

КРИМІНАЛЬНЕ ПРАВО ТА КРИМІНОЛОГІЯ; КРИМІНАЛЬНО-ВИКОНАВЧЕ ПРАВО

УДК 343

DOI <https://doi.org/10.32782/TNU-2707-0581/2025.4/19>**Луценко Ю. В.**

Таврійський національний університет імені В.І. Вернадського

ПРОБЛЕМИ ПРОТИДІЇ ЗЛОЧИННОСТІ В СУЧАСНИХ УМОВАХ

У статті здійснена спроба висвітлити проблеми протидії злочинності в сучасних умовах. У ході дослідження звернута увага, що стрімкий розвиток суспільних правовідносин, демократизація державних інституцій неможлива без наступальної боротьби зі злочинністю у різних її проявах. Держава в особі компетентних органів визначає правила поведінки, що спрямовані на гарантування безпеки кожній особі, а також встановлення стану захищеності суспільства та держави від різного роду протиправних посягань на охоронювані законом інтереси. Наголошено, що порушення цих приписів може призвести до завдання неоправної шкоди ефективній діяльності держави у різних її сферах.

Сьогодні в умовах глобалізації суспільства організована злочинність, у тому числі транснаціональна є закономірним результатом розвитку злочинної діяльності в державі, її організованих сфер і являє собою найбільш високолатентну й небезпечну систему організованої злочинної діяльності.

Наголошено, що на відміну від традиційних видів злочинів, історія яких налічує століття, кіберзлочинність, так само як і кібершахрайство є явищем новітньої, цифрової доби. Сама природа мережі Інтернет сприяє вчиненню кіберзлочинів. Такі її властивості як глобальність, трансграничність, анонімність користувачів, їх широка аудиторія слугують кіберзлочинцям на всіх етапах вчинення шахрайських дій та інших суспільно небезпечних діянь, а також дозволяють ефективно уникати кримінального переслідування правоохоронними органами.

У ході дослідження звернута увага, що проблеми протидії злочинності залишаються однією з ключових у сфері забезпечення національної безпеки, правопорядку та стабільності суспільства і держави. Незважаючи на розвиток правової системи, реформи правоохоронних органів та впровадження новітніх технологій, злочинність продовжує еволюціонувати, пристосовуючись до нових реалій. Основні проблеми протидії злочинності в сучасному суспільстві умовно можна поділити на наступні групи: зростання кіберзлочинності, корупція та зловживання владою, недостатній рівень довіри до правоохоронних органів, проблеми законодавчого забезпечення, організована злочинність і транснаціональні загрози, низький рівень правової культури населення, недостатня координація між правоохоронними та іншими державними органами, вплив воєнного стану та соціальної нестабільності.

Ключові слова: корупція, злочин, злочинні угруповання, наркотики, незаконний обіг зброї, шахрайство, кіберзлочинність, цифрове середовище, криптовалюта, тероризм, транснаціональні загрози, війна, воєнний стан, злочини проти основ національної безпеки України, державна таємниця, диверсія, шпигунство, легалізація (відмивання) майна, одержаного злочинним шляхом, колабораціонізм, латентність, правоохоронні органи.

Постановка проблеми. Стрімкий розвиток суспільних правовідносин, демократизація державних інституцій неможлива без наступальної боротьби зі злочинністю у різних її проявах. Держава в особі компетентних органів визначає правила поведінки,

що спрямовані на гарантування безпеки кожній особі, а також встановлення стану захищеності суспільства і держави від різного роду суспільно небезпечних посягань на охоронювані законом інтереси. Порушення цих вимог може призвести

до завдання непоправної шкоди ефективній діяльності держави у різних її сферах суспільних відносин [8, с. 5–19; 11, с. 75; 16, с. 364; 18, с. 389; 24, с. 364–365].

Історія людської цивілізації свідчить, що будь-який розвиток та прогрес, який приносив суспільству нові цивілізаційні блага та можливості, завжди супроводжувався негативними явищами. Сучасна масова цифровізація та стрімкий розвиток комп'ютерних технологій, які значно спростили життя людині, не стали винятком [10, с. 80–82; 15, с. 59].

Сьогодні в умовах глобалізації транснаціональна організована злочинність є закономірним результатом розвитку злочинної діяльності в державі, її організованих сфер і являє на даний час найбільш високолатентну і небезпечну систему організованої злочинної діяльності [9, с. 132].

