РОЗДІЛ 8. БУХГАЛТЕРСЬКИЙ ОБЛІК, АНАЛІЗ ТА АУДИТ

ПРОБЛЕМИ ІДЕНТИФІКАЦІЇ В ОБЛІКУ КОРИСТУВАЧІВ КРИПТОВАЛЮТИ

PROBLEMS OF IDENTIFICATION IN ACCOUNTING OF CRYPTOCURRENCY USERS

УДК 657.333
https://doi.org/10.32843/bses.60-39

Макурін А.А.
к.е.н., доцент,
доцент кафедри обліку і аудиту
Національний технічний університет
«Дніпровська політехніка»;
докторант кафедри фінансів, кредиту
та банківського страхування
Харківський державний університет
харчування та торгівлі

Makurin Andrii
Dnipro University of Technology;
Kharkiv State University
of Food Technology and Trade

У статті розглянуто основні загрози інформаційній безпеці. Установлено, що у цифровому середовищі особливу увагу варто приділити кіберзагрозам та кібератакам, які націлені на отримання прибутку через заволодіння певними інформаційними ресурсами або інформацією. Наведено перелік та проаналізовано їхній вплив на користувачів у мережі Інтернет, оскільки криптовалюта є набором цифрової інформації, і такі загрози, які існують у мережі, негативно впливають на бажання використовувати цифрові валюти. У ЄС оператори криптовалютних бірж зобов'язані верифікувати користувачів та відстежувати транзакції «традиційних» фінансових установ. Під контроль підпадають усі транзакції із сумою більшою ніж 150 євро (раніше цей поріг був вищий та становив 250 євро). Фінансові регулятори України також зазначили, що продовжують опрацювання питання правового положення криптовалют та законодавчого врегулювання операцій із ними, беручи до уваги позицію регуляторів інших країн та останні тенденції в розвитку таких технологій. Для регулювання анонімності та ідентифікації в обліку користувачів криптовалютою з подальшим визначенням об'єкта та бази оподаткування пропонуються вдосконалення, які наведено в дослідженні. Виокремлено основні напрями забезпечення кібербезпеки криптовалют.
Ключові слова: *облік, фінансові регулятори криптовалюти, ідентифікація, кіберзагрози, інформаційна безпека.*

В статье рассмотрены основные угрозы информационной безопасности. Установлено, что в цифровой среде особое внимание следует уделить киберугрозами и кибератакам, которые нацелены на получение прибыли путем овладения определенными информационными ресурсами или информацией. Приведен перечень и проанализировано их влияние на пользователей в сети Интернет, так как криптовалюта является набором цифровой информации, и существующие в сети угрозы негативно влияют на желание использовать цифровые валюты. В ЕС операторы криптовалютных бирж обязаны верифицировать пользователей и отслеживать транзакции «традиционных» финансовых учреждений. Под контроль подпадают все сделки с суммой больше чем 150 евро (ранее этот порог был выше и составлял 250 евро). Финансовые регуляторы Украине также отметили, что продолжают проработку вопроса правового положения криптовалют и законодательного урегулирования операций с ними, принимая во внимание позицию регуляторов других стран и последние тенденции в развитии таких технологий. С целью регулирования анонимности и идентификации в учете пользователей крипто валютой с последующим определением объекта и базы предлагаются усовершенствования, которые приведены в исследовании. Выделены основные направления обеспечения кибербезопасности криптовалют.
Ключевые слова: *учет, финансовые регуляторы криптовалюта, идентификация, киберугрозы, информационная безопасность.*

