МЕНЕДЖМЕНТ

УДК 334: 658.114

Д. А. Арзянцева, Н. П. Захаркевич
Хмельницький університет
управління та права імені Леоніда Юзькова

ПРОБЛЕМИ ВИКОРИСТАННЯ ЦИФРОВИХ АКТИВІВ У ДІЯЛЬНОСТІ ВІРТУАЛЬНИХ ОРГАНІЗАЦІЙ

Визначено ризики використання цифрових активів у діяльності віртуальних підприємств, до яких зараховано можливість використання віртуальних платформ для легалізації доходів, отриманих злочинним шляхом; фінансування тероризму тощо; тінізацію доходів, отриманих суб'єктами купівлі-продажу віртуальних товарів, уникнення оподаткування; здійснення розрахункових операцій та укладання смарт-договорів особами, що не досягли відповідного віку або з обмеженою дієздатністю; поширення шахрайства, зокрема цифрового шахрайства (кібератаки, корпоративне шпигунство тощо).

Ключові слова: ризики, цифрові активи, віртуальні організації, віртуальні речі, цифрові товари, цифрові шахрайства.

Постановка проблеми

Процеси проникнення в усі сфери діяльності людини, суспільства і держави інформаційно-комп'ютерних технологій та телекомунікаційних мереж стають каталізаторами розвитку цивілізації в XXI столітті. Нові технології та засоби комунікації забезпечують економію часу та ресурсів, дозволяють отримувати політичні, економічні, технологічні та інші переваги як у плані досягнення інтересів окремої особи, так і в масштабах груп людей, країни, регіону, світової спільноти. Формується нова якість економічних взаємовідносин – цифрова економіка. Разом з поширенням творчих можливостей, виникненням нових форм електронної комерції, яке створює електронне середовище, інтенсивний розвиток інформаційно-комунікаційних технологій створює нові можливості для реалізації загроз як національній, так і приватній безпеці. Такі загрози можуть бути пов'язані з порушенням визначених режимів використання інформаційних та комунікаційних систем, використання можливостей сучасних інформаційних технологій для ворожих, терористичних та інших протиправних дій. На сучасному етапі питань формування цифрової економіки в науковій літературі ризикам використання цифрових активів у діяльності віртуальних підприємств приділяють недостатню увагу, що зумовлює необхідність проведення теоретичних та прикладних досліджень у цьому напрямку.

Аналіз останніх досліджень і публікацій

Теоретико-правові та методичні основи вивчення віртуальних відносин було закладено багатьма вітчизняними та зарубіжними вченими, що забезпечило базу для дослідження проблем формування і управління віртуальною організацією. Розробленням цих проблем займалися такі

вчені, як І. Г. Горбунов, К. В. Єфремова, С. С. Зайкова, Д. В. Іванов, Л. А. Лейнонен, В. М. Русинов, О. І. Шалева, І. Нонака, М. Уорнер, М. Вітцель та інші. На сучасному етапі питанням формування та управління віртуальною організацією в науковій літературі приділяють недостатньо уваги, що зумовлює необхідність проведення теоретичних та прикладних досліджень у цьому напрямі, зокрема щодо практичних аспектів використання цифрових активів у діяльності підприємств.

Цілі статті

Мета роботи полягає в ідентифікації ризиків використання цифрових активів у діяльності віртуальних підприємств, визначенні економічних та соціальних наслідків для суб'єктів віртуальних відносин.

Викладення основного матеріалу

Масове перенесення людьми їх інформаційної активності у віртуальний всесвіт, формування онлайнових спільнот, створення в віртуальному просторі цифрової економіки підвищують роль віртуальних організацій у розвитку інформаційного суспільства. Саме віртуальні структури є сьогодні найбперспективнішими формами удосконалення управління організацією, підвищення ефективності та якості, продуктивності та конкурентоспроможності в умовах глобальної (інформаційної) економіки.

У новому інформаційному суспільстві практично всі об'єкти набувають віртуальної форми: організації, фактори виробництва, гроші, навіть людські емоції і почуття. Віртуальні організації – це мережеві організації, які заміщають фізичну структуру комунікативними технологіями. В економіці термін "віртуальна організація" має величезний діапазон значень і визначень. Наприклад, Давидов (Davidow) і Мелоун (Malone) використовували термін "віртуальна корпорація" для позначення будь-яких нових організаційних форм, життєвий цикл яких обмежений певними часовими рамками, а центральне місце займають інформаційні технології [1]. На противагу цьому Бурне (Byrne) запропонував використовувати той самий термін для тимчасового набору електронних телекомунікаційних зв'язків між ефемерними утвореннями, які жертвують рівнем своєї компетенції на користь ефективного взаємного співробітництва. Мартін (Martin) запропонував термін "кібернетична корпорація", в основу якого покладено високошвидкісні канали зв'язку, що є в мережі Інтернет. Всупереч цьому деякі автори або не допускають можливості існування віртуальних організацій без електронних взаємозв'язків, або ж повністю заперечують їх необхідність [5].

