DOI: https://doi.org/10.26642/jen-2023-4(106)-155-166
УДК 336.74:004.056.5

С.В. Миненко, PhD
К.О. Могильна, студентка
Сумський державний університет

Оцінка впливу використання криптовалют на кібербезпеку: досвід Європейського Союзу

Економічні наслідки кіберзлочинності часто є руйнівними. Кіберзлочинність призводить до фінансових втрат внаслідок викрадення коштів, витрат на розслідування і нейтралізацію наслідків злочинів, відновлення довіри громадян і впровадження покращень безпеки, зниження рівня суспільної довіри та інвестиційної привабливості країн і компаній. Усе це робить питання розвитку та вивчення кібербезпеки стратегічно важливими. Одним з ключових факторів, які впливають на національний рівень кібербезпеки, є поширеність і використання населенням сучасних технологій, зокрема криптовалют, при цьому вплив використання населенням криптовалют та їх регулювання на кібербезпеку не є очевидним. Тому дослідження впливу використання криптовалют на кібербезпеку наразі є актуальним питанням.

Метою дослідження є вивчення впливу використання криптовалюти на кібербезпеку в країнах Європейського Союзу. Створена регресійна модель підтвердила статистичну значущість впливу на оцінку кібербезпеки країни таких аспектів використання криптовалюти, як поширеність, правове регулювання, інвестиційні навички користувачів та використання даркнету. Найбільш позитивно на оцінку кібербезпеки країни впливає впровадження правових заходів у сфері регулювання цифрових активів, що доводить ефективність правового регулювання цифрових активів у країнах ЄС. Найбільш негативно на оцінку кібербезпеки впливає збільшення кількості активних користувачів криптовалют (таких, які користуються мобільним додатком для інвестування в криптоактиви раз на тиждень і частіше).

Практична значущість дослідження полягає у тому, що воно має потенціал для сприяння майбутній розробці політики регулювання цифрових активів в Україні, яке забезпечувало б баланс між мінімізацією ризиків кібербезпеки і сприянням інноваціям. Доведення позитивного впливу європейських практик правового регулювання цифрових активів створює перспективу для подальших досліджень ефективності окремих регуляторних заходів та можливості їх адаптації до українських реалій.

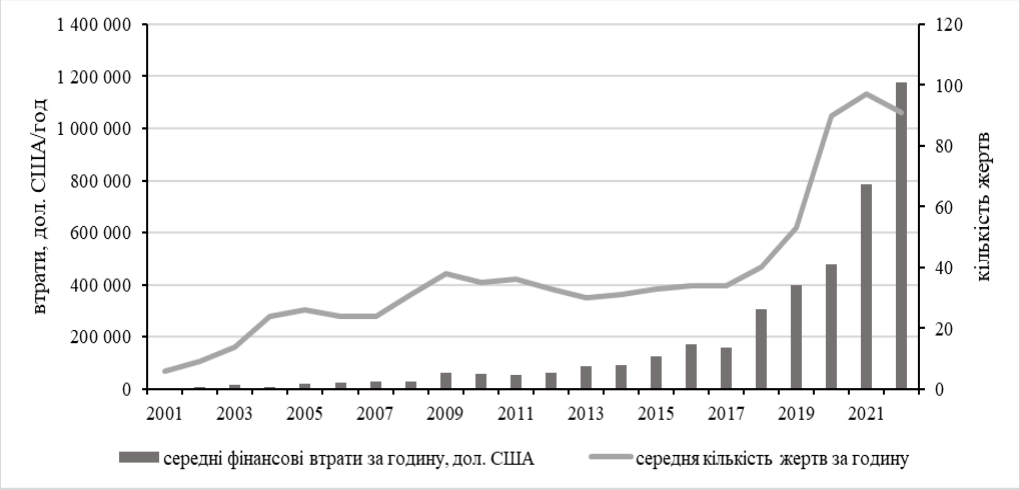
Ключові слова: *кібербезпека; кіберзлочинність; криптовалюти; цифрові активи; регулювання криптовалют; регресійний аналіз.*

Актуальність теми. Кібербезпека відповідає за низку важливих для суспільства завдань, зокрема вона значно та багатогранно впливає на економіку країни. Наприклад, порушення кібербезпеки призводить до прямих фінансових втрат внаслідок крадіжки, шахрайства або відмивання коштів, вимагає подальших витрат на підвищення рівня безпеки, відновлення репутації, нейтралізацію наслідків збоїв у роботі критичної інфраструктури, викликаних кібератаками тощо. Водночас розвиток технологій та методів цифрових злочинців, вразливість критичної інфраструктури, підвищення залежності життя суспільства від технологій і поширення цифровізації, прискорені пандемією COVID–19, сприяють поступовому збільшенню економічної шкоди, спричиненої кібератаками. Прослідкувати цю тенденцію можна за рисунком 1. Європейські країни не є виключенням із загального тренда, за даними Європейського Союзу з кібербезпеки (ENISA), у 2020 році було зареєстровано 304 786 кібератак, що на 36 % більше, ніж у попередньому році [1]. Повномасштабне вторгнення росії в Україну також сприяло підвищенню активності хакерів та кіберзлочинців за спонсорства країни-агресора, прикладом цього є найбільша за всю історію, за даними ENISA[2], атака типу DDoS в Європі у липні 2022 року та низка атак, спрямованих на інфраструктуру України, зокрема кібератака, яка у перший день повномасштабного вторгнення паралізувала роботу американської телекомунікаційної компанії Viasat на території України, створивши проблеми з доступом до інтернету для багатьох українських компаній і державних служб.

Через збільшення кількості кібератак, підвищення хакерської активності та цифровізації суспільства, уряди більшості країн у співпраці з організаціями приватного сектору, академічними колами та фахівцями з кібербезпеки змушені вдаватися до зважених заходів підвищення кібербезпеки для захисту національної безпеки й розвитку інформаційного сектору. Варто зауважити, що впровадження урядових політик і стратегій, спрямованих на підвищення кібербезпеки країни, вимагає проведення ґрунтованого дослідження та розуміння факторів, які впливають на поширення та активність цифрових загроз.

