Дмитро ЛЕЩЕНКО
доцент кафедри
адміністративно-правових
дисциплін та публічного управління
Дніпровського державного
університету внутрішніх справ,
адвокат (м. Дніпро, Україна),
кандидат юридичних наук, доцент
https://orcid.org/0009-0000-8955-8892

КІБЕРБЕЗПЕКА ВІРТУАЛЬНИХ АКТИВІВ: РЕГУЛЯТОРНІ РІШЕННЯ, СУДОВА ПРАКТИКА ТА ЗАХИСТ В УКРАЇНІ Й ЗА КОРДОНОМ

19.12.2024 відбулася наймасштабніша зовнішня кібератака на державні реєстри України, внаслідок якої було призупинено роботу єдиних та державних реєстрів, які перебувають у компетенції Міністерства юстиції України.

Відповідальність за кібератаку взяла на себе російська хакерська група XakNet Team, яка заявила, що зламала інфраструктуру ДП «Національні інформаційні системи», що керує реєстрами Міністерства юстиції України. У своїх телеграм-каналах вони стверджували, що завантажили понад мільярд рядків даних і видалили їх разом із резервними копіями. За даними СБУ, за атакою стояли російські спецслужби, зокрема угруповання, пов'язані з ГРУ [1].

Через зупинення роботи реєстрів частково припинили працювати деякі державні сервіси, які були зав'язані на роботі реєстрів. Зокрема, сервіси платформи «Дія», як-от: перереєстрація авто, бронювання працівників, «єВідновлення», витяги з ЄДР та ін. Також тимчасово недоступним стало оформлення відстрочок у застосунку «Резерв+». Крім того, викликані кібератакою збої зупинили реєстрацію нових компаній, унеможливили видачу ліцензій, ускладнили перевірку керівників і заблокували взаємодію бізнесу з державою. Розмір збитків в межах країни ще не підраховано, але він, беззаперечно, чималий.

Згідно з доповіддю Cybersecurity Ventures, збитки внаслідок дій кіберзлочинців у 2023 р. сягнули 8 трлн дол. У 2025 р. ця цифра може зрости до вражаючих 10.5 трлн дол. Кібератаки не обмежуються лише державними інституціями чи великими корпораціями. В поле зору хакерів потрапляє критична інфраструктура (яскравий приклад – масована атака на телеком-оператора «Київстар»), МСБ, неурядові організації. Цей сплеск зумовлений дедалі складнішими кібератаками, інцидентами з програмами-вимагачами та витоками даних, що збільшуються щороку в усьому світі [2].

Не становлять винятку і криптобіржі, що використовують блокчейн-технологію, яка пропонує безпечну архітектуру збереження та передачі даних та базується на принципах криптографії, децентралізації та консенсусу.

Одна з найгучніших та найбільших історій – це злам FTX у 2022 р., який призвів до краху однієї з найбільших криптовалютних бірж. Він особливо цікавий тим, що показав уразливість навіть найбільших гравців ринку і важливість правильного зберігання віртуальних активів. Внаслідок кібератаки було викрадено понад 477 млн дол. у віртуальній валюті. Подія викликала паніку на крипторинку та обвал цін. Як наслідок, посилився нагляд за криптобіржами, до яких багато інвесторів втратили довіру, та почалося розслідування з боку FBI і SEC (слідство все ще триває, і досі не знайдено всіх вкрадених коштів).

Збанкрутіла криптобіржа FTX подала в суд на Binance та її колишнього гендиректора Ч. Чжао, вимагаючи повернути майже 1,8 млрд дол. Позов проти Binance – один із багатьох, поданих FTX проти колишніх інвесторів, партнерів та клієнтів у суді штату Делавер. Серед інших відповідачів – колишній співробітник Білого дому Е. Скарамуччі, криптобіржа Crypto.com та політичні організації, включаючи засновану М. Цукербергом FWD.US.

У 2023 р. і сама криптобіржа Binance зазнала кібератаки, що призвела до викрадення понад 100 млн дол. у криптовалюті. Після атаки уряди США та ЄС посилили вимоги до безпеки криптобірж. Binance частково компенсувала втрати користувачів через страхові фонди. А Інтерпол та Європол активізували зусилля з пошуку кіберзлочинців.

