

9. Lisa Theresa Lenz, Kai Christian Weist, Jan Winkels et. al. (2021). Multi-criteria decision support in construction management: life cycle-oriented investigation of the economic efficiency. European Conference on Computing in Construction. Online e Conference. (pp. 143-152).

Ihor Kharchenko, Associate Professor, PhD in Economics (Candidate of Economic Sciences)

Volodymyr Zaichenko, Professor, Doctor of Economics

Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine

Determination of the Criterion of Economic Efficiency of Design Solutions in Industries with a Long Life Cycle (on the Example of the Construction Industry)

The purpose of this article is to define the criterion of economic efficiency in the construction industry for each of the participants in the construction process and to justify specific formulas that can be easily applied and would show the best option for project developers, project executors (i.e. contractors) and operators, i.e. those who operate the building.

The paper considers in detail the criterion of cost-effectiveness in the form of annualized or total costs, depending on the situation and the position of the participant in the construction process. The nature and composition of capital investments and current costs, taking into account the specifics of the construction industry, with considerable attention paid to determining the discount rate are analyzed. It is proposed to use the discount rate not as for ordinary industries, such as mechanical engineering, but to take into account the peculiarities of construction. These peculiarities are that different structures have different service lives and, accordingly, different discount rates will be applied. It is also substantiated to use depreciation rates for calculating operating costs not as for accounting calculations, but based on actual service lives, which will contribute to a more accurate determination of actual costs.

Based on the above refinements, formulas for calculating the actual costs of contractors and building operators are derived. It is substantiated that the proposed formulas will contribute to the fact that the construction contractor and the operator will have accurate information about the most economical, from their point of view, the designed construction solution and its implementation. This information can be used to more accurately position construction companies and construction customers in the competition and help strengthen their position in the market.

cost (estimated cost) of construction and installation works, economic efficiency, criterion, capital investment, current (operating) costs, capital investment life, discount rate, product life cycle

Одержано (Received) 10.02.2024

Прорецензовано (Reviewed) 02.03.2024

Прийнято до друку (Approved) 27.05.2024

УДК 657.631.6

JEL Classification: F51; H83; M21

DOI: [https://doi.org/10.32515/2663-1636.2024.11\(44\).65-84](https://doi.org/10.32515/2663-1636.2024.11(44).65-84)

І.В. Гайдуков, директор ТОВ ВКФ "ІЛВІС"

І.О. Андрощук, доц., канд. екон. наук

Центральноукраїнський національний технічний університет, м. Кропивницький, Україна

Особливості корпоративного шахрайства у бізнесі: сутність, наслідки та протидія в контексті опору змінам

У статті розглянуто особливості корпоративного шахрайства у бізнесі. Метою дослідження є аналіз корпоративного шахрайства безвідносно до місць виникнення, його ознак та засобів протидії саме як системи, що об'єднує як превентивні заходи, так і контрольні. Здійснено аналіз підходів до класифікації шахрайства та їх найбільш поширених видів. Встановлено розмір фінансових втрат від здійснення шахрайства. Проведено аналіз факторів, які спонукають співробітників до шахрайства. Проаналізовано структуру трикутника шахрайства: мотивація, можливість та раціоналізація. Сформовано «типовий вигляд» шахрая. Встановлено риси, які притаманні шахраям. Здійснено аналіз структурних підрозділів підприємств із точки зору рівня ризику виникнення шахрайства. Розглянуто компоненти ефективної стратегії протидії шахрайству, а саме: створення гідної етичної культури, навчання та підвищення обізнаності щодо ризиків шахрайства, механізми звітності та повідомлення про корупцію, побудова системи внутрішнього контролю, перевірка перед прийомом на роботу.

© І.В. Гайдуков, І.О. Андрощук, 2024

Здійснено аналіз джерел надходження інформації про можливі випадки шахрайства. Досліджено методи виявлення шахрайських дій. Визначено ключові індикатори шахрайства: попереджувальні знаки та «дзвінки» про шахрайство. Запропоновано перелік «дзвінків», які слугують сигналом у вчиненні шахрайських дій. Сформовано ключові аспекти внутрішнього шахрайства у бізнесі, які визначають його складність та важливість боротьби з цією проблемою, зокрема: соціально-економічні причини, непередбачувані наслідки, різноманітні види шахрайства, складність виявлення, практичні труднощі в зборі статистики.

корпоративне шахрайство, бізнес, опір змінам, вище керівництво, трикутник шахрайства

Постановка проблеми. Одним із ключових векторів розвитку української економіки в напрямку досягнення європейських стандартів виступає формування довіри в суспільстві. Важливим чинником, який перешкоджає цьому, є шахрайство, як один з видів економічного злочину. Звісно, жодна економіка світу, побудована на товарно-грошових відносинах, не є повністю позбавленою цього явища. Проте, вивчаючи досвід розвинених країн та застосовуючи його на протидію шахрайству в нашій країні, можна досягти досить вагомих результатів у короткий проміжок часу. Слід також зазначити, що у повосенний період відновлення Україна буде потребувати залучення великих обсягів іноземних інвестицій. І не в останню чергу в залежності від того, наскільки ці інвестиції будуть захищені й від впливу шахраїв, що актуалізує обрану тематику дослідження.

Аналіз останніх досліджень і публікацій. Вивченню внутрішнього (корпоративного) шахрайства присвячено багато публікацій як вітчизняних, так і зарубіжних авторів. Так, наприклад, Борис С. в межах своїх досліджень, звертає увагу та причини, наслідки, способи виявлення та протидії фактам шахрайства на підприємстві [1]. Тоді як результатом наукового пошуку Хамиги Ю. виступає проблема фінансового шахрайства з точки зору економіки та фінансів з одночасним використанням надбань інших наукових напрямів (юриспруденції, соціології, психології тощо) [5]. Поряд із тим, на наш погляд, шахрайство за своєю природою не обмежується виключно фінансовим моментом.

Климко Т. та Мельник О. досліджували особливості корпоративного шахрайства в контексті сучасних реалій, фокусуючи увагу на першопричинах виникнення [2]. Тоді як Нежива М. вивчала вплив економічних злочинів та шахрайства на розвиток підприємництва в Україні та акцентувала увагу на актуальності перешкоджання шахрайству як способу стабілізації економічної системи [4].

Поряд із тим, на наш погляд, вищезгадані дослідження не містять системного підходу до дослідження аспекту корпоративного шахрайства. Більшість таких публікацій має акцент, направлений, скоріше, на правове регулювання цього явища, не зважаючи на економічну та етичну складову. Також більшість публікацій стосуються фінансового шахрайства та його виявлення за допомогою аудиту. Саме тому актуальним аспектом даної проблеми виступає дослідження саме економічної природи наслідків вчинення працівниками спроби шахрайства та особливості реагування на такі факти зі сторони вищого керівництва, беручи до уваги індивідуальні особливості кожного працівника.

Постановка завдання. Метою дослідження є аналіз корпоративного шахрайства безвідносно до місць виникнення, його ознак та засобів протидії саме як системи, яка об'єднує як превентивні заходи, так і контрольні. Оскільки, на нашу думку, саме ґрунтовне вивчення механізмів, способів та спонукань людей до вчинення корпоративного шахрайства буде підґрунтям для створення ефективних механізмів протидії цьому явищу. Причому, основну увагу слід приділити саме проактивній частині попередження корпоративного шахрайства, що, в свою чергу, дасть змогу забезпечити підвищення ефективності діяльності сучасних підприємств.

Виклад основного матеріалу. Зазвичай термін «шахрайство» включає такі дії, як крадіжку, корупцію, змову, розкрадання, відмивання грошей, хабарництво та здирицтво. Законодавство різних країн трактує шахрайство по-різному.

Шахрайство, за своєю суттю, передбачає використання обману для неправомірного отримання особистої вигоди для себе та/або створення збитків для іншої особи. І хоча визначення різняться, більшість базується на цих загальних визначеннях. Так, Кримінальний Кодекс України класифікує шахрайство як «заволодіння чужим майном або придбання права на майно шляхом обману чи зловживання довірою» [3]. Як бачимо, в законодавстві України не передбачена класифікація шахрайства як дій, які направлені на створення збитків сторонній особі.