Одним з факторів, який може впливати на кібербезпеку, є цифровізація суспільства. Поширення нових технологій, таких як штучний інтелект, Інтернет речей, хмарні обчислення або криптовалюти,

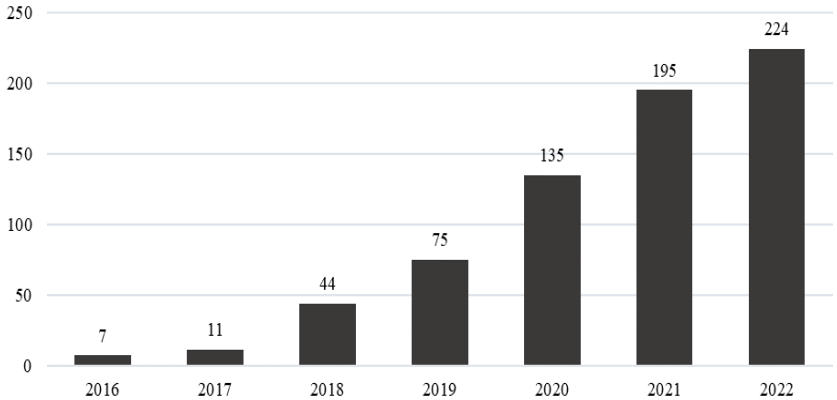
може створювати нові вектори атак кіберзлочинців, потенційні ризики для інформаційної безпеки, потребу розробки нових стандартизованих практик перевірки та протидії виявленим методам злочинності тощо. Наприклад, криптовалюти, через децентралізацію, слабке регулювання й конфіденційність блокчейн-технологій, можуть використовуватися кіберзлочинцями для відмивання грошей, платежів програм-вимагачів і фінансування злочинних дій. Крім того, конфіденційність платежів може створити перепони для відстеження та розслідування кіберзлочинів правоохоронними органами. Більш повне розуміння впливу криптовалют на кібербезпеку може допомогти урядам у розробці ефективних програм для підвищення кібербезпеки та боротьби з цифровими атаками.



Джерело: створено авторами на основі Статистики кіберзлочинності. Surfshark [3]

Рис. 1. Динаміка втрат від кіберзлочинності у світі протягом 2001–2022 років

Аналіз останніх досліджень та публікацій, на які спираються автори. Підвищення актуальності теми кібербезпеки з наведених раніше причин, а також поширення криптовалют сприяють підвищенню уваги науковців до вивчення взаємного впливу цих явищ. Цей тренд можна простежити за значним збільшенням чисельності наукових робіт, що містять словосполучення, близькі до «impact of cryptocurrencies on cyber security», опублікованих у базі наукових публікацій Science Direct протягом 2016–2022 років, що відображено на рисунку 2.



Джерело: створено авторами на основі інформації бази даних опублікованих наукових досліджень Science Direct [4]

Рис. 2. Кількість статей, що містять словосполучення, схожі до «impact of cryptocurrencies on cyber security», опублікованих у Science Direct протягом 2016–2022 років

Очевидно, що тема взаємозв'язку цифрової безпеки та використання криптовалют цікавила багатьох українських та закордонних дослідників. Прикладами робіт вітчизняного авторства на цю тему є тези В.Черновола на тему шахрайства із використанням криптовалюти [5], І.Абузова з вивчення шахрайських схем з використанням біткоїнів [6], В.Ковтун і П.Клімушина про прихований майнінг криптовалюти й обмеження браузерного криптоджекінгу [7]. Усі названі роботи об'єднує спрямованість на вивчення

окремого виду кіберзагрози (шахрайства або ж криптоджекінгу) з використанням криптовалют і акцентуація уваги переважно на технічному аспекті кібербезпеки та злочинних схем.

Серед іноземних науковців тему взаємозв'язку криптовалют та кібербезпеки вивчали С.Рамос, Л.Мелон, Д.Еллул у статті на тему розвитку технічного регулювання кібербезпеки блокчейну і регулювання криптоактивів у ЄС [8], Д.Кірутика і К.Ренганатан у роботі присвяченій заходам щодо стримування кіберзагроз, пов'язаних з криптовалютами [9], Д.Тібіна Апурі в статті про еволюцію та поточні підходи до протидії використанню біткоїнів кіберзлочинцями [10]. Як ми бачимо, у наведених роботах переважно розглядають підходи до державного регулювання криптовалют з метою запобігання і зменшення кіберзлочинності.

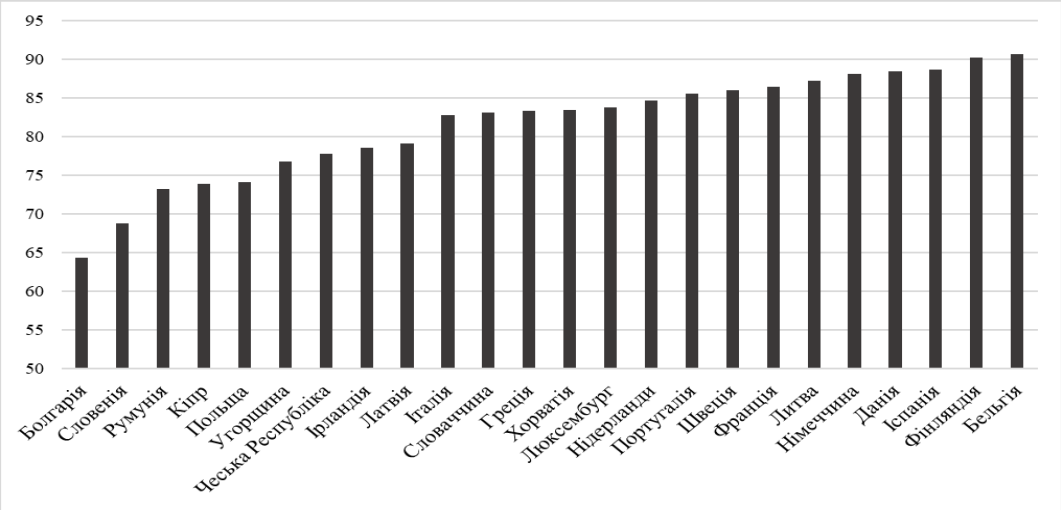
Таким чином, проведений нами аналіз наукової літератури дозволяє зробити висновок, що тема взаємозв'язку поширеності й використання криптовалют на кібербезпеку є актуальною і користується увагою наукової спільноти. Проте розглянуті нами роботи зосереджувалися переважно на технічному та правовому аспектах поширеності та використання криптовалют у цифровій злочинності, в той час як тема впливу окремих аспектів використання криптовалют на кібербезпеку країни лишається недостатньо дослідженою та потребує більшої уваги науковців.

Метою статті є вивчення впливу аспектів використання криптовалют (зокрема, їх поширеності, цифрових та інвестиційних навичок населення, обсягу тіньової економіки та використання громадянами даркнету) на кібербезпеку країни, на прикладі країн Європейського Союзу.

Викладення основного матеріалу. З огляду на проведений аналіз та сформульовану мету дослідження для досягнення наших цілей доцільно побудувати економетричну модель множинної регресії, яка демонструє вплив використання криптовалюти на оцінку кібербезпеки держави. Аналіз економічного змісту проведеного моделювання і перспектив державного регулювання криптовалютної діяльності дозволить підвищити рівень кібербезпеки країни.

Для проведення моделювання нами було зібрано набір даних, з десятьма факторними змінними, які характеризують аспекти використання криптовалюти, і однією результатною змінною, яка демонструє рівень кібербезпеки країни. Набір даних зібраний щодо 24 країн Європейського Союзу у 2020 році.

