Отримано: 26 листопада 2021 р.

Прорецензовано: 11 грудня 2021 р.

Прийнято до друку: 15 грудня 2021 р.

e-mail: gogrya@gmail.com

DOI: 10.25264/2311-5149-2021-23(51)-23-28

Гонак І. М. Особистий кіберзахист економічного суб'єкта криптовалютного бізнесу. *Наукові записки Національного університету «Острозька академія». Серія «Економіка» : науковий журнал.* Острог : Вид-во НаУОА, грудень 2021. № 23(51). С. 23–28.

УДК: 336.744

JEL-класифікація: E49

ORCID-ідентифікатор: https://orcid.org/0000-0002-7427-1415

Гонак Ігор Михайлович,
кандидат економічних наук, кафедра міжнародної економіки
Західноукраїнського національного університету

ОСОБИСТИЙ КІБЕРЗАХИСТ ЕКОНОМІЧНОГО СУБ'ЄКТА КРИПТОВАЛЮТНОГО БІЗНЕСУ

У статті розглянуто основні кібернетичні ризики, які супроводжують здійснення криптовалютного бізнесу економічними суб'єктами. Охарактеризовано найбільші втрати, понесенні економічними суб'єктами криптовалютного ринку через вплив кібернетичних правопорушень та недостатньо ґрунтовних знань щодо захисту власних інформаційних ресурсів. Розглянуто основні інструменти, які можуть бути використані економічними суб'єктами криптовалютного ринку для захисту своїх акаунтів та криптовалютних активів.

Ключові слова: *криптовалютний ринок, криптовалютний бізнес, кібератака, кіберправопорушення, криптовалюта, криптомонета, Bitcoin, Ethereum, криптовалютний гаманець, криптогаманець, гарячий криптогаманець, холодний криптогаманець, двофакторна аутентифікація, приватний ключ, акаунт, логін, пароль, брутфорс, Blockchain.*

Гонак Игорь Михайлович,
кандидат экономических наук, кафедра международной экономики
Западноукраинського национального университета

ЛИЧНАЯ КИБЕРЗАЩИТА ЭКОНОМИЧЕСКОГО СУБЪЕКТА КРИПТОВАЛЮТНОГО БИЗНЕСА

В статье рассмотрены основные кибернетические риски, сопровождающие осуществление криптовалютного бизнеса экономическими субъектами. Охарактеризованы наибольшие потери, понесенные экономическими субъектами криптовалютного рынка из-за влияние кибернетических правонарушений и недостаточно основательных знаний по защите собственных информационных ресурсов. Рассмотрены основные инструменты, которые могут использовать экономические субъекты криптовалютного рынка для защиты своих аккаунтов и криптовалютных активов.

Ключевые слова: *криптовалютный рынок, криптовалютный бизнес, кибератака, киберправонарушение, криптовалюта, криптомонета, Bitcoin, Ethereum, криптовалютный кошелек, криптокошелек, горячий криптокошелек, холодный криптокошелек, двухфакторная аутентификация, частный ключ, аккаунт, логин, пароль, брутфорс, Blockchain.*

Igor Gonak,
PhD in Economics, Department of International Economics
Western Ukrainian National University

PERSONAL CYBER DEFENSE OF THE CRYPTOCURRENCY BUSINESS ECONOMIC ENTITY

The article deals with the main cyber risks that accompany cryptocurrency business carried out by economic entities. The biggest losses incurred by economic entities in the cryptocurrency market due to the impact of cybercrime and lack of thorough knowledge on the protection of their own information resources are described. The main tools that can be used by economic entities of the cryptocurrency market to protect their accounts and cryptocurrency assets are considered.

Keywords: *cryptocurrency market, cryptocurrency business, cyber attack, cybercrime, cryptocurrency, cryptocurrency, Bitcoin, Ethereum, cryptocurrency wallet, crypto wallet, hot crypto wallet, cold crypto wallet, two-factor authentication, password authentication, private key.*

Постановка проблеми. Значення криптовалют на початку третього десятиліття XXI ст. зайняли чільне місце в особистих фінансах економічних суб'єктів.