Сьогодні віртуальні підприємства в Україні представлені широким спектром ІТ-компаній та мережею підприємств, що спеціалізуються на електронній комерції. Торгівля в Інтернеті є галуззю, яка демонструє доволі швидкі темпи зростання серед усіх галузей національної економіки. Приблизний товарообіг послуг та товарів на ринку e-commerce сьогодні становить близько 50 мільярдів грн. [7]. У 2018 році зросла кількість підприємців, які почали продавати в мережі Інтернет. Щороку тільки на майданчику Prom.ua починають працювати понад сто тисяч новачків, і кількість тих, хто займається електронною комерцією понад три роки, також зростає. Разом із безперечними перевагами для власників/організаторів бізнесу інтернет-торгівлі посилюється проблема тінізації економіки, адже сьогодні активно продають товари через соціальні мережі та мобільні додатки (зокрема, Facebook, Viber та ін.) незареєстровані суб'єкти господарювання, які уникають сплати податків, не сплачують податок на доходи фізичних осіб, ЄСВ, військовий збір, податок на прибуток/єдиний податок та інші. Крім того, поширення таких форм торгівлі викликає стурбованість щодо забезпечення права на безпечні продукти харчування, предмети побуту та інших прав споживачів через неможливість отримання достовірної інформації про товари, відсутність гарантії на них, можливості обміну/повернення, непроходження ними сертифікаційних процедур. Також такі тенденції загострюють проблему неправомірних і несанкціонованих дій різних суб'єктів, які використовують засоби електронно-інформаційного середовища, до яких належать і цифрові активи.

До цифрових активів у діяльності віртуальних підприємств можна зарахувати "віртуальні речі" : електронні об'єкти (цифрові товари), які в силу своєї віртуальності не є матеріальними речами, проте мають всі ознаки речей (товару). Вони існують лише у мережі Інтернет. Віртуальна річ / віртуальне майно є частиною віртуального простору, наприклад, файли, які являють собою ті елементарні частинки, які утворюють його. Вони є послідовністю даних (цифр) та володіють визначеністю, яка виражена в структурних характеристиках (наприклад, файл залежно від формату має власну назву, структуру і якість, а також розмір, вимірюваний, як правило, в байтах). Цифрові товари або електронні товари – це нематеріальні товари, які існують у цифровому вигляді [6]. В електронній комерції ЄС поняття "цифрові товари" є загальним терміном, який використовують для опису будь-яких товарів, які зберігають, доставляють і використовують в електронній формі.

Цифрові товари поставляють в електронному вигляді споживачеві через електронну пошту або завантажують з Інтернету. Зазвичай при купівлі цифрових товарів в Інтернеті після того, як оплату отримано, продавець надає цифровий елемент як вкладення на електронну пошту або може надати безпечне з'єднання, через яке можна завантажити елемент. Володіння віртуальними речами виражається у збереженні на своєму комп'ютері або в частині віртуального простору, до якої відкритий доступ користувачу (наприклад, на власному чи орендованому сервері). Можливість користування віртуальними речами виражаються у використанні її корисних властивостей: інформації (текстової, звукової, візуальної тощо), що міститься в ній; функціональної складової, яка забезпечує її включення в процес роботи програмного забезпечення для створення нової віртуальної речі (наприклад, у ігровому просторі це може бути дорогоцінне озброєння персонажів у квестових іграх та стратегіях або "прокачка" віртуальної техніки, як у військових ігрових симуляторах). Власник такого об'єкта через відповідні платформи (наприклад, Steam) може його змінювати, переміщувати у віртуальному просторі, дарувати, міняти або продавати та за необхідності, навіть, знищити, тобто розпоряджатися цієї віртуальною річчю.