Отже, узагальнено, шахрайство можна поділити на:

- злочини проти споживачів, клієнтів або інших бізнесменів, наприклад, спотворення якості товарів, торговельні піраміди;
- шахрайство працівників проти роботодавців, наприклад, шахрайство з заробітною платою, фальсифікація заяв про витрати, крадіжка готівки, активів або інтелектуальної власності, фальшування бухгалтерського обліку;
- злочини компаній проти інвесторів, клієнтів або співробітників, наприклад, шахрайство з фінансовою звітністю, продаж підроблених товарів як справжніх, відсутність сплати податків або внесків.
- злочини проти фінансових установ, наприклад, використання втрачених або викрадених кредитних карток, шахрайство з чеками, шахрайство зі страховими виплатами;
- злочини окремих людей або компаній проти уряду, наприклад, шахрайство з цільовими коштами, шахрайство з виплатою соціального страхування, ухилення від сплати податків;
- злочини професійних злочинців проти організацій, наприклад, підробка печаток, шахрайство з іпотечними кредитами, шахрайство з корпоративними зобов'язаннями, відмивання грошей;
- кіберзлочини, наприклад, фішинг, спам, порушення авторського права, шахрайство за допомогою соціальної інженерії.

На наше переконання, саме внутрішнє шахрайство у бізнесі, яке направлено зсередини самої організації, з боку її працівників і є найбільш актуальним із точки зору дослідження аспектів виникнення неправомірної вигоди.

За даними Асоціації сертифікованих дослідників шахрайства (ACFE) [6], існують наступні основні види шахрайства, які впливають на організації в цілому.

Перше – це незаконне привласнення активів, яке передбачає крадіжку або нецільове використання активів підприємства: крадіжки запасів або готівки, фіктивні рахунку та акти, шахрайство з заборгованістю або заробітною платою.

Друга категорія – фальсифікована звітність. Зазвичай, це має форму фальсифікації фінансової звітності з метою отримання певної неправомірної вигоди. До цієї категорії також слід віднести фіктивні дані по співробітниках.

Третьою категорією шахрайства є корупція, яка включає такі дії як використання хабарів або отримання «відкатів», неналежне використання конфіденційної інформації, конфлікт інтересів та тендерні змови.

В світі було багато спроб виміряти чи просто усвідомити справжні масштаби шахрайства, проте зібрати надійні статистичні дані дуже непросто. Однією з ключових ознак шахрайства є обман, тож його важко однозначно виявити, а результати опитування можуть відображати лише ті випадки, які були фактично виявлені. Іноді важко відрізнити, чи відбулося саме шахрайство, чи це помилкове ведення обліку.

Проте, слід зазначити, що більшість випадків шахрайства залишаються непоміченими, та навіть коли шахрайство виявлено, компанії про нього можуть просто не повідомляти.

Далі, вважаємо за доцільне, розглянути основні причини такого приховування фактів шахрайства зі сторони бізнесу. За дослідженням Harvard Business Review [7], методом опитування представників різних організацій, респонденти вказали основною причиною те, що вони не довіряють правоохоронній системі.

Крім того, респонденти вказували, що поліція надавала перевагу випадкам, коли кошти втрачають приватні особи, а не організації. Іншою причиною була різниця в меті: правоохоронні органи мають на меті притягнення шахрая до відповідальності, а компанії - повернути втрачені кошти. Нарешті, ще однією причиною, за їх словами, є те, що правоохоронні органи страждають від браку технологічних ресурсів та досвіду, оскільки шахрайські схеми стають дедалі складнішими та заплутаними. Не ставлячи під сумнів досвід респондентів HBR, слід все ж зазначити, що подібна стратегія має дуже негативні довгострокові наслідки.

Для корпоративних менеджерів переваги такого *modus operandi* є очевидними: захист їх репутації та репутації їхньої організації, а також швидше відновлення бізнесу та, у деяких випадках, повернення втрачених коштів (хоча б частково). Однак керівники, які сьогодні приймають такі рішення, мають усвідомлювати, що такий підхід ґрунтується на короткостроковому мисленні, результати якого можуть бути проблематичними в довгостроковій перспективі.

Не повідомляючи про шахраїв до правоохоронних органів, вони дають змогу їм вільно переходити з однієї організації в іншу. Тоді керівникам або хедхантерам стає важче відрізнити надійних працівників від сумнівних під час прийому на роботу. Це також підвищує ризик того, що деякі шахраї матимуть можливість удосконалити свою тактику та стати «серійними шахраями» (*serial fraudsters*). Таким чином, намагання кулуарного внутрішнього вирішення проблеми шахрайства у довгостроковій перспективі негативно впливає не тільки на саму організацію, а й на бізнес-середовище взагалі.

Безсумнівно, результати опитувань і досліджень не можуть давати повної картини, але різні статистичні дані все ж дають змогу отримати корисну інформацію про масштаби проблеми. Немає жодного сумніву, що шахрайство дуже поширене в бізнес-середовищі і є серйозним викликом. Так, слід зазначити, що згідно з дослідженням Pricewaterhouse Coopers [9], в 2022 році більше 51% компаній у світі стикалися з випадками шахрайства. Це найвищий рівень шахрайства за 20 років, впродовж яких PWC проводить дослідження.

Згідно дослідження Kroll [9], 69% виконавчих директорів та спеціалістів з ризик-менеджменту очікують збільшення ризиків від шахрайства впродовж наступних 12 місяців.

За словами фінансових директорів, які були опитані ACFE [6], очікувані втрати від шахрайства становлять близько 5% загального обсягу оборотів компаній, що становить більше ніж 4.7 трильйонів доларів США. Ці ж величезні цифри підтверджує й Світовий Банк. Тобто сумарні втрати від шахрайства для світової економіки обходяться майже вдвічі більше, ніж її прогнозоване зростання згідно даних Міжнародного валютного фонду у 2024 році [11].

Далі, вважаємо за доцільне дослідити особливості організацій, середовище яких більш схильне до виникнення корпоративного шахрайства.

Шахрайство - це проблема, з якою можуть зіткнутися всі організації, незалежно від розміру, галузі чи країни. Якщо організація має хоч якісь цінності (грошові кошти,

товари, технологію, інформацію чи послуги), то вони не захищені від спроби шахрайства. У засобах масової інформації часто повідомляють про гучні шахрайства у великих багатонаціональних організаціях, а менші організації можуть вважати, що вони навряд чи стануть мішенню для шахраїв. Однак, згідно зі звітом ACFE [6], малі підприємства (класифіковані як ті, що мають менше ніж 100 співробітників) страждають від шахрайства частіше, аніж великі організації, і страждають від вищих середніх збитків. Коли невеликі компанії зазнають великих збитків через шахрайство, вони з меншою ймовірністю зможуть покрити збитки, ніж більші компанії, і в результаті, можуть навіть припинити свою діяльність.

Хоча шахрайство поширене в організаціях будь-якого розміру, у всіх секторах економіки і країнах, дослідження показують, що певні бізнес-моделі передбачають більший рівень ризику шахрайства ніж інші. Тож, контрольне середовище має бути скориговано відповідно до ступенів ризику виникнення шахрайства. Тому далі, вважаємо за доцільне, дослідити, ключові маркери оцінки ризиків та засобів їх контролю.

Не існує єдиної причини, яка спонукає людину до шахрайства, тож при будь-якому поясненні таких дій слід брати до уваги різні фактори, а саме:

- мотивацію потенційних порушників;
- умови, за яких люди можуть раціонально обґрунтувати свої можливі злочини;
- можливості вчинити злочин;
- уявна придатність цілей для шахрайства;
- технічні можливості шахрая;
- очікуваний та фактичний ризик виявлення після здійснення шахрайства;
- очікування наслідків виявлення (включаючи як некримінальні наслідки, такі як втрата роботи та осуд, конфіскація коштів, отриманих злочинним шляхом, так і традиційні кримінальні санкції);
- реальні наслідки викриття.

Відомою загальною моделлю, яка об'єднує кілька цих аспектів, є «трикутник шахрайства», який побудований на припущенні, що шахрайство, найчастіше, є результатом поєднання трьох факторів: мотивації, можливостей і раціоналізації (рис.1).



Рисунок 1 - Трикутник шахрайства

Джерело: сформовано авторами на основі [15]

Таким чином, мотивація базується на жадібності або потребі. Виходячи з досліджень Стоя Хейворда (Stoy Hayward) (BDO), жадібність продовжує залишатися основною причиною шахрайства, у 63% випадків. Іншими причинами були проблеми через борги та азартні ігри. Багато людей стикаються із самою можливістю вчинити шахрайство, проте лише меншість (жадібних або нужденних) це робить. Важливу роль також грають особистісні характеристики людини, її темперамент, в тому числі й те, як люди реагують на можливі наслідки у випадку викриття. Деякі люди із, здавалося б, непохитними принципами, можуть потрапити в безвихідне або скрутне становище, що спокушає їх вдатися до шахрайства.