Криптовалютний бізнес в Україні через фактичну відсутність інвестиційних альтернатив розвивається надзвичайно швидкими темпами (Україна в Глобальному індексі прийняття криптовалют (The 2020 Global Crypto Adoption Index) займає перше місце на планеті за загальною криптовалютною активністю зі 154 країн, відображених у рейтингу [1].

Криптовалютний бізнес супроводжує значна кількість кібернетичних ризиків, тому знання основ кібернетичної безпеки для економічних суб'єктів криптовалютного бізнесу є надзвичайно важливою складовою господарської діяльності підприємців, що здійснюють свою діяльність на криптовалютному ринку, і вимагає значних інвестицій особистого часу та фінансово-економічних ресурсів для підвищення якості власної кібернетичної безпеки.

Аналіз останніх досліджень і публікацій. Дослідженню особливостей особистої кібернетичної безпеки діяльності економічного суб'єкта криптовалютного бізнесу присвятила свої роботи значна кількість науковців. Окремі аспекти особистої кібернетичної безпеки функціонування діяльності економічного суб'єкта криптовалютного бізнесу розглядали такі науковці та експерти: О. Бентон, І. Гонак, Дж. Лопп, М. Ребрик, Дж. Сонг та ін.

Аналізуючи наукові праці вчених щодо особистої інформаційної безпеки функціонування криптовалютного ринку, слід зазначити, що наукові дослідження кібернетичної безпеки не можна визнати достатньо ґрунтовними і тема потребує подальших опрацювань та наукових досліджень.

Мета і завдання дослідження: опрацювати теоретичні й практичні аспекти особистої кібернетичної безпеки діяльності економічного суб'єкта криптовалютного бізнесу.

Виклад основного матеріалу. Активний розвиток криптовалютного бізнесу в другому та на початку третього десятиліття XXI ст. супроводжується значним зростанням кількості та масштабів кібернетичних небезпек для діяльності економічних суб'єктів криптовалютному бізнесу як на макро-, так і на макрорівні.

Криптовалютний бізнес супроводжується такими кібернетичними ризиками:

– негативний вплив на здійснення криптовалютного бізнесу економічними суб'єктів здійснює *вплив та використання шкідливих програм* (вірусів, програм-вимагачів, підмін (фальшивих посилань) та фішингу (несанкціонованого доступу до особистої інформації)). Для надійного захисту функціонування криптовалютних операцій є необхідність користуватись надійним антивірусним захистом, проводити перевірку використовуваних електронних адрес та не відкривати неперевірені посилання через те, що шкідливі програми мають можливість проникати на ПК із відкритих сайтів і можуть здійснити активацію всюди, де буде можливо і, у тому числі, на пристроях власників криптовалютних гаманців;

