

Габрелян А.Ю.

доктор філософії в галузі права,
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
ORCID: <https://orcid.org/0000-0001-9337-7920>

Дяковський О.С.

кандидат юридичних наук
старший викладач кафедри інформаційного,
господарського та адміністративного права,
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
ORCID: <https://orcid.org/0000-0003-3412-9278>

Habrelian Andrii, Diakovsky Oleksandr

National Technical University of Ukraine
“Igor Sikorsky Kyiv Polytechnic Institute”

ТІНЬОВИЙ ОБІГ ПЕРСОНАЛЬНИХ ДАНИХ ЯК СЕГМЕНТ ЦИФРОВОЇ ТІНЬОВОЇ ЕКОНОМІКИ: МЕХАНІЗМИ МОНЕТИЗАЦІЇ ТА ЗАГРОЗИ ЕКОНОМІЧНІЙ БЕЗПЕЦІ УКРАЇНИ

У статті розглянуто тіньовий обіг персональних даних як економічно значущий сегмент цифрової тіньової економіки та джерело ризиків для економічної безпеки України. Увагу зосереджено на розмежуванні неправомірних операцій з даними, що не мають економічного результату, та економічно значущих практик, пов'язаних з одержанням доходу, економією витрат, конкурентною перевагою, доступом до майнових благ або використанням даних як ресурсу іншої тіньової діяльності. Розглянуто ланцюг монетизації персональних даних, підходи до оцінювання економічного результату, канали впливу на економічну безпеку та розподіл пов'язаних вигод і втрат. Окрему увагу приділено ризик-орієнтованому регулюванню, простежуваності юридично значущих операцій, аналізу пов'язаних фінансових потоків, корпоративному комплаєнсу, аудиту та захисту цифрової інфраструктури.

Ключові слова: тіньовий обіг персональних даних, цифрова тіньова економіка, монетизація персональних даних, економічна безпека, ризик-орієнтоване регулювання, детінізація, цифрова інфраструктура.

Постановка проблеми. У цифровій економіці персональні дані є важливим інформаційним ресурсом для дистанційної ідентифікації, кредитного скорингу, персоналізації послуг, електронної комерції та маркетингової аналітики. Їх економічна цінність значною мірою пов'язана з можливістю багаторазового використання, комбінування з іншими масивами та одержання нової інформації [18]. Ці властивості водночас підвищують привабливість даних для неправомірного використання.

Для України проблема посилюється поширенням електронних реєстрів, цифрових державних і фінансових сервісів, онлайн-банкінгу та безготівкових розрахунків. Накопичені ідентифікаційні, контактні й фінансові відомості можуть неправомірно використовуватися для продажу, доступу до майнових благ, шахрайства, зменшення витрат на залучення клієнтів або

формування конкурентної переваги. Матеріали EuroPol підтверджують функціонування ринку викрадених даних та їх використання в різних видах протиправної діяльності [13]. Такі практики виходять за межі суто інформаційно-правової проблематики, однак до цифрової тіньової економіки слід відносити лише ті з них, що забезпечують економічну вигоду або використовують персональні дані як ресурс іншої дохідної тіньової діяльності [2].

Недостатньо визначеними залишаються економічні межі такого обігу, механізми його монетизації, канали впливу на економічну безпеку України та способи обмеження тіньового використання даних без надмірного регуляторного навантаження на правомірну цифрову діяльність.

Аналіз останніх досліджень і публікацій. Дослідження персональних даних у науковій літературі зосе-



реджені переважно на їх економічній цінності, правовому обігу та захисті. У «World Development Report 2021: Data for Better Lives» Світовий банк пов'язує економічну й соціальну цінність даних з їх повторним використанням і комбінуванням [18]. О.С. Дяковський розглядає обіг інформації, що містить персональні дані, через процеси її збирання, реєстрації, зберігання, використання та поширення [4], а також досліджує аудит захисту персональних даних як інструмент виявлення недоліків системи захисту й оцінювання ризиків [3]. Праці О.С. Дяковського дають правову й організаційну основу для аналізу обігу та захисту персональних даних, однак питання економічної вигоди від їх неправомірного використання окремо не досліджується. А.Ю. Габрелян обґрунтовує поділ тіньової економіки на приховану, неформальну та нелегальну складові й відносить цифрові практики до сучасних форм тінізації [2]. К.В. Лагунов розвиває ризик-орієнтований підхід до її оцінювання, за яким поряд з інтегральним рівнем враховуються структура і концентрація ризиків, їх потенційні наслідки та значущість для економічної безпеки [6].

У матеріалах Europol висвітлено практичні форми неправомірного використання даних, зокрема функціонування ринків викрадених даних, торгівлю доступом до скомпрометованих систем та їх використання для шахрайства й інших видів кіберзлочинної діяльності [13; 14]. У «NIST Privacy Framework 1.0», підготовленому К. Бекл і Н. Лефковіц, запропоновано підхід до управління ризиками приватності, орієнтований на ризики та результати [12]; відповідні організаційні засади закріплено також у «ISO/IEC 27001:2022» та «ISO/IEC 27701:2025» [15; 16]. Однак ці документи не розкривають економічних механізмів тіньової монетизації персональних даних. Попри значний масив праць із правового режиму даних, інформаційної безпеки та кіберзлочинності, їх неправомірна монетизація саме як економічне явище залишається дослідженою фрагментарно.