The article considers the main threats to information security. It is established that in the digital environment, special attention should be paid to cyber threats and cyber-attacks that are aimed at making a profit through the acquisition of certain information resources or information. Attackers constantly seize a certain number of crypto coins, exchanges and owners of crypto wallets suffer losses, but the cyberpolice cannot react because cryptocurrency in Ukraine is not in the legal field. The list and analysis of their impact on users on the Internet, as cryptocurrency is a set of digital information, such threats that exist in the network negatively affect the desire to use digital currencies. At the legislative level in different countries, it is mandatory to identify users of cryptocurrency on cryptocurrency exchanges and monitor large tranches of cryptocurrency, as there is a possibility of terrorist financing, purchase of drugs and weapons for these virtual currencies. Such countries that have already determined the status of cryptocurrency and monitor transactions with it on stock exchanges include the United States, Singapore, European countries, Britain, Canada, Australia, China and others. For example, in the EU, cryptocurrency exchange operators are required to verify users and track transactions of "traditional" financial institutions. All transactions with an amount of more than 150 euros are subject to control, previously this threshold was higher and amounted to 250 euros. Financial regulators of Ukraine also noted that they continue to work on the legal status of cryptocurrencies and the legal regulation of transactions with them, considering the position of regulators in other countries and recent trends in the development of such technologies. In order to regulate the anonymity and identification of cryptocurrency in the accounting of users with the subsequent definition of the object and the tax base, improvements are proposed, which are presented in the study. The main directions of cybersecurity of cryptocurrencies are highlighted. World practice shows that if the crypto exchange has a reasonable suspicion that a transaction is suspicious, it has the right to block such a transaction and identify such a user.
Key words: *accounting, financial regulators of cryptocurrency, identification, cyber threats, information security.*

Постановка проблеми. Із розвитком сучасних технологій та цифрового суспільства основною метою функціонування телекомунікаційних зв'язків є захист інформації. Збереження цінності інформаційних ресурсів та її захист впливають на зберігання, обробку та пошук інформації. Будь-які інформаційні технології повинні враховувати особливості інформації, яку обробляють, та її цінність, давати змогу користувачам різних категорій ефективно працювати з такими ресурсами.

Можна виділити такий перелік загроз інформаційній безпеці:

– протизаконна діяльність економічних структур у сфері формування, поширення і використання інформації;

– порушення регламентів збору, обробки і передачі інформації;

– навмисні дії, спрямовані на некоректність уведення даних в інформаційну систему;

– помилки в проєктуванні інформаційних систем.

У цифровому середовищі особливу увагу варто приділити кіберзагрозам та кібератакам, які націлені на отримання прибутку через заволодіння певними інформаційними ресурсами або інформацією. Такі атаки не спрямовані на конкретних користувачів, зловмисники намагаються здійснити несанкціоноване втручання до певної мережі та на більшість користувачів цієї мережі.

Зростання популярності криптовалюти і криптовалютних бірж супроводжується зростанням інтересу хакерів зламати біржу, гаманець або чиїсь акаунти для розкрадання криптовалюти. Відповідно, щороку вимоги до криптобірж щодо забезпечення захисту і підвищення безпеки зберігання і подальшого використання криптовалюти зростають. У сучасному світі практично кожну діючу криптобіржу за рівнем безпеки можна порівняти з банківськими системами. Але навіть цей факт дає змогу хакерам здійснювати кібератаки і викрадати цінну криптовалюту.

Основні загрози, які існують у мережі Інтернет та впливають на інформацію про користувачів крипто валютою, наведено нижче:

Ботнет – комп'ютерна мережа, що складається з великої кількості хостів і запущених ботів, які працюють автономно. Найчастіше вони прикріплені до звичайного програмного продукту, та як тільки користувач установлює його на свій пристрій, бот автоматично встановлюється. Такий комп'ютер вже є інфікований. Хакер зможе викрасти інформацію про користувача, здійснити розсилку від його імені, перебрати паролі від гаманців та отримати доступ до кредитних карток.

Наприклад, використання мережі Wi-Fi в готелі не є безпечним, оскільки на пристрої може з'явитися прохання оновити програмне забезпечення чи ще якийсь його компонент, що автоматично дає можливість установити Backdoor, який виступає віддаленим керуванням девайсу. Уся інформація з пристрою доступна не тільки його власнику.

Фішинг – вид шахрайства, метою якого є отримання прибутку чи конфеденційної інформації. Приклад фішингу – SMS-повідомлення та дзвінки від незнайомих осіб, а також відправляння листів електронною поштою від імені певних користувачів, яким довіряє особа.

Малвертайзинг – поширення шкідливого програмного забезпечення через онлайн-ресурси, закриття реклами на певній сторінці активує код, і вся інформація з пристрою передається хакеру.

