ЗБІРНИК МАТЕРІАЛІВ

II МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ПРОТИДІЇ ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ В УМОВАХ ЗБРОЙНОГО КОНФЛІКТУ»

16 ЖОВТНЯ 2025 РОКУ

ДЕПАРТАМЕНТ СТРАТЕГІЧНИХ РОЗСЛІДУВАНЬ

CUESC

УДК 341.3:343.9

Інформаційне забезпечення протидії організованій злочинності в умовах збройного конфлікту: матеріали ІІ Міжнародної науково-практичної конференції (в авторській редакції), (м. Кропивницький, 16 жовтня 2025 року). Кропивницький, 2025. 456 с.

Затверджено до друку
Вченою радою Донецького державного університету внутрішніх справ
(протокол № 5 від 26 листопада 2025 року)

Публікується за матеріалами ІІ Міжнародної науково-практичної конференції «Інформаційне забезпечення протидії організованій злочинності в умовах збройного конфлікту», 16 жовтня 2025 року.

Збірник містить тези доповідей учасників ІІ Міжнародної науково-практичної конференції «Інформаційне забезпечення протидії організованій злочинності в умовах збройного конфлікту», яка відбулася 16 жовтня 2025 року на базі Донецького державного університету внутрішніх справ. Збірник розраховано на наукових та науково-педагогічних працівників закладів освіти й наукових установ, здобувачів вищої освіти юридичного і правоохоронного напрямів, а також на тих, хто цікавиться питаннями забезпечення протидії організованій злочинності в умовах збройного конфлікту; застосування кримінального, реалізації прав людини у діяльності правоохоронних органів.

Матеріали збірнику опубліковані в авторській редакції.

© ДонДУВС, 2025
© Автори тез доповідей, 2025

Зміст

Секція 1.

ФОРМУВАННЯ ДЕРЖАВНОЇ ПОЛІТИКИ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ПРОТИДІЇ ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ В УМОВАХ ЗБРОЙНОГО КОНФЛІКТУ.

ВОЛОБОЄВ Артур 17
МЕХАНІЗМИ ДЕРЖАВНОГО ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ БОРОТЬБИ З ОРГАНІЗОВАНОЮ ЗЛОЧИННІСТЮ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ

ВОЛОБОЄВА Злата, ГАБОРЕЦЬ Ольга 22
ЗНАЧЕННЯ ЦИФРОВОЇ ГРАМОТНОСТІ У ФОРМУВАННІ БЕЗПЕЧНОГО ІНФОРМАЦІЙНОГО СЕРЕДОВИЩА

ДРАГОНЕНКО Анна 25
ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ РЕСУРСІВ У СКЛАДІ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ ПРОТИ ГРОМАДСЬКОЇ БЕЗПЕКИ

ДРАНИЙ Валерій 29
ОСОБЛИВОСТІ КВАЛІФІКАЦІЇ ЗЛОЧИНІВ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ВОЄННОГО СТАНУ

ДУНЯШЕНКО Олександр, БЕРЕЗНЯК Василь 34
КВАЛІФІКАЦІЯ ХУЛІГАНСТВА В УМОВАХ ВОЄННОГО СТАНУ ТА ЗБРОЙНОГО КОНФЛІКТУ: ПРОБЛЕМИ ВІДМЕЖУВАННЯ ВІД СУМІЖНИХ ЗЛОЧИНІВ ТА ВИКЛИКИ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ РОЗСЛІДУВАННЯ

ЄГОРОВА Наталія 38
КОЛІЗІЇ НАЦІОНАЛЬНОГО ТА МІЖНАРОДНОГО ПРАВА

ЗАЧЕК Олег, РУДИЙ Тарас 44
ПРОБЛЕМНІ ПИТАННЯ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ КІБЕРБЕЗПЕКИ

КУЛИК Олександр 48
ІНФОРМАЦІЙНО-АНАЛІТИЧНА СИСТЕМА ДОСЛІДЖЕННЯ ТЕНДЕНЦІЙ ОРГАНІЗОВАНОЇ ЗЛОЧИННОСТІ В УКРАЇНІ

ЛИТВИНЕНКО Ольга 52
ДОКАЗУВАННЯ У КРИМІНАЛЬНИХ ПРАВОПОРУШЕННЯХ, ВЧИНЕНИХ ОРГАНІЗОВАНИМИ ГРУПАМИ

ПУГАЧ Світлана 56
ФОРМУВАННЯ ДЕРЖАВНОЇ ІНФОРМАЦІЙНОЇ СТРАТЕГІЇ У СФЕРІ ПРОТИДІЇ ЖІНОЧИМ ФОРМАМ ОРГАНІЗОВАНОЇ ЗЛОЧИННОСТІ ПІД ЧАС ВІЙНИ

САЙЧУК Дмитро, ГРІДІНА Наталія 61
ЗАБЕЗПЕЧЕННЯ ПРАВ І СВОБОД ГРОМАДЯН ПІД ЧАС РЕАЛІЗАЦІЇ ПОЛІЦЕЙСЬКИХ ПОВНОВАЖЕНЬ ЩОДО ПРОТИДІЇ ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ В УМОВАХ ЗБРОЙНОГО КОНФЛІКТУ

САМОЙЛЕНКО Олена 66
ПРОБЛЕМИ ПРОТИДІЇ ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ: АНАЛІТИЧНИЙ ОГЛЯД ТА ВИСНОВКИ

ТАТАРЕНКО Світлана, ВЕРГУН Дмитро 70
АКТУАЛЬНІ ПИТАННЯ ЩОДО НЕОБХІДНОСТІ ВНЕСЕННЯ ЗМІН ДО КРИМІНАЛЬНОГО ПРОЦЕСУАЛЬНОГО КОДЕКСУ УКРАЇНИ СТОСОВНО ПРОВЕДЕННЯ ОКРЕМИХ СЛІДЧИХ (РОЗШУКОВИХ) ДІЙ

ТОКАР Петро, КРІЦАК Іван 73
ІСТОРИКО-ЕТНО-КУЛЬТУРНІ ТА МІЖНАРОДНІ АСПЕКТИ ПРОБЛЕМИ ОРГАНІЗОВАНОЇ ЗЛОЧИННОСТІ: НА ПРИКЛАДІ ХАРКІВСЬКОГО РЕГІОНУ

ТУРЕНКО Олег 87
НЕВИЗНАЧЕНІСТЬ ПОНЯТТЯ «ПРИМУС ДО ПРАЦІ» В ЗАКОНОДАВСТВІ УКРАЇНИ – ПОШУК ІНФОРМАЦІЙНО-НАУКОВИХ ДЕФІНІЦІЙ

УДОД Андрій 91
ФОРМУВАННЯ СИСТЕМИ КРИМІНАЛЬНО-ПРАВОВОГО ЗАХИСТУ ОСІБ, ЯКІ ПОСТРАЖДАЛИ ВІД ЗБРОЙНОЇ АГРЕСІЇ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ

ФЕДОРЧАК Ірина, СНІЖКО Софія 96
ЗАКОНОДАВЧЕ РЕГУЛЮВАННЯ ДОСТУПУ ДО ІНФОРМАЦІЙНИХ РЕСУРСІВ У КОНТЕКСТІ ПРОТИДІЇ ЗЛОЧИННОСТІ

ФІГУРА Віталій 100
API/PNR, ЯК ОДНЕ З ТЕХНОЛОГІЧНИХ РІШЕНЬ У СИСТЕМІ ПРОТИДІЇ ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ

ШЛЯХОВИЙ Ярослав, ГРІДІНА Наталія 103
ЗАБЕЗПЕЧЕННЯ ПРАВ ЛЮДИНИ В АДМІНІСТРАТИВНІЙ ПРАКТИЦІ ПОЛІЦІЇ ПРИ ВПРОВАДЖЕННІ ІННОВАЦІЙНИХ ЗАСОБІВ КОНТРОЛЮ

ТА МОНІТОРИНГУ В УМОВАХ ВОЄННОГО СТАНУ

Секція 2.
РОЛЬ КРИМІНАЛЬНОГО АНАЛІЗУ У ПРОТИДІЇ ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ ПІД ЧАС ЗБРОЙНОГО КОНФЛІКТУ.

ГОРОЦЮК Юлія, МОВЧАН Анатолій 108
ВИКОРИСТАННЯ КРИМІНАЛЬНОГО АНАЛІЗУ ДЛЯ ВИЯВЛЕННЯ ТА ДОКУМЕНТУВАННЯ ОРГАНІЗОВАНИХ ЗЛОЧИННИХ УГРУПОВАНЬ

ГАШЕНКО Сергій, ГРІДІНА Анастасія 112
ВОГНЕВА ПІДГОТОВКА ТА ЇЇ ВПЛИВ НА ДІЯЛЬНІСТЬ ОРГАНІЗОВАНИХ ЗЛОЧИННИХ ГРУП У ЗОНІ КОНФЛІКТУ

ДЗЮБА Нікіта, ВАЛЄЄВ Руслан 117
АНАЛІЗ КРИМІНАЛЬНИХ ЗАГРОЗ: НЕЗАКОННИЙ ОБІГ НАРКОТИКІВ У ПЕРІОД ЗБРОЙНОЇ АГРЕСІЇ

ДРОБЕНКО Діна, СНІЖКО Софія 121
ЗАСТОСУВАННЯ КРИМІНАЛЬНОГО АНАЛІЗУ ДЛЯ ВИЯВЛЕННЯ СХЕМ НЕЛЕГАЛЬНОГО ОБІГУ ЗБРОЇ

КАРПЕНКО Артем, НАЗИМКО Єгор 125
СТРАТЕГІЧНИЙ АНАЛІЗ ЗЛОЧИННОЇДІЯЛЬНОСТІ ОРГАНІЗОВАНИХ ЗЛОЧИННИХ ГРУП ТА ЗЛОЧИННИХ УГРУПУВАНЬ, ЩО ВЧИНЯЮТЬ ЗЛОЧИНИ У СФЕРІ ОБІГУНАРКОТИЧНИХ ЗАСОБІВ

КОБИЛИНСЬКИЙ Дмитро, ВАЛЄЄВ Руслан 129
МІСЦЕ ТА РОЛЬ КРИМІНАЛЬНОГО АНАЛІЗУ У ПРОАКТИВНІЙ ПОЛІЦЕЙСЬКІЙ ДІЯЛЬНОСТІ

ЛУНГОЛ Ольга, ШЕВЧЕНКО Андрій 133
КРИМІНАЛЬНИЙ АНАЛІЗ ЯК ІНСТРУМЕНТ ВИЯВЛЕННЯ ОРГАНІЗОВАНИХ ЗЛОЧИННИХ УГРУПОВАНЬ В УМОВАХ ЗБРОЙНОГО КОНФЛІКТУ

МАКАРЕВИЧ Владислав, ГАБОРЕЦЬ Ольга 136
ЗАСТОСУВАННЯ КРИМІНАЛЬНОГО АНАЛІЗУ В ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ У ПЕРІОД ЗБРОЙНОЇ АГРЕСІЇ

МАКАРЕНКОВ Олексій 138
КРИМІНОЛОГІЧНИЙ АНАЛІЗ КОРЕКЦІЙ ПІДКУПІВ ЧИНОВНІКІВ ЗІ ЗЛОЧИНАМИ ПРОТИ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ПІД ЧАС ВІЙНИ ІЗ ЗОВНІШНІМИ АГРСОРОМ

МАРЖАН Єлизавета, ПЕКАРСЬКИЙ Сергій 143
КРИМІНАЛЬНИЙ АНАЛІЗ ЯК ІНСТРУМЕНТ ВИЯВЛЕННЯ ТА РОЗСЛІДУВАННЯ ВОЄННИХ ЗЛОЧИНІВ

СЛАВІНСЬКА Аліна, ГАБОРЕЦЬ Ольга 147
ЗАСТОСУВАННЯ КРИМІНАЛЬНОГО АНАЛІЗУ У БОРОТЬБІ З ОРГАНІЗОВАНОЮ ЗЛОЧИННІСТЮ В УМОВАХ ЗБРОЙНОГО КОНФЛІКТУ

СНІЖКО Софія, ДРОБЕНКО Діна 152
ЗАСТОСУВАННЯ КРИМІНАЛЬНОГО АНАЛІЗУ ДЛЯ ВИЯВЛЕННЯ СХЕМ НЕЛЕГАЛЬНОГО ОБІГУ ЗБРОЇ

ШЕВЦОВА Анастасія, МОВЧАН Анатолій 156
РОЛЬ КРИМІНАЛЬНОГО АНАЛІЗУ У ПРОТИДІЇ ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ ПІД ЧАС ЗБРОЙНОГО КОНФЛІКТУ

Секція 3.
РОЗВИТОК ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ОПЕРАТИВНО РОЗШУКОВОЇ ТА КРИМІНАЛЬНОЇ ПРОЦЕСУАЛЬНОЇ ДІЯЛЬНОСТІ В УМОВАХ ВОЄННОГО СТАНУ.

