

5. ГРОШІ, ФІНАНСИ І КРЕДИТ

DOI: <https://doi.org/10.32782/2523-4803/72-3-8>

УДК 336:343.53

Данік Н.В.

кандидат економічних наук, доцент,
Миколаївський національний університет імені В.О. Сухомлинського

Рудь І.Ю.

кандидат економічних наук, доцент,
Миколаївський національний університет імені В.О. Сухомлинського

Пащенко О.В.

магістрант,
Миколаївський національний університет імені В.О. Сухомлинського

Danik Nataliia, Rud Inna, Pashchenko Olena

Mykolaiv National University named after V.O. Sukhomlynskyi

ОЦІНКА СТРАТЕГІЙ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ ФІНАНСОВОМУ ШАХРАЙСТВУ ЗА ВИДАМИ

У статті розглянуто найпоширеніші види, типи та способи здійснення фінансових шахрайств у світі. Вивчено найнебезпечніші схеми шахрайства. Досліджено вплив шахрайських дій на виробничу діяльність підприємств, фінансову діяльність банків, та взагалі життя пересічних громадян, адже фінансове шахрайство є проблемою з далекосяжними наслідками у фінансовій індустрії, уряді, корпоративному секторі та для звичайних споживачів. Проаналізовано наслідки від здійснення різного виду шахрайств. Наведено статистичні дані щодо кількості здійснених шахрайств у сферах, де вони були викриті чи про них відомо, адже щохвилини посилюється залежність від нових технологій, таких як хмарні та мобільні обчислення, що дуже ускладнює проблему. Надано пропозиції щодо попередження, ухвалення чи запобігання шахрайських дій.

Ключові слова: фінансове шахрайство, втрати, методи виявлення шахрайства, аналіз даних, втрати, попередження, запобігання.

Постановка проблеми. Фінансове шахрайство є проблемою, яка несе негативні наслідки як у фінанси установ і організацій, так і у повсякденне життя людей. Шахрайство знижує довіру до банків, фінансових посередників, дестабілізує економіку та впливає на вартість життя людей. Тому, вирішення цієї проблеми має глибоку практичну значимість та науковий інтерес.

Аналіз останніх досліджень і публікацій. Значний внесок у дослідження різних аспектів економічної злочинності, зокрема й у сфері фінансів зробили такі зарубіжні та вітчизняні вчені: Дж. Іген, П. Ван дер Нет, О. Карповіч, В. Кіп, Т. Коєнен, Д. Крессі, Х. Кроял, В. Ларічев, Т. Робен, І. Сюзерленд, Д. Хіман, Дж. Хюгес, Г. Возняк, О. Кириленко, Т. Кізима, Ю. Клапків, О. Колодізєв, С. Мельник, Л. Шарінян, С. Юшко. Отже, невеликий обсяг досліджень у сучасній українській фінансовій науці, які б цілеспрямовано і комплексно висвітлювали проблему фінансового шахрайства з точки зору його фінансових ефектів та

економічних наслідків, обумовив актуальність теми даної статті, та визначив її мету, завдання і структуру.

Формулювання цілей статті. Дослідити можливості виявлення та запобігання випадкам фінансового шахрайства.

Виклад основного матеріалу. Фінансове шахрайство – це давній бізнес. Так, саме бізнес. Відомо, що перше зареєстроване шахрайство сталося в Стародавній Греції, коли двійко хитрих морських торговців намагалися вчинити шахрайство, навмисно потопивши свій застрахований човен (але один з них невдало втопився під час цієї спроби). Однак сьогоднішнє шахрайство інформаційної епохи є набагато витонченішим і менш схильним до водних небезпек. Але багато шахраїв все ще використовують ті самі стратегії, перевірені та вдосконалені шахраями протягом століть. Здатність виявляти та запобігати випадкам шахрайства ще ніколи не була такою важливою для фінансових організацій усіх видів як зараз.