Формулювання цілей статті. Метою статті є обґрунтування місця економічно значущого тіньового обігу персональних даних у структурі цифрової тіньової економіки, систематизація механізмів його монетизації, визначення каналів впливу на економічну безпеку України та обґрунтування напрямів детінізації відповідного сегмента.

Виклад основного матеріалу. Для визначення меж досліджуваного явища слід розмежувати обробку персональних даних, їх обіг і тіньову економічну діяльність. Закон України «Про захист персональних даних» від 01.06.2010 р. № 2297-VI встановлює, що обробка має здійснюватися для конкретних і законних цілей, визначених за згодою суб'єкта або законом (ч. 1, 5 ст. 6), визначає поширення персональних даних як їх передавання та допускає його без згоди лише у передбачених законом випадках (ч. 1, 2 ст. 14) [8]. Технічна можливість одержання чи передавання інформації сама по собі не робить її подальше використання правомірним.

Обіг інформації, що містить персональні дані, охоплює їх збирання, реєстрацію, зберігання, використання та поширення [4]. Для економічного аналізу важливий не перелік окремих операцій, а їх послідовність: економічна вигода може виникати після копіювання, перевірки, поєднання з іншими масивами, передавання або кінцевого використання даних. Тому аналіз має охоплювати весь ланцюг їх економічного використання.

Неправомірність окремої операції ще не означає її належності до тіньової економічної діяльності. Наприклад, несанкціонований службовий доступ до бази, який не використовується для одержання доходу, економії витрат або створення переваги для третьої особи, є насамперед порушенням встановленого режиму обробки даних. Економічного змісту така практика набуває, коли доступ стає етапом копіювання клієнтської бази, її продажу, передавання конкуренту чи іншого використання, спрямованого на одержання вигоди.

До цифрової тіньової економіки слід відносити ту частину неправомірного обігу персональних даних, що пов'язана з одержанням економічної вигоди [2]. Тіньовий обіг персональних даних пропонується визначати як економічно значущий неправомірний рух або використання персональних даних, що прямо чи опосередковано забезпечує дохід, економію витрат, конкурентну перевагу, доступ до майнових благ або ресурс для іншої дохідної тіньової діяльності. Такий критерій окреслює предмет економічного дослідження, не підмінюючи юридичної кваліфікації конкретних дій.

Економічна цінність даних не перетворює їх на звичайний товар, яким можна вільно розпоряджатися поза встановленим правовим режимом. GDPR закріплює принципи законності, справедливості, прозорості, обмеження мети та мінімізації даних (ст. 5), а також умови правомірності обробки (ст. 6) [17]. У цьому дослідженні монетизація означає одержання економічної вигоди від персональних даних або за їх допомогою; йдеться не про визнання самостійного майнового права на такі дані.

На відміну від матеріальних ресурсів, дані можуть багаторазово використовуватися без вичерпання первинного масиву, а їх поєднання з іншими джерелами створює додаткову цінність [18]. Для тіньового сегмента це означає можливість повторної монетизації того самого інформаційного ресурсу.

Економічно значущий тіньовий обіг персональних даних може проявлятися в різних складових тіньової економіки [2]: продаж викрадених ідентифікаційних або платіжних даних має ознаки нелегальної складової; приховане використання клієнтської бази зареєстрованим підприємством – прихованої; платне агрегування даних без належного оформлення господарської діяльності – неформальної. Персональні дані не утворюють окремої складової тіньової економіки, а є інформаційним ресурсом різних моделей тіньової діяльності.

Оцінювання такого обігу лише за вартістю реалізованих масивів не відображає його фактичного масштабу. Дані можуть мати самостійну ціну або використовуватися для доступу до коштів, захоплення облікових

записів чи недобросовісного залучення клієнтів. Оцінювання має охоплювати три складові: надходження від безпосередньої реалізації даних; майнову вигоду від подальших операцій з їх використанням; економію витрат завдяки неправомірному використанню інформаційного ресурсу. Ризик-орієнтоване оцінювання має також враховувати структуру, джерела та управлінську значущість окремих проявів [6].

При оцінюванні слід окремо враховувати характеристики інформаційного масиву, спосіб його монетизації та кінцеві економічні наслідки. Однакові за обсягом масиви можуть істотно відрізнятися за цінністю залежно від актуальності, повноти, можливості поєднання з іншими відомостями та способу кінцевого використання.

Кількість витоків або скомпрометованих записів сама по собі відображає масштаб інформаційного ризику, але не масштаб тіньової економічної діяльності. Для віднесення відповідної практики до тіньової економічної діяльності необхідно встановити зв'язок між неправомірним обігом даних і конкретним економічним результатом; за його відсутності йдеться про порушення у сфері захисту персональних даних, а не про тіньову економіку.

Монетизація персональних даних зазвичай має ланцюговий характер. Спочатку дані одержують і накопичують шляхом неправомірного копіювання, фішингу, використання скомпрометованих облікових записів, зловживання службовим доступом або придбання готового масиву. Саме первинне одержання ще не визначає економічного результату – він залежить від подальшого використання.