З точки зору можливостей, шахрайство більш імовірне в компаніях, де є слабка система внутрішнього контролю, погана безпека власності компанії, невеликий страх перед викриттям, взагалі низька ймовірність виявлення або нечітка політика щодо прийнятної поведінки. Дослідження показали, що деякі люди є абсолютно чесними, деякі - абсолютно нечесними, але на дуже багатьох, навіть тих, хто ніколи не думав про вчинення шахрайських дій, і впливає й спокушає до них саме існування такої можливості.

Багато людей живуть та працюють у рамках закону, тому що вірять у нього та/або бояться бути присоромленими або осудженими людьми, які їм небайдужі, у випадку, якщо їх можливі незаконні дії розкриють.

Проте деякі люди пояснюють шахрайські дії наступним чином:

- необхідно – особливо коли це робиться для бізнесу;
- нешкідливо – жертва достатньо велика, щоб погасити удар («що їм буде, вони й так багаті»);
- виправдано – тому що жертва «zasлужила це» або «тому що зі мною погано поводитися».

Одним із найефективніших способів вирішення проблеми шахрайства є застосування методів чи засобів, які зменшать мотив чи можливість, або, краще, обидва ці чинники. Раціоналізація є дуже індивідуальним чинником для кожної людини, тому з нею важче боротися. Проте, якщо компанія декларує та дотримується сильної етичної культури та пропагує чіткі цінності, цей фактор також можна зменшити.

Саме тому виникає логічне питання - хто може виступати суб'єктом шахрайства. Звичайно, досить складно, явно окреслити «типовий вигляд» шахрая. Проте, певні дослідження показали деякі різновиди типів людей, які вдаються до шахрайства. Зазвичай їх поділяють на три категорії:

- шахраї, що планують дії заздалегідь. Вони із самого початку діють з наміром вчинити шахрайство. Це можуть бути короткострокові шахраї, наприклад, ті, хто використовує щойно вкрадені кредитні картки, або можуть бути довготерміновими, наприклад ті, хто застосовує складні схеми відмивання грошей.
- шахраї середнього рівня, які починають працювати чесно, але вдаються до шахрайства, коли настають тяжкі життєві події або є термінова потреба у коштах. До них також відносяться ті, хто відчуває роздратування через те, що їх несправедливо не підвищують або вважають, що їх недостатньо цінують тощо.
- шахраї, які просто не можуть зупинитися у марнотратстві. Вони продовжують витратити кошти навіть тоді, коли об'єктивно не в змозі сплатити свої борги. До них можуть відноситися як звичайні люди, так і великі бізнесмени.

Дослідження компанії KPMG [8], проведене в різних країнах, дозволило виявити риси, які притаманні шахраям:

- злочинці зазвичай є чоловіками з вищою освітою;

- більшість шахраїв у віці від 36 до 45 років (проте, 3% шахраїв, старших за 60 років, наносять медіанну шкоду, яка у 8 разів перевищує таку ж для вказаного віку [8]);
- медіанні збитки від чоловіків на 25% більші, аніж від жінок;
- шахрайство найчастіше вчиняється проти власного роботодавця;
- шахраї найчастіше мають дотичність до фінансових функцій або ролей;
- найчастіше займають керівні посади;
- співробітники, які працюють більше 10 років, схильні вчиняти набагато більші шахрайства;
- шахраї зазвичай працюють у змові з іншими порушниками.

В свою чергу, у звіті ACFE також встановлено, що тип особи, яка вчинила злочин, залежить від характеру вчиненого шахрайства. Рядові співробітники частіше всього причетні до незаконного привласнення активів, тоді як власники та керівники несуть відповідальність за більшість шахрайств з фінансовими звітами.

Зі звичайних співробітників найбільший відсоток схем був задіяний у бухгалтерії. Ці працівники відповідають за обробку та реєстрацію фінансових операцій організації і тому часто мають найбільший доступ до її фінансових активів і більше можливостей для приховування шахрайства.

Третім кроком оптимізації було визначення співставних продуктів, що по факту є заміниками один одного. Основною мобільною технікою, на якій використовується продукція підприємства, є автобетонозмішувачі. На базі цього сегменту проілюструємо застосування методології, що аналогічним чином була застосована і для інших сегментів (табл. 1).

Таблиця 1 — Відділи організацій з найвищими ризиками шахрайства

Відділ/напрямок	Кількість випадків	Частка від загальної кількості, %	Середні втрати, дол. США
Операційна діяльність	273	15	74 000
Облік/бухгалтерія	230	12	155 000
Вищий менеджмент	206	11	500 000
Продажі	203	11	100 000
Підтримка покупців	140	8	40 000
Закупівлі	131	7	129 000
Адміністративна підтримка	131	7	90 000
Фінанси	95	5	160 000
Рада директорів	58	3	500 000
ІТ	53	3	150 000
Склад	58	3	116 000
Виробництво	63	3	100 000
Технічне обслуговування	49	3	58 000
Маркетинг	35	2	112 000
Відділ кадрів	29	2	100 000
Дослідження та розробка	17	1	75 000

Джерело: складено авторами на основі [8]

Підсумовуючи вищевикладене, можна сказати, що основна причина, чому люди вчиняють шахрайство, полягає в тому, що їм це дозволено. Є широкий асортимент загроз, з якими стикається бізнес. Загроза шахрайства може виходити зсередини або

ззовні організації, але ймовірність того, що шахрайство буде вчинено, суттєво зменшується, якщо потенційний шахрай буде розуміти, що зиск буде невеликим, що він буде виявлений або що потенційне покарання буде неприйнятно високим та невідворотним.

Основним способом досягнення цього має бути створення комплексної системи контролю, спрямованої на запобігання шахрайству, а там, де шахрайство з якоїсь причини й не було попереджено, суттєво збільшується ймовірність його виявлення та сильно зростають ризики та наслідки для шахрая.

Ризик-менеджмент визначається як «процес розуміння та управління ризиками, яким суб'єкт господарювання неминуче піддається, намагаючись досягти своїх корпоративних цілей» (офіційна термінологія СІМА [13]).

Для організації ризики – це потенційні події, які можуть вплинути на досягнення цілей організації. Управління ризиками полягає в розумінні природи таких подій і, якщо вони становлять загрозу, у складанні позитивних планів їх пом'якшення.

Шахрайство є серйозним ризиком, який загрожує не тільки бізнесу з точки зору фінансового здоров'я, а також іміджу та репутації.

Ризик шахрайства є одним із компонентів операційного ризику. Операційний ризик – це такий тип ризиків, який зосереджується на операціях, пов'язаних з помилками або подіями під час обробки транзакцій або інших бізнес-операцій. Аналіз ризиків стосовно шахрайства розглядає, чи можуть ці помилки або події бути результатом навмисної дії, спрямованої на користь зловмисника. Перевірки ризиків для встановлення або спростування факту шахрайства мають детально розглядатися та проводитися командами, які поєднують глибокі знання бізнесу та ринку з детальними знаннями та досвідом протидії шахрайству.

Такі ризики, як неправдива бухгалтерська звітність або крадіжка готівки чи активів, необхідно враховувати для кожної бізнес-одиниці організації. Часто підприємства зосереджуються на обмеженій кількості ризиків і найчастіше на крадіжках третіми особами. Щоб уникнути цього, ризики слід класифікувати за можливим видом правопорушення та потенційним злочинцем.

Ризики шахрайства варто оцінювати для кожної сфери та процесу бізнесу, наприклад, грошові виплати, грошові надходження, продажі, закупівлі, витрати, запаси, нарахування заробітної плати, основні засоби та позики.

Таким чином, управління ризиком шахрайства в принципі таке ж, як управління будь-яким іншим бізнес-ризиком. По-перше, необхідно зрозуміти потенційні наслідки шахрайства для організації. Після цього ризики слід зменшити шляхом розробки та впровадження стратегії боротьби з шахрайством у всій організації. До цього найкраще підходить системно, як на організаційному рівні, наприклад, використовуючи політику етики та політику боротьби з шахрайством, так і на операційному рівні, запроваджуючи відповідні засоби контролю та процедури.

Враховуючи поширеність шахрайства та пов'язані з ним негативні наслідки, немає сумніву, що організації повинні витратити час і ресурси на боротьбу з шахрайством. Однак іноді ведуться дискусії щодо того, чи слід спрямовувати ці ресурси на запобігання чи виявлення шахрайства.