Шахрайська діяльність виснажує фінансові рахунки мільйонів щороку. Зі зловмисниками, які постійно адаптуються до нових заходів безпеки та перехитрують навіть добре продумані засоби внутрішнього контролю, комплексне запобігання шахрайству може здаватися непомірно дорогим і неефективним. Але, і протидія шахрайству, необхідна для прийняття організацією обґрунтованих рішень щодо виявлення та запобігання шахрайству, має перспективи на майбутнє.

Шахрайство не тільки підриває всі аспекти суспільства, від окремих домогосподарств до інтересів національної безпеки, але також завдає виняткової шкоди фінансовим організаціям. Випадки шахрайства можуть призвести до: масових фінансових втрат, втрати довіри та впевненості в їхніх послугах, державних розслідувань та карних заходів, втрати доходу [1, с. 185–190].

Банківські установи в усьому світі втрачають приблизно 5% доходу на рік через шахрайство. Витрати через шахрайство швидко перевищують витрати на моніторинг та запобігання шахрайству.

Згідно з останніми звітами, справжня ціна шахрайства зростає. Кожен долар, втрачений через шахрайство, тепер коштує фінансовим компаніям 4,00 долара, що на 27% більше, ніж у 2020 році. Ці витрати включають: втрачені транзакції, комісії та відсотки під час обробки, витрати на повернення коштів, витрати на розслідування та відновлення, штрафи та інші судові витрати. Це означає, що якщо клієнта ошукано на 800 доларів США, фактична вартість для його банку тепер становитиме 3200 доларів США. Помножьте це на тисячі або навіть мільйони клієнтів, і навіть дрібні схеми шахрайства стануть масштабною проблемою [2].

Більшість людей не почуватимуться в безпеці, якщо їхні заощадження засунуті під матрац або гроші, вкладені в компанію, яку буде легко пограбувати. Банки призначені для захисту фінансів і активів. Втрата репутації безпосередньо призводить до зниження довіри клієнтів та інвесторів. Управління репутаційним ризиком фінансової організації має включати запобігання фінансовому шахрайству. Дослідження показують, що репутаційна шкода коштує так само дорого, як і державні штрафи, головним чином, коли це впливало на ціни акцій.

Якщо розслідування шахрайства виявить систематичні порушення безпеки або корупцію, фінансова установа також може втратити прибуткові ділові відносини. Це включає сторонніх продавців, постачальників і підрядників. Послідовні дослідження показали, що протягом десятиліть заощадження клієнтів були вирішальними для отримання прибутку. Відносини між клієнтом і банком ґрунтуються на довірі з обох сторін.

Банк не можуть мати багато клієнтів, які втрачають свої зарплати, іпотечні кредити чи заощадження через шахрайство. Це означає, що від шахрайства банки втрачають подвійно: або відшкодовують втрачені кошти, або втрачають понад чверть своєї клієнтської бази. Перед банками стоїть додаткове завдання зробити виявлення шахрайства максимально простим.

Будь-який бізнес із надто великими перебоями, включаючи банки, необанки, фінтех-компанії тощо, зрештою зазнає краху, оскільки клієнти все частіше вибирають більш зручні альтернативи.

Уряди все більше втрачають терпіння щодо фінансових злочинів фінансових установ. Як наслідок, у 2020 році штрафи за боротьбу з відмиванням коштів досягли рекордних значень у загальній сумі понад 10 мільярдів доларів, оскільки фінансові організації не змогли перешкодити шахраям скористатися пандемією. Після фінансової кризи загальна вартість штрафів показує, чому інвестори та споживачі залишаються обережними. Фінансові служби зацікавлені в рішеннях для виявлення шахрайства. Попри всі втрати доходу, репутації та вартості акцій у поєднанні з можливими мільйонами-мільярдами штрафів, компаніям вигідніше запобігати фінансовому шахрайству, ніж дозволяти йому зникнути. Як ми вже зазначали вище, проблема фінансового шахрайства зростає. Оскільки серед споживачів зростає електронна комерція, онлайн-банкінг і мобільні платежі, разом із цим зростають і можливості шахрайства. Звичайні зображення шахраїв у голлівудських блокбастерах цікаві, але рідко правдиві. Зазвичай шахрайство не вчиняється розпатланим геніальним хакером, який люто друкує на клавіатурі, щоб зламати алгоритми безпеки. Схеми шахрайства можуть виходити від невинної на вигляд людини в соціальних мережах. Або це може бути складна мережа кіберзлочинців, яка масово розгортає соціальну інженерію. Шахрайство може бути вчинене навіть інсайдерами – співробітниками, підрядниками або партнерами у вашій організації [3, с. 24–26].

