5. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. *Відомості Верховної Ради України*. 2017. № 45. Ст. 403. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 10.10.2026).

6. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» : Указ Президента України від 28 груд. 2021 р. № 685/2021. URL: https://www.president.gov.ua/documents/6852021-41069 (дата звернення: 10.10.2026).

7. Шевчук М. О. До питання генези поняття інформаційної безпеки як складової національної безпеки. *Науковий вісник Ужгородського Національного Університету. Серія: Право*. 2023. Вип. 78, ч. 2. С. 134–139. DOI: https://doi.org/10.24144/2307-3322.2023.78.2.21

Анасенко К.В., здобувач
Науковий керівник: Чугаєвська А.В.,
кандидат юридичних наук, доцент, доцент кафедри кримінального права
Національна академія внутрішніх справ

ПРОБЛЕМИ ЗАКОНОДАВЧОГО ВРЕГУЛЮВАННЯ НЕЗАКОННОГО ВИКОРИСТАННЯ ПЛАТІЖНИХ ІНСТРУМЕНТІВ У ЗЛОЧИННІЙ ДІЯЛЬНОСТІ

Однією з актуальних проблем сучасної протидії злочинності є залучення фізичних осіб до незаконного обігу коштів шляхом використання належних їм банківських рахунків і платіжних інструментів. У правоохоронній практиці таких осіб називають «дропами» або «грошовими мулами» [1]. Дроп-рахунки використовуються для переміщення незаконно отриманих коштів, а також для ухилення від сплати податків. Залучення таких рахунків ускладнює встановлення фактичних учасників фінансових операцій і відстеження походження доходів.

Актуальність даної проблеми підтверджується інформацією, наданою Департаментом кіберполіції Національної поліції України. Для порівняння, у 2020 році було виявлено 2 194 «грошових мулів», то лише за дев'ять місяців 2025 року їх кількість зросла до 26 700 осіб [2]. Крім того, після початку функціонування системи «Antifraud» з 1 травня 2025 року було зареєстровано 4 539 подій онлайн-шахрайства з використанням платіжних реквізитів [3]. За даними кіберполіції, приблизно у 70 % випадків кібершахрайства платіжні засоби «дропів» використовувалися для отримання та легалізації незаконно одержаних коштів. У свою чергу, за оцінкою Національного банку України, через картки «дропів» може проходити близько 200 млрд грн щороку [4]. Наведені статистичні дані свідчать про значне поширення використання платіжної інфраструктури у протиправній діяльності та обґрунтовують необхідність удосконалення законодавства.

З огляду на це, особливого значення набуває Законопроєкт №16013 зареєстрований 2 вересня 2026 року та визначений Президентом України як невідкладний [5]. Поданий законопроєкт спрямований на вдосконалення механізмів кримінально-правового захисту майнових прав громадян, забезпечення безпеки платіжної інфраструктури та приведення законодавства України у відповідність до вимог Директиви ЄС 2019/713 від 17.04.2019 про боротьбу з шахрайством та підробкою безготівкових платіжних засобів шляхом внесення змін до Кримінального та Кримінального процесуального кодексів України, далі - КК України, КПК України відповідно.

Законопроєктом № 16013 пропонується значно розширити статтю 200 КК України, змінивши її назву, оновивши термінологію та перелік кримінально караних діянь. Передбачається конкретизація понять, пов'язаних із платіжними інструментами, електронними гаманцями тощо, криміналізація незаконного заволодіння платіжними засобами й доступом до рахунків, а також закріплення повторності та попередньої змови групи осіб як кваліфікуючих ознак. Крім того, пропонується посилити санкції.

Головним нововведенням цього проєкту є доповнення КК України статтею 200-1, яка встановлюватиме відповідальність за незаконні дії з платіжними інструментами та отриманням доступу до них за наявності спеціальної мети - для вчинення шахрайства або іншого кримінального правопорушення. Саме ця мета є ключовою суб'єктивною ознакою складу правопорушення, оскільки відмежовує кримінально карані дії від інших випадків передачі чи набуття платіжних засобів.

