі побудови запитів з метою попередження фальсифікації вхідних та вихідних запитів;

2) система побудована на процедурах обробки даних (запитів) з низкою логічних дій, що дають можливість користувачу вибирати необхідне значення (перелік можливих дій), а системі проводити складні арифметичні та логічні обчислення. Внутрішньому аудитору необхідно дослідити транзакції та процедури КОД з метою визначення можливості несанкціонованого проведення нетипових операцій;

3) на автоматизованому робочому місці в автоматичному режимі формуються результативні операції, суттєві для бізнесу товариства – внутрішній аудитор застосовує до КОД процедури тестування на можливість фальсифікації або викривлення показників фінансової звітності;

4) обсяг операцій, проведених з використанням КІС, досить значний, у результаті чого складно відстежити помилки, допущені в процесі введення та обробки даних – внутрішнім аудиторам необхідно запровадити контрольні процедури з метою підсилення контролю за процесом введення інформації до КІС.

Для посилення контролю за КОД в КІС внутрішнім аудиторам необхідно застосувати такі методи:

- метод формально-правової перевірки бухгалтерської документації, що дозволяє отримати аудиторські докази відносно дотримання правил складання, оформлення та змісту операції (результативній інформації) відповідно до вимог чинного законодавства та внутрішньо-корпоративних регламентів;

- метод фактичної перевірки, що дозволяє отримати аудиторські докази щодо наявності або відсутності фактів шахрайства в процесі документального та облікового оформлення господарських операцій в КІС.

Застосування цих методів дозволяє керівнику СВА визначити факти шахрайства та на їх основі розробити ефективні заходи протидії потенційним ризикам шахрайства в системі внутрішнього контролю і обліку акціонерного товариства за умов застосування КОД;

5) системою використовуються процедури обміну даними з іншими користувачами через комунікаційні Інтернет-технології – внутрішньому аудитору необхідно:

- використати методи тестування з метою оцінки надійності захисту КІС;

- визначити можливість несанкціонованого доступу користувачів (агентів загроз шахрайства) до конфіденційної інформації за ключовими бізнес-операціями (бізнес-процесами) або викривленням даних через незахищеність наявних в системі корпоративного управління комунікаційних технологій;

6) в програмний модуль системи інтегровано програмні модулі сторонніх розробників – внутрішнім аудиторам необхідно провести незалежне тестування програм (програмних модулів) з метою нівелювання ризику промислового шпигунства та шахрайства з використанням стороннього програмного забезпечення;

7) в системі корпоративного управління запроваджено механізми захисту комп'ютерної бази даних та ієрархічну структуру доступу до введення і обробки інформації – внутрішнім аудиторам необхідно визначити можливість шахрайства серед персоналу акціонерного товариства, пов'язаного з маніпулюванням (фальсифікацією) бухгалтерських проведень.

Запропонована модель (рис.1) дозволить внутрішнім аудиторам:

- на стадії організації перевірки визначити перелік процедур роботи з КІС і ступінь складності комп'ютерної системи обробки даних;

- знизити аудиторський ризик, пов'язаний з використанням автоматизованих (комп'ютерних) методів і процедур, виходячи із поставленої мети та завдань.

Для підвищення ефективності профілактики (попередження) зловживань серед управлінського персоналу товариства та протидії шахрайству в умовах КОД рекомендуємо внутрішнім аудиторам застосовувати такі контрольні процедури:

- перевірку наявності затвердженого керівництвом переліку осіб, відповідальних за експлуатацію системи КОД. Застосування даної процедури дозволяє визначити перелік осіб та умови (регламент) внесення змін у алгоритми КОД;

- перевірку повноважень і прав доступу співробітників до бази даних комп'ютерної інформаційної системи. Використання даної процедури спрямоване на виявлення порушень і/або попередження шахрайства серед користувачів програмного забезпечення за рівнями АРМ і доступу до даних, відповідно до затверджених у товаристві посадових інструкцій та регламентів;