Ефективне запобігання фінансовому шахрайству залежить від знання різних видів шахрайства в бізнес-операціях. Ця інформація допоможе створити більш надійну адаптивну систему боротьби з шахрайством.

Шахрайство з платежами – це загальний термін для будь-яких фінансових втрат від несанкціонованих платежів. Шахрайство з платежами може статися щоразу, коли чиясь інформацію викрадають або несвідомо передають шахраям. Це шахрайство може включати складну романтичну аферу між двома людьми або масовий витік корпоративних даних за допомогою зловмисного програмного забезпечення. У результаті – технологія виявлення шахрайства потребуватиме динамічних та адаптивних систем для пошуку нових форм шахрайства з платежами.

Електронне шахрайство є одним із найпоширеніших і найприбутковіших методів. Шахраї заробляють мільярди, використовуючи злочинне програмне забезпечення, фішинг та інші методи онлайн-переказу, щоб отримати доступ до фінансів жертви, у багатьох випадках з її згоди, нічого не підозрюючи.

Електронне шахрайство використовує електронний зв'язок та/або телекомунікації (телекомунікації) для обману жертви (жертв). Це включає: телебачення; телефон; голосові повідомлення; факс; радіо; інтернет-сайти; соціальні мережі; текстові повідомлення;

відео конференції. Шахрайство електронною поштою також підпадає під шахрайство. Міністерство юстиції передбачає наявність таких елементів, щоб вважатися шахрайством: відповідач (шахрай) був добровільним і навмисним учасником схеми шахрайства; шахрай мав намір ошукати; було цілком очевидно, що для шахрайства буде використано міждержавний датовий зв'язок.

Збитки від шахрайства з картками в усьому світі сягнули понад 28,5 мільярдів доларів у 2020 році. Крім того, внаслідок витоку корпоративних даних кіберзлочинці можуть отримати мільйони записів про кредитні картки для продажу в темній мережі. Шахрайство з дебетовими та кредитними картками є відносно простим і знайомим більшості людей. Будь-яке несанкціоноване використання картки для здійснення покупок є шахрайством з картою. Завдяки системам онлайн-платежів шахраям більше не потрібно красти фізичну копію вашої картки, щоб нею скористатися. Хоча номери верифікаційного значення картки (CVV) є одним з рівнів захисту, шахраї також можуть отримати CVV або знайти способи його обійти.

Шахрайство з передплаченими дебетовими картками є ще однією формою шахрайства з картками. Передплачені дебетові картки вже ризиковані, оскільки кошти не завжди застраховані. Шахраї можуть використовувати передплачену інформацію для здійснення шахрайських покупок. Вони також можуть використовувати викрадені облікові дані кредитної картки, щоб купувати передплачені картки, і брати участь у злочинній діяльності, як-от відмиванні грошей і торгівлі наркотиками.

Окрім витоку даних, шахраї також можуть використовувати фішингові та підроблені веб-сайти, щоб отримати інформацію. Зловмисне програмне забезпечення з реєстраторами натискань клавіш може навіть викрасти CVV і платіжну інформацію.