АНДРУХ Віталій 160
ЩОДО ОСКАРЖЕННЯ НЕДОТРИМАННЯ РОЗУМНИХ СТРОКІВ У ДОСУДОВОМУ КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

АФАНАСЬЄВА Валерія, ЯНКОВИЙ Микола 163
OSINT ЯК КРИМІНАЛІСТИЧНИЙ ІНСТРУМЕНТ ДОКУМЕНТУВАННЯ ВОЄННИХ ЗЛОЧИНІВ: ПЕРЕВАГИ ТА ОБМЕЖЕННЯ

БОЙЧУК Владислав, БЕЙКУН Андрій 166
ТЕНДЕНЦІЇ ПРАВОВОГО РЕГУЛЮВАННЯ КІБЕРПРОСТОРУ ЯК ФІЗИЧНОГО ПРОСТОРУ ТЕАТРУ ВОЄННИХ ДІЙ

БОНДАРЕНКО Артем, КВАШУК Олександр 172
ЗНАЧЕННЯ OSINT-ТЕХНОЛОГІЙ ДЛЯ КРИМІНАЛЬНОЇ ПРОЦЕСУАЛЬНОЇ ДІЯЛЬНОСТІ

ВИНОГРАДОВА Ксенія, ВАРАВА Володимир 175
СУЧАСНІ ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ ОПЕРАТИВНО-РОЗШУКОВОЇ ДІЯЛЬНОСТІ В УКРАЇНІ

ВІННІЧЕНКО Іуліанія, ПЕКАРСЬКИЙ Сергій 178
ОПЕРАТИВНО-РОЗШУКОВА ПРОТИДІЯ ПІДРОЗДІЛАМИ КРИМІНАЛЬНОЇ ПОЛІЦІЇ ВЧИНЕННЮ ТЕРОРИСТИЧНИХ АКТІВ

ГОЛОВКІН Сергій 181
ДЕЯКІ ОСОБЛИВОСТІ ПРОВЕДЕННЯ СЛІДЧИХ (РОЗШУКОВИХ) ДІЙ ПРИ РОЗСЛІДУВАННІ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, ВЧИНЕНИХ ОРГАНІЗОВАНИМИ ГРУПАМИ

ДЕРЕВ'ЯНЧЕНКО Юрій 185
ПІДСТАВИ РОЗШУКУ ОСІБ, ЗНИКЛИХ БЕЗВІСТИ ЗА ОСОБЛИВИХ ОБСТАВИН

ДОРОШЕНКО Ростислав, ПЕКАРСЬКИЙ Сергій 190
ОСОБЛИВОСТІ ПРОТИДІЇ ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ, ПОВ'ЯЗАНОЇ З ОБІГОМ НЕБЕЗПЕЧНИХ МАТЕРІАЛІВ

ЄМЕЛЬЯНОВ Роман 194
ЩОДО ПИТАННЯ УЧАСТІ ОПЕРАТИВНИХ ПРАЦІВНИКІВ ПІД ЧАС РОЗКРИТТЯ ТА РОЗСЛІДУВАННЯ ЗЛОЧИНІВ ВЧИНЕНИХ ОРГАНІЗОВАНИМИ ГРУПАМИ

КИРИЛЬЧУК Анна, ЄМЕЛЬЯНОВ Роман 199
ЗАГАЛЬНІ ЗАСАДИ ОПЕРАТИВНО-РОЗШУКОВОЇ ДІЯЛЬНОСТІ В УКРАЇНІ: СУТНІСТЬ ТА СУЧАСНІ ВИКЛИКИ

КОВАЛЬ Микита, ВАЛЄЄВ Руслан 203
НАПРЯМИ РОЗВИТКУ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ПОЛІЦЕЙСЬКОЇ ДІЯЛЬНОСТІ В УМОВАХ ВОЄННОГО ЧАСУ

КОВТУНЕНКО Станіслав, ПУГАЧ Вячеслав 208
OSINT ЯК ІНСТРУМЕНТ В РОЗСЛІДУВАННІ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ

КОНОНЕНКО Віктор, БЕЙКУН Андрій 212
ОРГАНІЗАЦІЙНО-ПРАВОВА ПРОБЛЕМАТИКА ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ У СИСТЕМАХ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ В УМОВАХ ПОВНОМАСШТАБНОЇ ЗБРОЙНОЇ АГРЕСІЇ

КОРЕНСЬКОЙ Сергій, ЛОСКУТОВ Тимур 217
ЩОДО ОКРЕМИХ НЕДОЛІКІВ ПРОВЕДЕННЯ ОГЛЯДУ МІСЦЯ ПОДІЇ ПІД ЧАС РОЗСЛІДУВАННЯ ДОРОЖНЬО-ТРАНСПОРТНИХ ПРИГОД

КОСЯЧЕНКО Євгеній, ВАЛЄЄВ Руслан 221
ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ЯК ІНСТРУМЕНТ ПРОТИДІЇ ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ В УМОВАХ ЗБРОЙНОГО КОНФЛІКТУ

КРАВЧУК Дмитро, ДРОБЕНКО Діна 225
ЩОДО ЄДИНОЇ СИСТЕМИ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ В МІНІСТЕРСТВІ ВНУТРІШНІХ СПРАВ (СЕД): РОЛЬ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ В КРИМІНАЛЬНОМУ ПРОЦЕСІ

КРИВИК Аліна 230
ДАКТИЛОСОКПІЧНИЙ ОБЛІК ЯК ОСНОВНЕ ДЖЕРЕЛО НАКОПИЧЕННЯ ТА ЗБЕРІГАННЯ ДАКТИЛОСКОПІЧНОЇ ІНФОРМАЦІЇ

ЛЕЖЕНКО Олександр, ГАШЕНКО Сергій 233
РОЗВИТОК ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ОПЕРАТИВНО-РОЗШУКОВОЇ ДІЯЛЬНОСТІВ УМОВАХ ВОЄННОГО СТАНУ

ЛЄЙКО Міхаіл 238
ВИДИ НЕГЛАСНИХ СЛІДЧИХ (РОЗШУКОВИХ) ДІЙ

ЛОСКУТОВ Тимур 241
ЩОДО НОРМАТИВНОГО ЗАБЕЗПЕЧЕННЯ ЗАСАДИ СПЕЦІАЛЬНОЇ ПРОПОРЦІЙНОСТІ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ В УМОВАХ ВОЄННОГО СТАНУ

НУРГАЛІЄВ Едуард, ЛУНГОЛ Ольга 244
ЗНЯТТЯ ІНФОРМАЦІЇ З ЕЛЕКТРОННИХ КОМУНІКАЦІЙНИХ МЕРЕЖ ЯК ВАЖЛИВИЙ ЗАСІБ ОПЕРАТИВНО-РОЗШУКОВОЇ ДІЯЛЬНОСТІ В УМОВАХ ВОЄННОГО СТАНУ

ОПАНАСЕНКО Олена, ХИТРОВСЬКИЙ Дмитро 248
КІБЕРТЕРОРИЗМ ТА КІБЕРЗЛОЧИНИ: ЗАГРОЗИ В УМОВАХ ВІЙНИ

ОШЕДША Ангеліна, ГЛИНСЬКА Наталія 251
ЧАСОВІ МЕЖІ НАКЛАДЕННЯ АРЕШТУ НА МАЙНО У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ: ПРОБЛЕМИ ПРАВОВОЇ РЕГЛАМЕНТАЦІЇ

ПАТРЕЛЮК Дмитро 254
ОКРЕМІ НАПРЯМИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ КРИМІНАЛЬНОГО ПЕРЕСЛІДУВАННЯ

ПЕРМЯКОВ Дмитро, БЕЙКУН Андрій 258
ТРАНСФОРМАЦІЯ РОЗУМІННЯ ПРАВОВИХ КАТЕГОРІЙ У СФЕРІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ У СУЧАСНИХ РЕАЛІЯХ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ

ПОНОМАРЕНКО Віктор 263
ВИКОРИСТАННЯ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ ФІКСАЦІЇ ТА ДОКАЗУВАННЯ ВОЄННИХ ЗЛОЧИНІВ

ПОТОЦЬКИЙ Мирослав 266
ОКРЕМІ ОСОБЛИВОСТІ КРИМІНАЛЬНОГО ПРОВАДЖЕННЯ В УМОВАХ ВОЄННОГО СТАНУ

ПРОЦЕНКО Олександра, ГРУЗДЬ Олександр 270
СИНЕРГІЯ КРИМІНАЛЬНОГО АНАЛІЗУ ТА МІЖНАРОДНОГО СПІВРОБІТНИЦТВА У ПРОТИДІЇ ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ ПІД ЧАС ВІЙНИ

РАЗУВАЄВА Альбіна, ГАШЕНКО Сергій 276
РОЗРОБКА ІНТЕРАКТИВНИХ НАВЧАЛЬНИХ ПЛАТФОРМ ДЛЯ ВОГНЕВОЇ ПІДГОТОВКИ З УРАХУВАННЯМ ОПЕРАТИВНОЇ ІНФОРМАЦІЇ

РОМАНОВ Віталій 281
ДОСТУП ДО ІНФОРМАЦІЇ МОБІЛЬНИХ АБОНЕНТІВ: ПРАВОВІ ПРОБЛЕМИ ТА ШЛЯХИ ВДОСКОНАЛЕННЯ

САГАЙДАК Мирослава 284
ОПЕРАТИВНО-РОЗШУКОВЕ ВИЯВЛЕННЯ ЗЛОЧИНІВ, ПОВ'ЯЗАНИХ З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ (DEEPFAKE, AI-ШАХРАЙСТВА)

СИНИЦІНА Юлія 288
ІНТЕГРАЦІЯ НАЦІОНАЛЬНИХ І МІЖНАРОДНИХ ІНФОРМАЦІЙНИХ СИСТЕМ У ПРОТИДІЇ ВОЄННИМ ЗЛОЧИНАМ ТА ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ

СНІЖКО Софія, ПЕКАРСЬКИЙ Сергій 294
OSINT ЯК ІНФОРМАЦІЙНИЙ ІНСТРУМЕНТ ПРИ ПРОВЕДЕННІ ОПЕРАТИВНО-РОЗШУКОВИХ ЗАХОДІВ

СУПРОНЮК Віктор, КОПИЛОВ Едуард 298
НЕСПРАВЖНІ ІМІТАЦІЙНІ ЗАСОБИ: ПОНЯТТЯ, ЗНАЧЕННЯ, НАПРЯМИ ВИКОРИСТАННЯ

ТКАЧУК Вікторія, ПОТОЦЬКИЙ Мирослав 302
ЩОДО ЕЛЕКТРОННИХ ДОКАЗІВ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

ТОКОЛОВ Олександр, ЛІСНІЧЕНКО Дмитро 306
ВИКОРИСТАННЯ ЕЛЕКТРОННИХ ДОКАЗІВ У ПРОЦЕСІ ДОСУДОВОГО РОЗСЛІДУВАННЯ

ЦИПА Сергій, КОВАЛЬОВА Ольга 310
ІНФОРМАЦІЙНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ПРАВ ПОТЕРПІЛОГО: ОСОБЛИВОСТІ ДОСТУПУ ДО ІНФОРМАЦІЇ НА СТАДІЇ ДОСУДОВОГО РОЗСЛІДУВАННЯ В УМОВАХ ВОЄННОГО СТАНУ

ШОПІНА Ірина 314
ІНФОРМАЦІЙНІ МЕХАНІЗМИ ВПЛИВУ ДЕРЖАВИ-АГРЕСОРА НА ДІТЕЙ ТА МОЛОДЬ В УМОВАХ ЗБРОЙНОГО КОНФЛІКТУ

Секція 4.
ІННОВАЦІЙНІ МЕТОДИ, КРИМІНАЛІСТИЧНІ МЕТОДИКИ ТА ЕКСПЕРТНІ ДОСЛІДЖЕННЯ, ЗОКРЕМА ІЗ ЗАСТОСУВАННЯМ ПОЛІГРАФА, У ПРОТИДІЇ ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ.

АФТАНАСІВ Валерія 318
КРИМІНАЛІСТИЧНЕ ЗАБЕЗПЕЧЕННЯ ЕКСГУМАЦІЇ ТА ІДЕНТИФІКАЦІЇ ТІЛ ДЛЯ РЕПАТРІАЦІЇ

БОНДАРЕНКО Артем, БОНДАРЧУК Руслан 323
СУДОВА ПРАКТИКА З ПИТАННЯ ДОПУСТИМОСТІ РЕЗУЛЬТАТІВ ЕКПЕРТНИХ ДОСЛІДЖЕНЬ ІЗ ЗАСТОСУВАННЯМ ПОЛІГРАФА

ВОЙЧИШЕНА Марина 328
КРИМІНАЛІСТИЧНІ АСПЕКТИ ПРОТИДІЇ ЗЛОЧИННОСТІ В УМОВАХ ЗБРОЙНОГО КОНФЛІКТУ

ГРУЗДЬ Олександр 331
ЦИФРОВА ТРАНСФОРМАЦІЯ КРИМІНАЛІСТИКИ: СУЧАСНІ ПІДХОДИ ДО ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ СЛІДЧОЇ ДІЯЛЬНОСТІ

ГРУЗДЬ Олександр, БЕРЕЗА Юлія 335
ЦИФРОВІ ДОКАЗИ : ПОНЯТТЯ ТА ЗНАЧЕННЯ. ВАЖЛИВІСТЬ ЇХ ВИВЧЕННЯ ДЛЯ КРИМІНАСЛІСТИКИ В УМОВАХ ВОЄННОГО СТАНУ

ДЕРЕВ'ЯНКО Крістіна 339
ВИКОРИСТАННЯ БПЛА ЯК ІНОВАЦІЙНОГО МЕТОДУ РОЗСЛІДУВАННЯ ВОЄННИХ ЗЛОЧИНІВ ТА РЕАГУВАННЯ НА НАДЗВИЧАЙНІ ПОДІЇ