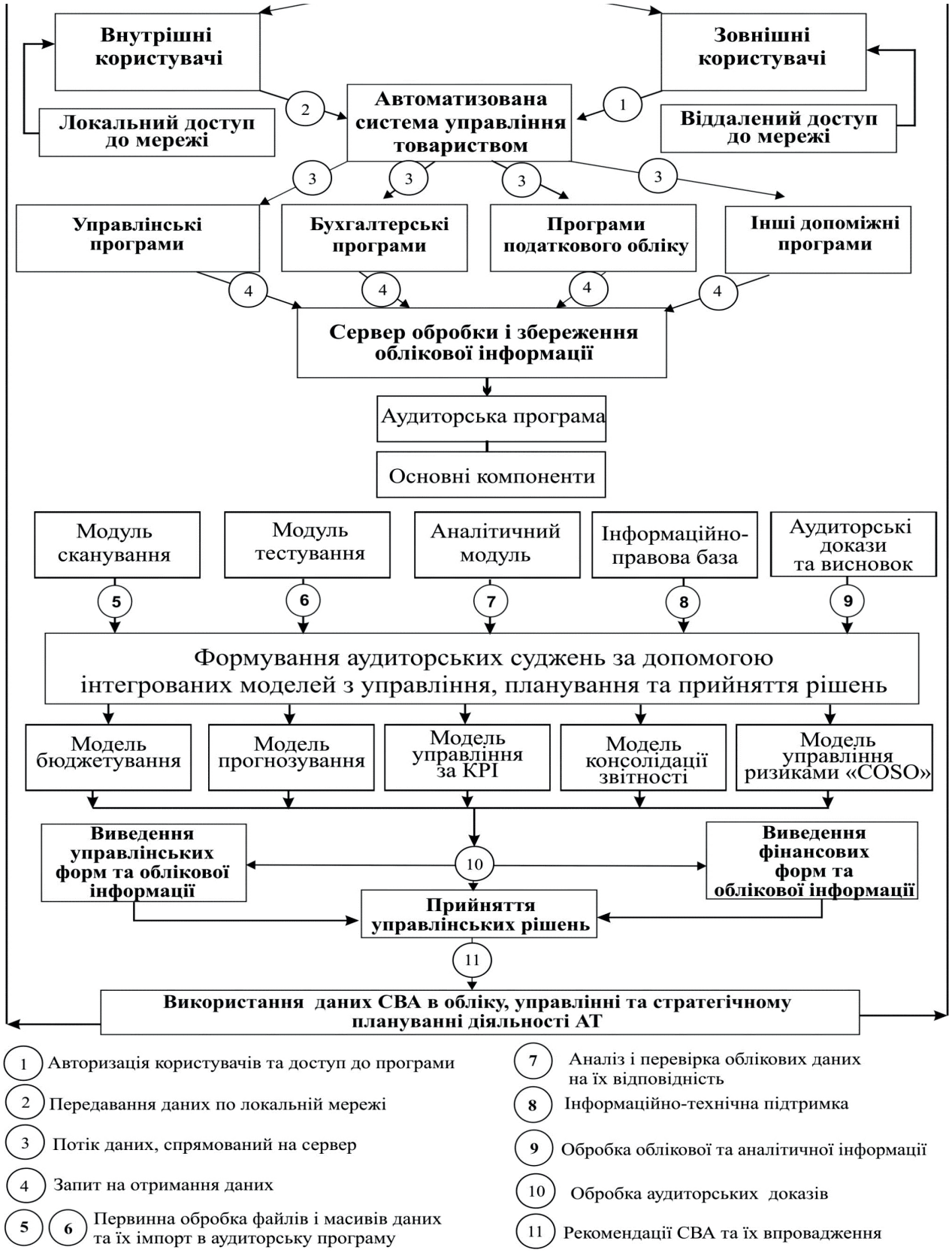

Рис. 1. Модель процесу внутрішнього аудиту в умовах комп'ютерної обробки даних [розроблено автором]

- перевірку плану заходів з резервного копіювання інформаційних баз і відновлення програмного забезпечення. За допомогою цієї процедури внутрішній аудитор визначає потенційно можливі порушення в частині відсутності плану заходів, пов'язаних з резервним відновленням програмного забезпечення та інформаційної бази даних у випадку їх програмного або фізичного пошкодження;

- контроль за введенням інформації до КІС – дозволяє внутрішнім аудиторам визначити найбільш уразливі з позиції шахрайства процедури введення та подальшого корегування управлінським персоналом товариства даних в КІС;

- визначення ступеня (рівня) автоматизації процесів обробки даних, результати яких мають суттєве значення для бізнесу суб'єкта господарювання – дозволяє отримати аудиторські докази стосовно ефективності та прозорості оформлення операцій з використанням комп'ютерних та ручних (неавтоматизованих) методів обробки даних;

