в умовах сучасного інформаційного суспільства.

1. Інституціональне забезпечення конкурентоспроможності національної економіки: монографія / за заг.ред. д.е.н., проф.С.Ю. Хамініч._ Дніпро : Арт-Прес.2023. 144с.

2. Alieksieieva S., Kozhusko O., Khaminich S. Information system protection as a factor in maintaining the leading positions in the enterprise development. Proceedings of the 3rd International Conference on Social, Economic, and Academic Leadership (ICSEAL 2019), Series: Advances in Social Science, Education and Humanities Research, https://doi.org/10.2991/icseal-19.2019.67. URL : https://www.atlantis-press.com/proceedings/icseal-19/articles. p.428-432/

3. Хамініч С.Ю. Інституціональні засади економічної безпеки України в умовах війни // Міжнародний науковий журнал «Інтернаука». Серія: «Економіка». 2023. № 2. URL : https://doi.org/10.25313/2520-2294-2023-2-8626.

УДК 004.738.5
DOI: 10.31733/15-03-2024/2/345-346

Олександр ТУБАНЬ
аспірант Науково-дослідного інституту
приватного права і підприємництва
імені академіка Ф. Г. Бурчака
НАПрН України

ОКРЕМІ АСПЕКТИ УБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ ВІД ЗАГРОЗ В ЕЛЕКТРОННИХ МЕРЕЖАХ

У сучасному світі надзвичайно швидко поширилися інформаційні технології, які супроводжують кожну галузь і сферу господарювання і повсякденного буття людини. Велику кількість угод можна укласти, не виходячи із дому чи офісу. Навіть сфера обігу національної валюти поступово втрачає вагу на фоні поширення обігу електронних грошей – криптовалют, ще генеруються на блокчейн-платформах. Навіть саме генерування, видобуток, виробництво або «майнінг» одиниць криптовалюти має децентралізований характер. Кожне підприємство або людина, які мають комп'ютери із сучасним програмним забезпеченням, можуть займатися «майнінгом» криптовалюти. А сама ця діяльність має значну схожість із класичними видами господарської діяльності [1]. Із п'яти ознак, що характеризують економічну сутність як правосуб'єктне утворення, чотири повною мірою притаманні таким особам та групам, а п'ята ознака має переважно суб'єктивний характер. Офіційне визнання державою законним видом господарської діяльності «майнінгу» криптовалюти та визнання господарськими операцій із її купівлі-продажу у комплексі з покладанням на «майнерів» обов'язку офіційно зареєструватись як суб'єкт підприємницької діяльності, поширенням на всіх учасників відносин на ринку криптовалюти дії законодавства про оподаткування та кримінальної, адміністративної, господарської відповідальності до порушників дасть змогу усунути невизначений або гібридний правовий статус суб'єктів та режим їхньої діяльності, а також наявні прогалини у праві та законодавстві [1]. Проте проблема у легітимації «майнерів» криптовалюти не є найскладнішою і не становить найвищої загрози кібербезпеці держави. Забезпечення кібербезпеки України важливе не лише для економічного розвитку, але й для забезпечення захисту національної безпеки та підвищення ступеня довіри громадян.

Проєктом Стратегії кібербезпеки України визначено пріоритети, цілі та завдання забезпечення кібербезпеки України з метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави [2].

Аналіз кіберзагроз та ризиків в контексті поширення обігу криптовалют у сучасному суспільстві стає критично важливим завданням для забезпечення кібербезпеки в електронних мережах України.

Сучасний кіберпростір спрямований на подальший розвиток технологій, але разом із тим породжує нові виклики та загрози. Аналіз кіберзагроз у сфері обігу криптовалют включає в себе вивчення різноманітних аспектів:

- фінансові шахрайства: передбачає дослідження методів та схем шахрайства, спрямованих на виведення коштів через використання криптовалют;
- технічні загрози: передбачає виявлення вразливостей у блокчейн-платформах, їх

використання для викрадення та маніпулювання активами;

- відмивання грошей: передбачає аналіз методів використання криптовалют для легалізації неправомірно отриманих коштів;

- кібератаки на блокчейн-мережі: передбачає вивчення загроз та можливостей кібератак на самі блокчейн-мережі;

- соціальна інженерія: передбачає аналіз соціальних аспектів кіберзагроз, зокрема, фішингу та інших методів соціальної інженерії;

- законодавчий аспект та регулювання: передбачає вивчення законодавства та регулювання у галузі обігу криптовалют для виявлення прогалин та розробки ефективної нормативно-правової бази.

Аналіз кіберзагроз та ризиків є необхідним етапом для розробки стратегій кібербезпеки, що дозволить уникнути негативних наслідків та забезпечити стабільність у функціонуванні криптовалютної інфраструктури.

Важливим кроком у забезпеченні кібербезпеки в контексті обігу криптовалют є розробка і прийняття чіткого та адаптивного законодавства [3]. Регулювання обміну криптовалют, контроль за ICO (Initial Coin Offerings) та інші нормативні аспекти є необхідними для забезпечення легального та безпечного використання цих технологій.

У мережі обігу криптовалют, де використовуються цифрові активи та здійснюються транзакції, розробка і вдосконалення технічних засобів кіберзахисту є надзвичайно важливою. Це включає в себе розробку сучасних систем виявлення аномалій, захист від хакерських атак та забезпечення конфіденційності особистих даних.

Україна повинна активно співпрацювати з іншими країнами, щоб обмінюватися інформацією про кіберзагрози та враховувати міжнародні стандарти кібербезпеки. Тільки через спільні зусилля можна ефективно протистояти глобальним кіберзагрозам у сфері обігу криптовалют.

Розвиток екосистеми криптовалют вимагає стимулювання інновацій та обміну досвідом. Фінансова підтримка для стартапів, активна участь у розробці нових технологій та обмін кращими практиками грають ключову роль у створенні безпечного та стійкого криптовалютного середовища.

Загальний успіх у забезпеченні кібербезпеки у сфері обігу криптовалют вимагає гармонійної взаємодії різних суб'єктів, починаючи від уряду та закінчуючи приватним сектором, активною участю громадян. Лише в такий спосіб Україна зможе стати не лише платформою для розвитку криптовалют, а й цілком захищеним та стійким актором у динамічному цифровому світі.

1. Деревянко Б.В. Про порівняння господарської діяльності з видобутком криптовалюти («майнінгом») та здійсненням операцій із нею. *Право України.* 2018. № 5. С. 164–175. URL : https://pravoua.com.ua/ua/store/pravoukr/pravo_2018_5/

2. Стратегія кібербезпеки України (2021 – 2025 роки): проєкт. Безпечний кіберпростір – запорука успішного розвитку країни. URL : https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf

3. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII. *Відомості Верховної Ради України.* 2017. № 45. Ст. 403.

УДК 004.738.5:316.472.4
DOI: 10.31733/15-03-2024/2/346-348

Дмитро ЮРЧЕНКО
аспірант кафедри
управління та адміністрування
Дніпропетровського державного
університету внутрішніх справ

ВИКОРИСТАННЯ КОМПЛЕКСНОГО АНАЛІЗУ СОЦІАЛЬНИХ МЕДІА В ДЕРЖАВНОМУ СЕКТОРІ

Комплексний аналіз соціальних медіа в державному секторі є невід'ємною частиною сучасної стратегії управління та комунікацій. Соціальні медіа стали не лише платформами для особистого висловлення, але й потужним інструментом для державних установ у взаємодії з громадськістю, формування довіри до владних структур, а також