Залежною ознакою нами було обрано загальну оцінку кібербезпеки країни відповідно до Глобального звіту про кіберзлочинність компанії SEON [11], оскільки вона оцінює за 100-бальною шкалою загальний рівень кібербезпеки країни, базуючись на таких аспектах, як Національний індекс кібербезпеки [12] (індекс, оцінюваний NCSI Project Team, який зосереджений на оцінці готовності країн запобігати кіберзагрозам за рівнем впровадження відповідних нормативно-правових актів), Глобальний індекс кібербезпеки [13] (показник, створений ITU-D, відділом Міжнародного союзу електрозв'язку, він, крім правових, оцінює технічні, організаційні, кооперацийні заходи, а також розвиток потенціалу країни у сфері кібербезпеки) і Індекс ризику кібербезпеки [14] (індекс, оцінюваний компанією PasswordsManagers.co, який базується на рейтингах країн за кількістю виявлених випадків цифрових загроз різних видів). Таким чином, загальна оцінка кібербезпеки країни враховує найбільшу кількість аспектів кіберебезпеки країни, починаючи від оцінки правового поля й закінчуючи кількістю виявлених кіберзлочинів, тому вона є репрезентативним показником загального рівня захищеності країни від цифрових загроз. Найвищі оцінки кібербезпеки за цим показником станом на 2020 рік мають такі країни Європейського Союзу, як Бельгія, Фінляндія й Іспанія (рис. 3).



Джерело: створено авторами на основі Глобального звіту про кіберзлочинність компанії SEON [11]

Рис. 3. Оцінка кібербезпеки (y_2) країн Європейського Союзу станом на 2020 рік

Список факторних змінних (табл. 1), характеризує 5 аспектів використання криптовалют населенням країни, зокрема:

— поширеність володіння та використання криптовалют серед населення країни (змінні x_1, x_3, x_4, x_8): популярність криптовалютного ринку може привернути додаткову увагу кіберзлочинців до можливостей шахрайства й викрадення коштів користувачів, криптоджекінгу, використання криптовалют для відмивання коштів або спонсорування злочинної діяльності тощо;

— державне правове регулювання використання криптовалют (змінна x_6): ефективне регулювання криптовалютної діяльності урядами та регуляторними органами може сприяти ідентифікації користувачів на криптовалютних біржах, забезпеченню заходів безпеки, запобіганню відмиванню грошей і фінансуванню тероризму; усе це має позитивно вплинути на кібербезпеку країни;

— цифрова грамотність населення (змінні x_2 і x_7): цифрова грамотність населення може знизити ризики кіберзлочинності з використанням криптовалют, адже допомагає користувачам бути обізнаними про поширені методи кіберзлочинності (зокрема фішинг, шахрайство, джекінг та ін.), створювати більш надійні ключі захисту до криптовалютних гаманців, виявляти підозрілі дії інших користувачів, користуватися більш захищеними біржами та іншими платформами з криптовалютними транзакціями тощо;

— інвестиційна грамотність населення (змінні x_8 і x_9): інвестиційна грамотність населення може позитивно впливати на рівень кібербезпеки країни, оскільки вона свідчить про обізнаність населення щодо інвестиційного шахрайства, розуміння нестабільності ринку і необхідності захисту інвестиційних платформ, можливості оцінки інвестиційних ризиків та ін.;

— поширеність у країні сфер злочинного використання криптовалют (x_5 і x_{10}): змінні цієї категорії характеризують обсяг ринку даркнету країни й обсяг її тіньової економіки, високий рівень обох змінних може негативно впливати на рівень кібербезпеки країни, оскільки оплата злочинних товарів і послуг за допомогою криптовалюти в даркнеті або поза державним обліком і контролем (тіньова економіка) може вказувати на нерегульованість криптовалютного ринку й свідчити про наявність злочинних криптовалютних транзакцій.

Таблиця 1

Факторні змінні, які характеризують аспекти використання криптовалют в країні

Змінна	Показник	Джерело даних
x_1	Відсоток населення, який має право власності на криптовалюти	Дані про право власності на криптовалюту. Криптовалюта в усьому світі. Triple-A [15]
x_2	Відсоток осіб з базовими або вище загальними цифровими навичками	ESS: опитування ЄС щодо використання ІКТ у домогосподарствах та окремими особами. Євростат [16]
x_3	Відсоток опитаних, який має або мав криптовалюти (інше джерело)	Flash Eurobarometer FL509: Роздрібні фінансові послуги та продукти [17]
x_4	Відсоток опитаних, який користується мобільним додатком для інвестування в криптоактиви раз на тиждень і частіше	
x_5	Загальний дохід ринку даркнету (в євро на душу населення)	Криптовалюти та наркотики: аналіз використання криптовалюти на ринках даркнету в ЄС та сусідніх країнах. Довідковий документ на замовлення EMCDDA [18]
x_6	Оцінка правових заходів у сфері регулювання цифрових активів (за 20-бальною шкалою)	Глобальний індекс кібербезпеки 2020. Вимірювання відданості кібербезпеці. Сектор розвитку Міжнародного союзу електрозв'язку [13]
x_7	Відсоток осіб, які користувалися Інтернетом протягом останніх 3 місяців	Використання ІКТ у домогосподарствах та окремими особами. Євростат [19]
x_8	Відсоток населення, який інвестує в криптовалюту	Flash Eurobarometer FL509: Роздрібні фінансові послуги та продукти [17]
x_9	Відсоток населення, який інвестує в традиційні активи	
x_{10}	Розмір тіньової економіки за 2020 рік (у % офіційного ВВП)	Оподаткування неформальної економіки в ЄС. Дослідження на запит комітету FISC [20]

Джерело: розробка авторів

Таким чином нами було створено набір даних для подальшої побудови регресійної моделі з метою оцінки впливу аспектів використання криптовалют на оцінку кібербезпеки країн Європейського Союзу (табл. 2).

Під час дослідження нами були використані такі загальнонаукові методи, як аналіз, синтез, абстракція, аналогія та узагальнення. Основним методом моделювання є використання багатофакторної регресії. Цей метод був обраний, оскільки він є простим та гнучким у вивченні впливу множини факторів на результатну змінну, а також дозволяє оцінити відносну важливість різних незалежних змінних у поясненні варіації залежної змінної і провести економічну інтерпретацію виявлених зв'язків.