На наступному етапі масив перевіряється, очищується, зіставляється з іншими джерелами, доповнюється та сегментується. Так розрізнені контактні чи ідентифікаційні відомості можуть перетворюватися на структурований профіль, а їх прикладна цінність зростає внаслідок обробки й збагачення.

Передавання або реалізація може набувати форми одноразового продажу, платного доступу, передплати на оновлення, надання відомостей за запитом, обміну масивами чи включення даних до комплексу інших незаконних цифрових послуг. Europol фіксує ринок викрадених даних і діяльність брокерів початкового доступу [13], а також розширення кіберзлочинних можливостей завдяки шифруванню, проксі-сервісам і штучному інтелекту [14]. На таких ринках продаються не лише самі дані, а й доступ до систем, інфраструктура та інструменти їх використання.

Кінцевий результат виникає під час перепродажу даних, доступу до коштів чи облікових записів, персоналізованого шахрайства, вимагання або скорочення витрат на залучення клієнтів. Частина доходу може спрямовуватися на придбання нових масивів, скомпрометованих облікових записів, програмних засобів та послуг посередників, формуючи механізм тіньової капіталізації, за якого попередня вигода стає ресурсом наступних операцій. Узагальнений ланцюг монетизації подано на рис. 1.

Не кожний випадок тіньового обігу охоплює всі наведені етапи. Запропонований ланцюг дає змогу визначити момент формування економічного результату, його одержувача та суб'єктів, які несуть пов'язані витрати.

Учасники ланцюга можуть бути різними: джерело даних, особа, яка їх первинно одержала, посередник і кінцевий користувач не обов'язково мають сталі організаційні зв'язки. Вигода формується на кількох етапах, а припинення окремого каналу передавання не завжди припиняє обіг уже створених копій.

Цифрова форма спрощує копіювання й транскордонне передавання даних, але їх економічна цінність змінюється в часі через оновлення контактів, паролів, платіжних реквізитів та інших характеристик. Тому важливим параметром є період збереження практичної цінності, який формує стимули до оперативної реалізації та регулярного оновлення масивів.

За способом одержання економічної вигоди можна виокремити п'ять механізмів монетизації: прямий, посередницько-аналітичний, інструментальний, конкурентно-комерційний та реінвестиційний. В одному фактичному ланцюзі вони можуть поєднуватися.

Пряма монетизація полягає у платному наданні масиву, окремого запису, сформованої вибірки, облікових даних або доступу до інформаційної системи. Результатом є дохід продавця, а можливість копіювання без втрати первинного масиву створює передумови для багаторазової реалізації того самого інформаційного ресурсу.

Посередницько-аналітична монетизація ґрунтується на підвищенні цінності вихідного масиву шляхом перевірки актуальності, усунення дублікатів, агрегування, сегментації та збагачення. Вигода формується як різниця між витратами на одержання й підготовку інформації та вартістю доступу до структурованого продукту. До тіньового сегмента такі операції належать лише тоді, коли неправомірність одержання або використання ресурсу поєднується з економічною вигодою.



Рис. 1. Ланцюг монетизації персональних даних

Джерело: розроблено авторами

Інструментальна монетизація виникає, коли дані не продаються безпосередньо, а забезпечують іншу майнову вигоду. Показовий приклад – шахрайська схема «Державна виплата 7200 грн», зафіксована Центром кіберзахисту Національного банку України (CSIRT-NBU) у лютому 2026 р. На фішинговій сторінці у користувачів виманювали номер мобільного телефону, реквізити платіжної картки, PIN-код та інші дані, які надалі використовували для онлайн-авторизації й викрадення коштів [11]. Економічне значення даних у такому разі визначається майновим результатом операції, яку вони забезпечили, а не умовною ціною самого інформаційного набору.

До цього механізму належить також використання даних для захоплення облікових записів, здійснення операцій від чужого імені, обходу процедур дистанційної ідентифікації чи персоналізованої соціальної інженерії. Дані виконують функцію проміжного ресурсу, що підвищує адресність і результативність наступної операції.

Конкурентно-комерційна монетизація охоплює неправомірне використання клієнтських, контактних або поведінкових даних у формально легальній господарській діяльності. Вигода проявляється у скороченні витрат на пошук аудиторії, маркетинг і збирання інформації або в одержанні додаткового доходу. Це ставить такого учасника у вигідніше становище порівняно із суб'єктами, які несуть витрати на законне одержання відповідних відомостей.

Економічно значущий тіньовий обіг персональних даних не обмежується кіберзлочинними ринками: відповідні практики можуть бути інтегровані в діяльність легального підприємства без формування окремого незаконного ринку.

Реінвестиційна монетизація характеризує відтворення тіньового циклу, коли частина одержаного доходу спрямовується на придбання нових даних, доступу до інформаційних систем, програмних засобів, проксі-сервісів або послуг посередників. Одержана раніше вигода стає ресурсом для продовження й масштабування тіньової діяльності, що узгоджується з даними Europol про спеціалізацію ринків викрадених даних і торгівлю доступом до систем [13; 14].

За економічною функцією прямий і посередницько-аналітичний механізми пов'язані з платною операцією щодо даних або сформованого на їх основі продукту; інструментальний і конкурентно-комерційний – з використанням даних для одержання іншої вигоди; реінвестиційний – з використанням уже одержаного доходу для розширення діяльності. Таке розмежування показує, чому облік продажу даних охоплює лише частину сукупного економічного результату.

