УДК 346.544
DOI https://doi.org/10.32782/klj/2024.2.12

Осінська О. А.,
аспірантка
Державної установи «Інститут економіко-правових досліджень
імені В. К. Мамутова Національної академії наук України»

КОМПЛАЄНС ТА ДЬЮ ДІЛІДЖЕНС ЯК ЗАСОБИ ЗАБЕЗПЕЧЕННЯ ГОСПОДАРСЬКОГО ПРАВОПОРЯДКУ У ЦИФРОВІЙ СФЕРІ

Анотація. Відсутність системності у правовому регулюванні цифрової сфери породжує можливості для порушення правового господарського порядку. Це призводить до підвищеної ризиковості. Комплаєнс та дью діліджене доцільно застосовувати для управління підприємницьким ризиком у контексті дотримання господарського правопорядку у цифровій сфері.

У цифрових відносинах ризик встановлення договірних відносин з неналежним суб'єктом має специфічний прояв: особи, які проводять комунікацію за допомогою мережі Інтернет одночасно перебувають в реальному світі і у цифровому. Для встановлення відносин у віртуальному просторі використовується цифровий профіль реальної особи. Проте реальна особа та її цифровий двійник можуть не співпадати між собою, що може ускладнити захист прав потерпілої особи. Передача цифрового профілю неіснуючої або померлої особи до осіб, які організують фіктивну діяльність дозволятимуть використовувати такі цифрові профілі для проведення фіктивної господарської діяльності. Крадіжка реальної цифрової особистості засновника, керівників підприємства дозволяє брати під контроль активи підприємства.

На державному рівні мають створюватись умови, в тому числі шляхом прийняття відповідних нормативно-правових актів, якими для господарської діяльності у цифровому просторі буде забезпечено реалізацію підходу: одна особа – одна цифрова ідентичність для чого можуть бути використані паспорти суб'єктів господарювання, а для цифрової ідентифікації осіб керівників, засновників підприємств технології поєднання біометрії та блокчейн-технологій.

В сучасних умовах для управління вказаним ризиком можуть застосовуватись комплаєнс та дью діліджене. Організація внутрішньогосподарських відносин контролю має відбуватись раціонально. Тому структура контрольних підрозділів не повинна бути занадто складною, а у випадку залучення на основі договору аутсорсингу для виконання функцій контролю сторонніх фахівців мають ретельно визначатись умови співпраці на основі відповідних положень договору аутсорсингу та локальних актів підприємства. Також доцільно проводити першим правовий дью діліджене, з метою зменшення трансакційних витрат, адже це одразу дозволить отримати стан відповідності нормам права організації діяльності підприємства. В той же час, віртуальне підприємство має суміщати правовий (юридичний) дью діліджене з інформаційним. Дью діліджене може бути складовою комплаєнсу за умови належної організації зовнішньо та внутрішньогосподарських відносин.

Ключові слова: *господарський правопорядок, дью діліджене, комплаєнс, цифровізація, віртуальне підприємство, господарський договір, господарські правовідносини.*

Osinska O. A. Compliance and due diligence as means of ensuring economic law and order in the digital sphere

Abstract. The lack of systematicity in the legal regulation of the digital sphere creates opportunities for violation of the legal economic order. This leads to increased risk. Compliance and due diligence are appropriate for business risk management in the context of compliance with economic law and order in the digital sphere.

In digital relations, the risk of establishing contractual relations with an improper subject has a specific manifestation: persons who communicate using the Internet are simultaneously in the real world and in the digital world. A digital profile of a real person is used to establish relationships in the virtual space. However, the real person and his digital counterpart may not match, which can make it difficult to protect the rights of the victim. The transfer of the digital profile of a non-existent or deceased person to persons who organize fictitious activities will allow the use of such digital profiles to conduct fictitious business activities. The theft of the real digital identity of the founder, managers of the enterprise allows to take control of the assets of the enterprise.

At the state level, conditions must be created, including through the adoption of relevant legal acts, which will ensure the implementation of the approach for business activities in the digital space: one person – one

digital identity, for which passports of economic entities can be used, and for digital identification of persons of managers, founders of enterprises technology of combination of biometrics and blockchain technologies.