Таблиця 2

Набір даних для побудови регресійної моделі

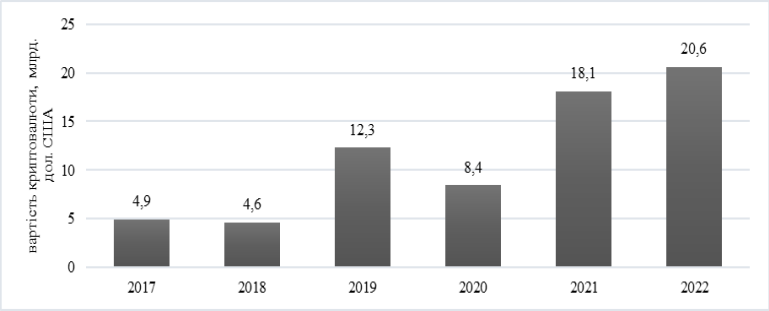
Країна	Змінна										
	y	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	x_{10}
Бельгія	90,7	1,4	54,2	6,5	4,3	260,9	20,0	81,1	6,0	32,0	16,2
Болгарія	64,4	2,2	31,2	13,1	10,8	328,9	17,3	19,8	13,0	13,0	32,9
Греція	83,4	1,5	52,5	10,0	8,0	110,8	19,4	54,0	10,0	11,0	20,9
Данія	88,4	1,2	68,7	7,6	6,4	244,0	19,3	95,7	8,0	36,0	9,8
Ірландія	78,6	1,1	70,5	10,9	6,7	310,4	20,0	77,7	11,0	21,0	9,9
Іспанія	88,6	3,0	64,2	7,8	7,7	154,6	20,0	69,4	8,0	27,0	17,4
Італія	82,8	2,4	45,6	5,7	7,7	79,1	19,7	55,3	6,0	31,0	20,4
Кіпр	73,9	1,2	50,2	13,1	9,9	386,0	20,0	71,3	13,0	10,0	24,3
Латвія	79,1	1,3	50,8	8,1	5,8	830,3	20,0	87,9	8,0	11,0	20,9
Литва	87,3	1,2	48,8	11,1	5,9	441,5	20,0	83,3	11,0	14,0	23,1
Люксембург	83,8	1,0	63,8	13,9	8,0	778,0	20,0	72,7	14,0	36,0	8,6
Нідерланди	84,7	2,7	78,9	11,6	8,5	454,7	20,0	96,0	12,0	19,0	8,1
Німеччина	88,1	4,2	48,9	6,4	9,4	174,4	20,0	55,1	6,0	33,0	10,4
Польща	74,1	2,8	42,9	8,1	9,2	171,6	19,4	61,2	8,0	14,0	22,5
Португалія	85,5	2,6	55,3	12,1	9,7	201,3	20,0	64,2	12,0	23,0	17
Румунія	73,2	1,6	27,8	8,2	9,4	127,0	18,6	18,5	8,0	12,0	29,3
Словаччина	83,1	1,4	55,2	12,2	8,3	347,4	20,0	65,1	12,0	25,0	14
Словенія	68,8	1,1	49,7	17,5	12,3	633,5	20,0	64,2	18,0	22,0	23,1
Угорщина	76,7	1,3	49,1	8,3	3,7	137,5	18,2	63,2	8,0	19,0	26
Фінляндія	90,2	1,4	79,2	9,1	7,5	494,3	20,0	96,4	9,0	42,0	11,4
Франція	86,4	5,9	62,0	4,7	5,7	156,1	20,0	78,2	5,0	22,0	13,6
Хорватія	83,4	1,2	63,4	16,1	10,7	206,5	20,0	68,4	16,0	17,0	29,6
Чеська Республіка	77,7	1,9	59,7	12,0	8,6	367,3	18,9	81,9	12,0	24,0	14,2
Швеція	86,0	1,6	66,5	9,9	5,0	516,0	20,0	86,3	10,0	60,0	11,7

Джерело: розробка авторів

Вперше поняття «криптовалюти» виникло в науковому середовищі в статті Сатоші Накамото, опублікованій у 2008 році, присвяченій ідеї Bitcoin, як однорангової електронної готівкової системи [21]. Особистість автора (або авторів) цієї статті лишається невідомою донині, проте самі криптовалюти продовжують набирати популярності й відкривати перед суспільством нові можливості фінансових операцій і користування цифровими активами. Наразі криптовалюти розуміють переважно як цифрові активи в системі, які криптографічно надсилаються від одного користувача мережі блокчейн до іншого за допомогою цифрових підписів із парами асиметричних ключів [22].

Незважаючи не переваги та можливості, які відкривають криптовалюти перед інвесторами та іншими користувачами, їх поширення також викликає занепокоєння, зокрема з приводу потенційного впливу криптовалют на кіберзлочинність. По-перше, через децентралізацію, низький рівень державного регулювання, труднощі ідентифікації учасників транзакцій, доступність, безвідкличність та низьку вартість переказів криптовалюти є привабливим інструментом для кіберзлочинців. По-друге, короткий

історичний досвід цих систем і відносна новизна механізмів, які забезпечують їх роботу, також можуть викликати питання щодо ризиків і надійності цих фінансових активів. Через це, не дивно, що обсяги криптовалюти, задіяної в злочинній діяльності, продовжують зростати. Наприклад, за даними дослідження Chainalysis Inc [23], у 2022 році вартість криптовалюти, отримання якої було пов'язано з злочинністю, досягла рекордного значення 20,6 мільярдів доларів США (рис. 4). Криптовалюти часто стають інструментом у таких цифрових злочинах, як незаконна цифрова комерція (переважно у даркнеті), відмивання грошей, хакерство, криптоджекінг і шахрайство тощо, при цьому впровадження криптовалют продовжує зростати, тому розуміння складного зв'язку між їх використанням і кіберзагрозами стає першочерговим для забезпечення надійних заходів цифрової безпеки.



Джерело: створено авторами на основі дослідження [23]

Рис. 4. Вартість криптовалюти, отриманої незаконними акаунтами у 2017–2022 роках

Країни Європейського Союзу відомі своєю прихильністю до інновацій, цифрової трансформації та захисту даних, тому ми обрали їх як середовище для вивчення впливу окремих аспектів використання криптовалют на кібербезпеку держави. З цією метою нами було побудовано множинну лінійну регресійну модель з покроковим виключенням змінних. Результати покрокового виключення змінних показано на рисунку 5.

variable	Results of stepwise regression step	R	R-square	R-square. corrected	F - incl/excl	p-value	number of
X10	-1	0,88	0,78	-0,00	0,01	0,94	7
X1	-2	0,88	0,78	-0,00	0,05	0,83	6
X3	-3	0,88	0,77	-0,01	0,64	0,43	5
X2	-4	0,86	0,75	-0,03	2,10	0,16	4
X9	-5	0,82	0,68	-0,07	5,28	0,03	3
X5	-6	0,77	0,60	-0,08	4,70	0,04	2

Рис. 5. Результати створення регресійної моделі з покроковим виключенням змінних

З рисунка 5 видно, що модель стає статистично значущою після четвертого кроку й виключення змінних x_{10}, x_1, x_3 і x_2. У результаті отримуємо модель з чотирма факторними змінними x_4 (відсоток населення, який користується мобільним додатком для інвестування в криптоактиви раз на тиждень і частіше), x_5 (загальний дохід ринку даркнету), x_6 (оцінка правових заходів у сфері регулювання цифрових активів) і x_9 (інвестування населення в традиційні активи). Така модель містить змінні, які описують чотири різні аспекти використання криптовалют населенням країни й є статистично значущою за F-критерієм Фішера, тому є цікавою для подальшого розгляду. Детальніше результати отриманої моделі з чотирма факторними ознаками показані на рисунку 6.

