РЕЗОЛЮЦІЯ

за результатами проведення

ІІ Міжнародної науково-практичної конференції

«ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ПРОТИДІЇ ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ В УМОВАХ ЗБРОЙНОГО КОНФЛІКТУ»

16 жовтня 2025 року організовано та проведено Донецьким державним університетом внутрішніх справ ІІ Міжнародну науково-практичну конференцію «Інформаційне забезпечення протидії організованій злочинності в умовах збройного конфлікту».

Мета науково-практичної конференції – розгляд актуальних питань інформаційного забезпечення протидії організованій злочинності в умовах збройного конфлікту, зокрема: кримінологічний аналіз злочинної діяльності організованих груп; використання поліграфа у боротьбі з організованою злочинністю; кримінальна відповідальність за злочини організованих груп, що використовують інформаційні технології; OSINT і цифрові докази у протидії організованій злочинності; особливості кваліфікації злочинів у сфері інформаційної безпеки; інформаційне забезпечення діяльності спільних слідчих груп (JIT); протидія організованій злочинності (кримінально-процесуальний та криміналістичний аспект); інформаційні механізми впливу держави-агресора; цифрова трансформація криміналістики; стратегічний аналіз злочинної діяльності організованих злочинних груп; слідова картина правопорушень, пов’язаних з використанням віртуальних активів; тактика огляду місця події під час фіксації наслідків збройного конфлікту; судова прийнятність результатів поліграфа; застосування кримінального аналізу для виявлення схем нелегального обігу зброї.

На ІІ Міжнародну науково-практичну конференцію було надіслано близько 108 доповідей з різних регіонів України, а також з інших держав.

На пленарному засіданні виступили представники закладів освіти і наукових установ, правоохоронних органів: Міністерства внутрішніх справ України; Департаменту стратегічних розслідувань Національної поліції України; Консультативної місії Європейського Союзу в Україні; Кіровоградської обласної прокуратури; Головного управління Національної поліції в Харківській області; Громадської організації «Міжнародна Асоціація Поліграфологів»; Юридичного інституту Університету Портукаленсе (Порто, Португалія); Криворізької центральної окружної прокуратури; Донецької обласної прокуратури; Департаменту кіберполіції Національної поліції України; Управління стратегічних розслідувань в Кіровоградській області; Одеського державного університету внутрішніх справ; Харківського національного університету внутрішніх справ; Львівського державного університету внутрішніх справ; Дніпровського державного університету внутрішніх справ; Донецького державного університету внутрішніх справ тощо.

За результатами обговорення доповідей учасниками ІІ Міжнародної науково-практичної конференції було сформульовано такі пропозиції:

– інформаційний вимір злочинів проти громадської безпеки в Україні є не лише технічним аспектом, а новим соціально-правовим феноменом, який

змінює структуру злочинності. Використання інформаційних ресурсів робить такі злочини масовими, координованими та важковиявними, що вимагає комплексної реакції – від удосконалення законодавства до розвитку спеціалізованих підрозділів кібербезпеки та криміналістики;

– подальший розвиток системи протидії гібридним загрозам має охоплювати такі пріоритетні напрями, як: створення державної платформи збору та обробки даних про гібридні загрози з використанням технологій розподіленого реєстру, що забезпечить надійність та прозорість інформаційних процесів; розробка спеціалізованих алгоритмів штучного інтелекту, здатних виявляти складні патерни координованих гібридних операцій на ранніх стадіях їх підготовки; впровадження квантово-стійких технологій для захисту каналів обміну інформацією від потенційних загроз; створення дієвих механізмів державного контролю за використанням розширених аналітичних можливостей для запобігання зловживанням та захисту прав громадян;

– цифрова грамотність виконує багатогранну функцію: захищає особистість від кіберзагроз, зміцнює суспільну стійкість до інформаційних атак та забезпечує реалізацію державної стратегії у сфері інформаційної безпеки. Її розвиток має розглядатися як ефективний ресурс держави, нарівні з освітою, економікою та національною обороною. Цифрова грамотність є необхідною умовою стабільного розвитку інформаційного суспільства та ключовим фактором безпечного функціонування цифрового середовища. Вона захищає людину від деструктивних інформаційних впливів, сприяє розвитку освітніх і професійних можливостей, підвищує рівень громадянської відповідальності та зміцнює довіру до суспільних і державних інституцій. Для України, яка перебуває в умовах збройного конфлікту та масштабних інформаційних атак, цифрова грамотність населення стає стратегічним пріоритетом. Тому слід продовжувати розвиток державних та освітніх програм, спрямованих на підвищення цифрових компетентностей, бо від цього залежить не лише безпека кожного громадянина, а й стійкість держави загалом;