З приводу того, чи є віртуальні об'єкти майном, досі точаться дискусії. З огляду на міжнародну практику можна з упевненістю стверджувати, що такі держави, як Південна Корея, Китай, Тайвань уже опрацювали це питання і заклали правовий фундамент у цьому напрямку. Ще в 2001 році Міністерство юстиції Тайваню постановою визнало, що віртуальні об'єкти є майном, яке може бути відчужено і / або передано будь-кому. Дії, які вчиняються щодо таких об'єктів, варто розцінювати як такі, що вчиняються зі звичайною власністю [2, с. 44].

Враховуючи зазначені позиції, спробуємо сформулювати наше бачення "віртуальних речей" ; ними є речі (товари, наділені споживчою та міновою вартістю), створені в мережі Інтернет за допомогою цифрових технологій, набуті в результаті смарт-угод та спожиті у спосіб, який задовольняє потреби інтернет-користувача. До таких речей належать: файлове сховище (дисковий простір сервера), електронні кошти; електронні книги, музичні твори і фільми в електронній формі, передачі радіо і телебачення, записані в електронній формі, комп'ютерні програми та інші.

Проте за безневинною, на перший погляд, діяльністю у світі інтернет-розваг приховуються певні проблеми, які пов'язані з неконтрольованістю перебігу процесів створення та обігу віртуальних речей. Основні ризики обігу цифрових активів у діяльності віртуальних підприємств систематизовано у таблиці. Особливо проблемними це явище стає у сучасну добу боротьби з "відмиванням" коштів та фінансуванням тероризму. Найяскравішими прикладами є відносини з біржової торгівлі (та прирівняні до них – зокрема "ігрові" біржі типу "Форекс"), віртуальні казино тощо. Так, проведений аналіз окремих ігрових платформ показує, що такі товари можуть продавати за достатньо високою ціною, яка може сягати декількох тисяч доларів [8]. Враховуючи, що ціни на такі товари формується не за витратним методом, а на основі суб'єктивного сприйняття покупцями цінності товару, на нашу думку, його ціна може штучно збільшуватись і досягати кількох мільйонів. Проблема загострюється через те, що інтернет-користувачі отримують право "виводити" набуті віртуальні активи в реальний світ. Тобто чином, відкривається можливість масштабного та абсолютно неконтрольованого відмивання грошових потоків. Також необхідно враховувати ускладнений процес ідентифікації учасників економічних відносин у цифровому просторі. Як правило, для операцій із віртуальними товарами достатньо зареєструвати акаунт через надання

поштової інтернет-скрині, оплата цифрового товару здійснюється через I-box або через інтернет-карту, що унеможливлює персоналізацію особи, яка здійснила платіж. При цьому доходи, які отримує власник такої цифрової речі, не оподатковуються, що свідчить про ризик тінізації економічних відносин за участі віртуальних організацій. Частка обсягу безготівкових операцій із використанням платіжних карток, емітованих українськими банками, за підсумками 2018 року досягла 45,1 %, що на 5,8 в. п. більше порівняно з результатами 2017 року (39,3 %) [4]. За даними українського процесингового центру, на одну активну банківську карту он-лайн-покупця в нашій країні припадає в середньому 5,6 покупок на місяць. Загальна кількість операцій із використанням платіжних карток за дев'ять місяців 2018 року склала 2,8 млрд. шт., а їх обсяг – понад 2 трлн. грн. І це йдеться лише про купівлю "реальних" товарів, без врахування операцій на віртуальних біржах, казино, ігрових платформах, зокрема букмекерських конторах тощо.

Таблиця 1

Основні ризики обігу цифрових активів у діяльності віртуальних підприємств

Ризик	Економічні наслідки	Соціальні наслідки
Відмивання грошей та фінансування тероризму	Через купівлю-продаж віртуальних (цифрових) товарів можуть переводитись значні суми грошей з метою легалізації доходів, отриманих злочинним шляхом	Соціальне напруження у суспільстві, зниження рівня безпеки окремих країн та всього суспільства
Уникнення оподаткування	Доходи від реалізації віртуальних активів важко контролювати, що ускладнює можливість їх оподаткування. Зменшення потенційних надходжень до відповідних бюджетів	Подальша диференціація населення за рівнем доходів. Посилення соціальної несправедливості
Посилення шахрайства (ненадання відповідного цифрового товару, підміна товару іншим, надання обмеженого доступу до користуванням товару тощо)	Економічні втрати для покупця, зниження добробуту покупця та членів його родини. Економічні втрати для віртуальних орагнізацій внаслідок викрадення/розповсюдження інформації, що становить комерційну таємницю; кібератак тощо.	Неможливість задовольнити відповідну потребу. Виникнення конфліктів. Зниження довіри до віртуальних підприємств.
Здійснення розрахункових операцій та укладання смарт-договорів особами, що не досягли відповідного віку або з обмеженою дієздатністю	Економічні втрати родини в результаті неконтрольованого доступу зазначених осіб до персональних даних (зокрема банківських рахунків), зниження добробуту покупця та членів його родини.	Доступ до товарів і послуг (зокрема інформації), заборонених для користування особами, що не досягли відповідного віку або з обмеженою дієздатністю. Виникнення конфліктів між батьками та дитиною (або представниками особи і особою з обмеженою дієздатністю).