N=24	Regression Outcomes R= ,86380253 R2= ,74615481 Correct. R2= ,69271372 F(4,19)=13,962 p<,00002 Standard estimation error: 3,8483 BETA	St. r. BETA	B	St. r. B	t(19)	p-value
intercept			-24,08	23,75	-1,01	0,32
X4	-0,37	0,12	-1,18	0,40	-2,98	0,01
X5	-0,32	0,12	-0,01	0,00	-2,61	0,02
X6	0,59	0,13	5,83	1,23	4,73	0,00
X9	0,30	0,13	0,17	0,08	2,30	0,03

Рис. 6. Отримана регресійна модель з чотирма факторними змінними

Множинний коефіцієнт кореляції (R) регресійної моделі дорівнює 0,86, що перевищує критичне значення 0,7, тобто вказує на сильний зв'язок між результатною та факторними ознаками. Множинний коефіцієнт детермінації доводить, що розподіл оцінки кібербезпеки серед країн Європейського Союзу у 2020 році на 74,62 % пояснюється варіацією факторних змінних.

Для створеної моделі F-критерій Фішера дорівнює 13,96, що з рівнем значущості $p < 0,05$ підтверджує статистичну значущість рівняння регресії, це означає, що з імовірністю 95 % отриманий результат може бути поширений на генеральну сукупність. Аналогічний висновок можемо зробити щодо статистичної значущості незалежних змінних, оскільки їх фактичні значення t-критерію Ст'юдента також мають рівень значущості $p < 0,05$, тобто усі змінні, включені в модель, є статистично значущими за t-критерієм Ст'юдента. Необхідно також провести перевірку масиву пояснюючих змінних на мультиколінеарність, оскільки її наявність може спричинити зниження точності та інтерпретованості результатів подальшого моделювання. Як критерій наявності колінеарності між факторними змінними було використано фактор інфляції дисперсії (variance inflation factor, або VIF), оскільки він дозволяє кількісно оцінити завищення дисперсії оцінок параметрів регресії через наявність мультиколінеарності. За результатами перевірки (табл. 3), очевидно, що значення VIF для жодної зі змінних не перевищує 5 (загальноприйнятого критичного значення), тому можна зробити висновок, що серед набору факторних змінних немає мультиколінеарності.

Таблиця 3

Перевірка на мультиколінеарність за допомогою фактора інфляції дисперсії (VIF)

Змінна	VIF
x_4	1,13
x_5	1,10
x_6	1,17
x_9	1,24

На рисунку 6 також можемо побачити оцінки параметрів рівняння отриманої моделі. Виходячи з їхнього значення, можемо записати вигляд рівняння регресії (1):

$$y_2 = -24,08 - 1,18x_4 - 0,01x_5 + 5,83x_6 + 0,17x_9 \quad (1)$$

де y_2 – загальна оцінка кібербезпеки країни, шкала від 0 до 100 балів (де 0 – мінімальна оцінка, а 100 – максимальна);

x_4 – відсоток населення, який користується мобільним додатком для інвестування в криптоактиви раз на тиждень і частіше;

x_5 – загальний дохід ринку даркнету, євро на душу населення;

x_6 – оцінка правових заходів у сфері регулювання цифрових активів, за 20-бальною шкалою (де 0 – мінімальна оцінка, а 20 – максимальна);

x_9 – відсоток населення, який інвестує в традиційні активи.

За цим рівнянням (1) можемо визначити прогнозовані за регресійною моделлю значення результатної ознаки та порівняти їх з фактично визначеним значенням загальних оцінок кібербезпеки країн. З рисунка 7 видно, що між цими значеннями існує позитивна кореляція, адже точки на графіку згруповані навколо діагональної лінії від нижнього лівого кута до верхнього правого кута. Це вказує на те, що регресійна модель працює добре та фіксує зв'язок між предикторами та результатною ознакою. Близькість точок до діагональної лінії також свідчить про те, що прогнози моделі є близькими до фактичних значень оцінок кібербезпеки країн.

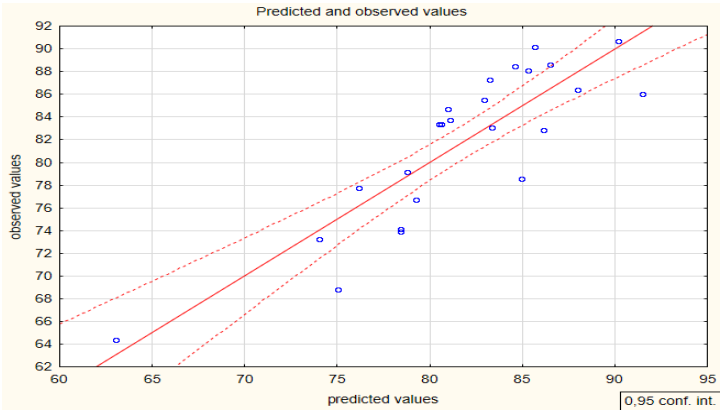


Рис. 7. Графік залежності між фактичними та прогнозами регресійної моделі

За оцінками параметрів регресії можемо висунути гіпотезу, що підвищення відсотка населення, який активно користується криптовалютами (x_4 – відсоток людей, які користуються мобільним додатком для інвестування в криптоактиви раз на тиждень і частіше) на 1 % у середньому може призвести до зниження оцінки кібербезпеки на 1,18. Це можна пояснити тим, що децентралізований характер і анонімність криптовалют роблять їх привабливими інструментами для кіберзлочинців. Правоохоронним органам важко відстежувати транзакції з криптовалютою, що також полегшує злочинцям здійснення незаконних транзакцій. При цьому впровадження надійних заходів безпеки та зростання обізнаності населення щодо безпечного використання цифрових активів можуть не встигати за швидким зростанням кількості користувачів криптовалюти. Такі процеси здатні привернути увагу хакерів, спонукати їх до використання криптовалют у кількох напрямках, зокрема як інструмент для:

– атак програм-вимагачів (злочинці шифрують дані жертв і вимагають викуп у криптовалюті за надання ключа дешифрування тощо);

– криптоджекінгу (кіберзлочинці використовують комп'ютерні ресурси жертв для майнінгу криптовалют без їх відома чи згоди, при цьому генеруючи нові цифрові активи за рахунок продуктивності системи жертви та споживання електроенергії);

– шахрайства, зокрема фішингу (кіберзлочинці видають себе за законні криптовалютні біржі, гаманці або початкові пропозиції монет (ICO), щоб обманом змусити користувачів розкрити їхні закриті ключі, паролі або надіслати кошти на шахрайські адреси);

– незаконної торгівлі у даркнеті (криптовалюти є поширеним способом оплати в торгівлі викраденими даними, хакерськими інструментами та іншими незаконними товарами у даркнет);

– відмивання грошей (злочинці можуть конвертувати свої незаконно отримані прибутки в криптовалюти, а потім назад у традиційні валюти різними способами, що ускладнює відстеження походження коштів).

З іншого боку варто зазначити, що, хоча в короткостроковій перспективі криптовалюти надали нові можливості для кіберзлочинців, вони за своєю суттю не пов'язані з кіберзлочинністю. Багато законних компаній і осіб використовують криптовалюти в законних цілях, а сама технологія має потенціал для підвищення безпеки та конфіденційності в різних сферах. Таким чином, вплив поширеності криптовалют на оцінку кібербезпеки в довгостроковому періоді є менш однозначним.