Кардинг – вид шахрайства, який здійснюється через використання платіжних карток та їх реквізитів, що не ініційовано власником такої картки. Реквізити платіжних карток, як правило, беруть зі зламаних серверів Інтернет-магазинів, платіжних і розрахункових систем, а також із персональних комп'ютерів.

Провайдер послуг з обміну або обмінний пункт Exchanger, що займається комерційною діяльністю та отримує з фізичних та юридичних осіб комісійну винагороду під час конвертації криптовалюти у будь-які активи.

Таким чином, усе це забезпечує такий рівень потенційної анонімності, який просто неможливий у випадку кредитних і дебетових карт або традиційних систем онлайнових платежів, таких як PayPal.

Аналіз останніх досліджень і публікацій. Велика кількість вітчизняних учених-обліковців займається питаннями відображення в обліку криптовалюти, операцій із нею та отриманих доходів й понесених витрат. Серед видатних вітчизняних учених – О.М. Петрук, С.Ф. Легенчук, Т.А. Тарасова, О.В. Усатенко, М.С. Пашкевич та багато інших. В.О. Осмятченко та В.С. Олійник досліджували тенденції розвитку бухгалтерського обліку в контексті зміни технологічних укладів та інформаційної безпеки обліку. О.В. Позднякова та О.І. Петренко досліджували основні переваги та недоліки використання блокчейн-технології в процесі управління поставками. А.С. Крутова визначила основні підходи до відображення в обліку криптовалюти та подальше її використання під час здійснення зовнішньоекономічної діяльності.

Постановка завдання. Метою дослідження є визначення пріоритетних напрямів інформаційної безпеки у суспільстві за рахунок використання криптовалюти та подальша ідентифікація учасників криптовалютних операцій в обліку.

Виклад основного матеріалу дослідження. Широке поширення віртуальної валюти також підвищує потенційні ризики у сфері протидії відмиванню коштів і фінансування тероризму. Системи віртуальних валют доступні через Інтернет у тому числі з мобільних пристроїв і можуть використовуватися для здійснення транскордонних платежів та переказів грошових коштів. Окрім того, віртуальні валюти, як правило, функціонують у рамках складної інфраструктури, що включає низку осіб, котрі перебувають у декількох різних країнах і забезпечують перекази грошових коштів та здійснення платежів. Така сегментація послуг ускладнює пошук злочинців. Більше того, дані і записи про операції та клієнтів можуть вестися і зберігатися у різних осіб, часто знаходяться в різних юрисдикціях, що додатково ускладнює їх доступність для правоохоронних і регулюючих органів.

Наприклад, у січні 2019 р. через проблеми з безпекою криптобіржа Cryptopia втратила всі циф-

рові активи. Досі ведеться судовий процес, а сама біржа недоступна. На сайті регулярно з'являється нова інформація про хід розслідування. Черговим великим майданчиком, котрий сильно постраждав від хакерів, стала криптобіржа Bithumb. Кіберзлочинцям удалося вивести із цієї біржі 31 млн дол. у криптовалютах EOS і Ripple. Це вже другий великий злом і злив цифрової валюти із цієї біржі після 2018 р. У 2019 р. цей список поповнила одна з найбільших криптобірж – Binance. У травні 2019 р. хакери викрали понад 7 тис біткоінів із гарячого гаманця, отримавши доступ до API-ключів і 2FA-кодів, що було еквівалентно на той момент 40 млн дол. Для самої біржі втрати виявилися не такими істотними, адже становили лише 2% від загального сховища.

Криптовалюта виникла як анонімний платіжний інструмент, який можна використати під час розрахунку за певні товари, роботи та послуги й який не контролюється державою. Проте той, хто відправляє кошти, та той, хто їх отримує, проходять ідентифікацію у мережі блокчейн на основі криптогаманця. Будь-яка країна світу повинна контролювати фінансову систему, яка може використовуватися для відмивання коштів та фінансування тероризму.

