

Арзянцева Дар'я Андріївна

канд. екон. наук, доцент, доцент кафедри менеджменту, фінансів, банківської справи та страхування

Захаркевич Наталія Петрівна

канд. екон. наук., доцент, доцент кафедри

менеджменту, фінансів, банківської справи та страхування,

Хмельницький університет управління та права імені Леоніда Юзькова, м.Хмельницький, Україна

ПРОБЛЕМНІ АСПЕКТИ ВИКОРИСТАННЯ ЦИФРОВИХ АКТИВІВ У ДІЯЛЬНОСТІ ВІРТУАЛЬНИХ ОРГАНІЗАЦІЙ

Процеси проникнення в усі сфери діяльності людини, суспільства і держави інформаційно-комп'ютерних технологій та телекомунікаційних мереж стають каталізаторами розвитку цивілізації в ХХІ столітті. Поряд 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 провадження ворожих, терористичних та інших протиправних дій. На сучасному етапі питань формування цифрової економіки в науковій літературі ризикам використання цифрових активів у діяльності віртуальних підприємств приділяється недостатня увага, що обумовлює необхідність проведення теоретичних та прикладних досліджень в цьому напрямку.

У новому інформаційному суспільстві практично всі об'єкти приймають віртуальну форму: організації, фактори виробництва, гроші, навіть людські емоції і почуття. Поняття «цифрові товари» є загальним терміном, який використовується для опису будь-яких товарів, які зберігаються, доставляються і використовуються в електронній формі. До цифрових активів у діяльності віртуальних підприємств відносяться «віртуальні речі» – електронні об'єкти (цифрові товари), наділені споживчою та міноюю 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 необхідно віднести: файлові сховища (дисковий простір сервера), електронні кошти; електронні книги, музичні твори і фільми в електронній формі, пе-

редачі 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. Особливою проблематики це явище набуває у сучасну добу боротьби з «відмиванням коштів» та фінансування тероризму. Найбільш яскравими прикладами є відносини з біржової торгівлі (та прирівняні до них – в тому числі «ігрові» біржі), віртуальні казино тощо. Так, проведений аналіз окремих ігрових платформ вказує, що такі товари можуть продаватись за достатньо високою ціною, яка може сягати декількох тис. доларів [1]. 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 тим, що інтернет-користувачі отримують право «виводити» набуті віртуальні активи у об'єктивний світ. Таким 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 з віртуальними активами є достатнім реєстрація аккаунту через надання поштової інтернет-скрині, оплата цифрового товару здійснюється через I-box або через інтернет-карту, що унеможливує персоналізацію особи, яка здійснила платіж. При цьому, доходи, які отримує власник такої цифрової речі – не оподатковуються, що свідчить про ризик тінізації економічних відносин за участю віртуальних організацій.

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 не надання відповідного цифрового товару або надання обмеженого доступу до користуванням 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. На сьогодні біометричні технології використовують у сфері контролю фізичного доступу та доступу до інформації. Біометричні системи широко використовуються у сферах: приватній, корпоративній, державній та наддержавній. 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, які розшукуються, у громадських місцях або на транспорті, доступі до індивідуальних засобів (мобільних телефонів або ноутбуків). Використання таких технологій на платформах інтернет-розваг унеможливають неконтрольований обіг цифрових товарів, у тому числі з метою уникнення оподаткування та відмивання грошей.

Однак ризики використання віртуальних активів притаманні не лише для споживача чи суспільства, самі 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.

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 викликає нарощування соціальної напруги в суспільстві, призводить до дестабілізації відносин з політичних чи ідеологічних (у тому числі релігійних) мотивів.

Таким чином, до ризиків використання цифрових активів у діяльності віртуальних підприємств належить 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, у тому числі цифрового шахрайства (кібератаки, корпоративне шпигунство тощо). Можливим напрямом вирішення зазначених проблем є використання сучасних біометричних технологій, які

дозволяють здійснювати контроль доступу до інформації та забезпечити користувача від небезпек несанкційованого втручання в роботу електронних систем; перевірка доброчесності контрагентів, встановлення надійного програмного забезпечення протидії кібератакам. перспективи подальших досліджень ми вбачаємо у визначенні особливостей розвитку віртуальних організацій в Україні.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. STEAM – платформа для розваг / веб-сайт. URL https://steamcommunity.com/market/search?#p1_price_desc (Last accessed: 16.05.2019).