Меншою мірою на рівень оцінки кібербезпеки негативно впливає підвищення популярності використання даркнету (x_5 – загальний дохід ринку даркнету). За оцінкою параметра регресії, можемо припускати, що підвищення доходу ринку даркнету на 1 євро на душу населення у середньому може спричинити зниження оцінки кібербезпеки на 0,01. Такий вплив може бути спричинений тим, що ринок даркнету є одним з джерел фінансування для кіберзлочинців і використовуватися для продажу викрадених даних, адже використання криптовалют дозволяє покупцям і продавцям здійснювати транзакції, не розкриваючи свою особистість або місцезнаходження. Через це криптовалюти є основним способом оплати електронних транзакцій у Dark Web [24]. Таким чином, хоча криптовалюти можуть приносити користь у різних галузях, однак їх анонімність та децентралізація роблять криптовалюти привабливими для кіберзлочинців, які прагнуть здійснювати незаконну діяльність, зберігаючи певний ступінь анонімності.

Заходами, які пом'якшують негативний вплив поширення криптовалют на кібербезпеку, можуть бути розвиток цифрової та інвестиційної грамотності користувачів, підвищення обізнаності про ризики, пов'язані з криптовалютами та кіберзлочинністю, розробка профільного законодавства й контроль за надійністю протоколів безпеки криптовалютних бірж, запровадження правил і стандартів для забезпечення захисту коштів і особистої інформації користувачів, міжнародна співпраця, розробка та вдосконалення інструментів аналізу блокчейну тощо.

Значний позитивний ефект на оцінку кібербезпеки країни має підвищення оцінки правових заходів у сфері регулювання цифрових активів (x_6). За оцінкою відповідного параметра регресії, зростання оцінки правових заходів у сфері регулювання цифрових активів на 1 у середньому може призвести до підвищення оцінки кібербезпеки на 5,83. Це легко пояснити, адже правове регулювання криптовалют може сприяти прозорості, дотриманню стандартів ідентифікації користувачів і боротьби з відмивання грошей, міжнародній співпраці та обміну інформацією тощо.

Однак варто зауважити, що, хоча правове регулювання криптовалют може позитивно впливати на кібербезпеку, у ньому варто дотримуватися балансу між регуляцією та інноваціями, адже надмірні та обтяжливі правила можуть стримувати технологічний прогрес і перешкоджати законному використанню криптовалют. Частково визначити цей баланс можна, опираючись на урядові практики на прикладі країн Європейського Союзу з високими оцінками правових заходів у сфері регулювання цифрових активів (x_6). Наразі провідна політика регулювання цифрових активів у Європейському Союзі здійснюється відповідно до Звернення Комісії до Європейського Парламенту, Ради, Європейського економічного та соціального комітету та Комітету регіонів щодо стратегії цифрових фінансів для ЄС [25]. Згідно з цим документом основними цілями регулювання цифрових активів є:

– забезпечення правової визначеності;

– підтримка інновацій та усунення регуляторних перешкод, які можуть стримувати розвиток фінансових технологій, одночасно зі зменшенням ризиків, що виникають у зв'язку з цим;

– захист європейських користувачів, інвесторів і бізнесу, шляхом створення довіри та впевненості в цілісності ринку;

– підтримка фінансової стабільності на європейському рівні.

Таким чином, можемо ствердити, що впровадження ефективного правового регулювання цифрових активів, спрямованого на перераховані цілі, може сприяти значному підвищенню оцінки кібербезпеки країни.

Деякий позитивний вплив на оцінку кібербезпеки має також підвищення інвестиційної грамотності населення, яке представлене змінною x_9 (відсоток населення, що інвестує в традиційні активи). Підвищення цього показника на 1 % у середньому може призвести до підвищення оцінки кібербезпеки на 0,17. Причиною цього може бути те, що підвищення інвестиційної грамотності надає людям знання та навички для прийняття обґрунтованих фінансових рішень, розпізнавання потенційних кіберзагроз і вживання профілактичних заходів для захисту своїх інвестицій та особистої інформації.

Зрозуміло, що запровадження та реалізація згаданих заходів запобігання та протидії злочинному використанню криптовалют вимагають активних дій від багатьох зацікавлених сторін, зокрема криптовалютних бірж, урядів, регуляторних органів і окремих осіб для спільного вирішення проблем і пом'якшення негативного впливу криптовалют на кібербезпеку. Розробка і реалізація заходів безпеки, пов'язаних з використанням криптовалюти, можуть потребувати значних зусиль, проте вони здатні значно зменшити негативний вплив криптовалют на кібербезпеку.

Висновки та перспективи подальших досліджень. У межах дослідження було побудовано економетричну модель множинної регресії для вивчення впливу використання криптовалют на оцінку кібербезпеки країн Європейського Союзу. У результаті було отримано модель, яка містила чотири факторні змінні: відсоток населення, який регулярно користується мобільним додатком для інвестування в криптоактиви, загальний дохід ринку даркнету, оцінка правових заходів у сфері регулювання цифрових активів й інвестиції населення в традиційні активи.

Отримана модель підтвердила наявність впливу використання криптовалют на цифрову безпеку країни, вона була статистично значущою за F-критерієм Фішера та містила виключно статистично значущі змінні. Також за допомогою фактора інфляції дисперсії (VIF) було підтверджено відсутність мультиколінеарності між незалежними ознаками. Економічна інтерпретація оцінок параметрів рівняння регресії дозволяє стверджувати, що з розглянутих факторів на рівень кібербезпеки країни найбільше впливають кількість активних користувачів криптовалюти та державне регулювання цифрових активів.

За результатами моделювання, збільшення кількості користувачів, які користуються мобільним додатком для інвестування в криптоактиви раз на тиждень і частіше, є значним фактором підвищення ризиків кібербезпеки. З огляду на зростання популярності та вживаності криптовалют, цей факт вимагає уваги державних органів і організацій задля розробки ефективних стратегій і правил регулювання цифрових активів. Ще одним виявленим фактором зниження рівня кібербезпеки є підвищення доходу ринку даркнету, який є популярною платформою для продажу викрадених даних та інших незаконних товарів і послуг, часто використовуючи криптовалюту як засіб оплати.

Іншим висновком з моделі є виявлення значного позитивного впливу підвищення якості правових заходів у сфері регулювання цифрових активів на оцінку кібербезпеки країни. Існування чітких та ефективних нормативних актів значно сприяє запобіганню кіберзагроз, пов'язаних з використанням криптовалют, та їх швидкому виявленню. Це створює перспективи для майбутнього вивчення нормативно-правового поля країн Європейського Союзу з найвищими оцінками правових заходів у сфері регулювання цифрових активів і перспектив адаптації аналогічних правових практик в Україні. Іншим фактором, який позитивно впливає на рівень кібербезпеки держави, є інвестиційна грамотність населення. Імовірним поясненням цьому є те, що громадяни, які займаються інвестуванням у традиційні активи, підвищують свій рівень інвестиційної грамотності, яка допомагає їм розпізнавати ризики інвестування також і цифрових активів.