ДРОБЕНКО Діна 343
ІННОВАЦІЙНІ МЕТОДИ ТА КРИМІНАЛІСТИЧНІ ОСОБЛИВОСТІ РОЗСЛІДУВАННЯ НЕЗАКОННОЇ ПОРУБКИ, ПЕРЕВЕЗЕННЯ, ЗБЕРІГАННЯ ЧИ ЗБУТУ ЛІСУ, ВЧИНЕНИХ В УМОВАХ НАДЗВИЧАЙНИХ ПРАВОВИХ РЕЖИМІВ

ДРОБЕНКО Діна, МУКОСІЙ Єва 347
ЕФЕКТИВНІСТЬ ЗАСТОСУВАННЯ ПОЛІГРАФА У РОЗСЛІДУВАННЯХ ОРГАНІЗОВАНОЇ ЗЛОЧИННОСТІ: МЕТОДОЛОГІЯ, ОБМЕЖЕННЯ ТА ПРАКТИЧНІ РЕЗУЛЬТАТИ

ЗАВГОРОДНІЙ Євген, СЕНИЧАК Ольга 351
ЕТИЧНІ ТА ПРАВОВІ МЕЖІ ЗАСТОСУВАННЯ ПОЛІГРАФА ПІД ЧАС ДОПИТІВ : ГАРАНТІЇ ПРАВ ЛЮДИНИ

КВАШУК Олександр 356
ПРОБЛЕМНІ ПИТАННЯ ДІЯЛЬНОСТІ ЛІТ ІЗ РОЗСЛІДУВАННЯ ЗЛОЧИНІВ ОРГАНІЗОВАНИХ ГРУП В УМОВАХ ЗБРОЙНОГО КОНФЛІКТУ

КОМІСАРЧУК Руслан 361
ОСОБЛИВОСТІ СТАНОВЛЕННЯ ЦИФРОВОЇ КРИМІНАЛІСТИКИ В УКРАЇНІ

КРИВДЮК Сергій, ГЛУЩЕНКО Владислав 367
ВИКОРИСТАННЯ ПОЛІГРАФА У БОРОТЬБІ З ОРГАНІЗОВАНОЮ ЗЛОЧИННІСТЮ

КРІПАК Роман, ГАШЕНКО Сергій 371
ІННОВАЦІЙНІ ЗАСОБИ КОНТРОЛЮ ЕФЕКТИВНОСТІ СТРІЛЕЦЬКОЇ ТА ВОГНЕВОЇ ПІДГОТОВКИ: ПРАВОВІ Й КРИМІНАЛІСТИЧНІ АСПЕКТИ

РЯДІНСЬКА Валерія 375
ЗАСОБИ НЕЙРО-ПСИХОФІЗІОЛОГІЧНОГО ДОСЛІДЖЕННЯ ПОВЕДІНКИ ЛЮДИНИ ТА ПЕРСПЕКТИВИ ЇХ ЗАСТОСУВАННЯ В ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

САЄНКО Владлен, ГРУЗДЬ Олександр 382
СЛІДОВА КАРТИНА ЯК ЕЛЕМЕНТ КРИМІНАЛІСТИЧНОЇ ХАРАКТЕРИСТИКИ ПРАВОПОРУШЕНЬ, ПОВ'ЯЗАНИХ З ВИКОРИСТАННЯМ ВІРТУАЛЬНИХ АКТИВІВ

ТРЕТЯК Софія, ДРОБЕНКО Діна 387
ПРАВОВЕ РЕГУЛЮВАННЯ ВИКОРИСТАННЯ ПОЛІГРАФА У КРИМІНАЛЬНОМУ СУДОЧИНСТВІ

ШЕВЧУК Віктор 391
ІННОВАЦІЙНІ КРИМІНАЛІСТИЧНІ ТЕХНОЛОГІЇ, ЗАСОБИ І МЕТОДИ ПРОТИДІЇ КОРУПЦІЇ В СУЧАСНИХ УМОВАХ ВІЙНИ

ЯГОЛЬНИК Олег 397
ІННОВАЦІЙНІ КРИМІНАЛІСТИЧНІ ТЕХНОЛОГІЇ У ПРОТИДІЇ ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ: СУЧАСНИЙ СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ

Секція 5.
НОВІ СТАНДАРТИ ПРОФЕСІЙНОЇ ПІДГОТОВКИ ФАХІВЦІВ ДЛЯ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ПРОТИДІЇ ЗЛОЧИННОСТІ В УМОВАХ КОНФЛІКТУ.

ВАЛЄЄВ Руслан 402
ІНТЕГРАЦІЯ INTELLIGENCE-LED POLICING ТА ПЕРЕДОВИХ ТЕХНОЛОГІЙ ЯК ОСНОВА СУЧАСНОЇ МОДЕЛІ ПРОТИДІЇ ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ

ВОЛОБОЄВ Артур, ГАБОРЕЦЬ Ольга 406
РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ ТА СИСТЕМ ОБРОБКИ ВЕЛИКИХ ДАНИХ ПІД ЧАС ВІЙНИ

КАРПЕНКО Олександр 411
ВІРТУАЛЬНА РЕАЛЬНІСТЬ І ЛАЗЕРНІ СИМУЛЯТОРИ ЯК СУЧАСНІ ЗАСОБИ ПІДГОТОВКИ ПОЛІЦЕЙСЬКИХ ДО ВОГНЕВОЇ ПІДГОТОВКИ

КОРОВКА Дар'я, ХИТРОВСЬКИЙ Дмитро 415
МІЖНАРОДНІ СТАНДАРТИ ПРАВ ЛЮДИНИ ТА ЇХ ІМПЛЕМЕНТАЦІЯ У ПРОФЕСІЙНУ ПІДГОТОВКУ ПОЛІЦЕЙСЬКИХ

КОРОЛЬ Михайло, ТАРАСЮК Оксана 419
ВИКОРИСТАННЯ БІОМЕТРИЧНИХ ДАНИХ У СИСТЕМІ ПРИКОРДОННОГО КОНТРОЛЮ ЯК ЗАСІБ БОРОТЬБИ З ОРГАНІЗОВАНОЮ ЗЛОЧИННІСТЮ СЕРЕД ІНОЗЕМЦІВ

КОРОЛЬОВ Андрій 423
ЩОДО ОСОБЛИВОСТЕЙ ВИКОРИСТАННЯ БЕЗПІЛОТНИХ АВІАЦІЙНИХ СИСТЕМ ПОЛІЦІЄЮ: ЗАКОРДОННИЙ ДОСВІД

ОДЕРІЙ Олексій ЛИТВИНЕНКО Ольга 428
ПРОТИДІЯ ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ В УМОВАХ ВІЙНИ (КРИМІНАЛЬНО-ПРОЦЕСУАЛЬНИЙ АСПЕКТ)

ТІТЕНКО Всеволод 431
НОВІ СТАНДАРТИ ПРОФЕСІЙНОЇ ПІДГОТОВКИ ФАХІВЦІВ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ ДЛЯ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ПРОТИДІЇ ЗЛОЧИННОСТІ В УМОВАХ КОНФЛІКТУ

ХИТРОВСЬКИЙ Дмитро 436
ІНФОРМАЦІЙНА БЕЗПЕКА ТА ЕТИЧНІ СТАНДАРТИ В СИСТЕМІ ПРОФЕСІЙНОЇ ПІДГОТОВКИ ПРАЦІВНИКІВ ОРГАНІВ ВНУТРІШНІХ

СПРАВ ПІД ЧАС ВОЄННОГО СТАНУ

ШУЛЬГА Андрій 440
КІБЕРБЕЗПЕКА В КРИМІНАЛЬНИХ ПРОВАДЖЕННЯХ: ПРОТИДІЯ ДЕЗІНФОРМАЦІЇ ТА ГІБРИДНИМ ЗАГРОЗАМ

Секція 6.

МІЖНАРОДНЕ СПІВРОБІТНИЦТВО ПІД ЧАС ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ПРОТИДІЇ ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ В УМОВАХ ЗБРОЙНОГО КОНФЛІКТУ.

БРЕДІХІНА Марія, ВОЛОБОЄВ Артур 445
МІЖНАРОДНО-ПРАВОВІ МЕХАНІЗМИ ПРОТИДІЇ ТРАНСНАЦІОНАЛЬНІЙ ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ СУСПІЛЬСТВА

ЗАВГОРОДНІЙ Євген, СЕНИЧАК Ольга 449
ЕТИЧНІ ТА ПРАВОВІ МЕЖІ ЗАСТОСУВАННЯ ПОЛІГРАФА ПІД ЧАС ДОПИТІВ : ГАРАНТІЇ ПРАВ ЛЮДИНИ

ЛИСЮК Артьом, ЛОГВИНЕНКО Євгенія 454
ДОСВІД НАТО ТА ЄС У КООРДИНАЦІЇ ІНФОРМАЦІЙНОЇ ВЗАЄМОДІЇ ЩОДО ПРОТИДІЇ ОРГАНІЗОВАНИМ ЗЛОЧИННИМ УГРУПОВАННЯМ У КРИЗОВИХ СИТУАЦІЯХ

ЛЕПІШ Наталія 457
АДМІНІСТРАТИВНО-ПРАВОВІ ЗАСАДИ МІЖНАРОДНОГО ІНФОРМАЦІЙНОГО ОБМІНУ У СФЕРІ ПРОТИДІЇ ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ ПІД ЧАС ЗБРОЙНОГО КОНФЛІКТУ

МОВЧАН Анатолій, ГОРОШКО Олександр 460
ПРОВЕДЕННЯ СПІЛЬНИХ МІЖДЕРЖАВНИХ ОПЕРАЦІЙ У ПРОТИДІЇ ТРАНСНАЦІОНАЛЬНІЙ ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ

НОВІКОВ Євгеній 464
ІННОВАЦІЙНІ АДМІНІСТРАТИВНО-ПРАВОВІ ПІДХОДИ ДО ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ ПІД ЧАС СПІВПРАЦІ З МІЖНАРОДНИМИ ПРАВООХОРОННИМИ СТРУКТУРАМИ

ОЛІЙНИК Іван 469
ПЕРЕШКОДА ТА ПЕРСПЕКТИВИ У МІЖНАРОДНОМУ ІНФОРМАЦІЙНОМУ СПІВРОБІТНИЦТВІ ДЛЯ ПРОТИДІЇ ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ В УМОВАХ ЗБРОЙНОГО КОНФЛІКТУ

ОНДА Вікторія, КУРТОВ Анатолій 473
МІЖНАРОДНИЙ ДОСВІД ІНФОРМАЦІЙНОЇ ПОЛІТИКИ ПРОТИДІЇ ОРГАНІЗОВАНЙ ЗЛОЧИННОСТІ ПІД ЧАС ЗБРОЙНОГО КОНФЛІКТУ АГРЕСІЇ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ ПРОТИ УКРАЇНИ

ПЕРЕДЕРІЙ Олександр, ЯРЕМА Дар'я 477
ПРОБЛЕМАТИКА ФУНКЦІОНУВАННЯ МІЖНАРОДНОГО КРИМІНАЛЬНОГО СУДУ

ФІВКІН Петро, ПАРХОМЕНКО Олександра 480
МІЖНАРОДНЕ СПІВРОБІТНИЦТВО ПІД ЧАС ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ПРОТИДІЇ ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ В УМОВАХ ЗБРОЙНОГО КОНФЛІКТУ

ФРОЛОВ Федір 484
КРИМІНАЛЬНА ВІДПОВІДАЛЬНІСТЬ ЗА ЗЛОЧИНИ ОРГАНІЗОВАНИХ ГРУП, ЩО ВИКОРИСТОВУЮТЬ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ДЛЯ ПІДРИВУ ОБОРОНОЗДАТНОСТІ УКРАЇНИ: МІЖНАРОДНО-ПРАВОВИЙ ВИМІР

ЧЕРНЕЦЬКА Ірина 488
КРИМІНАЛЬНО-ПРАВОВА ПРОТИДІЯ ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ У СФЕРІ НЕЗАКОННОГО ВИКОРИСТАННЯ ПРИРОДНИХ РЕСУРСІВ В УМОВАХ ЗБРОЙНОГО КОНФЛІКТУ: ОСОБЛИВОСТІ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ТА МІЖНАРОДНОГО СПІВРОБІТНИЦТВА

ЧЕРНИХ Вадим 492
МІЖНАРОДНИЙ ДОСВІД ЗАТРИМАННЯ УПОВНОВАЖЕНОЮ ОСОБОЮ ОСОБИ, ПІДОЗРЮВАНОЇ У ВЧИНЕННІ ЗЛОЧИНУ

СЕКЦІЯ 1.
ФОРМУВАННЯ ДЕРЖАВНОЇ ПОЛІТИКИ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ПРОТИДІЇ ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ В УМОВАХ ЗБРОЙНОГО КОНФЛІКТУ.

ВОЛОБОЄВ Артур
начальник відділу організації освітнього процесу
Донецького державного університету внутрішніх справ,
доктор філософії в галузі права

МЕХАНІЗМИ ДЕРЖАВНОГО ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ БОРОТЬБИ З ОРГАНІЗОВАНОЮ ЗЛОЧИННІСТЮ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ

Збройна агресія російської федерації кардинально змінила природу організованої злочинності в Україні. Якщо раніше вона становила переважно кримінальну проблему, то сьогодні перетворилася на потужний інструмент гібридної війни. Саме тому І. В. Басиста слушно зазначає, що повномасштабне вторгнення вимагає принципово нового підходу до розуміння цієї проблематики. Організована злочинність тепер має розглядатися через призму її інституціоналізованості та тісного зрощення з терористичною діяльністю, яка здійснюється на користь країни-агресора. Особливо небезпечним є її поширення у цифровому просторі, де фактично одночасно ведуться «активні бойові дії» [1, с. 202].

