ПРАВОВА ПОЛІТИКА УКРАЇНИ В ПРАЦЯХ МОЛОДИХ ДОСІДНИКІВ

Абрамович Д.М., здобувач
Науковий керівник:Кучменко В.О.,
доктор наук з державного управління, кандидат економічних наук, доцент,
Державний університет «Житомирська політехніка»

ПРАВОВА ПОЛІТИКА УКРАЇНИ У СФЕРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ: ВІДПОВІДЬ НА ГІБРИДНІ ЗАГРОЗИ

Актуальність теми зумовлена необхідністю системного оновлення та зміцнення нормативно-правової бази України в умовах триваючої повномасштабної війни та багаторівневої гібридної агресії РФ, що поєднує воєнні дії, кібератаки, інформаційно-психологічні операції та економічний тиск. Формування ефективної правової політики у сфері національної безпеки є критично важливим для забезпечення стійкості державних інститутів, захисту об'єктів критичної інфраструктури, адаптації законодавства до стандартів НАТО та ЄС. Оскільки об'єктом атаки стає не лише суверенна територія, а й інформаційний простір та суспільна свідомість, формування цілісної правової політики у сфері національної безпеки є першочерговим завданням для забезпечення стійкості Української держави.

Теоретико-правові засади протидії гібридним викликам активно розробляються українськими науковцями. Стратегічні аспекти безпеки держави закладено у працях В. Горбуліна. Правову природу та міжнародні виміри гібридної війни досліджують І. Сопілко та Т. Рева, а питання інформаційного суверенітету й кіберзахисту – О. Алексеєва та О. Шевчук. Правові механізми балансу між державним контролем та захистом прав людини аналізує О. С. Горай. Проте динамічність гібридних загроз потребує постійного оновлення законодавчої бази.

Метою є комплексний аналіз чинного законодавства та стратегічних документів України у сфері національної безпеки щодо їхньої ефективності у протидії гібридним загрозам, з урахуванням сучасних правових доктрин.

Аналіз безпекової політики свідчить, що ще до початку відкритого гібридного конфлікту дослідники вказували на недостатній потенціал України у відбитті інформаційних атак. Головною причиною цього була відсутність цілісної та уніфікованої системи правового регулювання суспільних відносин в інформаційній сфері. Серед головних загроз називали дезінформацію в інтернеті, блокування чи перекручування новин, інформаційний тиск з боку інших країн та слабкий розвиток власної технічної інфраструктури.

Сьогодні, в умовах інтенсивних бойових дій, ці виклики значно загострилися, оскільки методи деструктивного впливу постійно вдосконалюються. Складність нормативного реагування посилюється тим, що сам феномен «гібридної війни» перебуває в процесі постійного наукового та юридичного переосмислення. Спираючись на дослідження Т. Андрієвського, гібридну війну слід інтерпретувати як багатовекторний міждержавний конфлікт, де агресор поряд із прихованим або опосередкованим застосуванням збройних сил комплексно використовує невійськові (політичні, економічні, інформаційні) заходи, диверсійні та підривні технології. Метою такого впливу є позбавлення держави-жертви фактичного суверенітету та створення штучних центрів маніпулювання її внутрішньою і зовнішньою політикою [2, с. 273].

Правовий фундамент безпекового сектору становить Закон України «Про національну безпеку України». Цей закон виступає основою для розгалуженої системи документів довгострокового планування. І. Бондар пропонує розділяти інформаційну безпеку на чотири рівні: особисту, суспільну, комерційну та державну. Найголовніша ідея тут у тому, що в центрі безпеки стоїть саме людина, а не комп'ютери [7, с. 137]. Інформаційна безпека – це стабільний стан, коли весь інформаційний простір захищений, а люди можуть безпечно діяти відповідно до своїх цінностей та потреб.

Однією з найважливіших складових правової відповіді на гібридні виклики є реалізація чинної Стратегії інформаційної безпеки. Нею визначено, що однією з головних стратегічних цілей держави є протидія дезінформації, іноземним інформаційним маніпуляціям та гібридним втручанням у наш інформаційний простір. Вказано, що досягнення цієї цілі можливе через побудову системи проактивних державних стратегічних комунікацій та підвищення медіаграмотності суспільства.

Паралельно розвивається сфера кібербезпеки. Закон України «Про основні засади забезпечення кібербезпеки України» заклав правові рамки захисту об'єктів критичної інфраструктури від кібератак, які часто виступають інструментом технічного компоненту гібридної агресії.

Реагуючи на подібні загрози, державні органи мають поєднувати превентивні безпекові заходи із захистом конституційного статусу особи. О. С. Горай зауважує, що утримання цієї межі є не компромісом, а прозорим юридичним механізмом. Він передбачає суворе дотримання пропорційності та підзвітності під час будь-якого вимушеного обмеження свобод. Нехтування цим балансом неминуче призводить до внутрішнього розколу та підриву легітимності владних структур [3, с 455].

Головним орієнтиром тут є Конституція України. Стаття 3 визначає людину, її життя і безпеку найвищою соціальною цінністю. Стаття 64 дозволяє тимчасово обмежувати деякі права під час воєнного стану, але чітко забороняє обмежувати базові права: на життя гідність, правову допомогу, презумпцію невинуватості – вони є абсолютно захищеними.

Велику роль відіграє Служба безпеки України, яка бореться з підривною діяльністю та інформаційними атаками ворога, але її робота чітко контролюється. Навіть під час слідства будь-яке обмеження свободи людини чи негласні обшуки можливі лише за дозволом суду. Такий підхід повністю відповідає європейським стандартам і практиці Європейського суду з прав людини. Важливим вектором правової політики залишається також адаптація українського законодавства до стандартів НАТО та нормативно-правової бази Європейського Союзу, що дозволяє посилювати спільну стійкість проти міжнародних гібридних мереж.

Отже, сучасна правова політика України у сфері національної безпеки будується як багаторівнева система захисту, проте її реальна ефективність на практиці безпосередньо залежить від прозорості безпекового сектору, належного судового й парламентського контролю та неухильного дотримання процесуальних гарантій. На основі аналізу нормативної бази визначено, що подальше вдосконалення вітчизняного законодавства має відбуватися шляхом системної реалізації вже закріплених у Стратегії інформаційної безпеки цілей із протидії дезінформації та ворожим інформаційним операціям. При цьому головним критерієм успішності правової політики залишається суворе збереження балансу між захисною функцією держави та захистом конституційного статусу особи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Алексеєва О. А. Правове забезпечення кібербезпеки об'єктів критичної інфраструктури. *Інформація і право*. 2023. № 4 (47). С. 168–176.

2. Воротинський В. В. Вплив гібридної війни на формування державного інформаційного суверенітету України. *Держава і право: збірник наукових праць. Серія: Політичні науки*. 2024. Вип. 95. С. 266–279. DOI: https://doi.org/10.33663/1563-3349-2024-95-266

3. Горай О. С. Баланс між безпекою та свободою: державний контроль і права людини в умовах гібридних загроз. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2026. Вип. 93, ч. 5. С. 452–461. DOI: https://doi.org/10.24144/2307-3322.2026.93.5.59

4. Про національну безпеку України : Закон України від 21 черв. 2018 р. № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19 (дата звернення: 09.10.2026).

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.