Дослідження дає підстави для підвищення громадської уваги до впровадження ефективного державного регулювання криптовалютної діяльності та сприяння інвестиційній грамотності населення, створення заходів, які покликані підвищити рівень кібербезпеки та забезпечити стабільний і безпечний розвиток цифрового середовища в країні. Такі дії потребують подальшого дослідження конкретних практик регулювання цифрових активів у країнах Європейського Союзу, аналізу їх придатності до українського контексту та розробки системи політичних практик мінімізації негативного впливу використання криптовалют на кібербезпеку.

Роботу виконано в межах науково-дослідних тем, що фінансуються за рахунок коштів державного бюджету (номер державної реєстрації 0121U100467, 0122U000783).

Список використаної літератури:

1. *Ozparlak L.* Some statistics about cybersecurity industry in european region / *L.Ozparlak* // Linkedin [Electronic resource]. – Access mode : https://www.linkedin.com/pulse/some-statistics-cybersecurity-industry-european-region-ozparlak.
2. Cybercrime statistics / Surfshark [Electronic resource]. – Access mode : https://surfshark.com/research/data-breach-impact/statistics.
3. From january 2019 to april 2020. The year in review ENISA, threat landscape / European Union Agency for Network and Information Security (ENISA). – 2020. – 26 p. [Electronic resource]. – Access mode : https://www.enisa.europa.eu/publications/year-in-review.
4. Science Direct [Electronic resource]. – Access mode : https://www.sciencedirect.com/.
5. *Черновол В.* Шахрайство із використанням електроннообчислюваної техніки: злочини з криптовалютою / *В.Черновол* // Науковий круглий стіл «Кібербезпека у системі національної безпеки України: пріоритетні напрями розвитку» : зб. матеріалів, 26 квіт. – Маріуполь, 2018. – С. 85–87.
6. *Абузов І.* Шахрайство з криптовалютою / *І.Абузов* // Інформаційні технології у науці, освіті, виробництві : збірник тез І Всеукраїнської науково-практичної Інтернет-конференції здобувачів вищої освіти і молодих учених, 26 квіт. – Маріуполь, 2018. – С. 146–148.
7. *Ковтун В.О.* Прихований майнінг криптовалюти й обмеження браузерного криптоджекінгу / *В.О. Ковтун, П.С. Клімушин* // Протидія кіберзлочинності та торгівлі людьми : зб. матеріалів міжнарод. наук.-практ. конф., 18 трав. – Харків, 2021. – С. 148–150.
8. *Ramos S.* Exploring Blockchains Cyber Security Techno- Regulatory Gap. An Application to Crypto-Asset Regulation in the EU / *S.Ramos, L.Mélon, J.Ellul* // 10th Graduate Conference in Law and Technology, Sciences Po, 16–17 July. – Paris, 2022. – P. 1–27.
9. *Kiruthika D., Renganathan K.* Measures to curb the cyber menace related to cryptocurrencies / *D.Kiruthika, K.Renganathan* // Journal of theoretical and applied information technology. – 2022. – Vol. 100, № 21. – P. 6621–6630.
10. *Apuri D.T.* Bitcoins usage by cybercriminals – evolution and current mitigating approaches / *D.T. Apuri* // Evolution and current mitigating approaches book chapter series on research nexus in IT, law, cyber security & forensics. – 2022. – Vol. 1, № 1. – P. 251–258.
11. *Fong J.* Global cybercrime report: which countries are most at risk in 2023? / *J.Fong* // SEON [Electronic resource]. – Access mode : https://seon.io/resources/global-cybercrime-report/.
12. NCSI / e-Governance Academy Foundation [Electronic resource]. – Access mode : https://ncsi.ega.ee/ncsi-index/.
13. Global Cybersecurity Index 2020. – Geneva, Switerland : International Telecommunication Union, 2023. – 172 p.
14. *Frisby J.* Cybersecurity Exposure Index (CEI) 2020 / *J.Frisby* // PasswordsManagers.co [Electronic resource]. – Access mode : https://passwordmanagers.co/cybersecurity-exposure-index/.
15. Cryptocurrency ownership data. Cryptocurrency across the world / Triple-A [Electronic resource]. – Access mode : https://triple-a.io/crypto-ownership-data/.
16. Individuals' level of digital skills / Eurostat [Electronic resource]. – Access mode : https://ec.europa.eu/eurostat/web/products-datasets/-/isoc_sk_dskl_i21.
17. Flash Eurobarometer FL509 : Retail Financial Services and Products / European data [Electronic resource]. – Access mode : https://data.europa.eu/data/datasets/s2666_fl509_eng?locale=en.
18. *Grauer K.* Cryptocurrencies and drugs: Analysis of cryptocurrency use on darknet markets in the EU and neighbouring countries / *K.Grauer, E.Jardine* // The European Monitoring Centre for Drugs and Drug Addiction (EMCDDA). – 2022. – 42 p.
19. E-banking and e-commerce / Eurostat [Electronic resource]. – Access mode : https://ec.europa.eu/eurostat/web/products-datasets/-/isoc_bde15cbc.
20. *Schneider F., Asllani A.* Taxation of the informal economy in the EU / *F.Schneider, A.Asllani* // European Parllament. Subcommittee on tax matters (FISC). – 2022. – 128 p.
21. *Nakamoto S.* Bitcoin: A peer-to-peer electronic cash system / *S.Nakamoto* // Decentralized Business Review. – 2008.
22. Blockchain technology overview / *D.Yaga and other*. – Gaithersburg : National Institute of Standards and Technology, 2018. – 68 p.
23. The 2023 crypto crime report. Everything you need to know about cryptocurrency-based crime / *K.Grauer and other*. – Chainalysis, 2023. – 109 p. [Electronic resource]. – Access mode : https://go.chainalysis.com/2023-crypto-crime-report.html.
24. *Naik S.* 'Dark Web' thriving in SA / *S.Naik, R.Serumula* // Independent Online (IOL) [Electronic resource]. – Access mode : https://www.iol.co.za/news/south-africa/dark-web-thriving-in-sa-1931641.
25. Communication from the Commission to the European Parliament, the European Council, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions on a Digital Finance Strategy for the EU / EUROPEAN COMMISSION, 23 September. – 2020. COM (2020)591

References:

1. Ozparlak, L. «Some statistics about cybersecurity industry in european region», *Linkedin*, [Online], available at: https://www.linkedin.com/pulse/some-statistics-cybersecurity-industry-european-region-ozparlak
2. «Cybercrime statistics», *Surfshark*, [Online], available at: https://surfshark.com/research/data-breach-impact/statistics
3. European Union Agency for Network and Information Security (ENISA) (2020), *From january 2019 to april 2020. The year in review ENISA. threat landscape*, 26 p. [Online], available at: https://www.enisa.europa.eu/publications/year-in-review