Практичне оцінювання може спиратися на вартість платного доступу, фактичний платіж, майновий результат наступної операції, розмір зекономлених витрат або кошти, спрямовані на тіньову інфраструктуру. Для уникнення подвійного рахунку дохід продавця даних і майновий результат їх використання покупцем слід обліковувати окремо – за відповідними суб'єктами й операціями. Узагальнену характеристику механізмів наведено у табл. 1.

Запропонована класифікація має економіко-функціональний характер і розмежовує способи використання персональних даних для одержання економічної вигоди.

Тіньова монетизація персональних даних створює ризики не лише для суб'єктів персональних даних, а й для фінансової сфери, конкурентного середовища та бізнесу, а також підриває довіру до цифрових сервісів. Для подальшого аналізу ці ризики згруповано у п'ять каналів: фінансово-фінансовий, конкурентно-підприємницький, інвестиційно-інноваційний, інституційний і криміногенно-безпековий [6].

Фінансово-фінансовий канал пов'язаний із неврахованими доходами від продажу даних або доступу до них та з майновими втратами громадян, бізнесу й фінансових установ. Масштаб платіжного середовища, у якому може реалізуватися такий ризик, ілюструють дані НБУ: у 2025 р. з використанням платіжних карток, емітованих українськими банками та фінансовими установами, здійснено 9 083,5 млн безготівкових операцій на суму 4 684,3 млрд грн, з них в інтернеті – понад 1,2 млрд операцій майже на 770 млрд грн [7]. Ці показники не характеризують масштаби шахрайства, але відображають обсяг платіжного середовища, у якому компрометація даних може спричинити значні втрати.

Таблиця 1

Механізми монетизації персональних даних у цифровій тіньовій економіці

Механізм	Об'єкт економічного використання	Спосіб формування або використання вигоди	Типовий результат
Прямий	база, запис, облікові дані, доступ	плата за передавання або доступ	тіньовий дохід
Посередницько-аналітичний	перевірений, агрегований або збагачений масив	плата за підготовлену інформацію	дохід від підготовки та надання даних
Інструментальний	ідентифікаційні, авторизаційні, фінансові відомості	використання для іншої операції	доступ до коштів чи інших майнових благ
Конкурентно-комерційний	клієнтські та поведінкові дані	економія витрат, конкурентна перевага	зниження витрат або додатковий дохід
Реінвестиційний	дохід від попередніх операцій	повторне вкладення у дані та інфраструктуру	масштабування тіньової діяльності

Джерело: розроблено авторами

Конкурентно-підприємницький канал виявляється в асиметрії витрат: суб'єкт, який неправомірно отримав клієнтську базу, може економити на маркетингу, пошуку аудиторії та збиранні інформації, тоді як добросовісний конкурент несе відповідні витрати. Для володільця скомпрометованих даних наслідками стають витрати на технічне відновлення, аудит, правове реагування, посилення захисту, комунікацію з клієнтами та відновлення репутації.

Управління такими ризиками має поєднувати правовий комплаєнс з управлінням інформаційною безпекою та приватністю. Ризик-орієнтовані підходи закріплено в «NIST Privacy Framework 1.0» [12], «ISO/IEC 27001:2022» [15] та «ISO/IEC 27701:2025» [16], що дає підстави розглядати захист персональних даних як складову корпоративного управління ризиками й операційної стійкості.

Інвестиційно-інноваційний канал пов'язаний з додатковими витратами на захист інформаційних систем, контроль доступу та реагування на інциденти. За системного неправомірного використання даних частина ресурсів, які могли б спрямовуватися на розвиток продуктів та інновацій, витрачається на захист інформаційних систем і мінімізацію цифрових ризиків, а обережніша поведінка користувачів може знижувати ефективність сервісів, що ґрунтуються на дистанційній ідентифікації та довірі користувачів.

Інституційний канал відображає подвійний ефект цифровізації: електронні реєстри й автоматизований обмін підвищують прозорість, але концентрують значні інформаційні масиви. За недостатньої координації, прозорості та цифрової простежуваності відповідні системи можуть посилювати ризики для добросовісних суб'єктів господарювання [5]. Систематичні інциденти з даними знижують довіру до електронної взаємодії й можуть послаблювати стимули до формалізації економічної діяльності.

Криміногенно-безпековий канал виникає, коли дані використовуються для шахрайства, вимагання, доступу до фінансових активів, викрадення цифрової ідентичності чи інших дій, спрямованих на майнову вигоду. У таких моделях персональні дані можуть бути проміжним ресурсом для одержання значно більшої

майнової вигоди та полегшувати здійснення інших тіньових операцій, збільшуючи витрати держави, бізнесу, фінансових установ і громадян на їх запобігання та мінімізацію.

Закон України «Про національну безпеку України» від 21.06.2018 р. № 2469-VIII відносить сталий розвиток національної економіки до фундаментальних національних інтересів (п. 2 ч. 3 ст. 3), а державну політику спрямовує, зокрема, на забезпечення економічної, інформаційної безпеки та кібербезпеки (ч. 4 ст. 3) [9]. З огляду на це тіньовий обіг персональних даних слід розглядати як джерело взаємопов'язаних економічних, інформаційних і кібербезпекових ризиків. Систематизацію каналів і носіїв втрат наведено у табл. 2.