Аналіз останніх досліджень і публікацій. Серед вчених, які досліджували проблеми протидії злочинності в сучасних умовах можна відмітити роботи В. В. Арешонкова [12], А. А. Вознюка [30], М. М. Денисенка [13; 22], А. В. Діміч [28], Н. К. Макаренко [14], О. Б. Полторацького [16], А. В. Тарасюка [18; 19; 20; 21; 29; 31], С. О. Харитонова [27] та інших науковців.

Метою статті є дослідження актуальних проблем протидії злочинності в сучасних умовах.

Виклад основного матеріалу. Майже усі фахівці з кібербезпеки визнають, що кіберзлочини сьогодні є одними з динамічніших груп суспільно небезпечних діянь, які завдяки технологіям є відносно безпечними для діяльності різноманітних злочинних угруповань та відкривають нові «горизонти». Наразі нікого не дивує існування Інтернет-мереж, за допомогою яких злочинці фактично створили чорний ринок для збуту наркотиків, зброї, крадених речей та вчинення інших шахрайських дій [3].

Останнім часом, у зв'язку із ситуацією, яка склалася з коронавірусною хворобою у минулих роках, подальшою швидкою діджиталізацією бізнесу, вторгненням РФ в Україну, буде посилюватися й кримінальний тренд – кіберзлочинність та шахрайство [12, с. 79–84].

На відміну від традиційних видів суспільно небезпечних діянь, історія яких налічує століття, кіберзлочинність, так само як і кібершахрайство, є явищем новітньої, цифрової доби. Сама природа мережі Інтернет сприяє вчиненню кіберзлочинів. Такі її властивості як глобальність, трансграничність, анонімність користувачів, їх широка аудиторія слугують кіберзлочинцям на

всіх етапах вчинення шахрайських дій та інших злочинів, а також дозволяють ефективно уникати кримінального переслідування правоохоронними органами.

Сьогодні в науці відсутній єдиний підхід щодо поняття «кіберзлочинність». Так, наприклад В. М. Болгов вважає, що кіберзлочини – це сукупність передбачених чинним законодавством кримінально караних, суспільно небезпечних діянь (дій чи бездіяльності), що посягають на право захисту від несанкціонованого поширення та використання інформації, негативних наслідків впливу інформації чи функціонування інформаційних технологій, а також інші суспільно небезпечні діяння, пов'язані з порушенням права власності на інформацію та інформаційні технології, права власників або користувачів інформаційних технологій вчасно одержувати або поширювати достовірну й повну інформацію [2, с. 132].

На думку Б. М. Головкина, кіберзлочинність являє собою сукупність суспільно небезпечних діянь, що вчиняються у віртуальному просторі за допомогою комп'ютерних систем або через використання комп'ютерних мереж та інших засобів доступу до віртуального простору, в межах комп'ютерних мереж, а також проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних [4, с. 34].

Можна з повною відповідальністю стверджувати, що кіберзлочинність – це будь-яка злочинна діяльність, яку здійснюють у цифровому просторі. Часто ми уявляємо кіберзлочинність як «хакерство», що в цьому контексті означає несанкціоноване проникнення у цифрове середовище, але ж у цифровому всесвіті існує багато інших типів злочинів, в тому числі фізичних.

До категорії «кіберзлочинів» відноситься багато речей – від торгівлі дитячою порнографією, криптовалютою або незаконного зняття коштів з рахунку клієнта за допомогою інсайдера в банку до крадіжки вихідного коду. Успішно вчинений кіберзлочин часто виявляє порушення права на конфіденційність. Наприклад, коли компанія неналежним чином зашифрувала особисті дані, і їх було викрадено, це є порушенням правил конфіденційності користувачів з боку компанії та водночас кіберзлочин з боку тих, хто викрав дані [7].