Примітка. Систематизовано авторами.

Окрема проблема стосується участі дітей та підлітків (а також осіб з обмеженою дієздатністю) в операціях купівлі-продажу віртуальних товарів. Через відсутність економічних знань щодо механізму формування вартості товару вони можуть не усвідомлювати реальної цінності цифрових товарів та використати персональні дані батьків/представників (паспорт, банківські картки) для здійснення платежів. Збільшується і ризик збільшення випадків інтернет-шахрайства, що в умовах функціонування цифрових товарів може набувати форми ненадання відповідного цифрового товару або надання обмеженого доступу до користування товаром, підміна товару іншим тощо. Слід зазначити, що покупець не завжди здатний ідентифікувати віртуальний товар, оцінити його якість, комплектність чи розрізняти інші характеристики, як при купівлі "реального товару". Можливим напрямом вирішення зазначених проблем є сучасні біометричні технології. Сьогодні біометричні

технології використовують у сфері контролю фізичного доступу та доступу до інформації. Біометричні системи широко використовують у приватній, корпоративній, державній та наддержавній сферах. Практично біометрія поширена у системі доступу до комп'ютерної мережі, біометричних документах, які посвідчують акти цивільного стану, у сферах електронної торгівлі, банках, у роздрібній торгівлі, контролі фізичного доступу та реєстрації робочого часу, ідентифікації осіб, яких розшукують, у громадських місцях або на транспорті, доступі до індивідуальних засобів (мобільних телефонів або ноутбуків).

Так, наприклад, компанія Lenovo постачає індійським покупцям нові ноутбуки Y300 та Y500. Ця система ідентифікує власника ноутбука за його обличчям. Миттєве фото господаря перетворюється на цифрову карту, а вона – на пароль для доступу до Windows та прикладних програм. Тобто паролі власника ноутбука створювати або запам'ятовувати не потрібно. Більше того: якщо ноутбук "вирішить", що до його ресурсів намагається отримати доступ незареєстрований користувач, він також фотографує правопорушника та зберігає знімок у своїй пам'яті для подальшої демонстрації власнику. Компанія Ok: Electric Industry Co., Ltd оголосила про завершення розроблення нової системи ідентифікації користувачів за райдужною оболонкою ока, з використанням звичайних фотокамер, вмонтованих у телефони або комунікатори. Використання таких технологій на платформах інтернет-розваг унеможливлять неконтрольований обіг цифрових товарів, зокрема з метою уникнення оподаткування та відмивання грошей.

Однак ризики використання віртуальних активів притаманні не лише споживачми чи суспільству; самі віртуальні підприємства також можуть стати середовищем для збільшення випадків шахрайських дій: кібератаки, корпоративне шпигунство та багато інших. У цьому контексті інформаційна безпека стає невід'ємним компонентом успішного функціонування віртуальної організації. Цифрове шахрайство стає дедалі складнішим, його важко попередити або знайти "замовника" чи "виконавця". Лише один з багатьох прикладів – це кібератака на магістральну електромережу України. Хакери змогли успішно проникнути до інформаційних систем трьох енергорозподільних компаній в Україні та тимчасово припинити постачання електроенергії кінцевим споживачам. Внаслідок цієї атаки близько 230 тисяч громадян залишалися без електроенергії протягом 1–6 годин [2].

Ще більшу загрозу становлять кібератаки, спрямовані не на завдання прямої матеріальної шкоди, а на знищення репутації організації, викрадення і розповсюдження персональних даних та інтелектуальної власності, отримання даних для віддаленого доступу до критично важливої інфраструктури, що спричиняє посилення соціального напруження в суспільстві, призводить до дестабілізації відносин з політичних чи ідеологічних (зокрема релігійних) мотивів. При цьому "замовниками" таких дій можуть бути як фізичні, так і юридичні особи, уряди держав, терористичні організації тощо. За даними дослідження [3], кіберзлочини є одним із найпоширеніших видів економічних злочинів, від яких постраждали 31% організацій в Україні. У зв'язку із зазначеним, віртуальним організаціям в Україні варто посилити заходи забезпечення безпеки взаємодії з третіми сторонами (агенти, постачальники та клієнти) шляхом корпоративної розвідки, перевірки доброчесності контрагентів, встановлення надійного програмного забезпечення протидії кібератакам.