Вигоди й витрати такого обігу розподіляються асиметрично: вигода концентрується у продавців, посередників і кінцевих користувачів даних, тоді як основні витрати несуть суб'єкти персональних даних, підприємства, фінансові установи та держава.

Наслідки можна поділити на прямі, похідні та системні. Прямі охоплюють майнові втрати й невідкладні витрати на відновлення та блокування доступу; похідні – відтік клієнтів, зростання витрат на захист, недобросовісну конкуренцію й перебудову бізнес-процесів; системні – зниження довіри до цифрових сервісів та інституцій, підвищення вартості управління ризиками і зменшення готовності учасників надавати дані в межах правомірної цифрової взаємодії.

З огляду на зазначені загрози детінізація не повинна зводитися до максимального контролю всіх операцій з персональними даними. Надмірне регуляторне навантаження підвищує витрати правомірної діяльності, тому завдання державного регулювання полягає у зменшенні можливостей одержання тіньової вигоди без створення невинуватених перешкод для законного використання даних. Насамперед необхідно забезпечити простежуваність юридично значущих операцій. Закон України «Про захист персональних даних» покладає на володільців, розпорядників і третіх осіб обов'язок захищати дані від незаконної обробки та доступу (ч. 1 ст. 24) [8]. GDPR закріплює принцип підзвітності (п. 2 ст. 5) та вимогу належних технічних і організаційних заходів відповідно до ризику (ст. 32)

Таблиця 2

Канали впливу тіньового обігу персональних даних на економічну безпеку

Канал	Основний економічний наслідок	Носії втрат (за ступенем безпосередності впливу)
Фіскально-фінансовий	невраховані доходи, звуження податкової бази, майнові втрати	держава, фінансові установи, населення, бізнес
Конкурентно-підприємницький	економія витрат недобросовісного учасника, витрати на відновлення і захист	бізнес
Інвестиційно-інноваційний	зростання вартості цифрового ризику та захисних витрат	бізнес, інвестори, користувачі цифрових сервісів
Інституційний	зниження довіри до цифрової ідентифікації, реєстрів і сервісів	держава, бізнес, населення
Криміногенно-безпековий	майнові втрати та відтворення суміжних тіньових практик	населення, фінансові установи, бізнес, держава

Джерело: розроблено авторами

[17]. Закон України «Про публічні електронні реєстри» передбачає автоматичне протоколювання операцій електронної взаємодії (ч. 2 ст. 7) і використання відповідної Системи електронної взаємодії (ст. 43) [10]. Це дає змогу фіксувати та перевіряти значущі операції без суцільного контролю кожної технічної дії.

Окреме значення має ризик-орієнтоване виявлення потенційно небезпечних операцій. Індикаторами можуть бути аномальні обсяги вивантаження, нетипова частота запитів, невідповідність доступу службовим функціям або різке зростання активності щодо певного масиву. Такі ознаки мають бути підставою для поглибленої перевірки, а не самостійним доказом порушення. Контрольні пріоритети визначаються з урахуванням концентрації ризиків, потенційних наслідків та значущості відповідного сегмента [6].

Протидія систематичній монетизації потребує поєднання контролю відповідних операцій, аналізу пов'язаних фінансових потоків і корпоративного комплаєнсу. На рівні підприємства доцільно застосовувати розмежування прав доступу, контроль масових вивантажень, управління ризиками підрядників, багатфакторну автентифікацію, аудит і виявлення аномальної активності. Аудит захисту персональних даних дає змогу виявляти слабкі місця й оцінювати ризики [3]; для цілей економічної безпеки його слід доповнювати оцінкою можливих прямих і похідних економічних втрат.

Захисту потребує також державна цифрова та ідентифікаційна інфраструктура. Розвиток BankID, електронних реєстрів і міжвідомчої взаємодії має супроводжуватися мінімізацією даних, розмежуванням ролей і фіксацією значущих операцій. У Системі BankID НБУ персональні дані передаються між визначеними учасниками, а сама система їх не зберігає [1]; для публічних реєстрів закон передбачає електронну взаємодію та автоматичне протоколювання [10]. Ефективність цифровізації як інструменту детінізації залежить від якості, захищеності та контрольованості використання інформації.

Результативність політики слід оцінювати за тим, наскільки вона зменшує очікувану вигоду та підвищує витрати й ризики тіньової поведінки. Водночас детінізаційні заходи мають ускладнювати неправомірне одержання даних, їх монетизацію та повторне використання, не створюючи непропорційних витрат для добросовісного бізнесу.

Система показників має відображати не кількість перевірок, а зменшення економічного ризику: скорочення часу від виявлення компрометації до припинення доступу, частки повторних інцидентів та економічних втрат, підвищення повноти журналювання значущих операцій і недопущення надмірного зростання регуляторних витрат добросовісного бізнесу.

Інтенсивність контролю має залежати від категорії даних. Контактна інформація, платіжні й авторизаційні дані та комплексні ідентифікаційні профілі характеризуються різним рівнем економічного

ризик, тому оцінювання має враховувати характер і чутливість інформації, можливість її повторного використання, потенційну майнову вигоду та масштаб можливих втрат.

Висновки.