Шахрайство працівників є широко поширеною та дорогою проблемою. Це особливо згубно, коли шахрайство співробітників стосується вищого керівництва та навіть генеральних директорів. Шахрайство співробітників відбувається, коли працівники навмисно викрадають кошти своєї компанії та/або клієнтів своєї компанії. Є багато методів, за допомогою яких співробітники можуть вчинити шахрайство. Привласнення активів означає несанкціоноване використання активів компанії для особистої вигоди. Це може включати крадіжку фінансів або даних компанії. Розкрадання є поширеною формою незаконного привласнення активів.

Шахрайство постачальників відбувається, коли постачальник(и) та/або працівник обманюють свою компанію за допомогою платежів постачальників. Це включає завищені витрати, дублікати платежів або навіть створення підроблених послуг постачальників.

Співробітники використовують бухгалтерське шахрайство, щоб спотворити активи та зобов'язання компанії. Шахрайське збільшення активів і зменшення

зобов'язань може маніпулювати курсами акцій компанії або приховувати незаконне привласнення активів.

Працівники можуть використовувати шахрайство із заробітною платою, щоб отримати додаткову зарплату, яку вони не заробили. Це може включати підробку робочого часу, завищення ставки заробітної плати або збір авансів без повернення. Вони навіть можуть використовувати «примарну платіжну відомість», щоб отримати зарплату працівникам, яких не існує.

Корупція та хабарництво можуть спустошити цілу компанію, навіть якщо це обмежено лише одним керівником високого рівня. Отримані хвильові наслідки штрафів, судових витрат і скупчення запасів можуть вплинути на кожного в компанії.

Шахрайство з платежами та шахрайство співробітників вже є дорогими проблемами для компаній. Шахрайство з любовними стосунками, викрадення особистих даних і шахрайство з захопленням облікових записів є додатковими проблемами, які вимагають рішень для виявлення шахрайства.

За повідомленнями, у 2020 році загальні витрати на викрадення особистих даних становили величезні 43 мільярди доларів у всьому світі. Крім того, 38% жертв викрадення особистих даних залишили свою фінансову установу після того, як вона не змогла належним чином вирішити шахрайство, яке там сталося. Крадіжка особистих даних відбувається, коли особисту інформацію і використовують для шахрайства. Ідентифікаційна інформація містить таку конфіденційну інформацію, як: повне ім'я, адреса, дата народження, податкова інформація, номери водійських прав, номери кредитних/дебетових карток, паспортні дані. Коли шахраї отримують достатньо ідентифікаційної інформації, вони можуть імітувати особу кількома способами. Вони навіть можуть використати часткову інформацію для створення нової підробленої особи, що називається крадіжкою синтетичної особи.

Шахраї можуть відкривати шахрайські кредити, рахунки або кредитні лінії на чуже ім'я. На жаль, деякі злочини, пов'язані з крадіжкою особистих даних, роками залишаються непоміченими. Згідно з останніми підрахунками, шахрайство з захопленням облікового запису завдало компаніям щонайменше 12,5 мільярдів доларів у всьому світі [4].

Шахрайство з захопленням облікового запису відбувається, коли шахраї використовують дані для входу жертви, щоб отримати контроль над їхнім обліковим записом і фінансами. Шахрайство з захопленням облікового запису є прибутковим для злочинців з кількох причин: це відносно легко зробити; важко виявити; воно може бути швидким і безповоротним; його можна автоматизувати; його можна використовувати для отримання контролю над іншими обліковими записами; як правило, це дуже прибутково для шахраїв. Коли облікові дані будуть отримані, у шахраїв з'явиться безліч можливостей. Шахрайство з захопленням облікового запису є формою крадіжки особистих даних. У багатьох випадках спамери використовують ідентифіка-

ційну інформацію для шахрайства або, навпаки, отримують ідентифікаційну інформацію через шахрайство. Шахрайства із захопленням облікового запису численні, і багато з них легко здійснити. До них належать: фішинг; внесення облікових даних; реєстратори ключових слів шкідливих програм; перехоплення Wi-Fi; підроблені сайти; SIM-карти.