Виходячи з вищесказаного варто відзначити, що один із найефективніших способів боротьби з проблемою шахрайства полягає в застосуванні методів, які зменшують мотиви, обмежують можливість і зменшують здатність потенційних шахраїв раціоналізувати свої дії. У випадку навмисних шахрайських дій метою превентивного контролю є зменшення можливостей і усунення спокуси у потенційних правопорушників. Методи запобігання включають запровадження політики, процедур і

заходів контролю, а також такі дії, як навчання та підвищення обізнаності про шахрайство, щоб запобігти йому.

Запобігти збиткам вигідно, а діяльність із запобігання шахрайству може допомогти забезпечити стабільність та подальше існування бізнесу. Однак, виходячи з останніх опитувань, багато організацій не мають офіційного підходу до запобігання шахрайству. Якщо шахрайство вже відбулося, ймовірність повернення вкрадених коштів у зловмисника або за допомогою страхування часто є відносно низькою. Згідно з опитуванням KPMG, лише 16% організацій, які постраждали від шахрайства, змогли відшкодувати свої збитки. Хтось все ще намагається повернути вкрадені активи, але процес часто складний і тривалий.

Принаймні половині організацій взагалі не вдалося повернути жодного з активів. Таким чином, в першу чергу краще спробувати запобігти втраті, і відоме твердження «запобігти краще, аніж лікувати», безумовно, стосується й шахрайства. Однак слід пам'ятати, що методи запобігання шахрайству, хоч і варті інвестування, не можуть забезпечити 100% захисту. Важко, навіть неможливо, усунути всі можливості для його вчинення. Оскільки методи запобігання шахрайству не можуть зупинити всіх потенційних зловмисників, організації повинні забезпечити наявність систем, які своєчасно виявлятимуть випадки шахрайства. Стратегія виявлення шахрайства повинна передбачати використання аналітичних та інших процедур для виявлення аномалій, а також запровадження механізмів звітності, які забезпечують комунікацію щодо підозрюваних шахрайських дій. Ключові елементи комплексної системи виявлення шахрайства включатимуть повідомлення про винятки, аналіз даних, аналіз тенденцій і поточну оцінку ризиків.

Система виявлення шахрайства може вказати на поточне шахрайство, яке має місце, або правопорушення, які вже відбулися й збитки були понесені. Потенційне відшкодування збитків не є єдиною метою, але шахрайську поведінку не слід ігнорувати лише тому, що збитки можуть не відшкодуватися. Виявлення шахрайства також дозволяє вдосконалити внутрішні системи та засоби контролю. Багато шахрайств використовують недоліки в системах контролю. Завдяки виявленню таких випадків контроль може бути посилений, що ускладнить дії потенційних зловмисників у майбутньому.

Запобігання шахрайству та виявлення шахрайства відіграють свою роль, і малоімовірно, що одне з них досягне повного успіху без іншого. Тому важливо, щоб суб'єкти господарювання враховували як запобігання шахрайству, так і його виявлення при розробці ефективної стратегії протидії цьому явищу.

Далі вважаємо за доцільне, розглянути компоненти ефективної стратегії протидії шахрайству.

Ставлення всередині організації часто закладає основу для середовища з високим або низьким ризиком шахрайства. Там, де можуть допускатися незначні неетичні практики (наприклад, дрібні крадіжки, шахрайство з витратами), більші шахрайства, вчинені вищими рівнями управління, також можуть розглядатися подібним чином. У цьому середовищі може виникнути ризик повного краху організації або через одне велике шахрайство або через сукупність багатьох дрібних.

Організації, які витратили час на те, щоб обміркувати свою позицію в етичних питаннях, усвідомили, що високі етичні стандарти приносять довгострокові переваги як клієнтам, постачальникам, співробітникам і спільнота усвідомлює, що має справу з надійною організацією. Крім того останні усвідомили, що сумнівні етичні або шахрайські дії спричиняють серйозні несприятливі наслідки для усіх груп стейкхолдерів у разі їх викриття.

Організації, які створили позитивну етичну культуру, зазвичай або керувалися відданим цій ідеї керівником, або були змушені це зробити через інциденти, які спричинили або майже спричинили значні збитки для неї.

Що стосується створення здорової етичної культури, СІМА рекомендує організаціям:

- розробити заяву про місію, яка стосується якості або етики та визначає, як організація хоче, щоб її сприймали ззовні;
- мати чіткі політичні заяви щодо ділової етики та боротьби з шахрайством із поясненнями прийняттого та неприйняттого в організації;
- формувати поведінку в умовах ризику шахрайства;
- мати чіткий алгоритм, за допомогою якого можна повідомити про підозру в шахрайстві;
- мати прописаний процес нагадування про політику етики та протидії шахрайству – наприклад, щорічний лист або декларація;
- мати й підтримувати агресивний процес аудиту, який зосереджується на ключових сферах ризику;
- мати керівництво, яке всіма своїми діями показує відданість декларованим принципам.

Однак наявності кодексу етики чи політики боротьби з шахрайством недостатньо для його запобігання. Потрібна етична поведінка має бути вбудованою в культуру організації. Ключовими є відданість цьому найвищого керівництва, яке задає тон всій організації. Співробітники з більшою ймовірністю будуть робити те, що бачать у своїх керівниках, ніж просто дотримуватися задекларованої етичної поведінки. Вкрай важливо, щоб керівництво не застосовувало в цьому подвійних стандартів.

Саме на вище керівництво слід покласти відповідальність за політику запобігання шахрайству, оскільки це надсилає повідомлення працівникам про те, що організація серйозно ставиться до шахрайства, і гарантує, що питання боротьби з шахрайством розглядатимуться на вищому рівні. Відповідні особи в організації (наприклад, керівництво та/або внутрішній аудит) мають регулярно контролювати дотримання правил і кодексів, а

Майже кожного разу, коли відбувається серйозне шахрайство, багато працівників є мимоволі дотичними до цього, якщо не шоковані, то дуже здивовані тим, що не знали про те, що відбувається. Тому важливо підвищувати обізнаність за допомогою офіційної програми навчання як частини загальної стратегії управління ризиками. Особливу увагу слід приділяти тим керівникам і персоналу, які працюють у сферах високого ризику, таких як закупівлі та оплата рахунків і для тих, хто бере участь у запобіганні та виявленні шахрайства, наприклад, кадрові служби та персонал, відповідальний за розслідування.

Шахрайство часто проявляється через певні показники, тому дуже важливо, щоб усі працівники знали про те, що є шахрайством, як визначити шахрайську поведінку та як реагувати, якщо вони підозрюють або виявляють випадки шахрайства. Іноді є побоювання, що співробітники, навчені розпізнаванню певних шахрайських поведінкових шаблонів, можуть самі спробувати обійти загороджувальні засоби протидії. Проте, досвід багатьох західних компаній свідчить про те, що подібне навчання швидше зменшить, ніж збільшить кількість шахрайських випадків.

Створення ефективних механізмів звітності є одним із ключових елементів програми запобігання шахрайству та може позитивно вплинути на виявлення шахрайства. Дослідження показують, що про багато шахрайств знають або підозрюють люди, які не причетні до них. Завдання керівництва полягає в тому, щоб заохотити цих «невинних» людей висловитися, продемонструвати, що також є зацікавленими у

висвітлення подібних подій. Дослідження Institute of Business Ethics (IBE, Велика Британія) [14] показало, що хоча кожен четвертий працівник знає про неналежну поведінку на робочому місці, більше половини цих співробітників мовчать.

Вважається, що саме у вітчизняній національній традиції інститут «інформаторів» є чимось непристойним чи неприйнятним, проте, IBE також вказує на те, що у цій сфері існує багато суперечливих емоцій, які впливають на потенційного «інформатора»: відданість робочій групі чи сім'ї; незацікавленість, а то й приховане захоплення шахраєм; страх перед наслідками для себе; підозра, а не доказ.

Культура організації по боротьбі з шахрайством і процеси звітності можуть мати великий вплив на інформатора, оскільки часто на перше місце виходить страх перед наслідками. Для інформатора наслідки висловлювання щодо потенційного шахрайства можуть бути досить суттєвими, починаючи від звільнення і до того, що його уникають інші співробітники. Якщо ж шахрайство вчиняється керівниками вищої ланки (а це може бути навіть генеральний директор), тоді скрутне становище, з яким стикається викривач, ще більше загострюється.

І саме в цьому полягає найбільший виклик для керівництва – переконати персонал, що кожен несе відповідальність за боротьбу з шахрайством і що здоров'я організації та, можливо, їхня майбутня робота можуть бути під загрозою саме через шахрайство.