4. *Science Direct*, [Online], available at: https://www.sciencedirect.com/
5. Chernovol, V. (2018), «Shakhraistvo iz vykorystanniam elektronnoobchysliuvanoi tekhniky: zlochyny z kryptovaliutoiu», *Naukovyi kruhlyi stil "Kiberbezpeka u systemi natsionalnoi bezpeky Ukrainy: priorytetni napriamy rozvytku"*, zb. materialiv, 26 kvit., Mariupol, pp. 85–87.
6. Abuzov, I. (2018), *Shakhraistvo z kryptovaliutoiu. Informatsiini tekhnolohii u nautsi, osviti, vyrobnytstvi*, zbirnyk tez I Vseukrainskoi naukovo-praktychnoi Internet-konferentsii zdobuvachiv vyshchoi osvity i molodykh uchenykh, 26 kvit., Mariupol, pp. 146–148.
7. Kovtun, V.O. and Klimushyn, P.S. (2021), «Prykhovanyi maininh kryptovaliuty y obmezhennia brauzernoho kryptodzhekinhu», *Protydiia kiberzlochynnosti ta torhivli liudmy*, zb. materialiv mizhnarod. nauk.-prakt. konf., 18 trav., Kharkiv, pp. 148–150.
8. Ramos, S., Mélon, L. and Ellul, J. (2022), «Exploring Blockchains Cyber Security Techno- Regulatory Gap. An Application to Crypto-Asset Regulation in the EU», *10th Graduate Conference in Law and Technology, Sciences Po*, 16–17 July, Paris, pp. 1–27.
9. Kiruthika, D. and Renganathan, K. (2022), «Measures to curb the cyber menace related to cryptocurrencies», *Journal of theoretical and applied information technology*, Vol. 100, No. 21, pp. 6621–6630.
10. Apuri, D.T. (2022), «Bitcoins usage by cybercriminals – evolution and current mitigating approaches», *Evolution and current mitigating approaches book chapter series on research nexus in IT, law, cyber security & forensics*, Vol. 1, No. 1, pp. 251–258.
11. Fong, J. «Global cybercrime report: which countries are most at risk in 2023?», *SEON*, [Online], available at: https://seon.io/resources/global-cybercrime-report/
12. e-Governance Academy Foundation, *NCSI*, [Online], available at: https://ncsi.ega.ee/ncsi-index/
13. *Global Cybersecurity Index 2020* (2023), International Telecommunication Union, Geneva, Switerland, 172 p.
14. Frisby, J. (2020), «Cybersecurity Exposure Index (CEI)», *PasswordsManagers.co*, [Online], available at: https://passwordmanagers.co/cybersecurity-exposure-index/
15. «Cryptocurrency ownership data. Cryptocurrency across the world», *Triple-A*, [Online], available at: https://triple-a.io/crypto-ownership-data/
16. Eurostat, *Individuals' level of digital skills*, [Online], available at: https://ec.europa.eu/eurostat/web/products-datasets/-/isoc_sk_dskl_i21
17. «Flash Eurobarometer FL509 : Retail Financial Services and Products», *European data*, [Online], available at: https://data.europa.eu/data/datasets/s2666_fl509_eng?locale=en
18. Grauer, K. and Jardine, E. (2022), «Cryptocurrencies and drugs: Analysis of cryptocurrency use on darknet markets in the EU and neighbouring countries», *The European Monitoring Centre for Drugs and Drug Addiction (EMCDDA)*, 42 p.
19. Eurostat, *E-banking and e-commerce*, [Online], available at: https://ec.europa.eu/eurostat/web/products-datasets/-/isoc_bde15cbc
20. Schneider, F. and Asllani, A. (2022), «Taxation of the informal economy in the EU», *European Parllament, Subcommittee on tax matters (FISC)*, 128 p.
21. Nakamoto, S. (2008), «Bitcoin: A peer-to-peer electronic cash system», *Decentralized Business Review*.
22. Yaga, D. et al. (2018), *Blockchain technology overview*, National Institute of Standards and Technology, Gaithersburg, 68 p.
23. Grauer, K. et al. (2023), *The 2023 crypto crime report. Everything you need to know about cryptocurrency-based crime*, Chainalysis, 109 p, [Online], available at: https://go.chainalysis.com/2023-crypto-crime-report.html
24. Naik, S. and Serumula, R., «"Dark Web" thriving in SA», *Independent Online (IOL)*, [Online], available at: https://www.iol.co.za/news/south-africa/dark-web-thriving-in-sa-1931641
25. «Communication from the Commission to the European Parliament, the European Council, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions on a Digital Finance Strategy for the EU» (2020), EUROPEAN COMMISSION, 23 September, COM (2020)591

Миненко Сергій Володимирович – кандидат технічних наук, асистент кафедри економічної кібернетики Сумського державного університету.

https://orcid.org/0000-0003-3998-9031.

Наукові інтереси:

– цифровізація економіки;

– протидія корупції;

– протидія легалізації незаконних доходів;

– економіко-математичні методи та моделі.

Могильна Ксенія Олегівна – студентка 3 курсу спеціальності 051 «Економіка» (Економічна кібернетика та бізнес-аналітика) Сумського державного університету.

https://orcid.org/0000-0002-7472-2458.

Наукові інтереси:

– впровадження передових технічних та технологічних практик у соціально-економічний розвиток України;

– зелена економіка та сталий розвиток.

Mynenko S.V., Mohylna K.O.

Assessing the impact of cryptocurrency usage on cybersecurity: the European Union experience

The economic consequences of cybercrime are often devastating. Cybercrime leads to financial losses, theft of funds, expenses for investigations and mitigating the effects of crimes, rebuilding trust among citizens, and implementing security improvements. It also reduces societal trust and the investment attractiveness of countries and companies. All these factors make the development and study of cybersecurity strategically important. One of the key factors influencing national cybersecurity is the prevalence and use of modern technologies by the population, including cryptocurrencies, and the impact of their usage and regulation on cybersecurity is not obvious. Therefore, researching the impact of cryptocurrency usage on cybersecurity is currently a relevant issue.

The purpose of this study is to investigate the impact of cryptocurrency usage on cybersecurity in European Union countries. A regression model has confirmed the statistical significance of the influence on cybersecurity assessment in a country of aspects related to cryptocurrency usage, such as prevalence, legal regulation, user investment skills, and the use of the darknet. The most positive impact on a country's cybersecurity assessment comes from the implementation of legal measures in the regulation of digital assets, demonstrating the effectiveness of legal regulation of digital assets in EU countries. The most negative impact on cybersecurity assessment is the increase in the number of active cryptocurrency users (those who use a mobile app to invest in crypto assets once a week or more).

The practical significance of this research lies in its potential to contribute to the future development of digital asset regulation policy in Ukraine, striking a balance between minimizing cybersecurity risks and fostering innovation. Demonstrating the positive impact of European practices in regulating digital assets opens prospects for further research into the effectiveness of specific regulatory measures and the possibility of adapting them to the Ukrainian context.

Keywords: cyber security; cybercrime; cryptocurrencies; digital assets; regulation of cryptocurrencies; regression analysis.

Стаття надійшла до редакції 08.09.2023.