– при недостатньому електронному захисті персональних комп'ютерів та акаунтів економічних суб'єктів криптовалютного бізнесу користувачі можуть зазнати впливу *хакерських атак*. Через зростання капіталізації ринку криптовалют (станом на 27 жовтня 2021 р. капіталізація Bitcoin склала біля 1113 млрд дол., Ethereum – майже 474 млрд дол., Ripple – 45 млрд дол., а Dogecoin – 32 млрд дол. [2], що, у сумі (1664 млрд дол.), більше за ВВП Канади (143,4 млрд дол.), Південної Кореї (1630,5 млрд дол.), Російської Федерації (1483,5 млрд дол.), Бразилії (1444,7 млрд дол.), Австралії (1330,9 млрд дол.), Іспанії (1281,2 млрд дол.), Індонезії (1058,4 млрд дол.) та багатьох інших країн у 2020 р. [3]), зростання ринкової ціни криптомонет і збільшення їх емісії кількість і якість кібернетичних атак на ринку криптовалют значно зростає. Біржі криптовалют хакери часто зламують і деякі криптовалютні біржі через це збанкрутували. Злам криптовалютної біржі Mt. Gox і виведення з її рахунків близько 460 млн дол. США зумовило подання біржею заяви про банкрутство у квітні 2014 р., а у середині 2021 р. кіберправопорушники зуміли отримати доступ до платформи по обміну криптовалют Poly Network і спромоглися вивести понад 604 млн дол. США, що ілюструє негативний зростаючий тренд. На активну увагу кіберправопорушників на криптовалютному ринку вказує те, що у 2020 р. кіберправопорушники скоїли 122 кібератаки і вивели 3,8 млрд дол., а із 2017 р. по 2020 р. кіберправопорушники змогли вивести криптомонет на 9,8 млрд дол. США [4, с. 15], хоча із 2012 р. по 2020 р. хакери зуміли викрасти 13,6 млрд дол. США в криптовалютних монетах, скоїли близько 330 зломів бірж, криптогаманців і децентралізованих застосунків. Отже, з 2017 р. по 2020 р. викрадено понад 70 % загальної за 10 років суми, а за 2020 р. скоєно близько третини кіберправопорушень і виведено близько 30 % загального обсягу коштів за період з 2012 р. по 2020 р. [5]. Кібератаки на біржі криптовалют із завданням максимальної економічної та технічної шкоди проілюстровано у табл. 1.

Таблиця 1

Кібератаки на біржі криптовалют із завданням максимальної фінансової шкоди із 2014 р. по 2021 р.

Назва біржі	Дата кіберкрадіжки	Втрати, млн дол. США	Втрати, у криптомонетах
Mt. Gox	02.2014	450–460	850000 BTC
Bitfinex	08.2016	72	120000 BTC
NiceHash	12.2017	64	4736 BTC
Coincheck	01.2018	533	523000000 NEM
Bitgrain	02.2018	170	17000000 NANO
CoinBene	03.2019	105	110 видів криптовалют
Binance	05.2019	40	7000 BTC
Upbit	11.2019	49	342000 ETH
KuCoin	09.2020	275	6 видів криптовалют, у т.ч. 1008 BTC, 11543 ETH
Poly Network	08.2021	604	2858 ETH (267 млн дол.), 6610 BNB (понад 252 млн дол.), USDC (приблизно 85 млн дол.)

Джерело: сформовано автором на основі [6, с. 83].

– криптовалютний бізнес супроводжує можливість банкрутства криптобірж та, відповідно, імовірність втратити криптомонети чи фіатні валюти, розміщені на рахунках цих бірж. Банкрутство криптовалютної біржі може бути внаслідок *технічних проблем*, які супроводжують роботу торговельних платформ для зберігання криптовалютних гаманців. Втрати власників криптогаманців не відшкодовують, незважаючи на те, внаслідок яких проблем втрачені активи – через незадовільний стан програмного забезпечення чи діяльність кіберправопорушників;

– існує ймовірність *втратити пароль від криптовалютного гаманця чи секретний персонального PIN-код*, через що може бути втрачений доступ до активів, розміщених на криптогаманці (фіатні гроші чи криптовалютні монети). Станом на 2021 р. втрачено значну частку криптовалютних активів – згідно даних компанії Chainalysis, з 18.926.599 Bitcoin, які є в обігу, близько п'ятої частини є втраченими, що при курсі монети Bitcoin у розмірі 62443,86 дол. США [2] станом на четверте листопада 2021 р. втрати складають понад 235 млрд дол. США, що незначно менше валового внутрішнього продукту у 2020 р. Румунії (247,8 млрд дол США) і Чехії (243,5 млрд дол. США) та більше, ніж ВВП Португалії (231,3 млрд дол. США) та Нової Зеландії (212,5 млрд дол. США) [3]. Зокрема, програміст із Каліфорнії С. Томас втратив пароль від захищеного зовнішнього жорсткого комп'ютерного диску, на якому зберігалися ключі від криптовалютного гаманця з 7000 монет Bitcoin [7];