Організації, які заохочують відкритість і зможуть подолати культуру мовчання, можуть отримати багато переваг, адже вони зможуть краще: стримувати протиправні дії; завчасно виявляти потенційні проблеми; забезпечити надходження важливої інформації до людей, які мають її знати та можуть вирішити проблему; продемонструвати зацікавленням сторонам, в т.ч. регуляторним органам, що вони підзвітні та добре керовані; зменшити ризик анонімних і зловмисних витоків; мінімізувати витрати та компенсації від нещасних випадків, розслідувань, судових процесів і регуляторних перевірок; підтримувати та підвищувати свою репутацію.

Зазвичай, одним із найкращих способів повідомити про шахрайство є конфіденційна цілодобова гаряча лінія. Однак відкриті канали зв'язку між співробітниками та керівництвом також є важливими для створення середовища, яке заохочує запобігання та виявленню шахрайства. Культура відкритості та чесності має підвищити моральний дух працівників і надати їм впевненості, щоб вільно висловлювати свої занепокоєння.

На підтвердження цих висновків наведемо деякі аналітичні дані [8] (рис. 2).



Рисунок 2 – Джерела надходження інформації про можливі випадки шахрайства
Джерело: сформовано авторами на основі [8]

Як видно з рис. 2, найбільшим джерелом детектування шахрайських випадків є інформування від «джерел», яке майже втричі перевищує традиційний «внутрішній аудит». Досить цікавим моментом дослідження являє факт встановлення хто саме входить до складу цих «інформаторів» (рис. 3).

Таким чином, з рис. 3, спостерігаємо, що більше половини всієї інформації про шахрайства, які стали відомі завдяки інституції «інформаторів», надходить саме від працівників компаній. А в загальному переліку всіх джерел (рис. 2), саме дані про шахрайства, отримані від працівників компанії дає більше інформації ніж внутрішній аудит. Безперечно, виключно системний підхід дозволяє вказаним компонентам доповнювати один одного та активно протидіяти шахрайствам.

ACFE вважає сильну систему внутрішнього контролю «найціннішим засобом запобігання шахрайству з великим відривом».

Загальна відповідальність за систему внутрішнього контролю організації має бути на найвищому рівні в організації. Тобто, тільки тоді, коли найвище керівництво організації формує ідеологію створення системи внутрішнього контролю та вимагає неухильного дотримання прописаних в неї процедур та механізмів, така система має шанс не тільки на ефективну роботу, а й взагалі на існування.

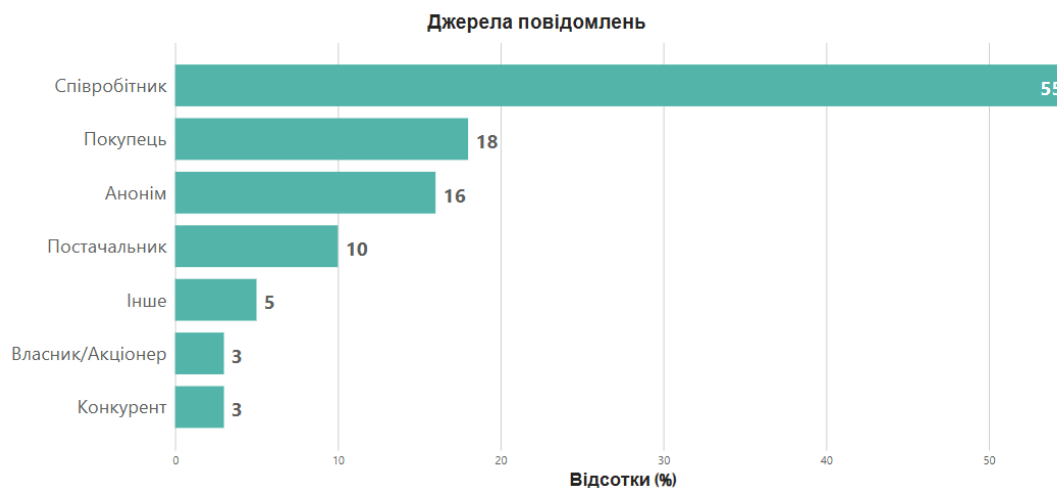


Рисунок 3 - Деталізація джерел надходження 42% інформації про шахрайство
Джерело: сформовано авторами на основі [8]

Система внутрішнього контролю включає в себе всі ті політики та процедури, які, разом узяті, підтримують ефективну роботу організації. Внутрішній контроль, зазвичай, стосується таких факторів, як процеси затвердження та авторизації, обмеження доступу та контроль транзакцій, звірка рахунків і безпека. Ці процедури часто включають розподіл обов'язків і систему стримувань і противаг, щоб зменшити ризик.

Скрізь, де запроваджуються нові процедури внутрішнього контролю, вони мають бути чітко та просто задокументовані, щоб можна було виявити будь-які відхилення. Внутрішній контроль слід регулярно переглядати як частину процесу управління ризиками, і слід постійно вдосконалювати контроль у світлі нових ризиків, таких як нові ринки та технології, зміни в структурі або нові інноваційні методи шахрайства. Зрештою, система внутрішнього контролю має бути вбудованою в культуру та діяльність організації.

Перевірка перед прийомом на роботу – це процес перевірки кваліфікації, придатності та досвіду потенційного кандидата на роботу. Використовувані методи

включають підтвердження освітньої та професійної кваліфікації, перевірку досвіду роботи, перевірку кримінальної історії тощо.

Перевірка кандидатів повинна зменшити ймовірність людей з проблемною історією, в т.ч. з вірогідністю вчинення в минулому шахрайських дій, і тому є важливою процедурою запобігання шахрайству. Значна частина резюме містить не тільки серйозні неточності, але й просто неправдиві відомості, а в розслідуваних випадках шахрайства часто є ознаки в минулому працівника, які були б попередженням для потенційного роботодавця, якби перевірку було проведено належним чином. Дослідження також показали, що роботодавці, які проводять перевірку перед прийомом на роботу, стикаються з меншою кількістю випадків шахрайства з боку працівників.

Організаціям слід принаймні розглянути можливість перевірки на посади, що працюють з готівкою, посади вищого керівництва та інші чутливі посади, такі як казначейство, робота з заборгованістю чи охорона. Перевірка також не повинна обмежуватися тільки новими співробітниками. Організація повинна проводити перевірки, перш ніж пропонувати просування по службі на більш високі або більш чутливі посади.

Далі, вважаємо за доцільне, більш детально зосередити увагу на методах виявлення шахрайських дій, певних індикаторах та засобах захисту.

Ретроспектива – чудова річ для аналізу випадків шахрайства та створення перешкод для подібних дій у майбутньому. Такі компанії, як PwC, Kroll, KPMG та ACFE постійно проводять дослідження для виявлення найбільш дієвих методів детектування шахрайських посягань.

На рис. 4 представлені найбільш поширені методи виявлення найбільш серйозних шахрайських дій для регіону Східна Європа та Західна/Центральна Азія (рис. 4).

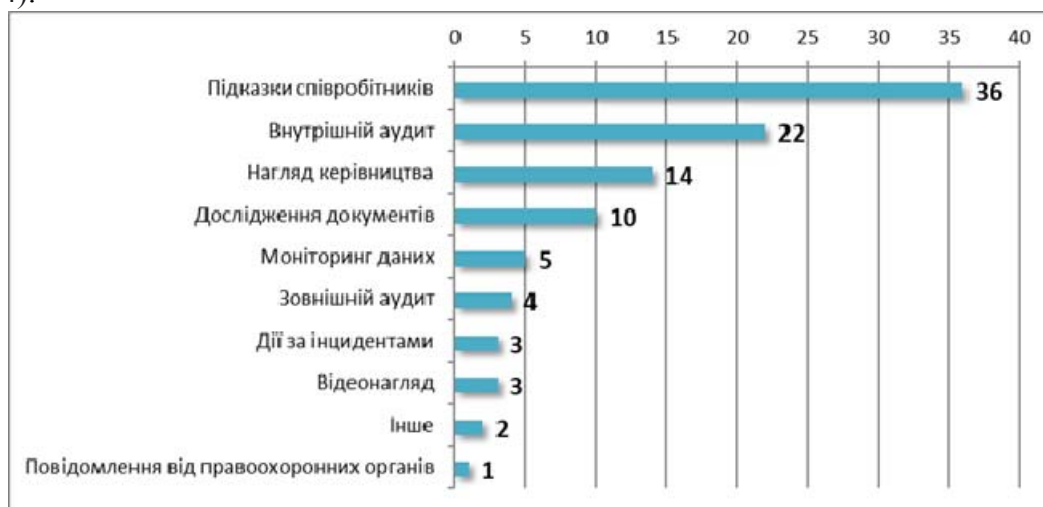


Рисунок 4 – Основні методи виявлення шахрайства для регіону Східна Європа та Західна/Центральна Азія, дані у % від загального числа виявлених випадків

Джерело: сформовано авторами на основі [8-10]

Як видно з рис. 4, зовнішні аудитори, як виявляється, є суттєво менш дієвим інструментом ніж внутрішній аудит. Таким чином, якщо ресурси дозволяють це, організація повинна створити сильну структуру внутрішнього аудиту, яка контролює та проводить консультації щодо управління ризиками та активно шукає випадки шахрайства.