У багатьох випадках шахрайство із захопленням облікового запису має ефект сніжної кулі. Шахраї використовують облікові дані, викрадені з одного облікового запису, для доступу до інших облікових записів. Це може статися за допомогою додавання облікових даних, яке автоматизує запити на вхід в Інтернеті, доки не знайде збіг. Або вони можуть взяти дані з одного облікового запису та використовувати їх для зміни інформації для входу в інші облікові записи.

На жаль, шахрайство – це проблема, яка не зникне сама по собі. Організація повинна залишатися пильною в боротьбі. Це означає аудит поточних процесів, створення стратегії виявлення та запобігання шахрайству та інвестування необхідне програмне забезпечення для виконання плану запобігання шахрайству.

Проведення оцінки ризиків є одним із перших кроків до зниження ризику шахрайства організації. Ретельна оцінка допоможе виявити будь-які слабкі місця, якими можуть скористатися зловмисники. Для цього потрібно буде переглянути заходи безпеки та протоколи. Окрім оновлення будь-яких застарілих комп'ютерів і програмного забезпечення, також слід переконатися, що співробітники мають доступ до навчання із запобігання шахрайству. Окрім переконання, що внутрішні системи оптимізовані для зменшення випадків шахрайства, слід також запровадити систему виявлення ризиків у клієнтській базі. Ще до того, як транзакція взагалі відбудеться, необхідно знати рівень ризику, пов'язаного з конкретним клієнтом. Використання належних процедур належної перевірки клієнта для оцінки потенціалу особи для вчинення шахрайства є важливою частиною управління ризиками протягом життєвого циклу клієнта. Лідери із запобігання шахрайству повинні створити процес, який включає оцінку поведінки клієнтів, моніторинг створення облікового запису або входу в систему, а також оцінку ризику для кожної дії, щоб створити повне уявлення про можливість шахрайства для кожного клієнта.

Програмне забезпечення для виявлення шахрайства є основою будь-якої стратегії боротьби з шахрайством. Найкращий спосіб запобігти втратам через шахрайство – використовувати сучасну технологічну систему для встановлення ризику та довіри на всьому шляху клієнта. Зараз у просторі багато сучасних гравців, деякі з яких мають більш зручні інтерфейси, ніж старіші гравці. Однак не всі ці рішення є достатньо гнучкими, щоб кодифікувати логіку компанії, яка вимагає покладатися на постачальників або команди інженерів для будь-якої підтримки чи оновлень. Деякі інструменти

пропонують продукти чорної скриньки з правилами та моделями протидії відмиванню коштів. Гарне рішення для виявлення шахрайства буде динамічним і легко налаштовуватиметься відповідно до мінливих потреб вашої організації [5].

В Україні майже відсутні офіційні статистичні дані стосовно показників фінансового шахрайства, оскільки це поняття фактично відсутнє в чинному українському законодавстві. Серед наявної в Україні нечисленної вибірки статистичних даних злочини, які правоохоронці кваліфікують безпосередньо як шахрайство, становлять близько 7–8% загальної кількості злочинів, що не відображає реального стану справ у цій сфері, оскільки шахрайство загалом і фінансове зокрема характеризується в Україні високим рівнем латентності (тобто значна кількість випадків вчинення шахрайств не фіксується органами внутрішніх справ). Так, за перше півріччя 2021 року в Україні зареєстровано більш ніж 50 тисяч випадків фінансового шахрайства. Щодня 1–2% українців стикаються з кіберзлочинцями по телефону, електронною поштою, в інтернет-крамницях, онлайн-сервісах з публікації оголошень, працевлаштування та кредитування тощо. Відповідно до статистики збитків від незаконних дій із платіжними картками у першому півріччі 2021 року щодня у середньому здійснюється 600 успішних для шахраїв незаконних операцій, тобто 30 на годину. За наявними даними, правоохоронцям вдається розкривати не більше 15–20% усіх випадків фінансових шахрайств, що можна пояснити як великою напруженістю в роботі правоохоронних органів, пов'язаною із складною соціально-економічною та політичною ситуацією в державі, викликаною військовими діями на сході країни, так і правовим нігілізмом наших громадян та надзвичайною спритністю, хитрістю і шахрайською «витонченістю» сучасних аферистів.