Починаючи з 2017 р. Європейський Парламент прийняв рішення та зобов'язав 24 європейські криптовалютні біржі та провайдерів криптовалютних гаманців здійснювати обов'язкову ідентифікацію користувачів. Таким чином, на використання криптовалюти накладено ті ж самі зобов'язання, що й на інші фінансові інструменти. Оператори криптовалютних бірж зобов'язані верифікувати користувачів та відстежувати транзакції «традиційних» фінансових установ. Під контроль підпадають усі транзакції із сумою понад 150 євро (раніше цей поріг був вищий та становив 250 євро).

Грошово-кредитне управління Сінгапуру оголосило про намір 13 березня 2014 р. врегулювати діяльність посередників, що здійснюють операції з віртуальними валютами (маючи на увазі під ними у тому числі біткоїни). Таких посередників, які виробляють обмін віртуальних валют на реальні, зобов'яжуть ідентифікувати своїх клієнтів і повідомляти у відповідне відомство про підозрілі транзакції. У цілому до посередників будуть пред'являтися ті ж самі вимоги, що і до підприємств, які займаються обміном реальних валют, а також забезпеченням грошових переказів. Мета зазначених заходів – мінімізувати ризики, пов'язані з відмиванням коштів та фінансуванням тероризму, що виникають з анонімної природи віртуальних валют.

Будь-які операції, пов'язані з біткоїнами, які здійснюються на території США, регулюються законодавством із власності. Податкове агентство США сформувало окремий відділ для контролю таких операцій. Власники вважають, що здійснюють операції анонімно, проте існуючі технології дають змогу проводити пошук у мережі блокчейн та ідентифікувати справжніх власників через біткоїн-адресу. Криптовалютна біржа зобов'язана моніторити всі криптовалютні транзакції, ідентифікувати і персоніфікувати суб'єкта криптовалютних операцій. Передбачається обов'язкове надання персональних даних учасників операцій із криптовалюти, що є позитивним моментом у розрізі того, що криптовалюта випускається необмеженим колом анонімних суб'єктів. Цей факт сприяє залученню учасників у протиправну діяльність, наприклад продаж наркотичних засобів, відмивання доходів, одержаних злочинним шляхом, фінансування тероризму.

Криптовалютна біржа забезпечує налагодження зв'язків між суб'єктами криптовалютних операцій, які здійснюють обмін криптовалюти на електронні гроші, валютні цінності, цінні папери. Здійснити такий обмін дають змогу і певні онлайн-сервіси з обміну криптовалюти, наприклад BestChange, проте використання таких ресурсів суб'єкти здійснюють на свій ризик, оскільки держава не контролює цю діяльність. Анонімність цифрових технологій не дає змоги забезпечити фінансову прозорість та унеможливлює боротьбу із зазначеними ризиками. Правилами, які розробляються НБУ, буде передбачено, що ці суб'єкти ідентифікуються за допомогою BankID («Положення про Єдину національну систему електронної дистанційної ідентифікації фізичних і юридичних осіб BankID Національного банку України», затв. Постановою НБУ № 378 від 30.08.16).

Фінансові регулятори України також зазначили, що продовжують опрацювання питання правового положення криптовалют та законодавчого врегулювання операцій із ними, беручи до уваги позицію регуляторів інших країн та останні тенденції в розвитку таких технологій. Метою такого врегулювання є захист прав споживачів, протидія відмиванню коштів та іншим протиправним діям, ідентифікація суб'єктів операцій (фінансовий моніторинг), механізм оподаткування отриманих доходів, декларування тощо. При цьому вважають, що процес внесення змін до законодавства України має відбуватися на основі глибокого і деталізованого дослідження цього явища, його впливу на фінансові ринки, досвіду та останніх рішень інших регуляторів світу.

Таким чином, для регулювання анонімності та ідентифікації в обліку користувачів криптовалют із подальшим визначенням об'єкта та бази оподаткування пропонуються такі вдосконалення:

1. Криптовалютні транзакції містять відомості про криптовалютний кошик, з якого виконано передачу, одержувача, обсяг переказу, тимчасові мітки, що визначають момент передачі. Тобто можна визначити реальну вартість криптовалюти

на певну дату, особу, яка здійснила такий переказ, та факт підтвердження такої операції (момент передачі).