Попри відсутність у науці єдиного підходу щодо розуміння кіберзлочинності, зазначимо, що це явище властиве всім країнам, які в силу свого наукового прогресу вступили у період широкої цифровізації своєї діяльності. Про це свідчить при-

йняття у листопаді 2001 року країнами ЄС Конвенції Ради Європи про кіберзлочинність, в якій виділяються наступні групи кіберзлочинів:

- 1) злочини проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему);
- 2) злочини, пов'язані з використанням комп'ютера як засобу вчинення злочинів, а саме – для маніпуляцій з інформацією (комп'ютерне шахрайство та комп'ютерні підроблення);
- 3) злочини, пов'язані з контентом (змістом даних);
- 4) злочини, пов'язані з електронною торгівлею;
- 5) злочини, пов'язані з порушенням авторського права і суміжних прав;
- 6) акти расизму та ксенофобії, вчинені за допомогою комп'ютерних мереж [26].

Виходячи з вищенаведеного, виокремлюють такі ознаки кіберзлочинності: неправомірне використання комп'ютерних технологій та віртуального простору (перш за все електронна торгівля); транскордонність; зміна кількісних та якісних показників кіберзлочинності, зокрема різке підвищення кримінального професіоналізму та високої мобільності злочинців; інтелектуальний характер та активна динаміка використання розвитку і поширення високих технологій; рівень кіберзлочинності тісно пов'язаний з економічним рівнем розвитку суспільства в різних державах та регіонах; кібернетичні загрози швидкозмінні та високотехнологічні; високий рівень латентності; залежність географії поширення від фактору урбанізації; активними учасниками (співучасниками) кіберзлочинів є різного роду шахраї, збирники, рекетири, терористи, сутенери, педофіли, торговці людьми, зброєю, наркотиками; наявність стійкої тенденції до організованості, груповий характер вчинення кіберзлочинів [6, с. 173–175].

На теперішній час можна виділити чотири етапи в розвитку кіберзлочинності:

- *перший етап* – поява кіберзлочинності та субкультури хакерів;
- *другий етап* – розповсюдження кіберзлочинності, поява спеціалізацій кіберзлочинності й національних груп хакерів;
- *третій етап* – набуття організованих форм й транснаціонального характеру у всіх сферах кіберзлочинності;
- *четвертий етап* – використання у військово-політичних цілях з метою дестабілізації ситуації в країні [5].

Кіберзлочинність має той самий набір ознак та характеристик, що й будь-яка професія. Відмінність лише в тому, що особа, яка володіє певними професійними навичками, при занятті легальною діяльністю використовує свої сили і знання для досягнення позитивної мети як для себе особисто, так і для суспільства й держави загалом. Кіберзлочинець, займаючись нелегальною, соціально шкідливою діяльністю, спрямовує зусилля для досягнення лише власної позитивної мети, яка є різко негативною для інших громадян, суспільства і держави.

Серед кіберзлочинців існує поділ злочинних ролей. Вони переважно дотримуються обраної спеціалізації, оскільки перехід до іншої сфери злочинності вимагає нових навичок та досвіду.

Так, різновидом шахрайства в банківській системі є кардінг – незаконні фінансові операції з використанням платіжної картки або її реквізитів, що не ініційовані або не підтверджені її держателем. Реквізити платіжних карт, як правило, беруть зі зламаних серверів Інтернет-магазинів, платіжних та розрахункових систем, а також з персональних комп'ютерів (безпосередньо чи через програми віддаленого доступу, так звані «трояни»).

У сфері електронної комерції та господарської діяльності, фішинг – виманювання у користувачів мережі Інтернет їх логінів та паролів до електронних гаманців, сервісів онлайн аукціонів, переказування або обміну валюти тощо. Шахраї найчастіше змушують користувачів самостійно розкрити конфіденційні дані – наприклад, посилаючи електронні листи із пропозиціями підтвердити реєстрацію облікового запису, що містять посилання на веб-сайт в Інтернеті, зовнішній вигляд якого повністю копіює дизайн відомих ресурсів.

Фішинг буває кількох видів: *СМС-фішинг*, коли потенційна жертва шахраїв отримує повідомлення про те, що її кредитну картку заблокував банк, а для розблокування необхідно надати реквізити, або ж про те, що власник картки отримав виграш, але потрібно заплатити за його доставку. Варіантів СМС-повідомлень безліч, тому потрібно бути особливо уважними, якщо ви отримуєте повідомлення; *Інтернет-фішинг*, коли шахраї створюють фішингові (підроблені) сторінки, які імітують офіційні сторінки банків, платіжних сервісів, Інтернет-магазинів, Інтернет-майданчиків тощо; *вішинг* – вид кіберзлочинів, у якому в повідомленнях міститься прохання зателефонувати на певний міський номер, а при розмові запитуються конфіденційні дані власника картки; *скімінг* – копіювання даних платіжної картки за допомогою

спеціального пристрою (скімера). Зазвичай відбувається під час здійснення карткових операцій із банкоматами. Для отримання даних злочинці використовують мінікамери або змінні клавіатури; *онлайн-шахрайство* – фальшиві Інтернет-аукціони, Інтернет-магазини, сайти й телекомунікаційні засоби зв'язку; *мальваре* – створення та поширення вірусів і шкідливого програмного забезпечення.