– Bitcoin, частка якого на криптовалютному ринку станом на 17 листопада 2021 р. складала 43,63 %, а Ethereum – 19,33 % [8]. Отже, операції із цими криптовалютами займають понад половину ринку. Але слід зазначити, що ці криптомонети необхідно називати скоріше обмежено анонімними чи псевдонімними, а не повністю анонімними (такими, що вміщують обсяг інформації, що дає можливість виявити власника криптовалютних коштів, і зацікавлена «третя особа» має змогу ідентифікувати особу, яка проводить транзакції із цими валютами). Тому, необхідно звести до мінімуму кількість особистої інформації, наданої криптовалютним біржам чи іншим суб'єктам криптовалютного ринку.

Отже, ми можемо констатувати, що потенційних проблем, які супроводжують здійснення криптовалютного бізнесу економічними суб'єктами та можуть привести до економічних втрат, є значна кількість. Обов'язком підприємця, що здійснює економічну діяльність у криптовалютній сфері, є максимально убезпечити свої криптовалютні активи від втрати через зовнішні фактори та особисту недбалість.

Достатні знання та уміння, що можуть бути застосовані для захисту особистого криптовалютного бізнесу, необхідні на всіх рівнях його здійснення.

Такими рівнями можуть бути: створення електронної пошти; приєднання до майнінг-пулу для майнерів; реєстрація і здійснення операцій на криптовалютній біржі; вибір криптовалютного гаманця для збереження криптовалютних активів.

Вимоги щодо максимального підвищення особистої кібербезпеки суб'єкта, який здійснює економічну діяльність на криптовалютному ринку:

1. Необхідне застосування *двофакторної аутентифікації* (2FA) на всіх рівнях здійснення криптовалютного бізнесу без використання SMS. Google аутентифікатор убезпечує економічного суб'єкта крипто-

валютного ринку від шахрайства з обміном SIM-карт. Необхідно використати саме додаток аутентифікатора 2FA, а не SMS 2FA, тому що SMS 2FA можна перехопити [9].

Слід зазначити, що безпека бізнесу, який провадиться в інтернеті, визначається міцністю найслабшої ланки. Наприклад, якщо адреса електронної пошти є вразливою, то є можливість (і ймовірність) атакувати акаунт економічного суб'єкта криптовалютного бізнесу. Тому необхідно налаштувати 2FA на кожен онлайн-акаунт, на якому тільки є така можливість.

2. Необхідний надійний захист приватних ключів. Захист особистих приватних криптоключів можна здійснити протягом трьох «кроків».

Першим кроком при захисті криптовалютних активів економічного суб'єкта крипторинку є тримання у безпеці та зняття грошей у довірених сторонніх кастодіанів (таких, як біржа), де придбано криптовалютні активи.

Другим кроком при захисті криптоактивів суб'єкта криптовалютного ринку є зберігання приватних ключів у офлайні та їх відсутність на пристрої, що є підключений до мережі Інтернет через ймовірність отримання доступу до них у кіберправопорушників.

Третім кроком для захисту криптовалютних активів є захист приватних ключів від ймовірності втрати через руйнування, створивши декілька безпечних резервних копій (наприклад, на кількох USB-носіях).

3. Через те, що криптокористувачі використовують подібні чи однакові логіни та паролі для різних акаунтів (мійнінг-пулів, криптогаманців, поштових скриньок та ін.), існує суттєва ймовірність для сторонніх осіб, що дізнались ці дані, порівняти їх з даними про криптовалютного користувача, що вже розміщені у Darknet, і деанонімізувати користувача чи викрасти криптоактиви. Тому необхідно для різних акаунтів використовувати різні паролі та логіни, щоби, отримавши доступ по одного акаунту, правопорушник не зміг отримати доступ до інших акаунтів.