Проте, основним методом протидії шахрайству є метод інформування від зацікавлених співробітників. Багато випадків шахрайства виявляється саме завдяки

вірно побудованої системи повідомлення про ознаки таких дій. І саме, коли кожний співробітник буде задіяний в процесі знаходження та повідомлення про можливі випадки шахрайства, та розуміти, що це в його інтересах, подібна практика буде все більше розповсюджуватися. Задачею ж керівництва є створення всіх умов, в т.ч. відповідних «гарячих ліній», механізмів звітності тощо, для сприяння цьому.

Повністю запобігти шахрайству не вдасться ніколи. Жодна система не є повністю захищеною від цього, оскільки багато шахраїв можуть обійти системи контролю. Однак більша увага до деяких найпоширеніших індикаторів може дати «раннє попередження» про те, що щось не так, і збільшити ймовірність того, що шахрая буде виявлено. Зважаючи на це, далі наведемо деталі деяких найпоширеніших ознак шахрайства.

Індикатори шахрайства можна поділити на дві категорії: попереджувальні знаки та «дзвінки» про шахрайство.

Попереджувальні знаки не обов'язково означають наявність шахрайських дій. Це, радше, інформація, на яку слід звернути увагу у разі її появи. Їх можна описати як певні індикатори ризику шахрайства, і деякі приклади наведено нижче. Для зручності їх було розділено на бізнес-ризик, фінансові ризик та ризик для ІТ та даних.

Бізнес-ризик, в свою чергу, можна поділити на аспекти корпоративної культури, управління, аспект щодо роботи співробітників, процесійний та транзакційний аспекти.

Аспект корпоративної культури:

- відсутність політики та культури боротьби з шахрайством;
- неспроможність керівництва запровадити надійну систему внутрішнього контролю та/або продемонструвати відданість їй у будь-який час.

Аспект управління:

- відсутність досвіду управління фінансами та професіоналізму щодо ключових принципів бухгалтерського обліку;
- напружені відносини всередині організації між керівництвом і внутрішніми або зовнішніми аудиторами;
- відсутність управлінського нагляду за персоналом;
- відсутність чіткого управлінського контролю відповідальності, повноважень, делегування тощо;
- бонусні схеми, пов'язані з амбітними цілями або безпосередньо з фінансовими результатами без урахування політики протидії шахрайству.

Аспект щодо роботи співробітників:

- неадекватні процеси найму та відсутність перевірки;
- незвично близькі стосунки – внутрішні та зовнішні;
- потенційне або фактичне скорочення чи звільнення робочої сили;
- незадоволені працівники, які мають доступ до бажаних активів;
- незвичайні моделі поведінки персоналу, особливо якщо вони виникли нещодавно;
- низький рівень заробітної плати ключового персоналу;
- незадовільний рівень поширення внутрішнього контролю;
- працівники, які багато працюють у додатковий час без нагляду;
- працівники, які не беруть щорічну відпустку;
- небажання розподіляти/делегувати власні обов'язки.

Процесійний аспект:

- відсутність розподілу робочих місць і незалежної перевірки ключових операцій;

- відсутність ідентифікації того чи іншого активу;
- незадовільний рівень підзвітності керівництва та системи звітності;
- незадовільний рівень фізичної безпеки активів;
- незадовільний рівень контролю доступу до фізичних активів та систем безпеки ІТ;
- відсутність та/або неадекватність внутрішнього контролю;
- незадовільний рівень документування внутрішнього контролю.

Транзакційний аспект:

- незадовільний рівень документального забезпечення для конкретних транзакцій, таких як знижки та відвантаження в кредит;
- великі обсяги операцій з готівкою;
- наявність активів, які можна легко незаконно привласнити.

Фінансовий ризик:

- компенсація керівництва сильно залежить від досягнення агресивних цільових показників;
- значний тиск на керівництво з метою отримання додаткового фінансування;
- широке використання різних, навіть законних, методів оптимізації оподаткування без чіткого бізнес-обґрунтування;
- занадто складні операції;
- невиправдане використання складних фінансових продуктів;
- складна юридична форма власності та/або організаційна структура;
- швидкі зміни прибутковості.

Ризик ІТ та даних:

- можливість несанкціонованого доступу до систем з боку співробітників або зовнішніх контрагентів;
- велика кількість незвичайного програмного забезпечення та інструментів;
- швидкі зміни в застосуванні тих чи інших інформаційних технологій;
- користувачі, які не застосовують належні методи безпеки комп'ютера, наприклад, не застосовують паролі, не оновлюють їх та/або обмінюються ними;
- можливість несанкціонованої та довільної зміни даних в облікових системах;
- порушення безпеки та конфіденційності даних з загрозою їх викрадення, втрати або витоку.

«Дзвінок» про шахрайство можна описати як конкретні події або «червоні прапорці» («red flags»), які можуть свідчити про шахрайство. Як і індикатори, наведені вище, вони не свідчать про те, що відбуваються саме шахрайські дії, проте, рівень тривоги значно підвищується. А якщо такі «червоні прапорці» накладаються на індикатори, то вірогідність вчинення шахрайських дій суттєво підвищується.

Перелік можливих «дзвінків» про шахрайство виглядає наступним чином:

- невідповідність заробітку й способу життя;
- незвично близькі відносини з постачальником або клієнтом;
- більш часті випадки усамітнення для ведення телефонних розмов;
- електронні листи, надіслані в незвичайний час, із непотрібними вкладеннями або незвичним адресатам;
- наявність проблем в сім'ї (фінансові труднощі, розлучення тощо);
- скарги на неадекватну оплату праці;
- незвичайна, ірраціональна або непослідовна поведінка, особливо якщо вона змінилася нещодавно, дратівливість, підозрілість та часта активація захисної поведінки;
- часта заміна документів або зміна записів в обліковій системі;
- наявність тільки копій документів замість оригіналів;

- широке використання факсиміле замість оригінального підпису;
- розбіжності в підписах та/або почерку;
- дії, які потребують авторизації або схвалення, виконуються без них;
- операції, ініційовані без відповідних повноважень;
- незрозумілі коригування запасів;
- широке використання тимчасових, «підвішених», документів замість остаточних;
- купівля матеріальних цінностей понад потребу;
- збільшення більше середньої кількості невдалих спроб авторизації у обліковій чи платіжній системах;
- доступ до систем у неробочий час або за межами звичайної робочої зони;
- елементи логуювання доступні для змінення або вимкнення.

Даний список не слід вважати вичерпним, оскільки такі «дзвінки» можуть існувати у багатьох різних формах залежно від сфери діяльності, практики ведення бізнесу та інших обставин. Також, як було вказано вище, для певних бізнес-процесів або напрямків діяльності вказані «дзвінки» можуть бути іншими або видозмінюватися.

Тренінги, які проходять співробітники, є гарною основою для впровадження програми боротьби з шахрайством. Широке розуміння бізнес-процесів, яке очікується від того ж бухгалтера з управлінського обліку, є важливою перевагою, як і його знання систем та процедур, які мають існувати в організації, щоб дозволити їй працювати ефективно та результативно. Ще одним активом є здатність мислити та діяти логічно, яка розвивається з досвідом. Тому першим важливим доступним інструментом є навчання та досвід.

Другим інструментом є необхідність прийняття того факту, що шахрайство завжди можливе. Під час розгляду ситуацій слід зберігати здорову частку професійного скептицизму щодо можливості шахрайства. Це не означає, що кожного разу, коли хтось працює понаднормово, не беручи відпустки, він перебуває в процесі вчинення шахрайства, або що неточності в облікових записах існують, щоб приховати шахрайство. Тим не менш, вони все ж таки можуть про це свідчити. Розглянувши можливість шахрайства, наступним кроком може бути проведення додаткових досліджень або інформування безпосереднього керівника про можливе джерело небезпеки.