- тестування та контроль процедур, що застосовуються у процесі експорту (імпорту) файлів (даних) з використанням технологій розподіленої обробки даних – спрямовано на контроль за процесом експорту-імпорту даних в КІС з метою протидії шахрайству в структурних підрозділах товариства, що мають регіональну віддаленість від головного офісу;

- контроль процедур комп'ютерної обробки даних – передбачає застосування фрагментарного методу тестування комп'ютерних процедур і алгоритмів обробки даних на можливість здійснення управлінським персоналом маніпуляцій, що приводять до викривлення облікових та управлінських даних;

- перевірка на відповідність функціонування програмного забезпечення до вимог чинного законодавства відносно правильності формування первинних документів, облікових регістрів та форм звітності. Застосування даної процедури дозволяє внутрішньому аудитору отримати аудиторські докази щодо правових результатів функціонування КІС та програмного забезпечення, а також визначити проблемні місця у документальному оформленні операцій відповідно до вимог чинного законодавства України та внутрішньокорпоративних регламентів акціонерного товариства;

- визначення слабких (вузьких) місць в системі КОД – передбачає застосування методів тестування, аналізу, фінансової математики з метою визначення наявних або потенційних порушень в КІС.

Досліджені процедури дозволять внутрішнім аудиторам визначити проблемні місця в системі КОД (КІС) та за умов розробки точкових заходів надати рекомендації з попередження фактів шахрайства і зловживань як серед управлінського персоналу АТ, так і з боку зовнішніх агентів загроз шахрайства.

Слід зазначити, що застосування розглянутих процедур стає найбільш ефективним за умов їх комплексного використання з аналітичними методами. Такий підхід дозволить внутрішнім аудиторам виявити приховані факти шахрайства як у процесі документального супроводу (оформлення) бізнес-операцій, так і у процесі їх комп'ютерної обробки спеціалізованим програмним забезпеченням.

Особливе значення у процесі виявлення факторів шахрайства та розробки заходів протидії йому є запровадження (інтеграція) в корпоративну інформаційну систему алгоритму ідентифікації ризиків, що базується на методі кількісної оцінки ризиків за ключовими показниками ефективності товариства.

Застосування цього методу дозволяє в умовах КОД:

1) сформувати точкові рекомендацій з проблемних питань щодо ймовірності настання кризових явищ і можливості їх нівелювання у поточному періоді та недопущенні їх у майбутньому.

2) отримати такі результати:

- систему аналітичних показників, за допомогою яких можна визначити перелік можливих заходів щодо поліпшення стану досліджуваної системи;

- економічні та прогнозні розрахунки ефективності реалізації запропонованих аудитором заходів, спрямованих на поліпшення досліджуваної системи;

3) визначити нетипові коливання за ключовими показниками ефективності, що з позиції внутрішнього аудиту шахрайства слід розглядати як ймовірні факти шахрайства;

4) розкрити логічні та функціональні зв'язки між різними елементами системи корпоративного управління, що дозволять визначити пріоритетні напрями та об'єкти, які є найбільш схильними до шахрайства.

Слід зазначити, що комп'ютерні методи внутрішнього аудиту шахрайства повинні базуватися на чітко визначених алгоритмах реалізації аудиторських процедур за умов їх інтеграції до корпоративної системи управління акціонерним товариством.

З метою удосконалення процесу протидії шахрайству в акціонерних товариствах за умови застосування комп'ютерних інформаційних систем рекомендуємо інтегрувати до КІС товариства розроблену модель внутрішнього аудиту в умовах комп'ютерної обробки даних (рис. 1). Це дозволить внутрішнім аудиторам вирішувати завдання, спрямовані на:

- внутрішній аудит комп'ютерної, програмної та інформаційної безпеки систем управління товариством;

- застосування розглянутих в аудиторській практиці методів, процедур та алгоритмів, що рекомендовано використовувати в автоматизованих інформаційно-аналітичних системах внутрішнього аудиту для контролю, аналізу та оцінки в он-лайн режимі системи збалансованих показників діяльності товариства;

- визначення чинників, що призводять до відхилень показників або зловживань серед управлінського персоналу;

- збір аудиторських доказів з метою формування аудиторського судження про наявні факти шахрайства та зловживання в акціонерному товаристві;

- розробку проекту рішення щодо усунення потенційних або наявних фактів шахрайства з акціонерним капіталом;

- визначення сильних і слабких місць в системі корпоративного управління товариством в умовах КОД.