2. Суб'єкт криптовалютних операцій самостійно гарантує проведення транзакцій криптовалюти. Суб'єкт криптовалютних операцій зобов'язується зберігати дані щодо проведених транзакцій протягом одного та трьох років. Строк позивної давності для операцій із передачі криптовалюти, вартість транзакції якої не перевищує 1 000 дол. США, становить один рік. Якщо під час транзакції сума криптовалюти у конвертації на долари США перевищує 1 001 дол., строк позивної давності становить три роки. Таким чином, суб'єкт повинен зберігати інформацію стосовно транзакції від одного до трьох років.

3. Порядок створення та діяльності криптовалютної біржі здійснюється виключно в порядку, встановленому Національним банком України. Криптовалютна біржа зобов'язана здійснювати моніторинг усіх транзакцій, ідентифікацію та персоніфікацію суб'єкта криптовалютних операцій у порядку, встановленому Національним банком України. Обмін криптовалюти на електронні гроші, фінансові цінності, цінні папери здійснюється виключно криптовалютною біржою. Дохід, отриманий криптовалютною біржою від здійснення криптовалютних операцій, підлягає оподаткуванню відповідно до вимог чинного законодавства України.

Блокчейн буде застосовуватися у найрізноманітніших сферах, таких як: грошові перекази, мікроплатежі, розумні контракти (або смарт-контракти), ідентифікація фізичних об'єктів та активів, державне управління, оборона і безпека, міжнародна діяльність тощо. У цілому передбачається, що в майбутньому технології блокчейн можуть стати драйвером радикальних змін у широкому спектрі галузей, бізнес-моделей, соціальних і операційних процесів. Тестування та впровадження технологій блокчейн розпочали в низці країн й у багатьох великих корпораціях.

Цифрові підписи схожі на підписи, які використовуються для засвідчення електронних документів. Однак коли йдеться про криптовалюти, цифрові підписи є ключами, які підходять лише до якогось конкретного електронного гаманця і слугують для його ідентифікації. Під час засвідчення особою здійснення будь-якого переказу цифровим підписом неможливо довести факт, що переказ криптовалют був здійснений з іншого електронного гаманця.

Криптовалюта має власний захист від кіберзагроз, які існують у мережі. Цифровий підпис – це один із компонентів її захисту, який забезпечує кібербезпеку. Таким чином, особливо важливо розглянути варіанти кібербезпеки криптовалюти, які впливають і на ідентифікацію користувачів таких активів у мережі блокчейн.

Існує три основні напрями кібербезпеки криптовалюти:

1) аудит;
2) холодне зберігання коштів;
3) страхування.

Наприкінці 2019 р. біржа Gemini пройшла аудит безпеки SOC2. У ролі аудиторської компанії виступала Deloitte & Touche з Великої четвірки. Аудит проводився вісім місяців і підтвердив, що засновники біржі створили найбезпечнішу криптобіржу у світі. Аудит був проведений згідно зі стандартом аудиту Service Organization Control 2 (SOC2), який було розроблено у 2011 р. Американським інститутом сертифікованих бухгалтерів (AICPA). Gemini поки що пройшла аудит тільки першого типу. Аудит другого типу більш складний, оскільки потребує перевірки безпеки протягом періоду, а не фіксування результатів на конкретну дату. Такий вид аудиту дуже специфічний, оскільки охоплює обмежену низку бізнес-процесів, пов'язаних з обробкою даних клієнтів. Зараз, на жаль, він ще не адаптований під специфіку блокчейн-технологій.

Основне завдання аудиту – визначити, наскільки провайдер послуг безпечно обробляє дані користувачів. Під обробкою даних користувачів слід розуміти:

– захист бази даних від несанкціонованого доступу;
– якість хостингу;
– політику обробки персональних даних.

Для того щоб переконатися в безпеці криптоплатформи у цілому, необхідні вузькоспеціалізовані рішення. Вони включають у себе глибокий аналіз коду вебінтерфейсу і мобільного додатку, перевірку кожного рядка смарт-контракту, тести проникнення, аналіз ризиків перехоплення аккаунта і фішингу.