1. Тіньовий обіг персональних даних як сегмент цифрової тіньової економіки доцільно визначати як економічно значущий неправомірний рух або використання даних, що прямо чи опосередковано забезпечує дохід, економію витрат, конкурентну перевагу, доступ до майнових благ або ресурс для іншої тіньової діяльності. Визначальною ознакою є економічний результат, а не сам факт порушення режиму обробки; персональні дані при цьому є інформаційним ресурсом прихованої, неформальної або нелегальної активності.

2. Економічний результат не може оцінюватися лише за ціною реалізованого масиву. Необхідно окремо враховувати дохід від продажу або доступу, майнову вигоду від наступних операцій та економію витрат, а також етапи одержання, збагачення, передавання, кінцевого використання й реінвестування. Розмежування результатів за суб'єктами та операціями запобігає подвійному рахунку.

3. За способом формування вигоди виокремлено прямий, посередницько-аналітичний, інструментальний, конкурентно-комерційний і реінвестиційний механізми. Перші два пов'язані з платним наданням даних або інформаційного продукту, наступні два – з використанням даних для одержання іншої майнової чи конкурентної вигоди, реінвестиційний – з відтворенням та масштабуванням тіньової діяльності. Класифікація має економіко-функціональний характер.

4. Вплив на економічну безпеку України реалізується через фіскально-фінансовий, конкурентно-підприємницький, інвестиційно-інноваційний, інституційний і криміногенно-безпековий канали. Вигода концентрується у продавців, посередників і кінцевих користувачів даних, тоді як прямі, похідні та системні витрати несуть населення, бізнес, фінансові установи й держава.

5. Детінізація має ґрунтуватися на пропорційному ризик-орієнтованому регулюванні, що поєднує простежуваність юридично значущих операцій, ризик-аналіз, контроль пов'язаних фінансових потоків, корпоративний комплаєнс, аудит і захист державної цифрової інфраструктури. Результативність таких заходів слід оцінювати за зменшенням повторних інцидентів та економічних втрат, швидкістю реагування і повнотою журналювання операцій. Інтенсивність контролю має залежати від чутливості даних, можливості їх повторного використання та масштабу потенційних втрат.

Перспективи подальших досліджень пов'язані з розробленням інструментарію кількісного оцінювання цього сегмента, формуванням галузевих ризик-профільів та апробацією індикаторів монетизації й економічних втрат залежно від категорії даних і способу їх використання.

Список літератури:

1. Валуєв А., Чернецький С., Кашкін Д., Габрелян А., Дяковський О. Розвиток системи BankID в Україні: особливості функціонування та нормативне забезпечення. *Вісник Київського національного університету імені Тараса Шевченка. Економіка*. 2026. № 2(229). С. 15–27. DOI: <https://doi.org/10.17721/1728-2667.2026/229-2/2>
2. Габрелян А. Ю. Тіньова економіка: сутність, ознаки, структура та форми прояву. *Успіхи і досягнення у науці*. 2026. № 5(27). С. 2944–2960. DOI: [https://doi.org/10.52058/3041-1254-2026-5\(27\)-2944-2960](https://doi.org/10.52058/3041-1254-2026-5(27)-2944-2960)
3. Дяковський О. С. Аудит захисту персональних даних: організаційно-правовий та адміністративний аспект. *Право і суспільство*. 2025. № 6. С. 182–188. DOI: <https://doi.org/10.32842/2078-3736/2025.6.26>
4. Дяковський О. С. Процесуальні особливості обігу інформації, що містить персональні дані. *Вчені записки Таврійського національного університету імені В.І. Вернадського. Серія: Юридичні науки*. 2018. Т. 29(68). № 1. С. 58–63.
5. Лагунов К. В., Габрелян А. Ю. Інституційно-організаційне забезпечення державної політики детінізації економіки в системі економічної безпеки суб'єктів господарювання. *Академічні візії*. 2026. № 54. DOI: <https://doi.org/10.66556/2786-586X.54.habrelian-a>
6. Лагунов К. В., Габрелян А. Ю. Методичні засади оцінювання тіньової економіки в системі ризик-орієнтованого управління економічною безпекою. *Наукові записки Львівського університету бізнесу та права*. 2026. Вип. 48. С. 705–721. DOI: <https://doi.org/10.66556/2663-0117.48.habrelian-a>
7. Національний банк України. Операції з платіжними картками у 2025 році: більшість – безготівкові. 16 лютого 2026 р. URL: <https://bank.gov.ua/ua/news/all/operatsiyi-z-platijnimi-kartkami-u-2025-rotsi-bilshist-bezgotivkovi>
8. Про захист персональних даних : Закон України від 1 червня 2010 р. № 2297-VI / Верховна Рада України. *Відомості Верховної Ради України*. 2010. № 34. Ст. 481. URL: <https://zakon.rada.gov.ua/laws/show/2297-17>
9. Про національну безпеку України : Закон України від 21 червня 2018 р. № 2469-VIII / Верховна Рада України. *Відомості Верховної Ради України*. 2018. № 31. Ст. 241. URL: <https://zakon.rada.gov.ua/laws/show/2469-19>
10. Про публічні електронні реєстри : Закон України від 18 листопада 2021 р. № 1907-IX / Верховна Рада України. *Відомості Верховної Ради України*. 2023. № 11. Ст. 27. URL: <https://zakon.rada.gov.ua/laws/show/1907-20>
11. Центр кіберзахисту Національного банку України (CSIRT-NBU). Шахрайська схема «Державна виплата 7200 грн». 3 лютого 2026 р. URL: <https://cyber.bank.gov.ua/news/206>
12. Boeckl K., Lefkovitz N. NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management. Version 1.0. Gaithersburg, MD : National Institute of Standards and Technology, 2020. DOI: <https://doi.org/10.6028/NIST.CSWP.10>
13. Europol. Steal, Deal and Repeat: How Cybercriminals Trade and Exploit Your Data. Internet Organised Crime Threat Assessment (IOCTA) 2025. Luxembourg : Publications Office of the European Union, 2025. URL: <https://europol.europa.eu/publication-events/main-reports/iocta-report>
14. Europol. The Evolving Threat Landscape: How Encryption, Proxies and AI Are Expanding Cybercrime. Internet Organised Crime Threat Assessment (IOCTA) 2026. Luxembourg : Publications Office of the European Union, 2026. DOI: [10.2813/5737847](https://doi.org/10.2813/5737847)
15. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. 3rd ed. Geneva : International Organization for Standardization, 2022.
16. ISO/IEC 27701:2025. Information security, cybersecurity and privacy protection – Privacy information management systems – Requirements and guidance. 2nd ed. Geneva : International Organization for Standardization, 2025.
17. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union*. 2016. L 119. 4 May. P. 1–88.
18. World Bank. World Development Report 2021: Data for Better Lives. Washington, DC : World Bank, 2021. URL: <https://wdr2021.worldbank.org/the-report/>