In modern conditions, compliance and due diligence can be used to manage this risk. The organization of intra-economic control relations must be rational. Therefore, the structure of the control units should not be too complicated, and in the case of involvement on the basis of an outsourcing contract to perform control functions, the terms of cooperation must be carefully determined based on the relevant provisions of the outsourcing contract and local acts of the enterprise. It is also advisable to conduct legal due diligence first, in order to reduce transaction costs, because this will immediately allow to obtain a state of compliance with the legal norms of the organization of the company's activities. At the same time, a virtual enterprise should combine legal due diligence with informational due diligence. Due diligence can be a component of compliance under the condition of proper organization of external and internal business relations.

Key words: *economic law and order, due diligence, compliance, digitalization, virtual enterprise, business contract, economic legal relations.*

Постановка проблеми. Правовий господарський порядок є фундаментом та необхідною умовою для провадження законної господарської діяльності. Проте наявність прогалин у правовому регулюванні створює умови для порушення прав та інтересів сумлінних суб'єктів господарювання. Особливо рельєфно це простежується при діджиталізації відносин у господарській сфері. Тут звичайний підприємницький ризик доповнюється ще і цифровим. Вказані фактори підвищують необхідність для бізнесу запроваджувати відповідні власні системи контролю з метою забезпечення управління ризиковістю, спираючись у їх регулюванні зокрема на локальні акти та господарські договори. Особливо важливим це є для таких учасників господарських відносин у цифровій сфері як віртуальні підприємства, адже у вітчизняній правовій системі відсутні нормативно-правові акти, які б забезпечували їх діяльність і вони створюються та функціонують на підставі господарських договорів.

Тому теоретичне осмислення напрямів застосування у господарських відносинах для управління цифровим ризиком комплаєнсу, дью ділідженс та їх правове забезпечення є важливим як з теоретичних, так і з практичних міркувань.

Аналіз останніх досліджень та публікацій. Питання функціонування віртуальних підприємств розкрили у своїх працях вітчизняні науковці: О.М. Вінник, О.С. Орлова, Б.С. Тетерятник, О.В. Шаповалова. Правове забезпечення застосування комплаєнсу дослідили такі вчені: О.В. Ковалишин, А. Коршун, П.С. Матвєєв, М.Ю. Можаровський, Н.Б. Пацурія, В.В. Поєдинок, С.С. Теленик. Різним аспектам господарського правопорядку як основи провадження господарської діяльності приділили увагу М.Д. Василенко, Р.А. Джабраілов, Д.В. Задихайло, Г.Л. Знаменський, В.Г. Олюха, О.П. Подцерковний, В.А. Устименко.

Окремі аспекти дью ділідженс вивчали вчені-економісти: Л.О. Волощук, І.М. Гноєва, Л.В. Гуцаленко, Д.В. Драгомир, А.О. Касич, В.В. Керімов, Б.В. Мельничук, І.М. Назаренко, А.І. Орєхова, Н.Є. Сілічева, С.В. Сирцева, І.М. Ткачук, О.Р. Форошевська.

Проте достатньої уваги питанням управління цифровим ризиком у контексті дотримання правового господарського порядку з використанням комплаєнсу, дью ділідженс в працях вітчизняних науковців не приділялось.

Метою статті є визначення напрямів застосування комплаєнсу, дью ділідженс для управління підприємницьким ризиком у контексті дотримання господарського правопорядку у цифровій сфері.

Виклад основного матеріалу. Правовий господарський порядок є основою для провадження будь-якого виду господарської діяльності, адже як вказується у ч. 3 ст. 5 ГК України суб'єкти господарювання здійснюють свою діяльність у межах встановленого правового господарського порядку, додержуючись вимог законодавства. По суті він є ідеальною моделлю, якій реальне ведення бізнесу відповідає не завжди або не повною мірою. Як вказує М.Д. Василенко, категорія правовий господарський правопорядок не повинна сприйматись тільки як позитивне явище. «Суспільна система, в якій дії всіх її елементів чітко підкоряються встановленим

правовим правилам зі стійкими структурними зв'язками, є більш умоглядною конструкцією. У будь-якому суспільстві одночасно існують зони юридичної впорядкованості, так і зони хаосу» [1, с. 194].