Серед комп'ютерних злочинів існують злочини і проти державної безпеки, серед яких необхідно виділити такі суспільно небезпечні діяння, як неправомірний доступ до державної таємниці на машинному носії та диверсію у сфері комп'ютерної інформації, комп'ютерне шпигунство [13, с. 72; 17, с. 32–33; 18, с. 389; 20, с. 140].

Як бачимо, кіберзлочинність спричиняє великі фінансові втрати, які складно прорахувати. Інвестор-мільярдер Воррен Баффет раніше стверджував, що він заохочує свій бізнес уникати ринку кіберстрахування, оскільки на ньому бракує даних для прогнозування можливих фінансових втрат. Цей важкопрогнозований ризик суттєво відрізняється від традиційних фінансових втрат від стихійних лих, таких як урагани чи повені, або від злочинної діяльності, як-от пограбування банків чи фізичних нападів. За даними таких джерел, як McAfee, Cybersecurity Ventures, інститут SANS та ФБР, збитки від кіберзлочинності уряду та бізнесу обчислюються трильйонами доларів.

Захист від кіберзлочинності швидко став одним із пріоритетів у питаннях безпеки. При цьому ця злочинна структура напрочуд схожа на корпоративний світ. Злочинні «стартапи» маленьких банд слабо пов'язані між собою спільною інтересами або географією, але вони процвітають, крадуть одне в одного знаряддя, співпрацюють та конкурують зі амбіціями та спритністю, гідними Кремнієвої долини. Великі гравці кримінального світу намагаються поєднати свої інтереси в Європі, Азії, Африці та США, наймаючи кримінальних рекрутерів, створюючи керівні центри, які поводяться як керівники звичайних відділів кадрів. Існують навіть сюрреалістичні служби підтримки клієнтів, де потерпілі можуть дізнатися, як створити біткойн-гаманець для оплати викупу.

Така незаконна діяльність часто бере початок або відбувається в так званому «даркнеті» – прихованому шарі Інтернету, зазвичай доступному лише через браузер Tor. У будь-який час там можна «податися» на роботу місцевим оператором мережі ботів-вимагачів, водієм Uber, який виконує фейкові

поїздки й так відмиває незаконно отримані гроші, або «грошовим мулом» – кур'єром, який за допомогою фальшивої картки спорожнить банкомат.

Наразі існує багато центрів, які моніторять і відстежують онлайн-атаки. Вони можуть дати корисні підказки з конкретних випадків. Найвідоміший такий центр знаходиться у США – Carnegie Mellon, де також базується американська Команда реагування на надзвичайні ситуації, пов'язані із комп'ютерами (CERT), яка відповідає за сповіщення про критичні вразливості. У Кембриджському університеті Великобританії також є Центр боротьби з кіберзлочинністю. Жертвами кіберзлочинності можуть бути не тільки люди, а й різноманітні установи, державні органи, групи, платформи соціальних мереж тощо [7].

Говорячи про причини та умови злочинності з врахуванням сучасних викликів та загроз необхідно звернути увагу, що під причинами злочинності в сучасній Україні розуміється система негативних соціально-психологічних явищ, пов'язаних із суперечностями суспільства і держави, що породжують злочинність.

Під умовами злочинності прийнято розуміти систему негативних економічних, організаційних, психологічних, соціальних, правових явищ, пов'язаних із суперечностями, які існують в суспільстві і державі, що створюють можливість формування причин і дії злочинності.

Причини й умови злочинності в основному зводяться до чотирьох підсистем – економічні причини й умови, причини та умови кримінальної агресивності, причини та умови кримінальної необережності і правові причини та умови [21, с. 321–322; 25].