Більшість криптогаманців розділяється на гаманці гарячого та холодного зберігання криптовалюти. Основна різниця в тому, що гарячий гаманець установлено на пристрої, який підключений до Інтернету, а холодний такого підключення не має. Поки гаманець відключений від мережі, хакери не можуть дистанційно його зламати. Будь-яка криптобіржа або криптопроцесинговий центр повинні тримати певний відсоток коштів на гарячих гаманцях, щоб забезпечити нормальне виведення коштів. Однак саме гарячі гаманці – мета зловмисників. Саме так постраждали Cryptopia, Binance, Coinbene, Bithumb, BITPoint і UpBit.

Криптовалютні трейдери все частіше починають використовувати операції хеджування. Проте для їх повноправного використання необхідно пройти ідентифікацію користувача для перекладання ризику на іншу особу або на страхову компанію. У зв'язку із цим актуальності набуває регулювання ринків криптовалют за допомогою хеджування ризиків на ринку цифрових активів із застосу-

ванням цінових механізмів. Водночас ефективне ціноутворення на цифрові валюти може бути використане й як інструмент хеджування ризиків і попередження криз. Інструменти хеджування ризиків на ринку криптовалюти в контексті попередження криз полягають, передусім, у знаходженні точки оптимуму між спекулятивним характером операцій із криптовалютами та їх властивостями хеджувати ризики.

Під ідентифікацією слід розуміти процедуру розпізнання користувача в системі за допомогою зазначеного логіну (ідентифікатора) або іншої інформації, яка сприймається системою. Сьогодні існує декілька способів ідентифікації користувачів.

Ідентифікацію й автентифікацію можна вважати основою програмно-технічних засобів безпеки, оскільки інші сервіси розраховані на обслуговування іменованих суб'єктів. Ідентифікація й аутентифікація – це перша лінія оборони, «прохідна» інформаційного простору.

Надійна ідентифікація й автентифікація ускладнена не тільки через мережеві загрози, а й із цілу низку причин. По-перше, майже всі автентифікаційні сутності можна довідатися, украсти або підробити. По-друге, є протиріччя між надійністю автентифікації, з одного боку, і зручностями користувача й системного адміністратора – з іншого. Так, із міркувань безпеки необхідно з певною частотою просити користувача повторно вводити автентифікаційну інформацію (адже на його місце могла сісти інша людина), а це не лише клопітно, а й підвищує ймовірність того, що хтось може підглянути за уведенням даних. По-третє, чим надійніший засіб захисту, тим він дорожчий, тому пропонується такий підхід до ідентифікації користувача криптовалюти (рис. 1).

У подальшому саме це дає можливість державі здійснювати контроль над операціями з криптовалютою та ідентифікувати користувачів. Але пропонується, якщо користувач не підпадає під обмеження за кожним пунктом перевірки, його не ідентифікувати. Тому пропонується ввести наступні обмеження для перевірки з ідентифікації та верифікації користувачів, дані яких криптобіржі повинні надати Міністерству цифрової трансформації в Україні.

Сьогодні існують три основні підходи до ідентифікації користувачів: парольна ідентифікація; апаратна (або електронна) ідентифікація (використання різноманітних токен, скреч-карт і т. д.); біометрична ідентифікація. Але поступово все більшого поширення набуває багатофакторна ідентифікація, коли для визначення особистості користувача застосовується відразу кілька параметрів. Утім, сьогодні в здебільшого використовується тільки одна пара: парольний захист і токен. У деяких системах для максимальної надійності процедури ідентифікації застосовуються одночасно паролі, токени та біометричні характеристики людини.

Висновки з проведеного дослідження. Таким чином, можна виділити такі переваги і недоліки ідентифікації користувача щодо його поведінки в інформаційній системі.

Переваги:

1) Простота реалізації і впровадження. Не потрібно спеціального апаратного забезпечення, дані беруться із системи моніторингу стану інформаційної системи, а отже, для використання не потрібне придбання ніякого додаткового обладнання. Це найдешевший спосіб ідентифікації по біометричних характеристиках суб'єкта доступу.