Зважаючи на це, державою створюються умови для спонукання суб'єктів господарювання до максимального слідування ідеальній моделі, визначеної нормами права. Проте існують сфери суспільного життя, де внаслідок стрімкого розвитку нових технологій виникають прогалини у їх правовому опосередкуванні: спочатку виникає певне явище, а тільки згодом відбувається прийняття нормативно-правових актів, спрямованих на встановлення необхідних правил. Така ситуація породжує додаткові ризики для добросовісних підприємців. Проте це не звільняє їх від обов'язку проявляти належну обачність та проводити необхідні для оцінки власного ризику розрахунки.

Особливо яскраво це можна простежити у сфері цифрового бізнесу. Підприємницька діяльність тут також має проводитись з дотриманням правових норм, але в Україні відсутня системність правового регулювання цифрової сфери. Тому створюються додаткові можливості для зловживань, що своєю чергою підвищує ризиковість цієї господарської діяльності. Відтак, хоча сучасні інтернет-технології і відкривають нові перспективи для бізнесу, але як і будь-яке явище воно має зворотній бік у вигляді підвищеної ризиковості, що вимагає додаткової уваги бізнесу до управління ризиком з метою запобіганню дії негативних факторів. Недаремно О.М. Вінник, констатуючи наявність прогалин в правовому регулюванні відносин цифровізації, визначає одним із головних завдань держави у цій сфері мінімізацію ризиків від неконтрольованого та/або недобросовісного використання цифрових технологій [2, с. 15].

Ризик є однією з істотних ознак підприємницької діяльності (ст. 42 ГК України). Безумовно, будь-якому виду підприємницької діяльності притаманна неможливість однозначно окреслити результати започаткованих бізнес-проектів. З іншого боку, положення статті 44 ГК України, де одним з принципів підприємництва є принцип комерційного розрахунку та власного комерційного ризику, дозволяють зробити висновок про те, що ризиковість підприємницької діяльності врахована у правовому господарському порядку у контексті покладення на підприємця обов'язку запровадження відповідних заходів щодо уникнення або зниження можливих негативних наслідків. Тобто мова іде не просто про ризиковість підприємницької діяльності як таку, але про необхідність особі, яка її здійснює, прораховувати види ризиків та запобігати ним, запроваджуючи відповідну систему.

Враховуючи засадничі положення щодо підприємницького ризику, закладені у ГК України, можна зробити висновок, що ризиковість будь-якого виду підприємницької діяльності, зокрема але не виключно і у цифровій сфері, має усуватись державою, шляхом належного правового регулювання, а також і підприємцями шляхом управління підприємницьким ризиком. Саме такий підхід закладає ч. 1 ст. 5 ГК України, коли вказує на те, що правовий господарський порядок в Україні формується на основі оптимального поєднання ринкового саморегулювання економічних відносин суб'єктів господарювання та державного регулювання макроекономічних процесів.

При розбудові системи управління підприємницьким ризиком маємо виходити з того, що загальні ризики, притаманні будь-якому виду підприємницької діяльності залишаються актуальними і для цифрової сфери, але мають тут свій специфічний прояв. Також існує сукупність ризиків, обумовлених специфікою цифрових технологій, наприклад, таких як крадіжка цифрової особистості директора підприємства шляхом злому акаунту для того, щоб вчинити незаконні дії з майном підприємства.

Одним із ризиків, породжених особливостями цифрових технологій, є ризик встановлення договірних відносин з неналежним контрагентом. Проблема ідентифікації особи підсилюється тим, що особливості комунікації в мережі Інтернет правовий господарський порядок, встановлений в Україні враховує не повною мірою, що вимагає від суб'єктів, які провадять діяльність у віртуальному просторі особливої уваги до створення системи контролю.

Які ж особливості породжуються Інтернет-технологіями? Особи, які проводять комунікацію за допомогою мережі Інтернет одночасно перебувають як в реальному світі, так і у цифровому. Фактично в результаті створення певного цифрового профілю особи виникає цифрова особистість, яка і вступає у соціальні відносини у віртуальному просторі, і в тому числі у такий їх вид як правовідносини. Проте правові наслідки виникають у реальної особи, адже тільки вона має особисту волю, а не її цифрова ідентичність.