Крім того, існують повсякденні методи, які допомагають ідентифікувати порушення, які, теоретично, можуть вказувати на шахрайство, і дослідити аномалію, щоб вирішити, чи потрібно вживати подальших заходів. Організації повинні забезпечити виділення ресурсів для виявлення таких аномалій і випадків шахрайства шляхом наступних заходів:

1. Постійна інформованість. Важливо бути в курсі тенденцій і проблем шахрайства. Серед джерел інформації можуть бути як звичайна преса, так і спеціальні видання, які часто публікують матеріали про випадки шахрайства. Також корисною є участь у тематичних заходах: вебінарах, конференціях, сесіях тощо.

2. Оцінка ризику. Необхідно провести оцінку ризику шахрайства та розробити спеціальні перевірки для виявлення значних потенційних видів шахрайства, які були виявлені (навіть потенційно) під час оцінки ризику. Необхідно добитися реакції керівництва на потенційні порушення, які викликають занепокоєння.

3. Компаративний аналіз. Порівняння одного фінансового періоду з іншим, або продуктивності одного центру витрат або бізнес-одиниці з іншим, або загальної ефективності бізнесу з галузевими стандартами. Все це може виявити аномалії, які заслуговують на подальше дослідження.

4. Аналіз систем. Важливо вивчити наявні системи (облікові, бізнесові, процедурні) та виявити будь-які слабкі місця, які можуть стати можливостями для шахраїв.

5. Аналіз співвідношення. Може використовуватися для виявлення будь-яких ненормальних чи незвичних тенденцій або моделей.

6. Математичні методи. Використання методів математичної статистики може допомогти визначити закономірності в облікових даних чи у певних подіях. Існують також спеціальні математичні моделі, такі як закон Бенфорда, який може допомогти виявити порушення в фінансових документах.

7. Спеціалізоване програмне забезпечення. Дозволяє проводити аналіз, наприклад оцінку транзакцій у режимі реального часу, цільовий аналіз після транзакцій або аналіз облікових записів.

8. Звітування про виняткові ситуації. Багато систем можуть створювати автоматичні звіти для результатів, які виходять за межі заздалегідь визначених порогових значень (винятки), що дозволяє негайно ідентифікувати результати, що відхиляються від норми. Завдяки сучасним технологіям можна відразу надіслати сповіщення електронною поштою або у месенджер безпосередньо відповідальній особі чи групі осіб. Також можна автоматично вести блог таких повідомлень, який сам по собі також може стати джерелом інформації для оцінювання ефективності системи внутрішнього контролю.

Багато з вказаних методів можна автоматизувати аби зробити процес більш ефективним. Системи виявлення шахрайства слід регулярно контролювати та оновлювати в контексті сучасних технологічних змін та нових методів маніпулювання.

Усі інструменти, розглянуті до цього моменту, застосовуються для виявлення невідповідності, але щоб бути ефективними, вони повинні поєднуватися з методичним підходом до аналізу виявленої проблеми. На цьому етапі це ще не розслідування шахрайства чи внутрішня перевірка, а аналіз проблеми, щоб вирішити, чи слід проводити таку перевірку. Далі, вважаємо за доцільне, навести один із підходів, який слід розглянути більш детально:

1. Необхідно встановити мету. Мета дослідження має бути чіткою, оскільки це дозволить прийняти рішення щодо найкращого шляху.

2. Необхідно визначити системи та процедури: проведення системного аналізу та аналізу ризиків, а також порівняння встановлених систем і процедур, які мали бути на місці, з тими, що фактично використовуються, може допомогти виявити системні або процедурні збої.

3. Необхідно встановити можливий масштаб ризику, що передбачає визначення потенційних втрат і оцінку їх суттєвості. По можливості слід визначити фактичні втрати, які вже є чи можуть бути на поточний момент.

4. Аналіз ситуації, що передбачає попередні дослідження, наприклад, пошуки кола причетних осіб та/або компаній.

5. Повний аналіз всіх доступних даних, що дасть розуміння того, коли, що і яким саме чином це сталося.

6. Розробити графічну форму представлення інформації: необхідно підготувати графічні представлення ситуації (графіки та/або таблиці за необхідністю), щоб ті, хто приймає рішення, проте не має специфічних фінансових або галузевих знань, було якомога легше зрозуміти, що відбулося та які наслідки.

7. Необхідно підготувати звіт, який має містити всі дані, які були отримані на попередніх етапах та, за потреби, графічну інформацію. Також слід дотримуватися того, щоб звіт містив встановлені факти і, якщо висловлюється думка, вона має бути

чітко визначена професійна та бути відокремлена від фактів, незважаючи на можливість того, що факти є її базисом.

Отже, наведені приклади конкретних сповіщень про шахрайство, пов'язаних із діяльністю, є характерними для більшості типів організацій. Однак жоден з них не принесе користі, якщо не буде прийнято, що шахрайство принципово можливе. Саме таке мислення, така обізнаність дозволить організації зупинити випадки шахрайства, перш ніж вони стануть катастрофічними. Всі попереджувальні сигнали та «дзвінки» не будуть ефективними, якщо після них не відбувається реагування. Механізми реагування на «red flags» заслуговують увагу в межах подальшої наукової розвідки, тож, можна лише зауважити, що вкрай важливо аби організації мали задокументований план реагування на підозрювані або виявлені випадки шахрайства. План протидії шахрайству повинен включати: чітке положення про корпоративну політику щодо боротьби з шахрайством; визначення ролей і обов'язків тих, хто бере участь у реагуванні на підозри; має бути описано, як слід проводити розслідування, забезпечуючи дотримання належної процесуальної процедури та збереження цілісності доказів; мають бути детально описані подальші дії, які буде вжито організацією у світлі встановлених випадків шахрайства.

Висновки та перспективи подальших досліджень. Таким чином, у підсумку можна виділити ключові аспекти внутрішнього шахрайства у бізнесі, які визначають його складність та актуальність боротьби з цією проблемою. Виникнення шахрайства пов'язане з рядом соціально-економічних чинників, що ускладнює виявлення та протидію; шахрайство, було, є і буде у бізнес-середовищі. Як наслідок, шахрайство призводить до серйозних фінансових втрат, погіршення репутації та втрати довіри співробітників та партнерів. Шахрайство може приймати різні форми, включаючи фінансове, корпоративне та кіберзлочини, що потребує різноманітних стратегій протидії. Поряд із тим, обманливий характер шахрайства та його часто непомітність роблять складним процес виявлення та усунення цього явища. Відсутність точних даних та неповна статистика ускладнюють оцінку розмірів проблеми та розробку ефективних стратегій протидії. З урахуванням цих аспектів стає очевидною необхідність системного підходу до протидії внутрішньому шахрайству в бізнесі, що включає в себе вдосконалення систем контролю, збільшення свідомості та етичної складової корпоративної політики. Також варто відмітити, що навіть у відомій моделі «Трикутник шахрайства», безпосередній адміністративний вплив можливий лише на один чинник – «можливість». Проте інші чинники («Мотивація» та «Раціоналізація») лежать за межами суто адміністративних дій. Їх природа криється радше у психології, тож питання протидії шахрайству більш ефективно, на нашу думку, буде вирішуватися на стику дисциплін: менеджменту та психології, що дає передумови до висунення гіпотез як до психологічного портрету потенціального корпоративного шахрая, так і до засобів його виявлення ще до того моменту, коли він може здійснити свої наміри. Перспективним напрямком подальших досліджень є адаптація зарубіжних практик протидії корпоративному шахрайству в сучасному бізнес-середовищі та розробка засобів зниження рівня опору змінам інституційного середовища.