Сучасні гібридні загрози являють собою складне об’єднання усталених злочинних практик, доповнених новітніми формами деструктивного впливу. Організовані злочинні формування вміло поєднують класичні кримінальні схеми з інформаційно-психологічними операціями, масштабними

кібератаками та цілеспрямованою підривною діяльністю проти об'єктів критичної інфраструктури. Умови воєнного стану створили для них додаткові можливості. Наприклад, послаблення державного контролю в окремих сферах дозволило розширити зони впливу та активніше виконувати завдання, спрямовані на підрив обороноздатності України.

Проблема полягає в тому, що існуюча нормативно-правова база виявилася неготовою до таких викликів. Основний документ у цій сфері – Закон України «Про оперативно-розшукову діяльність» [2], розроблявся для протидії традиційній злочинності та не враховує специфіки боротьби з організованими угрупованнями, які фактично стали агентами іноземного впливу. Хоча Стратегія інформаційної безпеки України, затверджена Указом Президента від 28 грудня 2021 року № 685/2021, окреслює концептуальні засади захисту від гібридних загроз [3], проте між стратегічними цілями та реальними операційними можливостями правоохоронних органів утворився значний розрив. У зв’язку з цим, подолання порушеного питання потребує створення якісно нової інтегрованої системи інформаційного забезпечення.

Так, досвід перших місяців повномасштабної війни продемонстрував вразливість централізованих підходів до інформаційного забезпечення. Цілеспрямовані атаки агресора на ключові вузли системи свідчили про необхідність переходу до більш стійкої моделі. Оптимальним рішенням стала децентралізована система, яка об'єднує відомчі інформаційні платформи таким чином, що система зберігає працездатність навіть при виході з ладу окремих її елементів.

В основі нової системи є мережа аналітичних підрозділів, діяльність яких регламентується статтею 8 Закону України «Про оперативно-розшукову діяльність» [2]. При цьому кожен підрозділ має свою спеціалізацію, зосереджуючись на конкретних аспектах гібридних загроз. Така структура дозволяє ефективно аналізувати різнотипні дані, залишаючись у межах визначених законом повноважень.

Технологічною основою системи стали графові бази даних, які дають

змогу моделювати надзвичайно складні мережеві зв'язки між учасниками організованої злочинної діяльності. На відміну від облікових баз, вони здатні виявляти не лише звичні ієрархічні структури, але й приховані горизонтальні зв'язки з терористичними організаціями та кібергрупами, де технологія блокчейн забезпечує незмінність даних, ефективно протидіючи спробам дискредитації або фальсифікації доказової бази.

Усі процедури в системі стандартизовані відповідно до Постанови Кабінету Міністрів України № 373 від 29 березня 2006 року [4], однак з урахуванням особливостей функціонування в умовах воєнного стану, що вносить свої корективи в операційну діяльність.

Слід зауважити, що розроблена система захисту поєднує кілька рівнів безпеки. Квантово-стійкі алгоритми шифрування забезпечили захист даних від можливих загроз, а динамічна автентифікація та детальний рольовий контроль доступу створили додаткові бар'єри для зловмисників.

Крім того, доречно та своєчасно було створено для забезпечення надійності даних багаторівневу систему резервування з географічно розподіленими центрами обробки інформації. Така структура мінімізувала ризики втрати критично важливої інформації внаслідок фізичного знищення інфраструктури, так і через масштабні кібератаки.

У такому контексті, М. В. Калатур справедливо зазначає, що інформаційне забезпечення діяльності правоохоронних органів – це складна частина механізму організації діяльності, що в адміністративно-правовому плані передбачає одержання, збирання, реєстрацію, обробку, передачу, збереження та надання інформації шляхом створення інформаційних ресурсів, баз і систем, автоматизованих робочих місць із використанням новітніх методів і технологій [5, с. 62]. Цей механізм має забезпечувати максимальну оперативність без порушення фундаментальних правових принципів. Обробка персональних даних здійснюється виключно в інтересах національної безпеки, спираючись на положення частини 6 статті 6 Закону України «Про захист персональних даних» [6]. Автоматизовані засоби контролю мають

гарантувати дотримання принципів пропорційності та необхідності навіть при масштабному аналізі великих масивів інформації.

Вважаємо, що перспективні технологічні рішення вже активно впроваджуються у практичну діяльність. Зокрема, квантові обчислювальні системи змінили підхід до аналізу складних мереж злочинних організацій, оскільки дозволяють швидко опрацьовувати великі масиви взаємопов'язаної інформації. Водночас нейроморфні процесори нового покоління відкрили можливість обробки терабайтів даних у режимі реального часу, а технології доповненої та віртуальної реальності сформували нові інструменти для тривимірної візуалізації загроз і створення максимально наближених до необхідних умов підготовки аналітиків. Завдяки подальшій автоматизації операційної діяльності з'являється можливість спрямувати інтелектуальний потенціал правоохоронних органів на вирішення завдань стратегічного планування та ефективне реагування на непередбачувані ситуації.

Отже, проведене дослідження механізмів державного інформаційного забезпечення протидії організованій злочинності в умовах гібридних загроз виявило необхідність системної трансформації всієї правоохоронної діяльності. Гібридна війна кардинально змінила природу організованої злочинності, перетворивши її з кримінального явища на потужний інструмент державної агресії. Ця трансформація вимагає своєчасні відповіді через розробку принципово нових підходів до протидії.

На нашу думку, 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.

Список використаних джерел:

1. Басиста І. В. Організована злочинність: сучасні українські реалії та кроки до протидії. *Науково-інформаційний вісник Івано-Франківського університету імені Короля Данила Галицького.* Вип. 15 (27). Том 2. С. 202–217. DOI: 10.33098/2078-6670.2023.15.27.2.202-217.

2. Про оперативно-розшукову діяльність. Закон України від 18.02.1992 № 2135-XII. *Офіційний вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/2135-12#Text.

3. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки». Указ Президента України від 28.12.2021 № 685/2021. *Офіційний вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text.

4. Правила забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах. Постанова Кабінету Міністрів України від 29.03.2006 № 373. *Офіційний вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text.

5. Калатур М. В. До проблеми визначення поняття інформаційного забезпечення діяльності слідчих органів України. *Актуальні проблеми держави і права.* Вип. 87. С. 59–64.

6. Про захист персональних даних. Закон України від 01.06.2010 № 2297-VI. *Офіційний вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text.

ВОЛОБОЄВА Злата
студентка 1 курсу навчально-наукового інституту права та соціального менеджменту Донецького державного університету внутрішніх справ

Науковий керівник:
ГАБОРЕЦЬ Ольга
доцент кафедри оперативно-розшукової діяльності та інформаційної безпеки навчально-наукового інституту підготовки фахівців для підрозділів кримінальної поліції Донецького державного університету внутрішніх справ,
доктор філософії, доцент

ЗНАЧЕННЯ ЦИФРОВОЇ ГРАМОТНОСТІ У ФОРМУВАННІ БЕЗПЕЧНОГО ІНФОРМАЦІЙНОГО СЕРЕДОВИЩА

Сучасний світ перебуває у стані глобальної цифрової трансформації, коли інформаційні технології охоплюють майже всі сфери життя – від повсякденного спілкування до наукових досліджень і державного управління. Такі зміни відкривають перед суспільством нові можливості, але водночас загострюють проблеми, пов’язані із захистом інформації та протидією її деструктивному впливу. В умовах збройного конфлікту та гібридної війни питання інформаційної безпеки стають особливо актуальними, адже Україна щодня стикається з масованими інформаційними атаками, поширенням дезінформації та кібератаками.

У цьому контексті значної ваги набуває формування цифрової грамотності громадян, яка є базовою компетентністю XXI століття та ключовим інструментом безпеки особистості й держави в цифровому

просторі.

Цифрова грамотність визначається як здатність особи ефективно, безпечно та критично використовувати сучасні інформаційно-комунікаційні технології, а також розуміти принципи їх роботи та наслідки застосування. Вона поєднує у собі кілька взаємопов'язаних елементів, як-то:

– інформаційну грамотність – уміння знаходити інформацію, аналізувати джерела, перевіряти достовірність, уникати маніпуляцій;

– медіаграмотність – критично оцінювати контент, розрізняти факти і судження, виявляти пропаганду чи фейки;

– технічні навички – робота з комп'ютерами, мобільними пристроями, програмним забезпеченням та онлайн-ресурсами;

– кібергігієну – дотримання правил безпеки в мережі, захист персональних даних, протидію шахрайству й кібератакам.

Зауважимо, що недостатній рівень цифрової грамотності породжує серйозні загрози як для особистості, так і для суспільства. Людина, яка не вміє критично сприймати інформацію, стає вразливою до дезінформаційних кампаній, що особливо небезпечно в умовах гібридної війни. Відсутність базових навичок кібергігієни призводить до поширення вірусних атак, витоку персональних даних, фінансових втрат. Суспільство, значна частина якого не має належного рівня цифрових компетентностей, втрачає здатність ефективно реагувати на інформаційні загрози, що підриває національну безпеку держави.

Водночас розвинена цифрова грамотність відкриває нові перспективи. Насамперед вона сприяє формуванню у громадян відповідальну культуру споживання та поширення інформації, знижуючи ризики маніпуляцій і панічних настроїв. По-друге, вона сприяє ефективному використанню цифрових інструментів у навчанні, науці та професійній діяльності, що підвищує конкурентоспроможність країни на міжнародному рівні. По-третє, цифрова грамотність підсилює інформаційну безпеку, адже освічений користувач стає активним учасником у протидії кіберзлочинності й дезінформації.

З огляду не це, формування цифрової грамотності є не лише завданням окремої особистості, а й складовою державної політики. Україна вже зробила кроки у цьому напрямі, зокрема шляхом створення національної онлайн-платформи «Дія.Цифрова освіта», впровадження освітніх програм із цифрової та медіаграмотності у школах і закладах вищої освіти, а також щодо підтримки ініціатив громадських організацій, спрямованих на підвищення цифрових навичок різних груп населення. Умови війни лише підтвердили важливість таких кроків – цифрова грамотність стала не тільки інструментом самореалізації та професійного розвитку, а й необхідною передумовою виживання в інформаційній війні.

Таким чином, 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.

ДРАГОНЕНКО Анна
доцент кафедри кримінального права та кримінології
Донецький державний університет внутрішніх справ
кандидат юридичних наук, доцент

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ РЕСУРСІВ У СКЛАДІ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ ПРОТИ ГРОМАДСЬКОЇ БЕЗПЕКИ

Актуальність теми зумовлена стрімким зростанням ролі інформаційних технологій у механізмі вчинення кримінальних правопорушень, що посягають на громадську безпеку. Сучасні соціальні процеси характеризуються глибокою цифровізацією суспільного життя, внаслідок чого криміногенне середовище набуває нових форм існування – віртуальних, мережевих, децентралізованих.

Упродовж останнього десятиліття інформаційні ресурси (інтернет-платформи, соціальні мережі, месенджери, форуми, системи електронних платежів тощо) перестали бути лише середовищем комунікації – вони стали інструментом організації, координації та маскування злочинної діяльності. Особливо це проявилося після початку збройної агресії РФ проти України, коли інформаційний простір став ареною гібридного впливу: дезінформаційні кампанії, психологічні операції, вербування учасників злочинних угруповань та поширення паніки стали елементами кримінально небезпечних процесів.

Як зазначає В.Таційй, інформаційна глобалізація створює нову парадигму кримінально-правової охорони – «від фізичної безпеки до інформаційної» [1, с. 251]. О. Джужа вказує, що цифрові технології «перетворили злочинність на систему, здатну функціонувати у кіберпросторі незалежно від кордонів і територій» [2, с. 429]. Таким чином, з'являється потреба у новому погляді на поняття громадської безпеки – не лише як фізичної, а й як інформаційної стабільності

суспільства, де загрози мають цифрову природу.

Зростає роль інформаційних операцій як складових діяльності організованих злочинних угруповань. Якщо раніше такі структури діяли переважно в економічній, політичній чи силовій площині, то нині вони активно використовують інформаційні інструменти для досягнення своїх цілей: створення каналів впливу на громадську думку (бот-мережі, фейкові ЗМІ, соцмережеві кампанії); маніпулювання масовою свідомістю з метою підриву довіри до державних інститутів; інформаційне прикриття незаконних операцій (відмивання коштів, торгівля зброєю, вербування); використання криптовалют і даркнету для фінансування терористичної та кримінальної діяльності.

На думку В. Голіна, «інформаційна злочинність – це не окремий вид злочинності, а нова форма її існування, що інтегрує технологічні, організаційні та комунікаційні можливості сучасного світу» [3, с. 21]. Цей феномен охоплює не лише кіберзлочини у вузькому сенсі, а й будь-які правопорушення, у яких інформаційний ресурс виконує системну роль – від планування до реалізації.

Інформаційний вимір сучасної злочинності є одним із найдинамічніших і водночас найнебезпечніших аспектів суспільного розвитку. Він полягає у тому, що інформаційні ресурси, технології та комунікаційні платформи дедалі частіше стають не лише фоном, а й ключовим інструментом організації, координації та реалізації злочинних діянь, спрямованих проти громадської безпеки.