Варто зазначити, що ситуації коли відповідність між реальною та віртуальною особами є повною на практиці існує не завжди, адже цифровий контент особи може відповідати повністю або тільки частково реальній особистості або й зовсім не відповідати їй. Ситуація з визначенням відповідності між цифровою та реальною особою ускладнена у випадку коли в Інтернеті заінтересованою особою створюється не один цифровий профіль, а декілька. При цьому у цифровому світі особа може використовувати вигадані найменування – нікнейм, псевдонім, зареєстровану торгову марку або ж навіть не зареєстровані назви які не матимуть жодного відношення до фізичної особи або підприємства, що існує в реальному світі. За допомогою сучасних комп'ютерних технологій може створюватись навіть зовнішній вигляд людини яка не існує.

Якщо невідповідний цифровий профіль застосовується для простого особистого спілкування в мережі Інтернет то безумовно, проблеми можуть виникати тільки морально-етичного характеру. Але проблема може виникати якщо цифрова особистість використовується для здійснення транзакцій в мережі Інтернет. В цифрові правовідносини тут вступає реальна особа, але за допомогою цифрової. Всі угоди, вчинені з використанням цифрової особистості мають породжувати правові наслідки саме для реальної особи. У випадку ж неможливості чітко визначити реальну особу учасника угоди складно буде визначити хто ж насправді вступає у правовідносини. А відтак і забезпечити дотримання правопорядку, зокрема захист прав потерпілої особи у разі їх порушення.

Отже, одна з проблем, що має потенціал до породження цифрового ризику для бізнесу може полягати в тому, що окремі цифрові особи однієї особистості з реального світу будуть не відповідати їй повністю або частково.

Цифрова та реальна особистість нерозривно пов'язані між собою, що обумовлено широким проникненням віртуального світу у реальний. В той же час, можуть виникати ситуації коли вони перестають бути єдиним цілим і цифрова особа починає «автономне» існування. Наразі поширюються крадіжки цифрової ідентичності через вкрадені облікові записи та доступи шляхом отримання даних за допомогою електронних листів надісланих начебто державними установами, компаніями або шляхом створення фальшивого профілю у соціальних мережах [3].

Також можлива ситуація коли після смерті фізичної особи продовжується існування цифрової особистості. Таке може відбутись у випадку коли певні особи мають доступ до цифрових даних померлої особи. Тут можуть породжуватися численні афери з використанням акаунту, цифрового підпису та дистанційного доступу до рахунку в банку від імені особи, яка вже припинила своє існування в реальному світі.

Статтею 55-1 ГК України визначено ознаки фіктивної діяльності суб'єкта господарювання, серед яких є і такі: зареєстровано (перереєстровано) у органах державної реєстрації фізичними особами з подальшою передачею (оформленням) у володіння чи управління підставним (неіснуючим), померлим, безвісти зниклим особам або таким особам, що не мали наміру провадити фінансово-господарську діяльність або реалізовувати повноваження. Не важко побачити, що таке порушення господарського правопорядку у цифровому просторі здійснювати набагато легше. Передача цифрового профілю фіктивного (підставного) засновника, директора підприємства або фізичної особи-підприємця до осіб, які організують фіктивну діяльність дозволятиме легко контролювати їм всі фінансово-економічні процеси такої структури. Також фіктивний суб'єкт господарювання може використовуватись для про-

ведення оборудок відносно добросовісних компаній. А у випадку крадіжки цифрової особистості директора та/або головного бухгалтера підприємства відкриваються додаткові можливості для рейдерського захоплення підприємства або протиправного заволодіння його майном.

Недаремно у вітчизняній науковій літературі ставиться питання про існування в умовах віртуалізації інфраструктури економіки ризику обрання контрагентів та партнерів з числа фіктивних суб'єктів господарювання та як засіб протидій цьому ризику пропонується запровадження паспортів суб'єктів господарювання [4, с. 44]. Ця пропозиція видається в цілому вірною, хоча залишається без відповіді питання про те, як видавати такі паспорти іноземним суб'єктам господарювання, з огляду на те, що «Інтернет-простір – транснаціональний, а, отже, діяти в ньому можна незалежно від місця фактичного перебування, яке до того ж нерідко важко визначити, якщо заінтересована в цьому особа не називає себе, надає хибну інформацію про себе або використовує можливості цифрових технологій для забезпечення своєї анонімності, бажаючи уникнути відповідальності за зловживання приватністю на шкоду іншим учасникам відносин» [5, с. 43].