У цілому за період з 2020 до 2025 р. кіберзлочинці значно активізували атаки на криптовалютні гаманці та криптобіржі, що призвело до суттєвих втрат для інвесторів та викликало необхідність посилення правового регулювання у цій сфері.

Інтеграція віртуальних валют у світову фінансову систему створила нові виклики для правового регулювання, особливо щодо захисту віртуальних активів у різних юрисдикціях.

Станом на 2025 рік правовий статус криптоактивів варіюється залежно від юрисдикції:

1) у США криптоактиви класифікуються або як цінні папери, або як товари (відповідно до визначення Комісії з торгівлі товарними ф'ючерсами, CFTC) [3];

2) в ЄС Регламент Markets in Crypto-Assets (MiCA) класифікує криптоактиви як фінансові інструменти особливого типу, встановлюючи вимоги до їхнього випуску та обігу [4];

3) в Україні закон «Про віртуальні активи» (який ще так і не набрав чинності) визнає віртуальні активи нематеріальними благами, що є об'єктами цивільних прав, мають вартість та виражені сукупністю даних в електронній формі. Віртуальні активи можуть посвідчувати майнові права, зокрема права вимоги щодо інших об'єктів цивільних прав [5].

Відсутність уніфікованого законодавства в світі ускладнює боротьбу з кіберзлочинністю та захист прав криптоінвесторів.

Показовими судовими прецедентами є:

I. Рішення Верховного Суду США у справі SEC v. Ripple Labs (2023) [6], де суд вперше визнав необхідність диференційованого підходу до регулювання різних видів криптоактивів;

II. Рішення Федерального суду Південного округу Нью-Йорка у справі United States v. Johnson (2024) [7], де суд встановив, що фішингова атака на криптогаманці підпадає під дію закону про шахрайство з цінними паперами, що створило важливий прецедент для подібних справ (шахрайство з використанням електронних засобів відповідно до § 1343, 18 U.S.C.).

За даними міжнародної юридичної фірми Clifford Chance, кількість судових справ, пов'язаних із кібератаками на криптоактиви, демонструє стійке зростання:

1) 2020 р. – 234 справи;
2) 2021 р. – 387 справ;
3) 2022 р. – 456 справ;
4) 2023 р. – 612 справ;
5) 2024 р. – 589 справ [8].

Ця тенденція свідчить про зростаючу активність кіберзлочинців та необхідність удосконалення правових механізмів захисту віртуальних активів.

Аналіз судової практики свідчить, що успішність повернення викрадених активів залежить від:

– юрисдикції криптобірж або платформ: у різних країнах діють різні правові режими щодо криптоактивів, що впливає на можливість повернення коштів;

– наявності страхового покриття: деякі криптобіржі забезпечують страхування віртуальних активів користувачів, що підвищує шанси на компенсацію втрат;

– швидкості реагування правоохоронних органів: оперативні дії можуть запобігти виведенню коштів за межі досяжності;

– міжнародної співпраці у розслідуванні: спільні дії правоохоронних органів різних країн підвищують ефективність розслідувань.

Станом на 2025 р. у світі діють такі ключові законодавчі ініціативи щодо захисту віртуальних активів:

а) а) у США ініційовано прийняття Digital Asset and Cyber Security Act (2024), який вимагає від криптобірж дотримання жорстких стандартів безпеки;

б) б) у ЄС розширено регламент MiCA, який зобов'язує криптоплатформи впроваджувати системи KYC (Know Your Customer) та AML (Anti-Money Laundering).

Щоб підвищити ймовірність повернення втрачених криптоактивів, інвесторам рекомендується:

– фіксувати всі трансакції та зберігати дані про операції на криптобіржах;

– оперативно звертатися до правоохоронних органів у разі підозрілих дій потенційних кіберзлочинців;

– використовувати міжнародні юридичні механізми, такі як арбітражні суди та адвокатські розслідування.

Юридичні аспекти кібербезпеки у сфері захисту віртуальних активів залишаються складними та динамічними. З кожним роком держави посилюють регулювання, але проблеми, пов'язані з кібербезпекою, все ще існують.