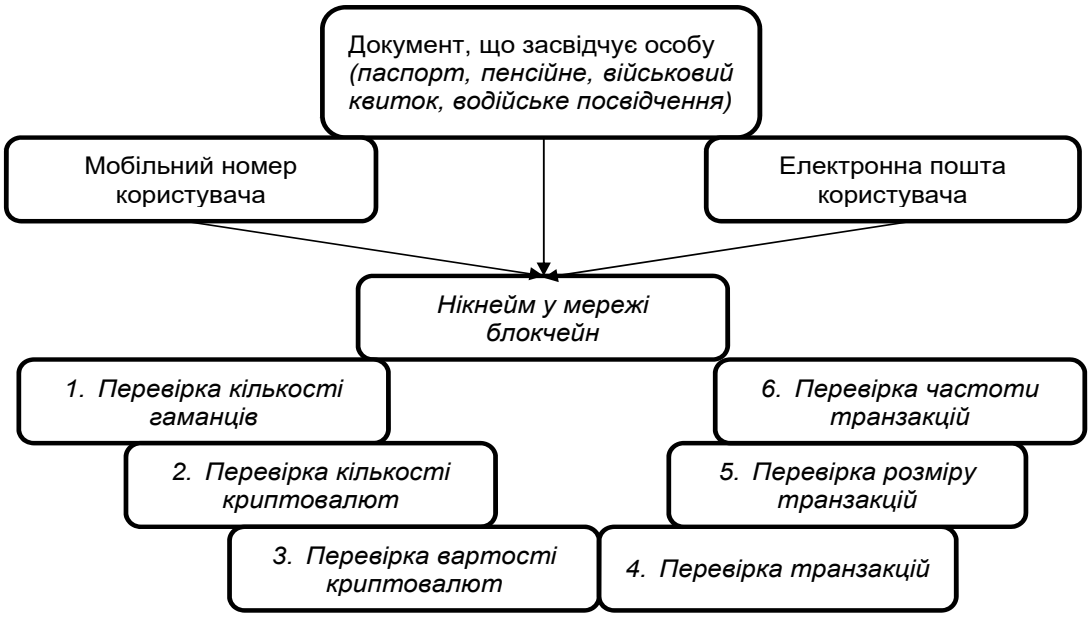

Рис. 1. Підхід до ідентифікації користувача криптовали в Україні

2) Не вимагає від користувача ніяких додаткових дій і навичок.

3) Не уявляється можливим скопіювати профіль поведінки автентифікованого користувача.

4) Можливість прихованої ідентифікації.

Недоліки:

1) На етапі первинного експлуатування потрібні додаткові витрати часу для побудови профілю поведінки.

2) Побудова профілю залежить від безлічі станів, в яких може перебувати конкретний користувач системи.

3) Держава не завжди може контролювати таку систему з автентифікованими користувачами.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Brukhanskyi R., Spilnyk I. Cryptographic Objects in the Accounting System. Proceedings of *9th International Conference on Advanced Computer Information Technologies, ACIT'2019.* (2019). P. 384–387.

2. Осмятченко В.О., Олійник В.С. Стан та перспективи розвитку бухгалтерського обліку в контексті зміни технологічних укладів. *Економічний вісник. Серія «Фінанси, облік, оподаткування».* 2018. № 2. С. 131–138.

3. Спільник І., Палюх М. Цифровий формат фінансової звітності: сутність, переваги, перспективи. *Цифрова економіка: тренди та перспективи* : матеріали міжнар. наук.-практ. конф., м. Тернопіль, 25 жовтня.

4. Халевський О.І. Цифрова трансформація в міжнародній банківській сфері. *Вісник студентського наукового товариства ДонНУ імені Василя Стуса.* 2019. Т. 1. №. 11. С. 226–230.

5. Khorunzhak N., Brukhanskyi R., Ivanyshyn V. Logic-statistical information models in control function of accounting. *Independent Journal of Management&Production.* 2019. Vol. 10. № 7. P. 846–871. DOI: http://dx.doi.org/10.14807/ijmp.v10i7.906.

6. Digital Financial Reporting. Available at: https://en.wikibooks.org/wiki/Digital_Financial_Reporting (дата звернення: 22.12.2020).

7. Accounting and features of mathematical modeling of the system to forecast cryptocurrency exchange rate / T. Tarasova et al. *Accounting.* 2020. Т. 6. № 3. P. 357–364.