Клер Салліван вказує, що у мережі Інтернет при офіційних відносинах з державою, а також для реалізації трансакцій, здійснення юридично значущих дій має бути застосований підхід: одна особа – одна цифрова ідентичність [6, с. 724]. Ана Бедуші цілком доречно як можливий напрям цифрової ідентифікації особи підтримує появу рішень поєднання біометрії та технологій блокчейн та вказує, що на даний момент кілька держав впроваджують або вже впровадили розглядаючи рішення цифрової ідентифікації з використанням цих технологій (Індія, Естонія запровадили цей підхід; Австралія, Канада наразі шукають шляхи впровадження цифрових технологій; у Західній Африці лідирують Гвінея та Кот-д'Івуар. [7, с. 2]. До слова, на момент завершення написання цієї статті було отримано новину про те, що «австралійський парламент нарешті ухвалив закон про цифрову ідентифікацію, який має на меті поширити використання державної системи цифрової ідентифікації на всю економіку, а не тільки урядові організації. Приватний сектор країни буде також запрошений до використання австралійської системи цифрової ідентифікації громадян» [8].

Отже, на державному рівні мають запроваджуватись заходи з забезпечення повної цифрової ідентифікації фізичних осіб-підприємців, засновників, керівників підприємств, а також і компаній, які проводять свою діяльність у цифровому просторі.

Проте навіть за відсутності належного впорядкування цього питання на державному рівні, суб'єкти господарювання мають самостійно запроваджувати відповідні системи управління ризиком які дозволять визначати повною мірою реальну особу контрагента та його керівників.

Для розуміння поняття управління ризиком можна взяти за основу визначення цього терміну, що надається у Постанові КМ України від 16 лютого 2011 р. № 232 «Про затвердження Методики виявлення ризиків здійснення державно-приватного партнерства, їх оцінки та визначення форми управління ними». Управління ризиками – процес, що триває протягом здійснення державно-приватного партнерства і передбачає виявлення, оцінку ризиків, визначення шляхів запобігання їх виникненню, ліквідацію негативних наслідків і передачу ризиків (включаючи страхування), а також прийняття ризиків. Це визначення можна екстраполювати і на сферу цифрових відносин, щодо ведення бізнесу у віртуальному просторі.

Підприємства мають враховувати також і сучасні світові вимоги до прозорості ведення бізнесу, оскільки їх ігнорування може поставити під сумнів дотримання правового господарського порядку. Однією з таких сучасних світових тенденцій є, за справедливим висновком В.В. Поєдинок, поширення у національних законодавствах економічно розвинутих країн вимог до великих компаній з забезпечення ними належної обачності щодо соціальних, екологічних, етичних ризиків у власних ланцюгах постачання та здійснення заходів ефективного управління такими ризиками [9, с. 100].

Системами контролю, які доцільно застосовувати для управління ризиком встановлення договірних відносин з неналежним суб'єктом є комплаєнс та дью діліджен с.

У науковій юридичній літературі запропоновано вважати, що «комплаєнс – це організований суб'єктом господарювання/організацією внутрішній процес забезпечення відповідності його/її діяльності вимогам законодавства, нормам міжнародно-правових актів екстериторіальної дії, локальним актам суб'єкта господарювання, стандартам саморегулівних організацій у певній сфері і найкращим практикам, шляхом формування корпоративної культури, здійснення комплаєнс-контролю ризиків, які можуть призвести до застосування до такого суб'єкта господарювання юридичних, фінансових санкцій, втрати ділової репутації або іншої шкоди, а також за допомогою інших засобів реалізації комплаєнсу» [10, с. 59]. Такий підхід доволі повно охоплює всі основні ознаки комплаєнсу та може бути взятий за основу для реалізації мети цього дослідження. Проте для повного розуміння сутності комплаєнсу необхідно зупинитись на його функціях.

В.А. Луньова запропонувала наступні функції комплаєнс-менеджменту на підприємствах: 1. Запобігання (ідентифікація стейкхолдерів та аналіз; оцінка комплаєнс-ризиків; розробка/актуалізація Кодексу поведінки та внутрішніх політик; визначення складу правил поведінки та алгоритмів прийняття рішень; закріплення на підприємстві комплаєнс-культури; опис базових процедур комплаєнсу, ролі та відповідності кожного співробітника у досягненні спільних цілей; навчання працівників; комплексна належна перевірка щодо контрагентів та топ-менеджменту).