4. Для здійснення активних транзакцій із криптовалютними активами для зберігання операційних коштів варто використовувати мобільний чи вебдодаток чи тонкий гарячий криптогаманець

5. Частину наявних криптовалютних активів (а при довгостроковому інвестуванні – всі криптовалютні активи) є сенс зберігати на холодних криптогаманцях, які є, фактично, пакетом інструментів на USB-носії, на яких є можливість зберігати інформацію, що необхідна для доступу до криптовалютних активів, і не потребують постійного інтернет-з'єднання. «Холодні» криптовалютні гаманці є найбільш надійним засобом зберігання криптовалютних активів і доступ до криптовалют забезпечується біометричними даними власника або введенням спеціальної комбінації [10].

«Холодні» криптовалютні гаманці (у формі звичайної флешки або великого накопичувача) під'єднуються через USB-порт до комп'ютера або мобільного телефону. Захист криптовалютних активів на «холодному» криптогаманці забезпечується пін-кодом і алгоритмом SEEED. При виборі «холодного» криптовалютного гаманця необхідно звернути увагу, роботу із якими криптовалютними монетами підтримує той чи інший гаманець.

Для зламу «холодних апаратних» криптовалютних гаманців є лише одна можливість – використати метод брутфорс (перебір усіх можливих варіантів приватного ключа чи мнемонічної фрази-пароля, а це може зайняти значну кількість часу). Застосування цього методу вимагає фізичного доступу до пристрою, що також є «ускладненим».

6. Використовувати тільки криптогаманці із відкритим вихідним кодом та для кожної криптомонети використовувати окремі криптовалютні гаманці.

5. Технологія Blockchain є, фактично, бухгалтерською книгою, у якій зареєстровані всі транзакції, що були проведені з моменту запуску криптовалюти і за даними, записаними у блокчейні, можна визначити криптокористувача. Тому суб'єктам криптовалютного ринку, які не мають бажання розкривати даних про себе, слід користуватися криптомонетами Monero, Zcash та Dash – ці валюти не розкривають ніяких даних про криптокористувача. Також, щоб мінімізувати можливості для ідентифікації користувача, при здійсненні конвертаційних транзакцій (зокрема, купівлі чи виведенні криптовалютних активів, необхідно максимально обмежити використання особистих банківських карток.

6. Переслідуючи мету щодо збільшення анонімності, криптокористувачу необхідно використовуати міксер-сервіси. З їх допомогою є можливість роздробити одну величезну транзакцію на значну кількість невеликих. Використання міксер-сервісів значно нівелює ймовірність встановлення повного ланцюжка транзакцій та їх деталей. Відомими часто використовуваними міксер-сервісами є BMC Mixer, BitcoinMixer, Blender.

7. Важливою (а, можливо, найважливішою) частиною безпечної діяльності на криптовалютному ринку є пильність, уважність, терпіння і обережність. Це необхідно при всіх аспектах здійснення криптовалютного бізнесу: при наданні особистої інформації інтернет-користувачам чи іншим стороннім особам;

при встановленні двофакторної аутентифікації; при зберіганні приватних ключів; при виборі «холодного» криптовалютного гаманця; при переведенні криптовалютних активів чи фіатних валют із одного криптогаманця на інший чи виведенні коштів із криптобіржі на банківський рахунок чи банківську картку (наприклад, загальновідомим способом викрадення криптовалютних активів із криптогаманців є вірус-кліпер, який, працюючи на зараженому пристрої, у момент заповнення даних для проведення криптовалютної транзакції, змінює адресу запланованого отримувача криптоактивів на дані криптовалютного правопорушника і неуважний відправник криптовалютних активів самостійно, без примусу, пересилає криптовалютні активи на хибну адресу); не слід переходити за «підозрілими» посиланнями, невідомо ким надісланими.

Отже, економічна діяльність на ринку криптовалютних монет потребує значних теоретичних знань, практичних навичок та значної обережності.

Висновки

1. Криптовалютна безпека є не менш важливою при веденні криптовалютного бізнесу, ніж юридичні та економічні знання, пов'язані з роботою криптовалютного ринку.