Попри таку невтішну статистику багатьом однаково здається, що їх це ніколи не зачепить, але 100% гарантій, що хтось може бути застрахований від фінансового шахрайства, немає.

Висновки. Зрештою, основною метою стратегії запобігання шахрайству має бути мінімізація загальної вартості шахрайства, а не лише швидкості, з якою воно відбувається. Щоб побудувати успішний план виявлення шахрайства, організації повинні розуміти, скільки шахрайство обходиться їхньому бізнесу. Це допоможе встановити основу для прийняття обґрунтованих рішень про те, скільки потрібно інвестувати у виявлення та запобігання шахрайству, а також як найкраще узгодити стратегію запобігання шахрайству з головними цілями організації. Хоча запобігання шахрайству є постійною боротьбою для фінансових організацій, це дуже легко стримувати належними заходами та засобами контролю. Важливо мати правильні інструменти та партнерів, які допоможуть організації боротися з шахрайством.

Список літератури:

1. Климко Т.Ю., Мельник О.О. Корпоративне шахрайство: реалії сучасності. *Науковий вісник Ужгородського університету. Економіка*. 2015. Вип. 46. С. 185–190.
2. Звіт Асоціації сертифікованих спеціалістів по розслідуванню шахрайств розміщений на офіційному сайті ASFE. URL: <http://www.acfe.com/> (дата звернення: 13.10.2022).
3. Гречаник Л. Фінансове шахрайство та протидія йому у компаніях. *Фінансовий ринок України*. 2010. № 4. С. 24–26.
4. Гарнага Є. Розробка комплексної програми дій для боротьби з шахрайством на підприємстві. *Ефективна економіка*. 2011. № 8. URL: <http://www.economy.nayka.com.ua/?n=8&y=2011> (дата звернення: 29.10.2022).
5. Альбрехт С., Венд Дж., Вільямс Т. Шахрайство. Промінь світла на темні сторони бізнесу. СПб.: Пітер, 1995. С. 35.

References:

1. Klymko, T.Yu. And Mel'nyk, O.O. (2015) Korporatyvne shakhraistvo: realii suchasnosti [Corporate Fraud: the realities of today]. *Naukovyy visnyk Uzhhorods'koho universytetu. Ekonomika*, vol. 46, pp. 185–190. (in Ukrainian)
2. Zvit Asotsiatsii sertyfikovanykh spetsialistiv po rozsliduvanniu shakhraistv rozmishchenyi na ofitsiinomu сайті ASFE [Report of the Association of certified specialists to investigate fraud on the official website ASFE]. Available at: <http://www.acfe.com/> (accessed: 13.10.2022).
3. Hrechanyk, L. (2010) Finansove shakhraistvo ta protyidiia yomu u kompaniiakh [Financial fraud and opposition to him in company]. *Finansovyy rynek Ukrayiny*, vol. 4, pp. 24–26. (in Ukrainian)
4. Harnaha, Ye. (2011) Rozrobka kompleksnoi prohramy dii dlia borotby z shakhraistvom na pidpriemstvi [Development of a comprehensive program of action to combat fraud in the company]. *Efektivna ekonomika*, vol. 8. Available at: <http://www.economy.nayka.com.ua/?n=8&y=2011> (accessed: 29.10.2022).
5. Al'brekht S. Vents Dzh. and Vil'yams T. (1995), *Shakhraystvo. Promin' svitla na temni storony biznesu* [Fraud. Ray of light on the dark side of the business]. Piter, SPb., p. 35. (in Ukrainian)