Оцінюючи кримінальні вміння кіберзлочинця крізь призму відповідності його навичкам, а також складності виконуваних завдань, слід зазначити, що кіберзлочинність дозволяє максимально скоротити термін від задуму до злочинного результату, що також говорить про її суспільну небезпеку.

Система кримінальних умінь кіберзлочинців базується переважно на технічних знаннях. Крім цього система включає актуальні та специфічні знання, до яких належать уявлення про основи кримінального, кримінального процесуального та іншого законодавства, знання стратегії й тактики діяльності правоохоронних органів, психологічних та віктимологічних особливостей взагалі, систем безпеки, а також окремих категорій потерпілих та іншу необхідну інформацію [23, с. 262].

До актуальних для конкретної ситуації вмінь й навичок відносяться такі, які в даній конкретній ситуації дозволяють найбільш ефективно та

успішно вчинити кіберзлочини. Зокрема, основними характеристиками особи кіберзлочинця є оригінальність мислення й поведінки, обережність, уважність. Такі особи зосереджують увагу на розумінні, передбаченні та управлінні процесами. Це є основою їх компетенції й професійної майстерності. До того ж, вони відзначаються уважністю та пильністю, їхні дії витончені, зухвалі, хитрі, супроводжуються відмінним маскуванню [1].

Висновки. Як бачимо, проблеми протидії злочинності залишаються однією з ключових у сфері забезпечення національної безпеки, правопорядку та стабільності в суспільстві та державі. Незважаючи на розвиток правової системи, реформи правоохоронних органів та впровадження новітніх технологій, злочинність продовжує еволюціонувати, пристосовуючись до нових реалій. Основні проблеми протидії злочинності в сучасному суспільстві можна умовно поділити на кілька груп:

1. *Зростання кіберзлочинності.* Цифровізація економіки, перехід до онлайн-середовища створили сприятливі умови для зловмисників: поширення фішингу, шахрайств у Інтернет середовищі; використання криптовалют для легалізації доходів; недостатній рівень кібербезпеки державних і приватних структур; обмежені технічні та кадрові ресурси у правоохоронців для боротьби з ІТ-злочинами.

2. *Корупція та зловживання владою.* Корупція підриває ефективність боротьби зі злочинністю, особливо на етапах розслідування та судового розгляду: вибіркове правозастосування; «витік» службової інформації; тиск на слідство або суд; нерідко – умисне затягування справ.

3. *Недостатній рівень довіри до правоохоронних органів.* Суспільна недовіра спричиняє низький рівень співпраці громадян з правоохоронними органами: небажання свідчити або повідомляти про злочини; страх репресій або помсти; уявлення про неефективність правоохоронних органів.

4. *Проблеми законодавчого забезпечення.* Існує низка труднощів, пов'язаних з нормативною базою: застарілі положення кримінального та кримінального процесуального законодавства; колізії та прогалини в законах та підзаконних нормативно-правових актах; повільна адаптація законодавства до нових видів злочинів (наприклад, кіберзлочинів, торгівлі персональними даними тощо).

Як бачимо, ефективна протидія злочинності в сучасних умовах потребує комплексного підходу, який буде включати: реформу правоохоронної системи; удосконалення законодавчої бази; розвиток міжнародного співробітництва з країнами-партнерами; підвищення правосвідомості громадян; активне впровадження інновацій у сфері безпеки та ін.

Список літератури:

- Біленчук П., Малій М. Кіберсвіт у новому тисячолітті. Хто вони: кіберзлочинці, кібершахраї, кібертерористи? URL: <https://lexinform.com.ua/dumka-eksperta/kibersvit-u-novomu-tysyacholitti-hto-vony-kiberzlochyntsi-kibershahrayi-kiberterorysty/>.
- Болгов В., Гадіон Н., Гладун О. Організаційно-правове забезпечення протидії кримінальним правопорушенням, що вчиняються з використанням інформаційних технологій: науково-практичний посібник. Київ: Національна академія прокуратури України, 2015. 202 с.
- Газізова Ю. Кіберзлочинність в Україні. Ера цифрових технологій – ера нових злочинів. URL: https://uz.ligazakon.ua/ua/magazine_article/EA013606.
- Голіна В. В., Головкін Б. М. Кримінологія: Загальна та Особлива частини. Навчальний посібник. Харків: Право, 2014. 284 с.
- Дзюндзюк В. Б., Дзюндзюк Б. В. Поява і розвиток кіберзлочинності. *Державне будівництво*. 2013. № 1. URL: http://nbuv.gov.ua/UJRN/DeBu_2013_1_3
- Іванченко О. Ю. Кримінологічна характеристика кіберзлочинності, запобігання кіберзлочинності на національному рівні. *Актуальні проблеми вітчизняної юриспруденції*. 2016. № 3. С. 172–177.
- Кіберзлочинність. URL: <https://gijn.org.ua/resurs-ua/kiberzlochinnist/>.
- Луценко Ю. В. Звільнення від кримінальної відповідальності за злочини проти основ національної безпеки України: монографія. Харків. Право. 2015. 200 с.
- Луценко Ю. В. Національний та зарубіжний досвід боротьби з корупцією та організованою злочинністю: сучасний контекст. Вчені записки ТНУ імені В. І. Вернадського. Серія: юридичні науки. 2024. Том 35 (74). № 3. С. 132–139.
- Луценко Ю. В. Протидія злочинності в сучасних умовах. Соціально-правові студії. 2020. Випуск 1(7). С. 79–84.
- Луценко Ю. В. Протидія організованих злочинності: національний та іноземний досвід. *Вчені записки ТНУ імені В. І. Вернадського. Серія: юридичні науки*. 2024. Том 35 (74). № 2. С. 75–81.

12. Луценко Ю. В., Арешонков В. В. Вплив організованої злочинності на світову безпекову політику, що викликана пандемією COVID-19. *Наукові записки Інституту законодавства Верховної Ради України*, 2022. № 1. С. 78–86.
13. Луценко Ю. В., Денисенко М. М. Протидія злочинності в умовах воєнного стану: теоретико-правові проблеми. *Прикарпатський юридичний вісник*. 2022. Випуск 3(44). С. 70–75.
14. Луценко Ю. В., Макаренко Н. К. Виконання спеціального завдання з попередження чи розкриття кримінально протиправної діяльності організованої групи чи злочинної організації, що вчиняють шахрайські та корупційні правопорушення. *Юридичний науковий електронний журнал*. 2023. № 7. С. 364–368.
15. Луценко Ю. В., Макаренко Н. К. Кіберзлочинність у сфері електронної торгівлі як прояв кримінального професіоналізму. *Право.ua*. 2023. № 3. С. 59–65.
16. Луценко Ю. В., Полторацький О. Б. Протидія злочинності в контексті світової безпекової політики. *Юридичний науковий електронний журнал*. 2024. № 2. С. 215–217.
17. Луценко Ю. В., Тарасюк А. В. Агресія проти України: причини, наслідки та уроки гібридної війни. *Правове забезпечення оперативно-службової діяльності: актуальні проблеми та шляхи їх вирішення: матеріали наук.-практ. семінару (Харків, 26 трав. 2017 р.)*. Харків, 2017. С. 31–35.
18. Луценко Ю. В., Тарасюк А. В. Актуальні проблеми удосконалення окремих положень кримінального та кримінального процесуального законодавства України. *Юридичний науковий електронний журнал*. 2023. № 1. С. 388–391.
19. Луценко Ю. В., Тарасюк А. В. Запобігання нелегальній міграції: у пошуках оптимальної моделі. *Часопис Національного університету «Острозька академія»*. Серія «Право». 2022. № 1(24). С. 1–24.
20. Луценко Ю. В., Тарасюк А. В. Проблеми запобігання корупційним правопорушенням юридичних осіб у сфері економіки, безпеки та оборони. *Вчені записки ТНУ імені В. І. Вернадського. Серія: юридичні науки*. 2025. Том 36 (75) № 1. С. 139–147.
21. Луценко Ю. В., Тарасюк А. В., Денисенко М. М. Кібербезпека та інформаційна безпека: співвідношення понять. *Юридичний науковий електронний журнал*. 2022. № 8. С. 320–323.
22. Луценко Ю. В., Тарасюк А. В., Денисенко М. М. Правове регулювання кібербезпеки людини на міжнародному рівні: порівняльно-правове дослідження. *Наше право*. 2022. № 3. С. 34–40.
23. Макаренко Н. К. Запобігання професійній злочинності в Україні: монографія. Київ: Нац. акад. внутр. справ, 2021. 455 с.
24. Макаренко Н. К., Луценко Ю. В. Виконання спеціального завдання з попередження чи розкриття кримінально протиправної діяльності організованої групи чи злочинної організації, що вчиняють шахрайські та корупційні правопорушення. *Юридичний науковий електронний журнал*. 2023. № 7. С. 364–368.
25. Причини й умови злочинності в Україні. URL: http://lib-net.com/content/9264_Prichini_i_ymovi_zlochinnosti_v_Ykraini.html
26. Про ратифікацію Конвенції про кіберзлочинність : Закон України від 7 вересня 2005 року № 2824-IV / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/2824-15#Text>
27. Lutsenko Yu., Kharytonov S. Countering Organized Crime in the European Context. *Theory and practice of jurisprudence*. 2024. № 1 (25). P. 141–152.
28. Lutsenko Yu., Tarasiuk A., Kryzhna V., Motyl V., Dimich A. (2021). Legal aspects of civil-military cooperation in comparative context. *Amazonia Investiga*, № 10(48), P. 138–149.
29. Lutsenko Yu., Motyl V., Tarasiuk A., Areshonkov V., Diakin Ya., Kamensky D. Globalization of White-Collar Crime: Far and Beyond National Jurisdictions. *CUESTIONES POLÍTICAS*. 2023. № 76. P. 64–75.
30. Movchan R., Dudorov O., Vozniuk A., Areshonkov V., Lutsenko Y.. Combating commodity smuggling in Ukraine: in search of the optimal legislative model. *Amazonia Investiga*, 2021. № 10(47), P. 142–151.
31. Tarasiuk A., Prokofieva-Yanchylenko D., Lutsenko Y., Danylevskyi A., & Makarenko T. (2023). Corporate liability and white-collar crime: Comparative review: Responsabilidad de las empresas y delitos de cuello blanco: Revisión comparativa. *Cuestiones Políticas*, 41 (78), P. 523–540.