2. Для максимального підвищення особистої кібернетичної безпеки економічного суб'єкта криптовалютному ринку необхідно застосовувати двофакторну аутентифікацію (2FA) на всьому, що можна, і не використовувати SMS; тримати приватні ключі в офлайні в безпеці на кількох безпечних резервних копіях; у разі довготермінового невикористання криптовалютних активів доцільне їх зберігання в «холодному» криптовалютному гаманці; бути пильним, уважним, терплячим та обережним.

3. Із розвитком ринку криптовалют є ймовірність появи нових способів підвищення особистої кібернетичної безпеки економічного суб'єкта криптовалютному ринку, що вимагатиме подальших наукових досліджень.

Література:

1. The 2020 Global Crypto Adoption Index: Cryptocurrency is a Global Phenomenon. *Chainalysis.* Available at: https://blog.chainalysis.com/reports/2020-global-cryptocurrency-adoption-index-2020 (дата звернення: 12.01.2022)

2. Статистика криптовалют: Bitcoin. *BitInfoCharts.* URL: https://bitinfocharts.com/ru/ (дата звернення: 12.01.2022).

Statystyka kryptovalyut: Bitcoin [Cryptocurrency statistics: Bitcoin]. BitInfoCharts. Available at: https://bitinfocharts.com/ru/ [in Russian]

3. Historical GDP by Country | Statistics from the World Bank | 1960-2020. *KNOEMA*. Available at: https://knoema.ru/mhrzolg/historical-gdp-by-country-statistics-from-the-world-bank-1960-2019 (дата звернення: 27.10. 2021).

4. Ребрик М. А. Криптоактиви: міфи vs факти та потенційний вплив на монетарну сферу. Київ, Національний банк України: Семінар для викладачів ЗВО. 29 травня 2021 р. 56 с. URL: https://bank.gov.ua/admin_uploads/article/Rebryk_2021-29-05.pdf?v=4 (дата звернення: 25.12.2021).

Rebryk M.A. (2021, May, 29) Kryptoaktyvy: mify vs fakty ta potentsiynyy vplyv na monetarnu sferu [Cryptocurrencies: myths vs facts and potential impact on the monetary sphere]. Kyiv: Natsional′nyy bank Ukrayiny: Seminar dlya vykladachiv ZVO. Available at: https://bank.gov.ua/admin_uploads/article/Rebryk_2021-29-05.pdf?v=4 [in Ukrainian].

5. Куницький О. Хакери викрали криптовалюту на понад $600 млн у Poly Network. Це найбільша крадіжка у децентралізованому фінансовому просторі. *Forbes*. 11 серпня 2021. URL: https://forbes.ua/news/khakeri-vikrali-kriptovalyutu-na-ponad-600-mln-u-poly-network-tse-naybilsha-kradizhka-u-detsentralizovanomu-finansovomu-prostori-11082021-2245 (дата звернення: 23.12.2021).

Kunytskyy, O. (2021, August, 11) Khakery vykraly kryptovalyutu na ponad $600 mln u Poly Network. Tse naybil′sha kradizhka u detsentralizovanomu finansovomu prostori [Hackers stole cryptocurrency worth more than $ 600 million from Poly Network. This is the biggest theft in the decentralized financial space]. *Forbes*. Available at: https://forbes.ua/news/khakeri-vikrali-kriptovalyutu-na-ponad-600-mln-u-poly-network-tse-naybilsha-kradizhka-u-detsentralizo-vanomu-finansovomu-prostori-11082021-2245 [in Ukrainian].

6. Гонак І. М. Ризики функціонування криптовалютного бізнесу. *Науковий вісник Херсонського державного університету. Серія «Економічні науки».* 2021. № 44. с. 81–86.

Honak, I. M. (2021) Ryzyky funktsionuvannya kryptovalyutnoho biznesu [The risks of operating a cryptocurrency business]. *Scientific bulletin of kherson state university. Series «Economic sciences»*, 44, 81–86 [in Ukrainian].