2. Виявлення (регулярний контроль та періодичне тестування ключових областей реалізації комплаєнс-ризиків; нагляд за своєчасним та повним виконанням нормативних зобов'язань; організація каналів консультації для співробітників, а також механізмів повідомлення про порушення; управління інцидентом: виявлення дій, які можуть свідчити про порушення; ініціація внутрішнього чи зовнішнього розслідування).

3. Реагування (реалізація процедур внутрішнього розслідування; створення комісії; збір та аналіз доказів; захист інформації та прав співробітників під час розслідування; відповідальність та дисципліна: ступінь відповідальності підприємства та/або окремого працівника за неналежне виконання вимог; коригувальні: внесення необхідних змін для протидії повторним порушенням та постійне вдосконалення процедур комплаєнс-менеджменту) [11].

В той же час, незважаючи на таку кількість функцій система комплаєнсу в компанії не має бути занадто складною. Адам Шауб вказує, що культура комплаєнсу компанії будується внутрішньо, але чим простіше фахівцям виконувати їх завдання, «тим більша ймовірність, що вони це зроблять, і тим більшого ризику фірма таким чином уникає» [12, с. 89]. Тобто організація внутрішньогосподарських відносин має бути проведена таким чином, щоб не створювались зайві структурні підрозділи контролю та їх функції не дублювались. У випадку залучення сторонніх фахівців на основі договору аутсорсингу передбачити на основі локальних актів та відповідних положень у договорі аутсорсингу порядок взаємодії між ними.

Дью діліджен с має спільну з комплаєнс функцію запобігання, але напрям її реалізації тут вужчий – виявлення на основі аналізу зібраної інформації потенційних ризиків співпраці з контрагентом або придбання певного активу. Тобто він також спрямований на управління ризиком і так само як і комплаєнс має виявляти потенційно проблемних контрагентів, але у вужчому напрямку.

Це є цілком логічним, адже як система контролю клієнтів дью діліджен с було започатковано у 1977 році швейцарськими банками. Між ними було укладено угоду, спрямовану на вироблення єдиного стандарту з проведення належної перевірки клієнтів з метою запобігання співпраці з сумнівними клієнтами та забезпечення належної обачності – The Swiss Bank Due Diligence Agreement. Положення цієї угоди оновлюються приблизно кожні п'ять років і наразі є чинною редакція 2020 року.

Згодом сфера його використання поширилась не тільки на банківську сферу, але і на

інші економічні галузі. «Due Diligence (DD) досить широко використовується у сфері економіки та права і призначений для збору та аналізу інформації на основі якої приймається рішення про доцільність співпраці із тарґет – підприємством» [13, с. 6-7]. Тобто в сучасних умовах він спрямований в першу чергу на усунення ризиковості на етапі встановлення договірних відносин. Разом з тим, дью діліджене може проводитись не тільки для визначення ризиковості контрагента, але і для оцінки рівня синергетичного ефекту від співпраці з ним.

Як справедливо вказують А.А. Касич та Я.Ю. Яковенко, дью діліджене «допомагає оцінити взаємний фінансовий вплив та підтвердити синергетичний ефект між компаніями» [14, с. 95]. Тому, за умови правильної організації та якісного проведення, він дозволяє усувати не тільки ризик щодо невизначеності особи контрагента, але і ризик неотримання очікуваного фінансово-економічного результату.

Л. В. Гуцаленко виокремлено такі види дью діліджене: 1) загальний Due diligence (General Due diligence); 2) правовий (юридичний) Due diligence (Legal Due diligence); 3) фінансовий Due diligence (Financial Due diligence); 4) бухгалтерський Due diligence; 5) податковий Due diligence (Tax Due diligence); 6) маркетинговий Due diligence; 7) інформаційний Due diligence; 8) управлінський Due diligence; 9) екологічний Due diligence; 10) технічний Due diligence; 11) операційний Due diligence (Operational Due diligence) [15, с. 25]. Всі вони спрямовані на з'ясування повної картини стану підприємства, потенціального контрагента.

У економічних дослідженнях процедури дью діліджене було наголошено на тому, що він може бути поділений на види, відповідно до ключового напряму проведення перевірки, з яких основними видами є бухгалтерський, фінансовий, податковий, управлінський, маркетинговий, юридичний, інформаційний та екологічний [16, с. 29].