Разом з цим, важливим є доповнення статті 96-3 КК України посиланнями на статті 200 і 200-1, що розширить можливості застосування заходів кримінально-правового характеру до юридичних осіб. В свою чергу, зміни до статей 214 і 216 КПК України стосуватимуться процесуальних аспектів розслідування відповідних правопорушень.

Водночас, запропоновані положення можуть викликати низку проблем.

По-перше, це невизначеність меж криміналізації. За висновком Головного науково-експертного управління, далі - ГНЕУ, проєкт у запропонованій статті 200-1 охоплює передачу платіжних інструментів не тільки для шахрайства, а для вчинення фактично будь-якого «іншого кримінального правопорушення». ГНЕУ прямо звертає увагу, що це ширше за мінімальні вимоги Директиви ЄС 2019/713, а належне обґрунтування такого розширення у супровідних документах відсутнє.

По-друге, це часткова конкуренція кримінально-правових норм. Згідно позиції ГНЕУ, нова редакція ст. 200 частково охоплює елементи складів правопорушень передбачених статтями 231, 361 та 362 КК України. Наприклад, індивідуальна облікова інформація та засоби доступу до банківського рахунку можуть одночасно становити комп'ютерну інформацію або банківську таємницю, а незаконні дії з ними - підпадати під ознаки кількох зазначених складів, що створює труднощі для їх розмежування.

По-третє, законопроєкт містить неузгодженість між положеннями КК та КПК України: ст. 96-3 КК передбачає можливість застосування заходів кримінально-правового характеру до юридичної особи за всіма частинами нової ст. 200-1 КК, тоді як відповідні зміни до ст. 214 КПК охоплюють лише ч.2 і 3 цієї статті. При цьому діяння, передбачене ч.1 ст. 200-1 КК, належатиме до кримінальних проступків, а процесуальний механізм ч.8 ст. 214 КПК стосується злочинів. ГНЕУ прямо наголошує на необхідності узгодження відповідних положень КК та КПК [6, с.3-5].

На особливу увагу також заслуговує проблема розмежування ч.2 нової редакції ст. 200 КК та шахрайства (ст. 190 КК України) [7], оскільки обидві норми передбачають заволодіння предметом шляхом обману або зловживання довірою. Водночас вони відрізняються предметом посягання: за ст. 190 ним є чуже майно або право на майно, тоді як за ч.2 ст. 200 - це платіжні інструменти, індивідуальна облікова інформація та інші засоби доступу до них. Такий частковий збіг об'єктивної сторони може створювати труднощі при кваліфікації діянь.

Узагальнюючи викладене, можна зробити висновок, що стрімке поширення використання «дропів» у злочинній діяльності та значні обсяги коштів, що проходять через відповідні рахунки, свідчать про актуальність даної проблеми. Законопроєкт №16013 є важливим кроком у цьому напрямку, оскільки передбачає розширення кримінальної відповідальності за незаконні дії з платіжними інструментами та доступом до рахунків і фактично формує спеціальний механізм протидії використанню таких засобів у злочинній діяльності. Водночас ефективність запропонованих змін залежить не лише від самого факту криміналізації відповідних діянь, а й від чіткості та узгодженості нових кримінально-правових норм зі вже існуючими. Виявлені проблеми щодо меж криміналізації, розмежування суміжних складів кримінальних правопорушень, а також узгодження положень КК і КПК України свідчать про необхідність подальшого доопрацювання законопроєкту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Кіберполіція застерігає: не стань пособником шахраїв. Департамент кіберполіції Національної поліції України. 20.02.2024. URL: https://cyberpolice.gov.ua/article/kiberpolicziya

2. Рахунок для прикриття. Як вербують власників банківських карток для відмивання коштів. Департамент кіберполіції Національної поліції України. 02.01.2026. URL: https://cyberpolice.gov.ua/news/raxunok-dlya-prykryttya-yak-verbuyut