EVALUATION OF DETECTION AND PREVENTION STRATEGIES FINANCIAL FRAUD BY TYPE

The rapid spread of globalization processes in the field of finance, active involvement of information technologies and Internet networks for servicing financial transactions contribute to the fact that financial systems of countries around the world are becoming increasingly vulnerable to fraud encroachments. The article discusses the most common types, types and methods of financial fraud in the world. The most dangerous fraud schemes have been studied. The influence of fraudulent actions on the production activity of enterprises, financial activity of banks, and in general the life of ordinary citizens is studied, because financial fraud is a problem with far-reaching consequences in the financial industry, the government, the corporate sector, and for ordinary consumers. The consequences of various types of fraud are analyzed. Statistics are given on the number of frauds committed in areas where they have been exposed or known, as the dependence on new technologies such as cloud and mobile computing increases every minute, which makes the problem very difficult. Suggestions for preventing, evading or preventing fraudulent activities are provided. The essence of financial fraud is revealed through the prism of the financial aspects of this concept, specified purpose, methods and consequences of financial fraud, and is also presented probable set of measures for prevention and minimization of financial fraud as a complete system capable of fundamentally affecting overcoming this socially dangerous phenomenon. Typology of financial fraud by institutional sectors has been carried out economy and depending on the object of fraudulent actions taking them into account rapid modernization and modification, which, unlike the existing classification, will contribute identifying the sectors most "sensitive" to financial fraud national economy and determination of priority and specific directions measures to counter this negative phenomenon. Socio-economic and political instability form a favorable basis for the spread of fraudulent schemes in the field of Ukraine. Nowadays, financial fraud is a significant threat, in particular for domestic business. It is emphasized that in modern realities digital technologies create new threats and challenges for companies and often can be used to implement various types of fraudulent schemes, including cyber attacks, corporate espionage and many others. However, modern technologies can also become an important tool for the protection of domestic ones organizations, the state and citizens from fraudulent encroachments.

Key words: financial fraud, losses, fraud detection methods, data analysis, costs, warning, prevention.

ВІДОМОСТІ ПРО АВТОРІВ

Баландіна Ірина Сергіївна – кандидат економічних наук, доцент кафедри туризму та готельного господарства, Харківський національний університет міського господарства імені О.М. Бекетова

Власенко Тетяна Анатоліївна – доктор економічних наук, професор, завідувач кафедри економіки підприємства та організації бізнесу, Харківський національний економічний університет імені Семена Кузнеця

Данік Наталія Вадимівна – кандидат економічних наук, доцент, Миколаївський національний університет імені В.О. Сухомлинського

Завадовська Юлія Юзефівна – здобувач, Львівський університет бізнесу і права

Павлова Ірина Олександрівна – кандидат економічних наук, старший викладач кафедри туристичного бізнесу та рекреації, Одеський національний технологічний університет

Павлова Олександра Олександрівна – студент, Харківський національний економічний університет імені Семена Кузнеця

Пащенко Олена Віталіївна – магістрант, Миколаївський національний університет імені В.О. Сухомлинського

Погуда Наталія Вікторівна – кандидат економічних наук, доцент, Харківський національний економічний університет імені Семена Кузнеця

Рудь Інна Юріївна – кандидат економічних наук, доцент, Миколаївський національний університет імені В.О. Сухомлинського

Сергєєва Яна Сергіївна – аспірантка кафедри менеджменту, Донбаська державна машинобудівна академія

Степаненко Сергій Віталійович – кандидат економічних наук, докторант кафедри менеджменту, бізнесу і адміністрування, Державний біотехнологічний університет

Філяк Максим Сергійович – докторант, Львівський університет бізнесу та права

Фінагіна Олеся Валентинівна – доктор економічних наук, професор, завідувач кафедри менеджменту та бізнес-адміністрування, Черкаський державний технологічний університет