– кваліфікація злочинів у сфері інформаційної безпеки в умовах воєнного стану характеризується низкою особливостей. По-перше, підвищується суспільна небезпека таких злочинів, оскільки вони можуть безпосередньо впливати на обороноздатність держави. По-друге, розширюється коло норм, за якими можуть кваліфікуватися діяння, включаючи норми про державну зраду, колабораційну діяльність, воєнні злочини. По-третє, ускладнюється процес доказування через транснаціональний характер кіберзлочинності та необхідність встановлення зв'язку з діяльністю держави-агресора. По-четверте, застосовуються спеціальні процесуальні механізми, передбачені законодавством про воєнний стан. Удосконалення правового регулювання є важливим завданням, яке потребує врахування як національного досвіду, так і міжнародних стандартів у цій сфері;

– формування державної інформаційної стратегії протидії жіночій організованій злочинності є нагальною потребою. Воєнний стан створив сприятливі умови для розвитку цього явища, яке набуло системного характеру. Жінки-злочинці використовують гендерні стереотипи та соціальні ролі для маскування злочинної діяльності. Ефективна протидія вимагає створення спеціалізованої аналітичної системи, проведення масштабних превентивних

кампаній, застосування гендерно-чутливих методів розслідування та активного міжнародного співробітництва. Удосконалення законодавства з урахуванням специфіки жіночих організованих груп, підготовка спеціалізованих кадрів правоохоронних органів, формування відповідної судової практики залишаються актуальними завданнями для правової системи України в умовах триваючої війни;

– незаконний обіг наркотиків у період збройної агресії має комплексний характер і підсилює інші загрози національній безпеці, включаючи тероризм, корупцію, соціальну дестабілізацію та руйнацію людського потенціалу країни. Протидія наркозлочинності у воєнний час повинна стати частиною загальної стратегії безпеки, яка поєднує правоохоронні, соціальні, медичні та інформаційні заходи. Системна та скоординована політика держави за підтримки міжнародної спільноти здатна мінімізувати загрози, пов'язані з незаконним обігом наркотиків в умовах збройного конфлікту;

– кримінальний аналіз у період збройної агресії виступає не лише допоміжним інструментом, а комплексним методологічним підходом, який поєднує сучасні інформаційні технології, методи обробки даних та правові механізми. Його застосування забезпечує підвищення ефективності протидії злочинності, формування науково обґрунтованих управлінських рішень та оптимізацію правозастосовної практики правоохоронних органів України в умовах сучасних загроз. Ефективність кримінального аналізу залежить від інтеграції новітніх технологій, таких як аналіз Big Data, штучний інтелект, та від професійної підготовки кадрів, здатних працювати з цими інструментами. Міжвідомча та міжнародна співпраця, а також постійне навчання фахівців є ключовими для забезпечення національної безпеки та стабільності. Адаптація кримінального аналізу до умов воєнного стану дозволяє не лише ефективно розслідувати та запобігати злочинам, а й формувати стратегічне розуміння криміногенної ситуації, що є основою для прийняття обґрунтованих управлінських рішень;

– оперативно-розшукова діяльність залишається важливим інструментом захисту національної безпеки, суспільства та прав громадян, особливо в умовах воєнного стану. Зміна безпекового середовища вимагає адаптації методів і засобів оперативно-розшукової діяльності до нових викликів, зокрема документування воєнних злочинів, роботи в умовах окупації та тісної взаємодії з міжнародними структурами. Для забезпечення законності, ефективності та дотримання прав людини під час проведення оперативних заходів необхідним є подальше вдосконалення нормативно-правової бази, розширення судового контролю та підвищення фахової підготовки працівників оперативних підрозділів;

– інформаційні технології відіграють визначальну роль у протидії організованій злочинності в умовах збройного конфлікту, надаючи правоохоронним органам ефективні інструменти для виявлення, моніторингу та нейтралізації злочинних мереж. Використання великих даних, аналізу соціальних зв'язків, геолокаційних даних, цифрової криміналістики та штучного інтелекту дозволяє виявляти ключових учасників злочинних структур, відстежувати їхні операції і прогнозувати ризики, що підвищує

оперативність і точність розслідувань. Паралельно інформаційні технології сприяють протидії кіберзлочинності та фінансуванню організованих груп, забезпечуючи захист критичної інфраструктури, контроль за фінансовими потоками і криптоактивами, а також підвищення кіберграмотності населення. Разом з тим ефективне застосування інформаційних технологій можливе лише за умови дотримання правових норм, прозорості алгоритмів, якісних даних та міжнародної співпраці. Таким чином, інтеграція інформаційних технологій у систему безпеки і правосуддя створює потужний потенціал для зниження злочинної активності, забезпечення стабільності та підвищення захищеності суспільства в умовах війни;

– поліграф у сучасній правозастосовній практиці України має допоміжний характер та використовується переважно як орієнтовне джерело інформації. Судова практика як на національному, так і на міжнародному рівнях підтверджує відсутність у його результатів самостійної доказової сили. Разом з тим, нормативне закріплення порядку застосування поліграфа та встановлення технічних стандартів свідчать про поступове інституціональне визнання його значення у сфері судових експертиз та оперативно-розшукової діяльності. Подальша інтеграція цього засобу у доказову систему потребує чіткого законодавчого врегулювання та уніфікації методичних підходів.

Організаційний комітет
ІІ Міжнародної науково-практичної конференції