Основними тенденціями, які потребуватимуть посиленої уваги та ретельного дослідження у короткостроковій перспективі, будуть збільшення кількості судових справ

щодо кіберзлочинів у криптосфері, посилення міжнародного регулювання та координації між правоохоронними органами, а також підвищення юридичної грамотності інвесторів для захисту своїх віртуальних активів.

Правове регулювання віртуальних активів – це сфера, що постійно розвивається. Ефективний юридичний захист інвесторів потребує не лише удосконалення чинного законодавства України, ЕС, США та інших країн, а й активної взаємодії з державними та приватними ініціативами щодо забезпечення кібербезпеки віртуальних активів у всьому світі.

1. Жахалов Я. Кібератака на реєстри Мін'юсту: чому це могло статися і які наслідки DOU.ua. URL : https://dou.ua/lenta/articles/cyberattacks-on-registries-and-vendor-locks/.
2. Боянжи В. Основні тенденції у кібербезпеці на 2024 рік: які виклики стоять перед бізнесом. ISSP. URL : https://www.issp.ua/post/main-cybersecurity-trends-in-2024.
3. Crypto Assets. Investor.gov. https://www.investor.gov/additional-resources/spotlight/crypto-assets.
4. Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937. EUR-Lex. URL : https://eur-lex.europa.eu/eli/reg/2023/1114/oj/eng.
5. Про віртуальні активи : Закон України від 17 лютого 2022 р. (не набрав чинності). URL : https://zakon.rada.gov.ua/laws/show/2074-20#Text.
6. SEC v. Ripple Labs, Inc. (2023). Case 1:20-cv-10832-AT-SN Document 874 Filed 07/13/23. URL : https://www.nysd.uscourts.gov/sites/default/files/2023-07/SEC%20vs%20Ripple%207-13-23.pdf.
7. United States v. Johnson, 383 U.S. 169 (1966). Justia. U.S. Supreme Court. URL : https://supreme.justia.com/cases/federal/us/383/169/.
8. Clifford Chance. Cyber security in the crypto-asset sector. 18 U.S.C. § 1343 – Fraud by wire, radio, or television.

Микола ПОЛІЩУК
доцент кафедри,
кандидат технічних наук
https://orcid.org/0000-0002-1218-5925

Лілія ПОЛІЩУК
асистент кафедри
комп'ютерної інженерії та безпеки
Луцького національного технічного
університету (м. Луцьк, Україна)

МЕТОДОЛОГІЧНІ АСПЕКТИ ТА СУЧАСНІ ПІДХОДИ ДО ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ВІЙНИ

В умовах російсько-української війни інформаційна безпека набуває критичного значення, оскільки комунікаційний простір стає полем бою, де ворог використовує дезінформацію, кібератаки та психологічний тиск для досягнення своїх цілей.

У сучасних умовах інформаційна безпека України постала як критично важливий елемент національної безпеки. Сучасні конфлікти характеризуються активним використанням інформаційних технологій для досягнення військових та політичних цілей, що вимагає нових підходів до забезпечення захисту інформаційного простору держави.

Таким чином, постає необхідність у розробці нових методологічних підходів, які б враховували специфіку сучасних інформаційних загроз та забезпечували ефективний захист національних інтересів. Це включає дослідження взаємодії між технологічними, соціальними та психологічними аспектами інформаційної безпеки, а також розробку комплексних стратегій протидії інформаційній агресії.

У наукових дослідженнях значна увага приділяється таким аспектам, як дослідження базових концепцій та підходів до забезпечення інформаційної безпеки держави, особливо в умовах збройних конфліктів [2], аналіз ролі державних та недержавних інституцій у формуванні та реалізації політики інформаційної безпеки в контексті гібридної війни [4] та вивчення новітніх загроз, таких як кібератаки, дезінформація та інформаційно-психологічні операції, а також розробка стратегій протидії цим загрозам [3].

Наукові джерела не лише узагальнюють теоретико-методологічні основи інформаційної безпеки, але й аналізують сучасні виклики та загрози в інформаційній сфері, пропонуючи практичні рекомендації для їх подолання.