Під інформаційним виміром таких злочинів слід розуміти сукупність процесів, технологій і засобів, що забезпечують підготовку, планування, виконання або приховування злочинів за допомогою інформаційних систем, цифрових каналів комунікації та мережевих ресурсів.

За визначенням В. Тація, громадська безпека – це стан захищеності життєво важливих інтересів особи, суспільства й держави від протиправних посягань, що загрожують масовим порушенням публічного порядку чи спричиняють небезпеку для великої кількості осіб [1, с. 260]. У цьому контексті інформаційні ресурси набувають подвійної природи: вони можуть

бути як засобом забезпечення безпеки, так і каналом поширення загроз.

Сучасна практика свідчить, що інформаційна складова пронизує практично всі види кримінальних правопорушень проти громадської безпеки, передбачені розділом IX Особливої частини КК України, зокрема:

- Терористичні акти (ст. 258 КК) – використовуються цифрові платформи для поширення ідеології тероризму, координації дій, вербування учасників, а також публікації відео актів насильства для залякування населення.
- Диверсія (ст. 113 КК) – через інформаційні канали передаються відомості про стратегічні об’єкти, місця розташування ЗСУ, інфраструктуру тощо.
- Масові заворушення (ст. 294 КК) – ініціатори поширюють заклики до протиправних дій, організовують натовпи через соціальні мережі та месенджери.
- Незаконне поводження зі зброєю (ст. 263 КК) – інформаційні ресурси використовуються для обміну інструкціями з виготовлення чи модифікації зброї, організації «чорного ринку» озброєння.

Як зазначає О. Джужа, «інформаційний простір перетворився на головний канал кримінальної мобілізації», а злочинні групи використовують мережеву комунікацію для створення штучного інформаційного хаосу, що підриває громадську довіру та дестабілізує державні інститути [2, с. 470].

Інформаційний вимір злочинів проти громадської безпеки проявляється у таких формах:

1. Координаційна – використання інтернету для планування, розподілу ролей, формування груп учасників.

2. Пропагандистська – поширення радикальних ідей, дезінформації, фейкових новин, які спонукають до дій, що загрожують публічній безпеці.

3. Технічна – використання цифрових технологій для передачі інструкцій, створення шкідливого програмного забезпечення, кібератак.

4. Комунікативна – налагодження контактів між учасниками злочину

через закриті чати, зашифровані канали, VPN-мережі.

5. Психологічна – здійснення інформаційно-психологічного впливу з метою радикалізації, паніки або підриву авторитету органів влади.

В. Голіна підкреслює, що в умовах гібридної війни інформаційний простір стає «плацдармом для злочинних і терористичних маніпуляцій», а тому кримінальне право повинно враховувати специфіку цифрових ризиків при оцінці суспільної небезпеки [3, с. 23].

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.

Список використаних джерел:

1. Кримінальне право України: Загальна частина : підручник / В. Я. Тацій, В. І. Тютюгін, В. І. Борисов та ін. ; за ред. В. Я. Тація, В. І. Тютюгіна, В. І. Борисова. – 6-те вид., перероб. і допов. Харків : Право, 2020. 584 с.

2. Кримінологія: підручник / Джужа О.М., Василевич В.В., Чернєй В.В., Чернявський С.С. та ін.; за заг. ред. д-ра юрид. наук, проф. В.В. Чернєя; за наук. ред. д-ра юрид. наук, проф. О.М. Джужі. Київ: Нац. акад. внутр. справ, 2020. 612 с.

3. Голіна В. В. Застосування високих технологій у забезпеченні громадської безпеки / В. В. Голіна, С. С. Шрамко // *Використання технологій штучного інтелекту у протидії злочинності: матеріали наук.-практ. онлайн-семінару (м. Харків, 5 листоп. 2020 р.).* Харків: Право, 2020. С. 21-23

ДРАНИЙ Валерій
заступник начальника комунального підприємства по утриманню будинків Кіровоградської обласної ради

ОСОБЛИВОСТІ КВАЛІФІКАЦІЇ ЗЛОЧИНІВ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ВОЄННОГО СТАНУ

Введення воєнного стану в Україні 24 лютого 2022 року внаслідок збройної агресії Російської Федерації істотно змінило правові умови функціонування держави. Особливого значення в умовах гібридної війни набула сфера інформаційної безпеки, адже кіберпростір став одним з основних театрів бойових дій. Злочини у сфері інформаційної безпеки в умовах воєнного стану характеризуються підвищеною суспільною небезпекою, оскільки можуть безпосередньо впливати на обороноздатність держави, життя військовослужбовців і цивільного населення, функціонування критичної інфраструктури.

Правовою основою кваліфікації є Кримінальний кодекс України від 05.04.2001 № 2341-III, Закон України "Про правовий режим воєнного стану" від 12.05.2015 № 389-VIII та Закон України "Про основні засади забезпечення кібербезпеки України" від 05.10.2017 № 2163-VIII [1; 2; 3]. Воєнний стан являє собою особливий правовий режим, що вводиться у разі збройної агресії чи загрози нападу та передбачає тимчасове обмеження конституційних прав і свобод, а також надання відповідним органам спеціальних повноважень для забезпечення національної безпеки [2]. За таких умов окремі злочини у сфері інформаційної безпеки можуть кваліфікуватися за нормами про воєнні злочини або злочини проти основ національної безпеки, що передбачає суворіші санкції.

Основними складами злочинів у сфері інформаційної безпеки є

насамперед злочини, передбачені розділом XVI Особливої частини КК України. Стаття 361 передбачає відповідальність за несанкціоноване втручання в роботу комп'ютерних систем, автоматизованих систем, комп'ютерних мереж [1]. В умовах воєнного стану кібератаки на об'єкти критичної інфраструктури, військові системи управління можуть кваліфікуватися за частиною четвертою статті 361, яка встановлює покарання від п'яти до десяти років позбавлення волі. Стаття 361-1 криміналізує створення та розповсюдження шкідливих програмних засобів [1]. Якщо такі дії спрямовані на підрив обороноздатності або здійснюються за завданням іноземної держави, вони можуть додатково кваліфікуватися за статтею 111 КК України як державна зрада. Стаття 361-2 встановлює відповідальність за несанкціоновані збут або розповсюдження інформації з обмеженим доступом, що зберігається в електронних системах [1]. В умовах воєнного стану розголошення відомостей про дислокацію військових частин, плани операцій з використанням комп'ютерних систем може кваліфікуватися за сукупністю з статтею 328 (розголошення державної таємниці). Стаття 363-1 передбачає відповідальність за перешкоджання роботі комп'ютерних систем шляхом масового розповсюдження повідомлень [1]. DDoS-атаки на державні ресурси, системи управління військами можуть розглядатися як акти диверсії або саботажу.

Особливу увагу заслуговує кваліфікація за нормами про злочини проти основ національної безпеки, передбаченими розділом I Особливої частини КК України. Стаття 111 встановлює відповідальність за державну зраду, яка може виявлятися у наданні іноземній державі допомоги в проведенні підривної діяльності проти України [1]. Кібератаки на українські об'єкти, здійснені за завданням держави-агресора, мають кваліфікуватися за цією статтею з покаранням від дванадцяти до п'ятнадцяти років позбавлення волі з конфіскацією майна. Стаття 111-1 передбачає відповідальність за колабораційну діяльність, що може включати надання інформаційно-технічної підтримки збройним формуванням держави-агресора [1]. Стаття 114-1

криміналізує перешкоджання законній діяльності Збройних Сил України через кібератаки на системи управління, зв'язку або логістики [1]. Стаття 436-1 передбачає покарання за публічне заперечення або виправдання збройної агресії Російської Федерації проти України, що часто здійснюється через соціальні мережі [1].

Можливість застосування норм про воєнні злочини є важливою особливістю кваліфікації в умовах воєнного стану. Стаття 438 встановлює відповідальність за порушення законів та звичаїв війни, що може включати кібератаки на цивільні об'єкти або критичну інфраструктуру [1]. Відповідно до міжнародного гуманітарного права та Таллінського посібника 2.0 з міжнародного права щодо кібероперацііій, кібероперації під час збройного конфлікту повинні відповідати принципам розрізнення, пропорційності та застережності [5]. Кібератаки, які не розрізняють між військовими та цивільними об'єктами або завдають надмірних цивільних втрат, можуть кваліфікуватися як воєнні злочини.

При кваліфікації важливе значення має встановлення об'єктивної та суб'єктивної сторони злочину. Об'єктивна сторона характеризується діями у кіберпросторі, які спричиняють шкоду або створюють загрозу об'єктам кримінально-правової охорони. Необхідно встановити причинно-наслідковий зв'язок між діями особи та наслідками у вигляді порушення функціонування інформаційних систем, витоку конфіденційної інформації, завдання збитків або загрози національній безпеці. Суб'єктивна сторона характеризується умислом. В умовах воєнного стану особливого значення набуває встановлення спеціальної мети – наміру сприяти державі-агресору, підірвати обороноздатність або дестабілізувати суспільно-політичну ситуацію. Суб'єктом може бути як загальний суб'єкт – осудна особа, яка досягла шістнадцятирічного віку, так і спеціальний суб'єкт – особи з доступом до державної таємниці, працівники органів державної влади, військовослужбовці [1].

Важливою проблемою є розмежування суміжних складів злочинів.

Несанкціоноване втручання в роботу комп'ютерних систем (стаття 361) слід відмежовувати від диверсії (стаття 113), якщо дії спрямовані на знищення критичної інфраструктури з метою ослаблення держави. Розголошення державної таємниці (стаття 328) слід відмежовувати від державної зради (стаття 111) за ознакою наміру надати іноземній державі допомогу у проведенні підривної діяльності. Вчинення злочинів організованою групою або злочинною організацією в умовах воєнного стану може кваліфікуватися як терористична діяльність або участь у незаконних збройних формуваннях.

Процесуальні особливості розслідування пов'язані з необхідністю оперативного збору та фіксації цифрових доказів. Відповідно до Кримінального процесуального кодексу України, можуть проводитися огляд та обшук електронних систем, тимчасовий доступ до них, зняття інформації з телекомунікаційних мереж [4]. В умовах воєнного стану законодавством передбачені спрощені процедури отримання дозволів та розширені повноваження правоохоронних органів. Враховуючи підвищену суспільну небезпеку таких злочинів, суди схильні застосовувати найсуворіші запобіжні заходи, зокрема тримання під вартою. Закон про воєнний стан передбачає можливість тимчасовогообмеження конституційних прав, включаючи таємницю кореспонденції, що може застосовуватися під час розслідування [2].

Таким чином, 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.

Список використаних джерел:

1. Кримінальний кодекс України: Закон України від 05.04.2001 № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14.

2. Про правовий режим воєнного стану: Закон України від 12.05.2015 № 389-VIII. URL: https://zakon.rada.gov.ua/laws/show/389-19.

3. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19.

4. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17.

5. Schmitt M.N. (ed.). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press, 2017. URL: https://ccdcoe.org/research/tallinn-manual/.

ДУНЯШЕНКО Олександр
курсант 4-го курсу ФПФОДР НПУ Дніпровського державного університету внутрішніх справ

Науковий керівник: БЕРЕЗНЯК Василь
завідувач кафедри кримінального права та кримінології Дніпровського державного університету внутрішніх справ доктор юридичних наук, старший науковий співробітник

КВАЛІФІКАЦІЯ ХУЛІГАНСТВА В УМОВАХ ВОЄННОГО СТАНУ ТА ЗБРОЙНОГО КОНФЛІКТУ: ПРОБЛЕМИ ВІДМЕЖУВАННЯ ВІД СУМІЖНИХ ЗЛОЧИНІВ ТА ВИКЛИКИ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ РОЗСЛІДУВАННЯ

Сучасні реалії воєнного стану та збройного конфлікту в Україні створюють нові виклики для правоохоронної системи, зокрема у сфері кваліфікації кримінальних правопорушень. Одним із найскладніших завдань у цій площині залишається правильне визначення складу злочину при вчиненні хуліганських дій, які в умовах збройної агресії нерідко супроводжуються підвищеною суспільною небезпекою, використанням зброї, координацією через цифрові канали та мають організований характер. У таких умовах відмежування хуліганства від суміжних складів злочинів: терористичних актів, диверсій, бандитизму, масових заворушень, незаконного обігу зброї, набуває особливої ваги для забезпечення правової визначеності та справедливості правосуддя. Воєнний стан значно ускладнює роботу слідчих та прокурорів, адже інформаційне середовище стає фактором ризику: активне поширення дезінформації, спотворення або приховування доказів, використання

соціальних мереж для організації злочинних дій – усе це створює суттєві перешкоди у зборі доказової бази. Водночас підвищується небезпека масового поширення вогнепальної зброї, що призводить до більшої жорстокості та організованості хуліганських проявів. У цьому контексті дослідження кримінально-правових та процесуальних аспектів кваліфікації хуліганства в умовах війни є вкрай актуальним. Воно спрямоване на вироблення єдиних підходів до застосування норм Кримінального кодексу України, врахування воєнно-правових обмежень та визначення меж відповідальності за злочини проти громадського порядку, що мають ознаки терористичної або диверсійної діяльності.

Проаналізувати сучасні виклики кваліфікації хуліганства під час збройного конфлікту, окреслити проблеми відмежування його від суміжних злочинів та розглянути питання інформаційного забезпечення розслідувань, яке стає ключовим чинником ефективності кримінального переслідування у нових безпекових реаліях.