8. Blockchain technology as an organization of accounting and management in a modern enterprise / Pashkevych M. et al. International Journal of Management (IJM) – Scopus Indexed. 2020. Vol. 11. Issue 6. P. 516–528.

9. Голубєва Н.Ю. Правове регулювання криптовалют: чи на часі? *Часопис цивілістики.* 2017. № 26. С. 22–28.

10. Пантелєєва Н.М. Фінансова безпека в умовах цифрової економіки: очікування і реальність. *Фінансовий простір.* 2020. № 2(38). С. 22–37.

11. Davoodalhosseini M., Rivadeneyra F., Zhu Y. CBDC and Monetary Policy. *Bank of Canada.* 2020. № 2020–4.

12. Ginneken C.L. Settlement of cross-border transactions through Central Bank Digital Currency (CBDC): analysis from a risk management perspective : dis. University of Twente, 2019.

REFERENCES:

1. Brukhanskyi R., Spilnyk I. (2010) Cryptographic Objects in the Accounting System. Proceedings of *9th International Conference on Advanced Computer Information Technologies, ACIT'2019,* pp. 384-387.

2. Osmjatchenko V.O., Olijnyk V.S. (2018) Stan ta perspektyvy rozvytku bukhghaltersjkogho obliku v konteksti zminy tekhnologhichnykh ukladiv [Status and prospects of accounting development in the context of changing technological ways]. *Ekonomichnyj visnyk. Serija: Finansy, oblik, opodatkuvannja,* vol. 2, pp. 131–138.

3. Spilnyk I., Palyukh M. (2018) Tsyfrovyy format finansovoyi zvitnosti: sutnist, perevahy, perspektyvy [Digital format of financial statements: the essence, advantages, prospects]. *Tsyfrova ekonomika: trendy ta perspektyvy :* materialy mizhnar. nauk.-prakt. konf., m. Ternopil, 25 zhovtnya 2018 r. Ternopil: FOP Osadtsa Yu.V., pp. 115–117. Available at: http://dspace.tneu.edu.ua/handle/316497/32763.

4. Khalevsjkyj O. I. (2019) Cyfrova transformacija v mizhnarodnij bankivsjkij sferi [Digital transformation in the international banking sector]. *Visnyk studentsjkogho naukovogho tovarystva DonNU imeni Vasylja Stusa*. T. 1, no. 11, pp. 226–230

5. Khorunzhak, N., Brukhanskyi, R., Ivanyshyn, V. (2019) Logic-statistical information models in control function of accounting. *Independent Journal of Management &Production,* vol. 10, no. 7, pp. 846–871. DOI: http://dx.doi.org/10.14807/ijmp.v10i7.906.

6. Digital Financial Reporting. Available at: https://en.wikibooks.org/wiki/Digital_Financial_Reporting (accessed 22 December 2020)

7. Tarasova T. et al. (2020) Accounting and features of mathematical modeling of the system to forecast cryptocurrency exchange rate. *Accounting.* T. 6, no. 3, pp. 357–364.

8. Maryna Pashkevych, Liudmyla Bondarenko, Andrii Makurin, Irina Saukh, Olena Toporkova (2020) Blockchain technology as an organization of accounting and management in a modern enterprise. International *Journal of Management (IJM) – Scopus Indexed,* vol. 11, Issue 6, pp. 516–528.

9. Golubyeva N.Yu. (2017) Pravove regulyuvannya kryptovalyut: chy na chasi? *Chasopys cyvilistyky,* vol. 26, pp. 22–28.

10. Pantyelyeyeva N.M. (2020) Finansova bezpeka v umovax cyfrovoyi ekonomiky: ochikuvannya i realnist. *Finansovyj prostir,* vol. 2, pp. 22–37. (in Ukrainian)

11. Davoodalhosseini M., Rivadeneyra F., Zhu Y. (2020) CBDC and Monetary Policy. *Bank of Canada*, vol. 4.

12. Ginneken C. L. (2019) Settlement of cross-border transactions through Central Bank Digital Currency (CBDC): analysis from a risk management perspective: dis. University of Twent.