Список літератури

1. Борис С. А. Шахрайство на підприємстві: причини та наслідки, виявлення та протидія. *Юрист Закон*. 2019. № 9. URL: <http://surl.li/gnlbe> (Дата звернення: 04.04.2024).
2. Клишко Т. Ю., Мельник О. О. Корпоративне шахрайство: реалії сучасності. *Науковий вісник Ужгородського університету. Серія: Економіка*. 2015. Вип. 2. С. 185-190. URL: http://nbuv.gov.ua/UJRN/Nvuuec_2015_2_33 (Дата звернення: 22.04.2024).
3. Кримінальний Кодекс України. URL: <https://zakon.rada.gov.ua/laws/show/2341-14#Text> (Дата

- звернення: 30.04.2024)
4. Нежива М. О., Мисюк В. О. Протидія шахрайству в умовах війни. *Бізнес Інформ*. 2023. № 1. С. 160 – 166. DOI: <https://doi.org/10.32983/2222-4459-2023-1-160-166> (Дата звернення: 22.04.2024).
 5. Хамига Ю. Я. Фінансове шахрайство: критерії ідентифікації та напрями мінімізації. Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 072 «Фінанси, банківська справа та страхування», 2020. 308 с.
 6. ACFE. Data on fraud, fraudsters and anti-fraud programs. URL: <https://www.acfe.com/fraud-resources/reports-and-statistics> (Дата звернення: 10.05.2024)
 7. IMF. World Economic Outlook. URL: <https://www.imf.org/en/Publications/WEO> (Дата звернення: 15.04.2024)
 8. KPMG. Global profiles of the fraudster. URL: <https://kpmg.com/be/en/home/insights/2016/05/global-profiles-of-the-fraudster.html> (Дата звернення: 12.05.2024)
 9. Kroll. Fraud and Financial Crime Report 2023. URL: <https://www.kroll.com/en/insights/publications/fraud-and-financial-crime-report> (Дата звернення: 10.04.2024)
 10. Occupational Fraud 2022: A Report to the Nations. URL: https://legacy.acfe.com/report-to-the-nations/2022/?_ga=2.81367959.1833531643.1704446443-705041068.1704446063 (Дата звернення: 10.04.2024)
 11. PwC's Global Economic Crime and Fraud Survey 2022. URL: <https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html> (Дата звернення: 14.04.2024)
 12. Research: Why Corporate Fraud Reports are Down. URL: <https://hbr.org/2020/07/research-why-corporate-fraud-reports-are-down> (Дата звернення: 12.04.2024)
 13. The Chartered Institute of Management Accounts. URL: <https://www.aicpa-cima.com/home> (Дата звернення: 17.04.2024)
 14. The Fraud Triangle. A model for identifying high risks of fraud highlights three factors that lead to fraud: motivation, opportunity, and rationalization. URL: <https://www.whistleblowers.org/> (Дата звернення: 10.04.2024)
 15. What is the ethical issue? URL: <https://www.ibe.org.uk/knowledge-hub/speak-up.html> (Дата звернення: 17.04.2024)

References

1. Borys S. A. (2019) Shakhraistvo na pidpriemstvi: prychyny ta naslidky, vyjavlennia ta protydiia [Fraud in the enterprise: causes and consequences, detection and counteraction]. *Yuryst Zakon – Lawyer Law*. <http://surl.li/gnlbe> [In Ukrainian]
2. Klymko T. Yu., Melnyk O. O. (2015). Korporatyvne shakhraistvo: realii suchasnosti [Corporate fraud: modern realities]. *Naukovyi visnyk Uzhhorodskoho universytetu – Scientific Bulletin of Uzhhorod University Seriya: Ekonomika*. <http://nbuv.gov.ua/UJRN/Nvuuec> [in Ukrainian].
3. Kryminalnyi Kodeks Ukrainy. <https://zakon.rada.gov.ua/laws/show/2341-14#Text> [in Ukrainian].
4. Nezhyva, M. O. & Mysiuk, V. O. (2023). Protydiia shakhraistvu v umovakh viiny [Anti-Fraud During the War]. *Biznes Inform – Business Inform*. <https://doi.org/10.32983/2222-4459-2023-1-160-166> [in Ukrainian].
5. Khamyha Yu. Ya. (2020). *Financial fraud: identification criteria and directions for minimization*. Candidate's thesis, 308.
6. ACFE. Data on fraud, fraudsters and anti-fraud programs. <https://www.acfe.com/fraud-resources/reports-and-statistics> [in English].
7. IMF. World Economic Outlook. <https://www.imf.org/en/Publications/WEO> [in English].
8. KPMG. Global profiles of the fraudster. <https://kpmg.com/be/en/home/insights/2016/05/global-profiles-of-the-fraudster.html> [in English].
9. Kroll. Fraud and Financial Crime Report 2023. <https://www.kroll.com/en/insights/publications/fraud-and-financial-crime-report> [in English].
10. Occupational Fraud 2022: A Report to the Nations. https://legacy.acfe.com/report-to-the-nations/2022/?_ga=2.81367959.1833531643.1704446443-705041068.1704446063 [in English].
11. PwC's Global Economic Crime and Fraud Survey 2022. <https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html> [in English].
12. Research: Why Corporate Fraud Reports are Down. <https://hbr.org/2020/07/research-why-corporate-fraud-reports-are-down> [in English].
13. The Chartered Institute of Management Accounts. <https://www.aicpa-cima.com/home> [in English].
14. The Fraud Triangle. A model for identifying high risks of fraud highlights three factors that lead to fraud: motivation, opportunity, and rationalization. <https://www.whistleblowers.org/> [in English].
15. What is the ethical issue? <https://www.ibe.org.uk/knowledge-hub/speak-up.html> [in English].

Ihor Haidukov, Director LLC "ILVIS"

Ilova Androshchuk, Associate Professor, PhD in Economy

Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine

Peculiarities of Corporate Fraud in Business: Essence, Consequences and Countermeasures in the Context of Resistance to Change

The paper is devoted to the peculiarities of corporate fraud in business: essence, consequences and countermeasures in the context of resistance to change. The purpose of the study is to analyze corporate fraud, regardless of the places of occurrence, its signs and means of countermeasures, precisely as a system that combines both preventive and control measures. The analysis of approaches to the classification of fraud was carried out. The most common types of fraud were thoroughly examined. The amount of financial losses from fraud was determined. The investigation of the factors that encourage employees to commit fraud was conducted. The structure of the fraud triangle was analyzed: motivation, opportunity and rationalization. The "typical look" of the fraudster has been formed. The traits that are characteristic of fraudsters have been established. The peculiarities of the structural divisions of enterprises from the point of view of the level of fraud risk were defined. The components of the effective anti-fraud strategy has been considered, namely: creating a decent ethical culture, training and raising awareness of fraud risks, mechanisms for reporting and reporting corruption, building an internal control system, and pre-employment screening. The analysis of the sources of information on possible cases of fraud was carried out. The methods of detecting fraudulent actions were studied. The key indicators of fraud have been identified as follows: warning signs and "calls" about fraud. A list of "calls" that serve as a signal to commit fraudulent actions has been proposed. The key aspects of internal fraud in business, which determine its complexity and the importance of fighting this problem, have been formulated, in particular: social and economic reasons, unforeseen consequences, various types of fraud, difficulty of detection, practical difficulties in collecting statistics.

corporate fraud, business, resistance to change, senior management, fraud triangle

Одержано (Received) 10.05.2024

Прорецензовано (Reviewed) 24.05.2024

Прийнято до друку (Approved) 27.05.2024

УДК 339.1

JEL Classification: M31

DOI: [https://doi.org/10.32515/2663-1636.2024.11\(44\).84-93](https://doi.org/10.32515/2663-1636.2024.11(44).84-93)

В.В. Голуб, здобувач третього (освітньо-наукового) рівня вищої освіти

Університет митної справи та фінансів, м. Дніпро, Україна

Соцмедіа як інструмент для політики просування та комунікації з споживачами

У статті розглядається використання соціальних медіа вітчизняними компаніями для спілкування зі споживачами та потенційними клієнтами. Виокремлено переваги їх використання, такі як низька вартість, простота та швидкість аналізу аудиторії, а також адаптація продуктів і послуг до потреб споживання людей. В умовах соціальної інформатизації мережа Інтернет відкриває безліч можливостей використання різних маркетингових інструментів для впливу на споживачів і просування продукції. Останніми роками соціальні медіа відіграли важливу роль у встановленні ефективних взаємовідносин між користувачами мережі Інтернет, у передаванні та обміні даними. Проте, не вся інформація в Інтернеті використовується повною мірою. Соціальні медіа допомагають змінити суспільний дискурс та надають платформу для формування маркетингової політики на найрізноманітніших ринках ведення підприємницької діяльності. У зв'язку з цим компаніям слід звернути на них особливу увагу.

Підприємства, новинні журнали та медіа-компанії дедалі частіше прагнуть використовувати соціальні медіа у своїх маркетингових комунікаціях для аналізу тенденцій й прогнозування майбутніх подій. Адже це ефективний маркетинговий інструмент, що дає змогу охопити широку аудиторію. Крім того, вони можуть істотно вплинути на формування думки користувачів про компанію, продукт або бренд. Сьогодні більшість підприємств створюють власні сайти і спільноти в багатьох популярних соціальних медіа, за допомогою яких взаємодіють зі своєю цільовою аудиторією. Водночас, хоча Інтернет є невід'ємною частиною економічної діяльності, не всі підприємства ефективно використовують інструменти соціальних медіа.

© В.В. Голуб, 2024