У сучасній кримінально-правовій та кримінологічній науці проблемі хуліганства присвячені праці, зокрема таких науковців, як: А. М. Бабенко, В. М. Бурдін, Б. М. Головкін, О. А. Івахненко, В. О. Калашнік, Г. І. Піщенко, М. О. Семенишин та інші.

Рівень хуліганства є достатньо високим та потребує ретельного вивчення причин та умов його вчинення. За родовим об’єктом злочинних посягань, хуліганство належить до кримінальних правопорушень проти громадського порядку (розділ XII КК України). Злочинів проти громадського порядку та моральності найбільше. Зазначений факт свідчить про необхідність розроблення ефективних заходів протидії цьому виду злочинів та посилення боротьби в даному напрямі. Найбільш поширеним видом хуліганства є дії, передбачені ч. 1 ст. 296 КК України, а також групове хуліганство (ч. 2 ст. 296 КК України) [3].

Хуліганство є найбільш поширеним серед кримінальних правопорушень, яке в частині 1 статті 296 КК України визначається

законодавцем як грубе порушення громадського порядку з мотивів явної неповаги до суспільства, що супроводжується особливою зухвалістю чи винятковим цинізмом Зміст наведеної норми статті 296 КК України свідчить про притаманність кримінальному правопорушенню, передбаченому цією статтею, декількох особливостей. По-перше, з урахуванням класифікації кримінальних правопорушень, закріпленої статтею 12 КК України, хуліганство за частиною 1 статті 296 цього Кодексу є кримінальним проступком, за частинами 2 і 3 вказаної статті – нетяжким злочином, а за частиною 4 статті зазначеної статті – тяжким злочином. По-друге, частина 1 статті 296 КК України містить низку оцінних понять «грубе порушення громадського порядку», «явна неповага до суспільства», «особлива зухвалість», «винятковий цинізм». Зазначені особливості впливають як на доктринальну характеристику хуліганства, так і на правозастосовну практику, що зумовлює потребу в їх науковій розробці [4].

Поняття «явна неповага до суспільства» є ключовим для кваліфікації злочину за ст. 296 Кримінального кодексу України (хуліганство) та полягає у відкритому, демонстративному нехтуванні загальновизнаними нормами поведінки, що супроводжується грубим порушенням громадського порядку. Оскільки суспільні відносини перебувають у стані підвищеної вразливості, а будь-які дії, що підривають громадську стабільність, можуть розцінюватися як такі, що створюють загрозу національній безпеці, це поняття набуває розширеного змісту. Основними критеріями визначення мотиву «явної неповаги до суспільства» у період воєнного стану є: демонстративність дій, що свідчить про виклик державі, військовим або іншим інституціям, які забезпечують оборону і порядок; зухвалість і особлива злісність, у тому числі з використанням зброї, вибухових речовин, під час комендантської години чи в умовах обмежень воєнного стану; мета дестабілізації, що виражається у провокуванні паніки, поширенні хаосу, приниженні органів державної влади, військових або правоохоронців. Таким чином, у воєнний період «явна неповага до суспільства» виходить за межі звичайних конфліктів побутового

характеру й охоплює дії, які прямо чи опосередковано підривають довіру до держави та здатні створити атмосферу страху серед населення.

В умовах збройного конфлікту та воєнного стану особливої складності набуває відмежування хуліганства від злочинів проти громадської безпеки, таких як терористичний акт (ст. 258 КК України), диверсія (ст. 113 КК України) та бандитизм (ст. 257 КК України). Ключові критерії відмежування: 1) мета злочину – хуліганство: основним мотивом є демонстрація зневаги до суспільства, бажання показати зухвалість або «силу», без цілі підриву державної безпеки; тероризм: має чітку політичну, ідеологічну або релігійну мету – залякування населення, вплив на органи влади, міжнародні організації; диверсія: спрямована на підрив обороноздатності, економічної або інформаційної безпеки держави; бандитизм: передбачає створення стійкої озброєної групи для систематичних нападів; 2) характер дій – хуліганські дії, навіть із використанням зброї, зазвичай носять одноразовий, спонтанний характер і не мають ознак організованої діяльності; терористичні акти, диверсія та бандитизм за своєю природою організовані, планові та спрямовані на досягнення стратегічних наслідків; 3) об’єкт посягання – хуліганство порушує громадський порядок та спокій; тероризм – національну безпеку та життя великої кількості осіб; диверсія – стратегічні об’єкти (транспорт, енергетика, зв’язок, військові склади); бандитизм – життя, майно та громадську безпеку через організовану злочинну діяльність; 4) доказова база – для хуліганства достатньо встановити факт грубого порушення громадського порядку та наявність мотиву явної неповаги, що супроводжується особливою зухвалістю чи винятковим цинізмом; для злочинів проти громадської безпеки обов’язковим є доведення умислу на досягнення конкретної антидержавної мети, участь у змові або організованій групі.

Результати проведеного дослідження дозволяють стверджувати, що в умовах воєнного стану для правильної кваліфікації діяння правоохоронці мають особливо ретельно встановлювати мотив, мету та організованість дій

правопорушників. Хуліганство, хоч і може супроводжуватися використанням зброї та створювати підвищену небезпеку, відрізняється від терористичних, диверсійних чи бандитських проявів відсутністю цілеспрямованого підриву державної безпеки та політичної мотивації. Чітке розмежування цих складів злочинів є запорукою обґрунтованої правової кваліфікації та справедливого правосуддя в умовах збройного конфлікту.

Список використаних джерел:

1. Булькевич А.В. Кримінально-правове значення хуліганського мотиву. АКАДЕМІЧНІ ВІЗІЇ. Випуск 31/2024. С. 1-12. URL: file:///C:/Users/%D0%9D%D0%B0%D1%82%D0%B0%D0%BB%D1%8C%D1%8F/Downloads/%D1%81%D1%82%D0%B0%D1%82%D1%82%D1%8F.pdf (дата звернення 15.09.2025).

2. Кримінальний кодекс України. Редакція від 17.07.2025, підстава - 4496-IX, 4499-IX. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення 15.09.2025).

3. Піщенко Г.І., Лисенко А.О. Кримінологічна характеристика хуліганства. Юридичний науковий електронний журнал. № 11/2024. С. 424-428. URL: http://lsej.org.ua/11_2024/100.pdf (дата звернення 15.09.2025).

4. Плохута Є.П. Суб'єктивні ознаки хуліганства: загальна характеристика. Juris Europensis Scientia. Випуск 1, 2024. С.145-148. URL: http://jes.nuoua.od.ua/archive/1_2024/28.pdf (дата звернення 15.09.2025).

ЄГОРОВА Наталія
Адвокат м. Київ

КОЛІЗІЇ НАЦІОНАЛЬНОГО ТА МІЖНАРОДНОГО ПРАВА

Співвідношення національного кримінального законодавства та міжнародного кримінального права є однією з найбільш складних проблем

сучасної кримінально-правової науки. Глобалізація злочинності, транснаціональний характер окремих суспільно небезпечних діянь, участь України у міжнародних договорах з питань боротьби зі злочинністю та виконання зобов'язань перед міжнародними судовими установами актуалізують питання колізій між нормами Кримінального кодексу України та міжнародно-правовими актами. Особливої гостроти ці питання набули в умовах збройної агресії Російської Федерації, коли Україна активно використовує механізми міжнародного кримінального права для притягнення до відповідальності за воєнні злочини, злочини проти людяності та геноцид.

Колізія в кримінальному праві являє собою розбіжність між нормами національного Кримінального кодексу та міжнародно-правовими актами щодо визначення складу злочину, меж кримінальної відповідальності, санкцій або процедури притягнення до відповідальності. Такі колізії можуть виникати на рівні криміналізації діянь, кваліфікації злочинів, визначення покарання та міжнародного співробітництва у кримінальних справах.

Основні види колізій у сфері кримінального права включають наступні категорії. По-перше, колізії щодо криміналізації діянь. Міжнародні конвенції зобов'язують держави криміналізувати певні діяння: тероризм, торгівлю людьми, наркотичні злочини, корупцію, легалізацію доходів, одержаних злочинним шляхом. Римський статут МКС визначає склади злочинів проти людяності, воєнних злочинів, геноциду, агресії [3]. Якщо такі діяння не передбачені КК України або передбачені з іншими ознаками, виникає колізія. Наприклад, стаття 6 Римського статуту визначає геноцид як діяння, вчинені з наміром знищити повністю або частково національну, етнічну, расову чи релігійну групу [3]. Стаття 442 КК України передбачає відповідальність за геноцид, але окремі ознаки складу злочину можуть тлумачитися по-різному [2].

По-друге, колізії щодо кваліфікації воєнних злочинів. Женевські конвенції та Додатковий протокол I встановлюють поняття "серйозних порушень" та інших порушень законів і звичаїв війни [5]. Стаття 438 КК

України встановлює відповідальність за порушення законів та звичаїв війни, стаття 438-1 – за піратство, стаття 438-2 – за найманство [2]. Проте конкретні склади злочинів у національному законодавстві можуть не повністю відповідати міжнародним стандартам. Наприклад, поняття "захищені особи", "військові об'єкти", "цивільні об'єкти" у міжнародному гуманітарному праві мають детальне тлумачення, яке не завжди знаходить відображення в КК України.

По-третє, колізії щодо імунітетів від кримінальної юрисдикції. Стаття 27 Римського статуту встановлює, що офіційна посада особи не звільняє її від кримінальної відповідальності за міжнародні злочини [3]. Водночас національне законодавство може передбачати імунітети для окремих категорій осіб. Стаття 3 КК України встановлює, що питання кримінальної відповідальності дипломатичних представників іноземних держав вирішуються згідно з нормами міжнародного права [2]. Це створює колізію, коли особа, що користується імунітетом за національним правом, має бути притягнута до відповідальності за нормами міжнародного права.

По-четверте, колізії щодо застосування принципів кримінального права. Принцип "nullum crimen sine lege" (немає злочину без вказівки про це в законі) є основоположним у кримінальному праві. Стаття 3 КК України встановлює, що злочинність діяння визначається тільки цим Кодексом [2]. Проте міжнародне звичаєве право визнає окремі діяння злочинними навіть без їх прямого закріплення в писаному праві. Це створює колізію при притягненні до відповідальності за злочини, які є такими за міжнародним звичаєвим правом, але не передбачені КК України.

Особливої уваги заслуговують колізії при застосуванні норм про злочини проти основ національної безпеки. Стаття 111 КК України встановлює відповідальність за державну зраду, стаття 111-1 – за колабораційну діяльність, стаття 113 – за диверсію, стаття 114 – за шпигунство [2]. Міжнародне право може кваліфікувати такі ж діяння як воєнні злочини або злочини проти людяності. Наприклад, діяльність осіб, які співпрацюють з

окупаційною владою, може кваліфікуватися як колабораційна діяльність за національним правом або як воєнний злочин за міжнародним правом залежно від конкретних обставин.

Колізії виникають також у сфері злочинів проти миру та безпеки людства. Розділ XX Особливої частини КК України містить статті про геноцид (стаття 442), планування, підготовку, розв'язування та ведення агресивної війни (стаття 437), порушення законів та звичаїв війни (стаття 438), застосування зброї масового знищення (стаття 439) [2]. Римський статут містить подібні норми, але з іншими ознаками складів злочинів. Стаття 8 Римського статуту детально перераховує воєнні злочини, включаючи діяння, які не всі передбачені в КК України: навмисне голодування цивільного населення, примусове призначення громадянина ворожої держави до участі у військових діях проти його країни, використання отрути або отруєної зброї [3].

Проблеми виникають при кваліфікації транснаціональних злочинів. Конвенція ООН проти транснаціональної організованої злочинності та протоколи до неї зобов'язують держави криміналізувати торгівлю людьми, незаконне переправлення мігрантів, торгівлю вогнепальною зброєю [7]. Стаття 149 КК України передбачає відповідальність за торгівлю людьми, але окремі форми експлуатації, передбачені Палермським протоколом, можуть тлумачитися по-різному [2]. Аналогічні проблеми виникають з кваліфікацією злочинів у сфері обігу наркотичних засобів (статті 305-320 КК України) відповідно до Конвенцій ООН 1961, 1971, 1988 років [2].

Способи вирішення колізій у кримінальному праві мають специфіку. Законодавча імплементація здійснюється шляхом внесення змін до КК України для приведення складів злочинів у відповідність з міжнародними зобов'язаннями. Після ратифікації Римського статуту МКС Україною були внесені зміни до Розділу XX КК України, які уточнили склади міжнародних злочинів. Судове тлумачення передбачає застосування судами міжнародно-правових актів при кваліфікації злочинів. Верховний Суд у своїх постановах роз'яснює порядок застосування міжнародних норм у кримінальних справах.

Пріоритет норм міжнародного кримінального права встановлюється через конституційні положення. Згідно зі статтею 9 Конституції, ратифіковані міжнародні договори є частиною законодавства [1]. Якщо міжнародним договором встановлено інші правила, ніж у КК України, застосовуються правила міжнародного договору. Проте це стосується лише процесуальних питань і не може змінювати принципу законності у кримінальному праві, згідно з яким злочинність діяння визначається лише КК України.

При кваліфікації злочинів важливе значення має врахування міжнародної судової практики. Рішення Міжнародного кримінального трибуналу по колишній Югославії, Міжнародного кримінального трибуналу по Руанді, Міжнародного кримінального суду формують прецедентне розуміння складів міжнародних злочинів. Національні суди можуть використовувати цю практику при тлумаченні відповідних статей КК України. Наприклад, поняття "широкомасштабного або систематичного нападу на цивільне населення" як ознака злочинів проти людяності отримало детальне тлумачення в практиці міжнародних трибуналів.