Висновки та перспективи подальших досліджень

Отже, визначено ризики використання цифрових активів у діяльності віртуальних підприємств, до яких належать: можливість використання віртуальних платформ для легалізації доходів, отриманих злочинним шляхом; фінансування тероризму тощо; тінізація доходів, отриманих суб'єктами купівлі-продажу віртуальних товарів, уникнення оподаткування; здійснення розрахункових операцій та укладання смарт-договорів особами, що не досягли відповідного віку або з обмеженою дієздатністю; розповсюдження шахрайства, зокрема цифрового шахрайства (кібератаки, корпоративне шпигунство тощо). Можливим напрямом вирішення зазначених проблем є використання сучасних біометричних технологій, які дають змогу контролювати доступ до

інформації та убезпечити користувача від небезпек несанкційованого втручання в роботу електронних систем; перевіряти доброчесність контрагентів, встановлювати надійне програмне забезпечення для протидії кібератакам. Перспективи подальших досліджень ми вбачаємо у визначенні особливостей розвитку віртуальних організацій в Україні.

Список літератури

1. Бейкер Д. Инновация модели бизнеса через “краудсорсинг” с использованием социальных сетевых платформ. URL: http://sun.tsu.ru/mminfo/2011/000393746/06/image/06-087.pdf (дата звернення: 16.05.2019).
2. Єфремова К. В. Об’єкти інтернет-правовідносин. Правове регулювання відносин у мережі Інтернет : кол. монографія / кол. авторів А. П. Гетьман [та ін.]; за ред. С. В. Глібко, К. В. Єфремова. – Харків, 2016. Розд. 1, підр. 1.2. – С. 36–51.
3. Зайкова С. С. Подход к организации электронного обмена данными между системами управления и исполнения цепей поставок на основе Electronic Data Interchange (EDI). 13-я научно-практическая конференция “Реинжиниринг бизнес-процессов на основе современных информационных технологий. Системы управления процессами и знаниями” (РБП-СУЗ 2010): Сборник научных трудов. – М.: Московский государственный университет экономики, статистики и информатики, 2009. С.51-55.
4. Огляд ринку платіжних карток та платіжної інфраструктури України за 2018 рік. Національний банк України : веб-сайт. URL : https://bank.gov.ua/doccatalog/document?id=88661687 (дата звернення: 16.05.2019).
5. Рудь Н. Т. Віртуальні підприємства: сутність та доцільність використання в інноваційній діяльності. Економічний форум. 2016. № 4. С. 197–207.
6. Beal Vangie. “Digital Goods”. Webopedia. Retrieved, 23 March 2013. https://www.webopedia.com/TERM/D/digital_goods.html (Last accessed: 16.05.2019).
7. European B2C E-commerce Report 2016 // [Електронний ресурс]. – Режим доступу: https://www.ecommerce-europe.eu/app/uploads/2016/07/European-B2C-E-commerce-Report-2016-Light-Version-FINAL.pdf.
8. STEAM – платформа для розваг / веб-сайт. URL https://steamcommunity.com/market/search?#p1_price_desc (Last accessed: 16.05.2019).