З цією думкою можна погодитись частково. Дійсно, на початковому етапі проводити дью діліджене у повному обсязі недоцільно, у зв'язку з високим рівнем витрат, що виникатимуть внаслідок залучення значної кількості фахівців без яких результати перевірки будуть недостовірними. Проте тільки правовий (юридичний) дью діліджене дозволяє одразу визначити правдивість інформації щодо осіб засновників, кінцевих бенефіціарів, керівників підприємства, перевірити дотримання реєстраційних та дозвільних процедур, стан виконання договірних зобов'язань, правову чистоту власності підприємства, у тому числі і його цифрових активів. Тому для будь-якого підприємства, що здійснює діяльність у цифровому просторі такий його вид як правовий (юридичний) дью діліджене доцільно проводити першим.

В той же час, віртуальне підприємство має суміщати правовий (юридичний) дью діліджене з інформаційним, який використовується для перевірки діючих інформаційних систем, забезпечення інформаційної безпеки та перевірки відповідності цифрових даних підприємства, його керівників реальному стану, а також наявність та чистоту цифрових активів підприємства. Тільки поєднання цих двох видів перевірки дозволить прийняти правильне рішення про доцільність проведення наступних видів дью діліджене, адже при виявленні проблем у колі вищенаведених питань інші види перевірки втрачають сенс.

На підставі вищевикладеного можна зробити висновок про можливість органічного поєднання цих двох систем контролю у діяльності підприємства. При цьому дью діліджене може бути складовою комплаєнсу за умови належної організації зовнішньо та внутрішньогосподарських відносин.

Висновки. Проведене дослідження дозволяє констатувати, що наявність прогалин у нормативно-правовому забезпеченні створює додаткові можливості для порушення правового господарського порядку у цифровій сфері, що підвищує ступінь ризиковості підприємницької діяльності, яка проводиться з використання Інтернет-технологій. Одним з таких є ризик встановлення договірних відносин з неналежним суб'єктом, який у цифрових відносинах має специфічний прояв, оскільки особи, які проводять комунікацію за допомогою мережі Інтернет одночасно перебувають як в реальному світі, так і у цифровому. У віртуальному просторі реальні особи проводять між собою комунікацію за допо-

могою цифрових особистостей. Ризиковість у таких відносинах полягатиме в тому, що реальна особа та її цифровий двійник можуть не співпадати між собою, що ускладнюватиме або навіть унеможливіть захист прав потерпілої від протиправних дій особи.

Також створюються можливості для проведення суб'єктом господарювання фіктивної діяльності. Передача цифрового профілю неіснуючої або померлої особи до осіб, які організують фіктивну діяльність дозволятимуть використовувати такі цифрові профілі для створення фіктивного (підставного) засновника, директора підприємства або фізичної особи-підприємця. Особи ж реальних осіб, що здійснюють фіктивну діяльність буде встановити складно. Наступна проблемна ситуація – крадіжка реальної цифрової особистості засновника, керівників підприємства дозволяє брати під контроль активи підприємства не тільки у віртуальному, але і у реальному просторі.

На державному рівні мають створюватись умови, в тому числі шляхом прийняття відповідних нормативно-правових актів, якими для господарської діяльності у цифровому просторі буде забезпечено реалізацію підходу: одна особа – одна цифрова ідентичність для чого можуть бути використані паспорти суб'єктів господарювання, а для цифрової ідентифікації осіб керівників, засновників підприємств технології поєднання біометрії та блокчейн-технологій.

В сучасних умовах для управління вказаним ризиком можуть застосовуватись комплаєнс та дью діліджанс. Функції комплаєнсу є ширшими ніж у дью діліджанс, але ці системи мають і спільну функцію – запобігання ризику встановлення договірних відносин з неналежним контрагентом. В той же час, організація внутрішньогосподарських відносин контролю має відбуватись раціонально. Тому структура контрольних підрозділів не повинна бути занадто складною, а у випадку залучення на основі договору аутсорсингу для виконання функцій контролю фахівців сторонніх організацій мають ретельно визначатись умови співпраці на основі відповідних положень договору аутсорсингу та локальних актів підприємства.