Використання на практиці запропонованого підходу до реалізації моделі процесу внутрішнього аудиту в умовах комп'ютерної обробки даних дозволить внутрішнім аудиторам:

1) підвищити ефективність внутрішнього аудиту шахрайства в КІС;

2) здійснювати моніторинг та оперативне реагування на відхилення ключових показників ефективності товариства;

3) проводити комплексний аналіз ефективності діяльності товариства;

4) нівелювати ризики шахрайства з активами та зобов'язаннями товариства;

5) попередити фальсифікацію фінансової звітності та даних бухгалтерського обліку;

6) здійснювати моніторинг та контроль за процесом КОД на різних ланках системи корпоративного управління, що дозволить нівелювати ризики шахрайства серед управлінського персоналу товариства.

Висновки і перспективи подальших досліджень. Підводячи підсумок, слід зазначити, що внутрішній аудит є ключовим елементом в системі корпоративного управління, що дозволяє за умов комплексного запровадження правових та комп'ютерних методів застосовувати ефективні методи (засоби) протидії шахрайству та проводити його профілактику як серед суб'єктів корпоративних правовідносин, так і серед зовнішніх агентів загроз.

Використання комп'ютерних методів в процесі проведення внутрішнього аудиту є ефективним тільки у разі наявності в товаристві корпоративних інформаційних систем управління, до складу яких входить спеціалізоване бухгалтерське і аудиторське програмне забезпечення, що дозволяє здійснювати комп'ютерну обробку даних (КОД), тестування програмних модулів та алгоритмів програмних модулів. В усіх інших випадках комп'ютерні методи виявлення шахрайства та протидії (боротьби) є недоцільними, а в деяких випадках неможливими або економічно нераціональними внаслідок збільшення термінів перевірки та зниження загальної ефективності проведення внутрішнього аудиту в умовах КОД.

Реалізація запропонованих в комп'ютерній моделі внутрішнього аудиту методів та процедур, визначають подальший розвиток у дослідженні аудиторських процедур, які доцільно застосовувати в КІС з метою своєчасного виявлення ознак кібершахрайства.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Артемьева Г. С. Мошенничество в современных телекоммуникациях Г. С. Артемьева, К. М. Петрухина // Технологии информационного общества. – 2013. – № 12. – С. 9–12.
2. Елинсон А. Борьба с корпоративным мошенничеством / А. Елинсон // ЗАО «Делойт и Туш СНГ». – 2007. – С. 1–28.
3. Елисеев С. В. Мошенничество персонала: основные схемы и методы борьбы / С. В. Елисеев // Экономическая безопасность: квалификация и расследование. – 2009. – № 7. – С. 22–30.
4. Ковасич Дж. Л. Противодействие мошенничеству: как разработать и реализовать программу мероприятий / Дж. Л. Ковасич; пер. с англ. – М.: Маросейка, 2010. – 307 с.
5. Ковтун Н. В. Методи індикативної оцінки можливого шахрайства у фінансовій сфері / Н. В. Ковтун // Вісник Київського нац. університету імені Тараса Шевченка. Економіка. – Випуск 123. – Київ: ВПЦ "Київський університет", 2011. – С. 11–15.
6. Пантелеєва О. С. Шахрайство у сфері обліку та шляхи його усунення на досвіді США / О. С. Пантелеєва // Управління розвитком. – 2012. – № 4. – С. 51–52.
7. Слабинский Д. В. Мотивы и методы выявления намеренного занижения прибыли как вида мошенничества в финансовой отчетности /Д. В.Слабинский //Международный бухгалтерский учет. – 2012. – № 32 (230). – С. 31–34.
8. Уэллс Дж. Т. Взяточничество: предупреждение и выявление корпоративного мошенничества / Дж. Т. Уэллс – М. : Лаборатория Книги, 2010. – 62 с.
9. Филатова О. Н. Методы обнаружения мошенничества в бухгалтерском учёте и отчётности: дис. … канд. экон. наук : 08.00.12 / О. Н. Филатова. – СПб., 2002. – 203 с.

Одержано 20.04.2015 р.