3. Щорічний звіт за 2025 рік. 2026. Департамент кіберполіції Національної поліції України. URL: https://cyberpolice.gov.ua/news/shhorichnyj-zvit-7096

4. Тимчасовий ліміт на суму переказів з «карти на карту» запобігатиме використанню платіжної інфраструктури в протиправних цілях та не вплине на діяльність волонтерів (уточнено). Національний банк України. 27.08.2024. URL: https://bank.gov.ua/ua/news/all/timchasoviy-limit-na-sumuperekaziv

5. Проєкт Закону про внесення змін до Кримінального кодексу України та Кримінального процесуального кодексу України щодо захисту громадян, їхніх коштів від незаконних дій з платіжними інструментами й банківськими рахунками : законопроєкт від 02.09.2026 № 16013. URL: https://itd.rada.gov.ua/billinfo/Bills/Card/70664 (дата звернення: 08.10.2026).

6. Висновок на проєкт Закону України «Про внесення змін до Кримінального кодексу України та Кримінального процесуального кодексу України щодо захисту громадян, їхніх коштів від незаконних дій з платіжними інструментами й банківськими рахунками» / Апарат Верховної Ради України, Головне науково-експертне управління. URL: https://itd.rada.gov.ua/billinfo/Bills/pubFile/3654043 (дата звернення: 08.10.2026).

7. Кримінальний кодекс України : Кодекс України від 05.04.2001 № 2341-III : станом на 18.09.2026. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 09.10.2026).

Анісімова К.А., здобувач
Науковий керівник: Ситніченко Олена Михайлівна, к.ю.н., доцент,
доцент кафедри правового забезпечення безпеки бізнесу,
«Державний торговельно-економічний університет»

АКТУАЛЬНІ ПИТАННЯ ПРАВОВОГО РЕГУЛЮВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ

Штучний інтелект упродовж останніх років перетворився з вузькоспеціалізованої технології на інфраструктурний чинник економічного, управлінського та суспільного розвитку. Алгоритмічні системи дедалі ширше застосовуються у фінансовому секторі, медицині, освіті, державному управлінні, сфері безпеки, правосудді та комунікаціях. Водночас швидкість технологічних змін істотно випереджає традиційні цикли нормотворчості. У результаті виникає фундаментальна проблема сучасної правової політики: держава має одночасно мінімізувати ризики, пов’язані із застосуванням штучного інтелекту, і не створити такого регуляторного середовища, яке блокуватиме інновації та послаблюватиме конкурентоспроможність економіки.

Європейський Союз одним із перших запропонував комплексну нормативну відповідь на цю проблему. Регламент (ЄС) 2024/1689, відомий як Artificial Intelligence Act, формує ризикоорієнтовану модель правового регулювання, за якої обсяг юридичних вимог залежить від потенційної небезпеки конкретного способу використання технології [1]. Такий підхід принципово відрізняється від спроб однаково регулювати всі системи штучного інтелекту. Європейська модель поєднує заборону окремих неприйнятних практик, підвищені вимоги до високоризикових систем, правила прозорості, механізми нагляду та спеціальні вимоги щодо моделей загального призначення. В її основі лежить ідея, що правове регулювання повинно бути пропорційним ризику та орієнтуватися не лише на технічні характеристики системи, а й на можливі наслідки для людини, суспільства і держави.

Особливе значення має те, що AI Act пов’язує регулювання штучного інтелекту із захистом фундаментальних прав, демократії та верховенства права. У цьому контексті Н. Рангоне та Л. Мегале звертають увагу на складність використання ШІ у правотворчості й правозастосуванні: алгоритмічні інструменти можуть підвищувати ефективність державних інституцій, але одночасно створювати ризики непрозорого впливу на рішення, які мають юридичні наслідки для громадян [2, p. 1082-1097]. Отже, питання полягає не лише в тому, чи є алгоритм технічно надійним, а й у тому, чи може особа зрозуміти логіку рішення, оскаржити його та отримати ефективний правовий захист.