Можна окреслити не менше 11 видів дью діліджанс, залежно від виду ризику для запобігання якому він використовується. Проте раціонально проводити першим правовий (юридичний) дью діліджанс, з метою зменшення трансакційних витрат, адже це одразу дозволить отримати стан відповідності нормам права організації діяльності підприємства. В той же час, віртуальне підприємство має суміщати правовий (юридичний) дью діліджанс з інформаційним.

Дью діліджанс може бути складовою комплаєнсу за умови належної організації зовнішньо та внутрішньогосподарських відносин.

Перспективним напрямом подальших досліджень є правове забезпечення запровадження віртуальним підприємством дью діліджанс та комплаєнсу як єдиної системи контролю.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ:

1. Василенко М.Д. Становлення господарського правопорядку в інноваційній сфері: до визначення пріоритетів. Часопис Київського університету права. 2010. № 2. С. 193-197.

2. Вінник О.М. Правові проблеми цифровізації в ракурсі нових загроз для суспільного благополуччя. Актуальні проблеми права: теорія і практика. № 1(39). 2020. С. 11-18.

3. Українцям все частіше загрожують крадіжки цифрової ідентичності. Що це та як захиститися? Fintex insider. 7 Жовтня 2023. URL.: https://fintechinsider.com.ua/ukrayinczyam-vse-chastishe-zagrozhuyut-kradizhky-czyfrovoyi-identychnosti-shho-cze-ta-yak-zahystytysya/

4. Шаповалова О. В., Шевченко Л. С., Стріжкова А. В. Правове забезпечення віртуалізації інфраструктури національної економіки України. Харків. НДІ прав. забезп. інновац. розвитку НАПрН України. 2019. 184 с.

5. Вінник О. М. Право цифрової економіки: монографія. Київ. НДІ приватного права і підприємництва імені академіка Ф. Г. Бурчака НАПрН України. 2021. 350 с.

6. Sullivan Clare. Digital identity – From emergent legal concept to new reality. Computer Law & Security Review. V. 34. № 4. 2018. P. 723-731.

7. Ana Beduschi. Digital identity: Contemporary challenges for data protection, privacy and non-discrimination rights. Big Data & Society. January–June 2019. P. 1-6.

8. Австралія надає банкам доступ до державної системи цифрової ідентифікації громадян. Fintex insider. 17 Травня 2024. URL.: https://fintechinsider.com.ua/avstraliya-nadaye-bankam-dostup-do-derzhavnoyi-systemy-czyfrovoyi-identyfikacziyi-gromadyan/

9. Поєдинок В.В. Корпоративна сталість: новий прядок денний для комплаєнсу й консалтингу. Вчені записки ТНУ імені В.І. Вернадського. Серія: юридичні науки. Том 34 (73). № 1. 2023. С 42-47.

10. Коршун А. Щодо визначення поняття «комплаєнс» і його характерних ознак у сфері господарювання. Вісник Київського національного університету імені Тараса Шевченка. № 5. 2022. С. 55-60.

11. Луньова В. А**.** Впровадження функцій комплаєнс-менеджменту для зростання прозорості бізнесу підприємств. Економіка та суспільство. № 56. 2023. URL.: ttps://economyandsociety.in.ua/index.php/journal/article/view/3086

12. Adam Schaub. Understanding the value of enterprise compliance technology. Journal of Securities Operations & Custody. Vol. 14. No 1. 2021. P. 78-91.

13. Балджи М.Д. Використання Due Diligence в обґрунтуванні передінвестиційних рішень у секторах національної економіки: колективна монографія / Балджи М.Д., Доброва Н.В., Карпов В.А. [та ін.]. Одеський національний економічний університет. Одеса. ПромАрт. 2018. 335 с.

14. Касич А.А., Яковенко Я.Ю. Дью Діліджене як ключовий інструмент аналізу доцільності інвестування. Облік і фінанси. № 4(70). 2015. С. 92-97.

15. Гуцаленко Л. В. Due diligence: еволюція та генезіс сутності. Економіка, фінанси, менеджмент: актуальні питання науки і практики. 2017. № 12. С. 21-29.

16. Форошевська О.Р. Суть та особливість поняття «due diligence». Матеріали студентської науково-теоретичної конференції «Участь молоді у розбудові агропромислового комплексу країни» 23-25 березня 2022 року. м. Миколаїв. С. 28-30.