References:

1. Valuiiev A., Chernetskyi S., Kashkin D., Habrelian A., Diakovsky O. (2026) Rozvytok systemy BankID v Ukraini: osoblyvosti funktsionuvannia ta normatyvne zabezpechennia [Development of the BankID system in Ukraine: features of functioning and regulatory support]. *Visnyk Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka. Ekonomika – Bulletin of Taras Shevchenko National University of Kyiv. Economics*, no. 2(229), pp. 15–27. DOI: <https://doi.org/10.17721/1728-2667.2026/229-2/2>
2. Habrelian A. Yu. (2026) Tinova ekonomika: sutnist, oznaky, struktura ta formy proiavu [Shadow economy: essence, features, structure and forms of manifestation]. *Uspikhy i dosiahnennia u nautsi – Successes and Achievements in Science*, no. 5(27), pp. 2944–2960. DOI: [https://doi.org/10.52058/3041-1254-2026-5\(27\)-2944-2960](https://doi.org/10.52058/3041-1254-2026-5(27)-2944-2960)
3. Diakovsky O. S. (2025) Audyt zakhystu personalnykh danykh: orhanizatsiino-pravovy i ta administratyvnyi aspekt [Personal data protection audit: organizational, legal and administrative aspect]. *Pravo i suspilstvo – Law and Society*, no. 6, pp. 182–188. DOI: <https://doi.org/10.32842/2078-3736/2025.6.26>
4. Diakovsky O. S. (2018) Protseesualni osoblyvosti obihu informatsii, shcho mistyt personalni dani [Procedural features of the circulation of information containing personal data]. *Vcheni zapysky Tavriiskoho natsionalnoho universytetu imeni V.I. Vernadskoho. Seriya: Yurydychni nauky – Scientific Notes of V.I. Vernadsky Taurida National University. Series: Juridical Sciences*, vol. 29(68), no. 1, pp. 58–63.
5. Lahunov K. V., Habrelian A. Yu. (2026) Instytutsiino-orhanizatsiine zabezpechennia derzhavnoi polityky detinizatsii ekonomiky v systemi ekonomichnoi bezpeky subiektiv hospodariuvannia [Institutional and organizational support for state

policy of de-shadowing the economy in the system of economic security of business entities]. *Akademichni vizii – Academic Visions*, no. 54. DOI: <https://doi.org/10.66556/2786-586X.54.habrelian-a>

6. Lahunov K. V., Habrelian A. Yu. (2026) *Metodychni zasady otsiniuvannia tinovoi ekonomiky v systemi ryzyk-orientovanoho upravlinnia ekonomichnoiu bezpekoiu* [Methodological principles for assessing the shadow economy in the system of risk-oriented economic security management]. *Naukovi zapysky Lvivskoho universytetu biznesu ta prava – Scientific Notes of Lviv University of Business and Law*, vol. 48, pp. 705–721. DOI: <https://doi.org/10.66556/2663-0117.48.habrelian-a>

7. National Bank of Ukraine (2026) *Operatsii z platizhnymy kartkami u 2025 rotsi: bilshist – bezgotivkovy* [Payment card transactions in 2025: the majority were cashless]. Available at: <https://bank.gov.ua/ua/news/all/operatsiyi-z-platijnimi-kartkami-u-2025-rotsi-bilshist-bezgotivkovy>

8. Verkhovna Rada of Ukraine (2010) *Pro zakhyst personalnykh danykh: Zakon Ukrainy vid 1 chervnia 2010 r. No. 2297-VI* [On Personal Data Protection: Law of Ukraine of 1 June 2010 No. 2297-VI]. *Vidomosti Verkhovnoi Rady Ukrainy – Bulletin of the Verkhovna Rada of Ukraine*, no. 34, art. 481. Available at: <https://zakon.rada.gov.ua/laws/show/2297-17>