References

1. Beiker D. Innovatsiia modeli biznesa cherez kraudsorsing s ispolzovaniem sotsialnykh setevykh platform [Business model innovation through “crowdsourcing” with the usage of social networking platforms]. Available at: http://sun.tsu.ru/mminfo/2011/000393746/06/image/06-087.pdf (accessed: 16.05.2019). (In Russian).
2. Yefremova K. V. (2016) Obiekty Internet-pravovidnosyn [Objects of Internet Legal Relations]. Pravove rehuliuvannia vidnosyn u merezhi internet: kol. monohrafiia/ kol. avtoriv A. P. Hetman ta in. [Legal Regulation of Internet Relations: coll. monograph / coll. authors A.P. Getman and others] (eds. S. V. Hlibko K. V. Yefremova). Kharkiv, rozd. 1, pidr. 1.2, pp. 36–51. (In Ukrainian).
3. Zaikova S. S. (2009) Podkhod k organizatsii elektronnogo obmena dannymi mezhdu sistemami upravleniia i ispolneniia tsepei postavok na osnove [An approach to organizing electronic data interchange between the systems of management and execution of supply chains based on Electronic Data Interchange (EDI)]. Proceedings of the Reinzhiniring biznes-protsessov na osnove sovremennykh informatsionnykh tekhnologii Sistemy upravleniia protsessami i znaniiami (RBP-SUZ 2010): 13-aia nauchno-prakticheskaia konferentsiia. Moscow: Moskovskii gosudarstvennyi universitet ekonomiki statistiki i informatiki, pp.51–55. (In Russian).
4. Ohliad Rynku Platizhnykh Kartok Ta Platizhnoi Infrastruktury Ukrainy Za 2018 Rik. Natsionalnyi Bank Ukrainy [Overview of the Payment Card Market and Payment Infrastructure of Ukraine in 2018. National bank of Ukraine]. Available at: https://bank.gov.ua/doccatalog/document?id=88661687 (accessed: 16.05.2019). (In Ukrainian)
5. Rud N. T. (2016) Virtualni pidpryiemstva: sutnist ta dotsilnist vykorystannia v innovatsiinii diialnosti [Intelectual potential: factures of formation and realization]. Ekonomic forum, no. 4, pp. 197–207.
6. Beal Vangie. “Digital Goods”. Webopedia. Retrieved, 23 March 2013. Available at: https://www.webopedia.com/TERM/D/digital_goods.html (accessed: 16.05.2019). (In Ukrainian)
7. European B2C E-commerce Report. (13 July, 2016). Available at: https://www.ecommerce-europe.eu/app/uploads/2016/07/European-B2C-E-commerce-Report-2016-Light-Version-FINAL.pdf. (accessed: 16.05.2019). 8. STEAM - game platform. Available at: https://steamcommunity.com/market/search?#p1_price_desc (Accessed: 16.05.2019).

D. A. Arzyantseva, N. P. Zakharkevych
Khmelnytsky University of
Management and Law named after Leonid Yuzkov

PROBLEMS OF USING DIGITAL ASSETS IN THE ACTIVITIES OF VIRTUAL ORGANIZATIONS

It has been established that today virtual structures are the most promising forms of improving the management of an organization, improving efficiency and quality, productivity and competitiveness in a global (informational) economy. At the same time, such tendencies exacerbate the problem of unlawful and unauthorized actions of various entities that use the means of electronic information environment, including digital assets. In this regard, the object of the paper is to identify the risks of using digital assets in the activities of virtual enterprises and to determine the economic and social consequences for subjects of virtual relations.

The article presents the authors' vision of the concept of "virtual things", by which it is proposed to understand things (goods endowed with consumer and exchange value) created on the Internet with the help of digital technologies, acquired as a result of smart transactions and consumed in a way that meets the needs of the Internet user. These things include: file repository (disk space of the server), electronic money; electronic books, musical works and films in electronic form, radio and television programs, recorded in electronic form, computer programs and others. The authors note that behind the innocent, at first glance, activity in the world of Internet entertainment, there are certain problems associated with the uncontrollability of the processes of creation and circulation of virtual things. A separate issue concerns the participation of children and adolescents (as well as persons with limited capacity) in the purchase and sale of virtual goods. It has been established that the risks of using virtual assets are inherent not only to a consumer or a society, the virtual enterprises themselves can also become an environment for increasing cases of fraud: cyber attacks, corporate espionage and many others. In connection with the above mentioned, virtual organizations in Ukraine should strengthen security measures for interaction with third parties (agents, suppliers and customers) through corporate intelligence, verification of counterparties' integrity, and establishment of reliable software for countering cyberattacks.

The scientific novelty of the results obtained is that the risks of using digital assets in the activities of virtual enterprises have been identified. They include the possibility of using virtual platforms for legalizing proceeds from crime; terrorist financing, etc.; shadowing of the proceeds received by the subjects of purchase and sale of virtual goods; tax avoidance; the implementation of settlement operations and the conclusion of smart contracts by persons who have not reached the appropriate age or by persons with limited capacity; the spread of fraud, including digital fraud (cyberattacks, corporate espionage, etc.).

The possible direction of solving these problems is the use of modern biometric technologies that allow controlling access to information and protecting the user from the dangers of unauthorized interference with the operation of electronic systems; verification of the integrity of counterparties, the installation of reliable software to counter cyber attacks.

Key words: risks, digital assets, virtual organizations, virtual things, digital goods, digital fraud.