Колізії виникають також при застосуванні норм про обставини, що виключають злочинність діяння. Міжнародне кримінальне право передбачає, що виконання наказу начальника вищого рівня не звільняє від відповідальності за воєнні злочини та злочини проти людяності, якщо особа знала про явно незаконний характер наказу. Стаття 41 КК України передбачає, що виконання наказу або розпорядження виключає кримінальну відповідальність, якщо воно було законним [2]. При кваліфікації міжнародних злочинів повинні застосовуватися більш суворі міжнародні стандарти.

Таким чином, колізії національного та міжнародного кримінального права є складною багатоаспектною проблемою. По-перше, існують розбіжності в криміналізації діянь, складах злочинів та санкціях між КК України та міжнародними конвенціями. По-друге, особливої уваги потребують колізії при кваліфікації воєнних злочинів, злочинів проти людяності та геноциду в умовах збройної агресії. По-третє, проблематичним є

застосування принципу універсальної юрисдикції та співвідношення національної та міжнародної кримінальної юрисдикції. По-четверте, вирішення колізій здійснюється через законодавчу імплементацію міжнародних норм, судове тлумачення з урахуванням міжнародної практики та забезпечення ефективного міжнародного співробітництва. Удосконалення кримінального законодавства з метою повної відповідності міжнародним стандартам залишається актуальним завданням для України.

Список використаних джерел:

1. Конституція України: Закон України від 28.06.1996 № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80.

2. Кримінальний кодекс України: Закон України від 05.04.2001 № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14.

3. Римський статут Міжнародного кримінального суду від 17.07.1998. URL: https://zakon.rada.gov.ua/laws/show/995_588.

4. Європейська конвенція про видачу правопорушників від 13.12.1957. URL: https://zakon.rada.gov.ua/laws/show/995_033.

5. Женевські конвенції від 12 серпня 1949 року та Додаткові протоколи до них. URL: https://zakon.rada.gov.ua/laws/show/995_153.

6. Про міжнародні договори України: Закон України від 29.06.2004 № 1906-IV. URL: https://zakon.rada.gov.ua/laws/show/1906-15.

7. Конвенція ООН проти транснаціональної організованої злочинності від 15.11.2000. URL: https://zakon.rada.gov.ua/laws/show/995_789.

8. Конвенція ООН проти корупції від 31.10.2003. URL: https://zakon.rada.gov.ua/laws/show/995_c16.

9. Кримінальна конвенція Ради Європи про боротьбу з корупцією від 27.01.1999. URL: https://zakon.rada.gov.ua/laws/show/994_101.

10. Європейська конвенція про взаємну допомогу у кримінальних справах від 20.04.1959. URL: https://zakon.rada.gov.ua/laws/show/995_036.

11. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17.

ЗАЧЕК Олег
завідувач кафедри інформаційних технологій Львівського державного університету внутрішніх справ, кандидат технічних наук, доцент
РУДИЙ Тарас
доцент кафедри інформаційних технологій Львівського державного університету внутрішніх справ, кандидат технічних наук, доцент

ПРОБЛЕМНІ ПИТАННЯ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ КІБЕРБЕЗПЕКИ

Інформаційне забезпечення протидії організованій злочинності в умовах збройного конфлікту не може бути організоване без забезпечення захисту інформації та кібербезпеки. Воєнний стан спричиняє суттєві зміни в підходах держави до захисту власного інформаційного та кіберпростору. Це, у свою чергу, впливає на ставлення до безпеки інформації, засобів її оброблення та кіберсередовища, у якому вона передається, а також на визначення об'єктів впливу та реалізацію заходів із забезпечення інформаційної та кібербезпеки. Поточні обставини, у яких Україна розвиває власний інформаційний та кіберпростір, вимагають термінового впровадження глибоких і системних змін. Необхідність таких перетворень підтверджується кібератаками на об'єкти критичної інфраструктури та численними іншими інцидентами, які противники, зокрема Китай та росія, активно використовують проти нашої держави. Це відбувається на тлі стрімкого прогресу інформаційних технологій, зростання технологічної складності зовнішніх загроз, активного

використання методів соціальної інженерії, штучного інтелекту, Інтернету речей та квантових технологій.

Кабінет Міністрів України (КМУ) розробив та впроваджує «План заходів на 2025 рік з реалізації Стратегії кібербезпеки України» [1]. Зазначені у цьому документі заходи мають чітко виражений прогресивний характер, але вони лише частково нейтралізують основні чинники, що сприяють активному зростанню кіберзагроз. До таких чинників і досі належать недосконаліть та застарілість нормативно-правової бази у галузі кібербезпеки, неспішний процес адаптації положень законодавства Європейського Союзу (ЄС) та НАТО до українських реалій, відсутність ефективної системи незалежного аудиту інформаційної та кібербезпеки, а також брак реальних механізмів оприлюднення інформації про вразливості в умовах швидкої цифрової трансформації державного управління та суспільного життя. Крім того, процес упровадження сучасної організаційно-технічної моделі кіберзахисту, яка б відповідала актуальним викликам, загрозам у кіберпросторі та глобальним тенденціям розвитку кіберіндустрії, досі не завершено.

У межах національної правової системи наразі лише два ключові нормативно-правові акти визначають стратегічні засади протидії кіберзлочинності на рівні державної політики. Це Закон України «Про основні засади забезпечення кібербезпеки України» та Указ Президента України, яким введено в дію рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» [2]. Ці документи офіційно закріпили пріоритетне значення кібербезпеки для діяльності державних органів та уряду. Особливого значення набуває розроблення та ухвалення нової Стратегії кібербезпеки України, яка має визначити ключові національні інтереси у галузі кібербезпеки, намітити цілі та завдання кіберзахисту держави й забезпечити умови для безпечного функціонування кіберпростору в інтересах особи, суспільства та держави. І при цьому виникає нагальна потреба перейти від формальних заяв до практичної реалізації конкретних заходів.

Необхідно осучаснити такі визначення як «обчислювальна машина» та

«електронна обчислювальна машина», а також ввести нові поняття. Зокрема, необхідно ввести поняття смартфона, бо це є гібридний пристрій, який поєднує у собі властивості комунікатора і комп'ютера, та став засобом скоєння значної кількості кіберзлочинів, а такого поняття в законодавстві немає, як немає і кваліфікування кіберзлочинів, скоєних з їх допомогою.

В Україні відсутнє правове регулювання сучасних технологій, таких як штучний інтелект (ШІ) та Інтернет речей (IoT). До 2027 року ринок ШІ у кібербезпеці прогнозовано сягне 46,3 млрд доларів США [3], при цьому його застосування спрощує проведення складних кібератак і ускладнює їхнє розкриття [4]. Сучасні системи кібербезпеки ще не адаптовані до нових загроз, а цілісної стратегії протидії атакам із використанням ШІ досі немає [5]. IoT, ставши невід'ємною частиною життя, також відкриває нові можливості для кібератак через обмежені засоби захисту пристроїв [6]. Таким чином, інтеграція цих технологій створює нові виклики для організаційно-правового забезпечення кібербезпеки на державному рівні.

На думку авторів, ключовою проблемою залишається неефективна нормативно-правова база та відсутність чіткого регламенту управління, що забезпечував би динамічний правовий супровід інформаційної та кібербезпеки в Україні [7]. Усі заходи з кібербезпеки слід об'єднати в єдину програму трансформації державного управління у цій сфері.

В Україні спостерігається відставання регуляторів у створенні правової бази для захисту критичної інфраструктури та наповненні рамкових законів у сфері кіберзахисту й кібербезпеки підзаконними актами. Наразі необхідно розробити та ухвалити нормативні документи щодо вимог до кіберзахисту, оцінки кіберзагроз і порядку аудиту інформаційної безпеки [8].

Висновки. Існуюча нормативно-правова база потребує суттєвого доповнення, оскільки не охоплює повністю сучасні загрози кібербезпеці держави; на організаційно-правовому рівні необхідно чітко визначати проблеми кібербезпеки та своєчасно впроваджувати ефективні правові механізми протидії загрозам. При розробці або оновленні Стратегії кібербезпеки слід

враховувати зміни ландшафту кіберзагроз, зокрема сукупність актуальних ризиків, загроз, технологій, інструментів та учасників, що впливають на захист інформаційних активів і даних у цифровому середовищі. Всі ініціативи у сфері кібербезпеки слід об'єднати в єдину програму трансформації державного управління, що спирається на розвиток правової системи кібербезпеки в Україні та забезпечує нормативно-правовий супровід поточних процесів в умовах війни.

Список використаних джерел:

1. Про затвердження плану заходів на 2025 рік з реалізації Стратегії кібербезпеки України : Розпорядження Кабінету міністрів України від 7 березня 2025 р. № 204-р. URL: https://zakon.rada.gov.ua/laws/show/204-2025-%D1%80#Text (дата звернення 30.09.2025).
2. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26 серпня 2021 року № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення 30.09.2025).
3. Роль штучного інтелекту в кібербезпеці: передбачення та запобігання атакам. URL: https://eba.com.ua/rol-shtuchnogo-intelektu-v-kiberbezpetsi-peredbachennya-ta-zapobigannya-atakam/ (дата звернення 30.09.2025).
4. Васильченко Максим. AI та кібербезпека: нові виклики для світу. URL: https://goit.global/ua/articles/ai-ta-kiberbezpeka-novi-vyklyky-dlia-svitu/ (дата звернення 30.09.2025).
5. Шимкович Валентина. «Штучний інтелект не захистить, якщо не використовувати інтелект природний»: як розвиток ШІ впливає на кібербезпеку. URL: https://robotdreams.cc/uk/blog/352-shtuchniy-intelekt-ne-zahistit-yakshcho-ne-vikoristovuvati-intelekt-prirodniy-yak-rozvitok-shi-vplivaye-na-kiberbezpeku (дата звернення 30.09.2025).
6. Бонк Макс. Зміна ландшафту кібербезпеки у 2025 році. URL: https://mediacom.com.ua/zmina-landshaftu-kiberbezpeky-u-2025-rotsi/ (дата

звернення 30.09.2025).

7. Живко З.Б., Рудий Т.В., Сеник В.В., Родченко С.С. Проблеми нормативно-правової бази забезпечення кібербезпеки в Україні: стан і перспективи. Соціально-правові студії. 2020. Вип. 3 (9). С. 18–25.

8. Котляров Юрій. Архітектура права сфери кібербезпеки в Україні. URL: https://www.asterslaw.com/ua/press_center/publications/architecture_of_the_cyber security_law_in_ukraine/ (дата звернення 30.09.2025).

КУЛИК Олександр
головний науковий співробітник відділу кримінологічних досліджень Науково-дослідного інституту вивчення проблем злочинності імені академіка В.В. Сташиса НАПрН України, доктор юридичних наук, професор

ІНФОРМАЦІЙНО-АНАЛІТИЧНА СИСТЕМА ДОСЛІДЖЕННЯ ТЕНДЕНЦІЙ ОРГАНІЗОВАНОЇ ЗЛОЧИННОСТІ В УКРАЇНІ[1]

Організована злочинність – складне соціальне явище, особливий феномен кримінальної протиправності постмодерну, який має відмінні специфічні ознаки порівняно з іншими злочинами [1, с. 191]. Вона проникла в ряд сфер економіки (будівництво, банківська діяльність, торгівля нерухомістю тощо) та управління, політичну систему [2, с. 61], що створює серйозну загрозу національній безпеці України, особливо в умовах війни. Важливою умовою успішної протидії цьому явищу є створення інформаційно-аналітичної системи моніторингу, аналізу та оцінки тенденцій її розвитку в країні та регіонах. Зазначена система може включати наступні елементи.

[1] *Примітка*. Тези підготовлені у межах розробки фундаментальної теми дослідження «Злочинність в Україні у повоєнний період: кримінологічні прогнози та заходи запобігання» відділу кримінологічних досліджень НДІ ВПЗ ім. акад. В. В. Сташиса НАПрН України (держ. реєстр. в УкрІНТЕІ № 0124U005211).

1. *Щорічний моніторинговий кримінологічний аналіз даних державної статистичної звітності щодо організованої злочинності в Україні*. Інформаційною базою для такого аналізу є Звіт про результати боротьби з організованими групами та злочинними організаціями (форма 1-ОЗ), затверджений наказом Генерального прокурора від 30.06.2020 №299 за погодженням з Державною службою статистики України. Досліджувати необхідно звіти по Україні та всім регіонам. Аналіз цих даних дозволить отримати кримінологічну характеристику організованих груп та злочинних організацій (ОГ та ЗО) за декількома важливими ознаками (їх розподіл за числом учасників, тривалістю існування, якісними особливостями складу угруповань тощо), встановити види злочинів, які найчастіше вчиняються членами ОГ та ЗО тощо.

Зрозуміло, що офіційна статистика злочинності, зокрема й організованої, завжди буде неповною, але вона певною мірою відображає реальні тенденції розвитку зазначеного явища. При здійсненні аналізу статистичних даних за поточний рік доцільно використовувати для порівняння аналогічні статистичні дані за достатньо тривалий порівняльний період – не менше 10 років, якщо за ці роки не відбулося значних змін у нормативно-правовій базі та організації правоохоронної діяльності в цій сфері протидії злочинності. Результати кримінологічного аналізу цих статистичних даних мають скласти первинну основу для визначення та оцінки тенденцій організованої злочинності.