9. Verkhovna Rada of Ukraine (2018) *Pro natsionalnu bezpeku Ukrainy: Zakon Ukrainy vid 21 chervnia 2018 r. No. 2469-VIII* [On National Security of Ukraine: Law of Ukraine of 21 June 2018 No. 2469-VIII]. *Vidomosti Verkhovnoi Rady Ukrainy – Bulletin of the Verkhovna Rada of Ukraine*, no. 31, art. 241. Available at: <https://zakon.rada.gov.ua/laws/show/2469-19>

10. Verkhovna Rada of Ukraine (2021) *Pro publichni elektronni reiestry: Zakon Ukrainy vid 18 lystopada 2021 r. No. 1907-IX* [On Public Electronic Registers: Law of Ukraine of 18 November 2021 No. 1907-IX]. *Vidomosti Verkhovnoi Rady Ukrainy – Bulletin of the Verkhovna Rada of Ukraine*, 2023, no. 11, art. 27. Available at: <https://zakon.rada.gov.ua/laws/show/1907-20>

11. Tsentr kiberzakhystu Natsionalnoho banku Ukrainy (2026) *Shakhraiska skhema “Derzhavna vyplata 7200 hrn”* [Fraud scheme “State Payment 7200 UAH”]. Available at: <https://cyber.bank.gov.ua/news/206>

12. Boeckl K., Lefkovitz N. (2020) *NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management*. Version 1.0. Gaithersburg, MD: National Institute of Standards and Technology. DOI: <https://doi.org/10.6028/NIST.CSWP.10>

13. Europol (2025) *Steal, Deal and Repeat: How Cybercriminals Trade and Exploit Your Data. Internet Organised Crime Threat Assessment (IOCTA) 2025*. Luxembourg: Publications Office of the European Union. Available at: <https://www.europol.europa.eu/publication-events/main-reports/iocta-report>

14. Europol (2026) *The Evolving Threat Landscape: How Encryption, Proxies and AI Are Expanding Cybercrime. Internet Organised Crime Threat Assessment (IOCTA) 2026*. Luxembourg: Publications Office of the European Union. DOI: <https://doi.org/10.2813/5737847>

15. International Organization for Standardization (2022) *ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements*. 3rd ed. Geneva: International Organization for Standardization.

16. International Organization for Standardization (2025) *ISO/IEC 27701:2025. Information security, cybersecurity and privacy protection – Privacy information management systems – Requirements and guidance*. 2nd ed. Geneva: International Organization for Standardization.

17. European Parliament and Council of the European Union (2016) *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. *Official Journal of the European Union*, L 119, pp. 1–88.

18. World Bank (2021) *World Development Report 2021: Data for Better Lives*. Washington, DC: World Bank. Available at: <https://wdr2021.worldbank.org/the-report/>

SHADOW CIRCULATION OF PERSONAL DATA AS A SEGMENT OF THE DIGITAL SHADOW ECONOMY: MONETIZATION MECHANISMS AND THREATS TO THE ECONOMIC SECURITY OF UKRAINE

The growing dependence of economic activity on digital identification, electronic payments, online services, and large-scale data exchange increases the economic significance of personal data and, at the same time, broadens the range of risks associated with their unlawful circulation. For Ukraine, this issue is particularly relevant because the expansion of public digital services, electronic registers, online banking, and other forms of digital interaction is accompanied by the accumulation and transfer of substantial volumes of identification, contact, and financial information. In this context, unlawful access to personal data, their transfer, or their use can no longer be viewed solely as a matter of privacy protection or cybersecurity, since such practices may also become part of shadow economic activity and affect the economic security of the state. The article considers the distinction between unlawful data operations that have no independent economic effect and practices in which personal data are used to obtain income, reduce costs, gain access to assets, create unfair competitive advantages, or support other income-generating shadow activities. Attention is paid to the economic logic of the shadow circulation of personal data, including the successive stages through which data may be acquired, accumulated, verified, enriched, transferred, used for economic gain, and reused. The discussion also covers the role of intermediaries, the use of personal data as an auxiliary resource in subsequent transactions, and

the reinvestment of proceeds in data, access to information systems, software, proxy services, and other resources that facilitate the continuation of shadow activity. The economic-security dimension is examined through possible effects on public finances, financial losses of individuals and businesses, competitive conditions, corporate risk management, investment and innovation activity, trust in digital services, and the functioning of digital institutions. The article further discusses approaches to limiting the shadow use of personal data through the traceability of legally significant operations, risk-oriented detection of suspicious activity, analysis of related financial flows, corporate compliance, auditing, differentiation of access rights, and protection of state digital and identification infrastructure. Particular attention is given to proportional regulation that reduces opportunities for unlawful monetization of personal data without imposing excessive compliance costs on legitimate digital activity or discouraging the use of lawful digital services.

Key words: shadow circulation of personal data, digital shadow economy, personal data monetization, economic security, risk-oriented regulation, de-shadowing, digital infrastructure.

Дата надходження статті: 19.08.2026

Дата прийняття статті до публікації: 14.09.2026

Дата публікації статті: 06.10.2026