7. Залишилось 2 спроби: програміст зі США забув пароль від гаманця з біткоїнами на 220 млн доларів. Економічна правда. 13 січня 2021 р. URL: https://www.epravda.com.ua/news/2021/01/13/669949/ (дата звернення: 03.08.2021).

Zalyshylos′ 2 sproby: prohramist iz SSHA zabuv parol′ vid hamantsya z bitkoyinamy na 220 mln dolariv [There are 2 attempts left: a programmer from the USA forgot the pass-word from his $ 220 million bitcoin wallet] (2021, January, 13). *Ekonomichna pravda*. Available at: https://www.epravda.com.ua/news/2021/01/13/669949/ [in Ukrainian].

8. Неделков К., Цяцьоркін М., Примак К. Хакери вкрали $1,1 млрд у криптовалюті лише за третій квартал 2021-го. Як зберегти криптокошти та анонімність рахунків. *Forbes*. 17 листопада 2021. URL: https://forbes.ua/

money/khakeri-vkrali-11-mlrd-u-kriptovalyuti-lishe-za-tretiy-kvartal-2021-yak-zberegti-kriptokoshti-ta-anonimnist-rakhunkiv-17112021-2796 (дата звернення: 12.01.2022).

Nedelkov, K., Tsyatsorkin, M., Primak, K. (2021, November, 17) Khakery vkraly $1,1 mlrd u kryptovalyuti lyshe za tretiy kvartal 2021-ho. Yak zberehty kryptokoshty ta anonimnist′ rakhunkiv [Hackers stole $ 1.1 billion in cryptocurrency in the third quarter of 2021 alone. How to keep cryptocurrencies and anonymity accounts]. *Forbes*. Available at: https://forbes.ua/money/khakeri-vkrali-11-mlrd-u-kriptovalyuti-lishe-za-tretiy-kvartal-2021-yak-zberegti-kriptokoshti-ta-anonimnist– rakhunkiv-17112021-2796 [in Ukrainian].

9. Сонг Дж., Лопп Дж., Бентон О. #StaySAFU: 5 порад безпеки від професіоналів. *BINANCE*. 29.06.2020. URL: https://www.binance.com/uk-UA/blog/all/staysafu-5-%D0%BF%D0%BE%D1%80%D0%B0%D0%B4-%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8-%D0%B2%D1%96%D0%B4-%D0%BF%D1%80%D0%BE%D1%84%D0%B5%D1%81%D1%96%D0%BE%D0%BD%D0%B0%D0%BB%D1%96%D0%B2-421499824684900668 (дата звернення: 26.12.2021).

Song, J., Lopp, J., Benton, O. (2020, June, 12). #StaySAFU: 5 porad bezpeky vid profesionaliv [#StaySAFU: 5 safety tips from professionals]. *BINANCE.* Available at: https://www.binance.com/uk-UA/blog/all/staysafu-5-%D0%BF%D0%BE%D1%80%D0%B0%D0%B4-%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8-%D0%B2%D1%96%D0%B4-%D0%BF%D1%80%D0%BE%D1%84%D0%B5%D1%81%D1%96%D0%BE%D0%BD%D0%B0%D0%BB%D1%96%D0%B2-421499824684900668 [in Ukrainian].

10. Що таке «холодний» крипто-гаманець та як захистити його від зламу? Поради. *cybercalm*. 12.06.2020. URL: https://cybercalm.org/novyny/shho-take-holodnyj-krypto-gamanets-ta-yak-zahystyty-jogo-vid-zlamu-porady/ (дата звернення: 05.01.2022).

Shcho take "kholodnyy" krypto-hamanets′ ta yak zakhystyty yoho vid zlamu? Porady. [What is a "cold" crypto-wallet and how to protect it from burglary? Advice]. (2020, June, 12). *cybercalm.* Available at: https://cybercalm.org/novyny/shho-take-holodnyj-krypto-gamanets-ta-yak-zahystyty-jogo-vid-zlamu-porady/ [in Ukrainian].