Lutsenko Yu. V. PROBLEMS OF COMBATING CRIME IN MODERN CONDITIONS

The article attempts to highlight the problems of combating crime in modern conditions. During the study, attention was drawn to the fact that the rapid development of social relations and the democratization of state institutions are impossible without an offensive fight against crime in its various manifestations. The state, represented by competent authorities, determines the rules of conduct aimed at guaranteeing the safety of each person, as well as establishing a state of protection of society and the state from various kinds of unlawful encroachments on interests protected by law.

It was emphasized that violation of these regulations could lead to irreparable harm to the effective functioning of the state in various spheres.

Today, in the context of globalization of society, organized crime, including transnational crime, is a natural result of the development of criminal activity in the state and its organized spheres and represents the most highly latent and dangerous system of organized criminal activity.

It is emphasized that unlike traditional types of crime, the history of which dates back centuries, cybercrime, as well as cyberfraud, is a phenomenon of the modern, digital age. The very nature of the Internet contributes to the commission of cybercrimes. Its properties such as globality, cross-border, anonymity of users, and their wide audience serve cybercriminals at all stages of committing fraudulent acts and other socially dangerous acts, and also allow them to effectively avoid criminal prosecution by law enforcement agencies.

The study noted that the problems of combating crime remain one of the key ones in ensuring national security, law and order, and the stability of society and the state. Despite the development of the legal system, reforms of law enforcement agencies, and the introduction of new technologies, crime continues to evolve, adapting to new realities. The main problems of combating crime in modern society can be conditionally divided into the following groups: growth of cybercrime, corruption and abuse of power, insufficient level of trust in law enforcement agencies, problems of legislative support, organized crime and transnational threats, low level of legal culture of the population, insufficient coordination between law enforcement and other state bodies, impact of martial law and social instability.

Key words: *corruption, crime, criminal groups, drugs, illegal arms trafficking, fraud, cybercrime, digital environment, cryptocurrency, terrorism, transnational threats, war, martial law, crimes against the foundations of national security of Ukraine, state secret, sabotage, espionage, legalization (laundering) of property obtained by criminal means, collaborationism, latency, law enforcement agencies.*

Дата надходження статті: 24.09.2025

Дата прийняття статті: 20.10.2025

Опубліковано: 15.12.2025