2. *Кримінологічний аналіз даних державної статистичної звітності щодо засуджених осіб, які вчинили певні види злочинів у складі організованої групи або злочинної організації.* Інформацію для такого аналізу можна отримати зі Звіту про осіб притягнутих до кримінальної відповідальності та види кримінального покарання (форма 6) та Звіту про склад засуджених

(форма 7), затверджених наказом Державної судової адміністрації України від 23.06.2018 № 325 за погодженням з Державною службою статистики України. В першому з них містяться дані щодо видів кримінальних покарань, які були призначені сукупності засуджених в цьому році членів ОГ та ЗО, але без їх розподілу за видами злочинів, за вчинення яких вони були засуджені. В другому звіті наводиться розподіл засуджених членів ОГ та ЗО за видами вчинених ними посягань. Обсяг даних незначний, але він дозволяє оцінити каральний вплив держави на представників організованої злочинності. При аналізі цих показників також доцільно використовувати для порівняння статистичні дані за попередні 10 років.

3. *Вибіркове поглиблене дослідження репрезентативного масиву судових рішень відносно членів ОГ та ЗО, отриманих з Єдиного державного реєстру судових рішень.* Мета такого дослідження отримати розгорнуту кількісно-якісну структуру проявів організованої злочинності в країні та регіонах за рядом ознак злочинних діянь та членів ОГ та ЗО, що їх вчинили, які відсутні в державній статистичній звітності; здійснити кримінологічну типологію таких злочинів як соціальних актів, більш глибоко оцінити ступінь розповсюдженості та характер суспільної небезпечності посягань кожного типу, визначити нові форми та способи вчинення злочинів. За допомогою такої інформації може бути визначено зв'язки між ознаками діянь та осіб, які їх вчинили. Ця інформація буде також придатною для якісного довготривалого прогнозу тенденцій організованої злочинності, зокрема прогнозування нових форм та способів вчинення злочинів, категорій осіб, які будуть виявляти найбільшу кримінальну активність тощо.

Це трудомістке і складне в методичному плані дослідження, здійснення якого потребуватиме значних витрат часу, людських ресурсів та організаційних зусиль. У зв'язку з цим воно може проводитись раз у два-три роки.

4. *Щорічне опитування експертів із зазначених питань*. В якості експертів слід запрошувати працівників правоохоронних органів, які

займаються практичною діяльності щодо протидії організованій злочинності – працівників відповідних підрозділів СБУ та Департаменту стратегічних розслідувань Національної поліції України, які мають спеціальний стаж роботи не менше 5 років. В ході такого опитування доцільно з'ясовувати оцінку експертами стану організованої злочинності в їх регіоні, відомості щодо нових сфер кримінальної активності ОГ та ЗО, способів вчинення злочинів, пропозиції щодо підвищення ефективності протидії організованій злочинній діяльності.

5. *Щорічне вибіркове дослідження матеріалів засобів масової інформації (ЗМІ) щодо проявів організованої злочинності в країні та регіонах*. На наш погляд, здійснення такого дослідження з урахуванням тієї величезної ролі, яку відіграють ЗМІ у житті сучасного українського суспільства, є необхідним. Вивченню підлягають матеріали журналістських розслідувань проявів організованої злочинності (контрабанда товарів, поширення наркотичних засобів; схеми розкрадання бюджетних коштів; корупція в різних сферах управління тощо); економічних та соціальних явищ, які сприяють формуванню злочинних угруповань (створення нових секторів тіньової економіки, неконтрольована міграція і створення закритих етнічних діаспор тощо). За результатами такого дослідження можна буде отримати додаткову інформацію щодо тенденцій організованої злочинності в країні, поширеність певних форм та видів злочинної діяльності, оцінити зміст інформації про організовану злочинність та діяльність правоохоронних органів щодо протидії їй, яку ЗМІ надають населенню, уявлення про ці проблеми, які формуються у громадян під впливом ЗМІ.

Особливим елементом даної системи має бути оперативно-розшукова інформація, отримана в процесі здійснення кримінальної розвідки, але така діяльність в країні досі не здійснюється.

Зазначена інформаційно-аналітична діяльність може здійснюватися науково-дослідною установою або аналітичним центром Національної поліції України.

Створення такої інформаційно-аналітичної системи дозволить підняти на новий рівень поінформованість держави й суспільства про стан та тенденції організованої злочинності в країні, поглибити знання щодо закономірностей її розвитку, розробити методи її середньо- та довгострокового прогнозування та визначити стратегію протидії цьому явищу.

Список використаних джерел:

1. Назимко Є. С., Пономарьова Т. І., Семенишина-Фіголь Б. М. Організована злочинність як феномен кримінології постмодерну. *Правова позиція*. 2023. № 1 (38). С. 190–194.

2. Бусол О. Ю. Організована злочинність в Україні: стан і проблеми реалізації державної політики у сфері протидії цьому явищу. *Юридичний часопис Національної академії внутрішніх справ*. 2019. №2 (18). С. 71.

ЛИТВИНЕНКО Ольга
доцент кафедри кримінального процесу та криміналістики факультету підготовки фахівців для органів досудового розслідування НПУ, майор поліції, доктор філософії

ДОКАЗУВАННЯ У КРИМІНАЛЬНИХ ПРАВОПОРУШЕННЯХ, ВЧИНЕНИХ ОРГАНІЗОВАНИМИ ГРУПАМИ

Організована злочинність є однією з найнебезпечніших форм кримінальної діяльності, що становить серйозну загрозу не лише для окремих громадян, але й для суспільства та держави в цілому. Кримінальні правопорушення, вчинені організованими групами, відзначаються високим рівнем планування, стійкою структурою злочинних об'єднань, конспіративністю дій та значним матеріальним, моральним і соціальним

збитком.

На відміну від одиночних кримінальних правопорушень, правопорушення, що скоюються організованими групами, мають складний характер: вони часто є багатоепізодними, вчиняються за попередньою змовою з розподілом ролей, із застосуванням ресурсів, зв'язків та сучасних технологій. Такі об'єднання можуть діяти тривалий час, охоплювати кілька регіонів чи навіть держав, мати корумповані зв'язки з представниками органів влади або бізнесу. У зв'язку з цим боротьба з такими правопорушеннями потребує комплексного, скоординованого та професійного підходу.

Виявлення злочинів – процес, під час якого приховані (латентні) кримінальні правопорушення стають відомими правоохоронним органам, і з цього моменту виникає законний обов'язок розглянути матеріали про наявність ознак кримінального правопорушення, розкрити та розслідувати його. Однією з причин неналежного розслідування є відсутність ефективної методики розслідування, неналежна організованість дій слідчого на початковому етапі розслідування [1, с.90].

Розслідування такої категорії справ варто доручати спеціальним слідчо-оперативним групам і обов'язково треба передбачати залучення співробітників спеціальних підрозділів по боротьбі із злочинними організаціями та злочинними угрупуваннями. Відповідно від цього також буде залежати ефективність розслідування та виявлення ознак вчинення злочину безпосередньо організованою групою [2, с.178].

Доказування в кримінальних провадженнях про злочини, вчинені злочинними спільнотами являє собою вид доказування про сукупність кримінальних правопорушень, основне «ядро» яких можуть складати як однорідні за кримінально правовими ознаками та тотожні за елементами кримінального процесуального предмета доказування, за криміналістичними засобами та прийомами виявлення їх джерел злочини. Водночас в єдиний предмет доказування можуть входити не тільки, наприклад, розбій, учинений членами злочинної спільноти, але й інші, учинені ними кримінальні

правопорушення [3, с.256].

Доказування ознак вчинення кримінального правопорушення організованою групою осіб є набагато складнішим в порівнянні з доказуванням, коли йдеться про звичайну групу або групу, яка діяла за попередньою змовою. Це обумовлено значно ширшим колом обставин, що підлягають встановленню у кримінальному провадженні. Фактично слідчому потрібно дослідити і належним чином зафіксувати не тільки обставини вчинення кримінального правопорушення, але й вузлові елементи формування і розвитку організованої групи як соціально-психологічного феномену. При цьому потрібно враховувати, що група осіб може набувати ознак організованості протягом досить тривалого часу [4, с.22].

До таких слід віднести: час та обставини створення організованої групи чи злочинної організації, її чисельність, місця базування, основна «спеціалізація»; відомості про особу організатора (лідера) організованої групи чи злочинної організації та її структуру; відомості про особи та розподіл ролей кожного члена групи чи організації, як при вчиненні окремих кримінальних правопорушень, так і діяльності групи загалом; способи залучення та встановлення індивідуальної ролі кожного учасника групи в підготовці, вчиненні та приховуванні слідів кожного вже вчиненого кримінального правопорушення, включаючи її організатора (лідера), пособників, підбурювачів тощо; відомості про кримінальні правопорушення, які готуються; критерії відбору нових членів групи; хто з членів долучився до групи нещодавно й хто з них брав участь у вчиненні найменшої кількості кримінальних правопорушень; взаємини між членами групи, наявність конфліктів; хто з членів групи користується авторитетом в інших учасників, а хто ні тощо; участь когось із учасників групи в інших злочинних угрупуваннях. Якщо так, то яких і коли; наявність конфліктів угрупування, до якого входить допитуваний, з іншими організованими групами чи злочинними організаціями. Якщо так, то з якими і в чому вони полягають; система розподілу доходів, здобутих злочинним шляхом; система покарань для тих

членів групи, які провинилися; озброєність групи, місця зберігається вогнепальної зброї і боєприпасів, джерела та механізми поповнення арсеналу; забезпеченість групи транспортними засобами (кількість, марки, моделі, колір, державні номери, включаючи підроблені) тощо; забезпеченість групи засобами зв'язку; наявність корупційних зв'язків із представниками органів державної влади, у т. ч. правоохоронних та судових органів тощо [5, с.9-10].

Ці обставини можуть бути встановлені на підставі сукупності доказів: показань учасників, свідків, матеріалів негласних слідчих (розшукових) дій, висновків експертиз, речових доказів, електронної інформації тощо.

Висока доказова складність таких проваджень обумовлює необхідність застосування комплексного підходу — поєднання криміналістики, фінансової розвідки, цифрових експертиз і соціологічного аналізу структури групи — для формування цілісного та переконливого доказового масиву.

Для забезпечення допустимості та результативності доказів рекомендується систематичне планування доказових дій, документування ланцюга зберігання доказів і ретельне обґрунтування процесуальних підстав для застосування негласних слідчих (розшукових) дій.

У процесі розслідування слід зберігати баланс між оперативною ефективністю і гарантіями прав учасників процесу; порушення останніх створює ризик визнання доказів недопустимими та підриває суспільну легітимність протидії організованій злочинності.

Список використаних джерел:

1. Мірковець О.М. Розслідування розбоїв, вчинених організованою групою в Україні: дис. к.ю.н.: 12.00.09. Маріуполь, 2021. 258с.. URL: https://dnuvs.in.ua/wp-content/uploads/2021/09/mirk_dys.pdf

2. Ковальова В.О. Розслідування злочинів, що вчиняються організованими групами: загальна характеристика. *Протидія організованій злочинності: проблеми теорії та практики*: матеріали всеукраїнського

науково-практичного семінару (м. Дніпро, 09 грудня 2022 р.). Дніпро: Дніпроп. держ. ун-т внутр. справ. 2022. 244с. С. 177-179

3. Бондар В.С. Обставини, які підлягають доказуванню у кримінальних провадженнях про злочини, вчинені злочинними спільнотами. *Київський часопис права*. 2024. № 1. С. 252-256

4. Волобуєв А. Ознаки організованої групи та їх доказування у кримінальному провадженні. *Актуальні проблеми державотворення, правотворення та правозастосування:* матеріали Всеукраїнської науково-практичної конференції (ДДУВС, 05.12.2024). С.20-23. URL:

5. Використання спеціальних знань під час розслідування кримінальних правопорушень, вчинених організованими групами чи злочинними організаціями / Коваленко В. В., Бондар В. С., Вигівський І. М., Дрозд В. Г., Слухаєнко Ю. М. Київ : Алерта, 2024. 136 с.

ПУГАЧ Світлана
аспірант Донецького державного університету внутрішніх справ

ФОРМУВАННЯ ДЕРЖАВНОЇ ІНФОРМАЦІЙНОЇ СТРАТЕГІЇ У СФЕРІ ПРОТИДІЇ ЖІНОЧИМ ФОРМАМ ОРГАНІЗОВАНОЇ ЗЛОЧИННОСТІ ПІД ЧАС ВІЙНИ

Воєнний стан докорінно змінив ландшафт організованої злочинності в Україні. Масові міграційні процеси, послаблення контролю на окремих територіях та економічна нестабільність відкрили нові можливості для злочинних мереж. Жіноча організована злочинність перестала бути маргінальним явищем. Жінки створюють власні злочинні структури, керують транснаціональними операціями з торгівлі людьми, організовують схеми легалізації злочинних доходів під виглядом благодійної діяльності. Традиційні

стереотипи про жінок як пасивних учасниць злочинів працюють на користь злочинцям – правоохоронці рідше підозрюють жінок у керівництві організованими групами. Державна інформаційна стратегія протидії цьому феномену вимагає переосмислення підходів до виявлення, розслідування та попередження жіночих форм організованої злочинності.

Жіноча організована злочинність як явище характеризується використанням гендерних стереотипів для досягнення злочинних цілей. Суспільство та правоохоронна система сприймають жінок як менш схильних до насильства та агресивної злочинної поведінки. Злочинниці експлуатують образи матерів з дітьми, вимушених переселенок, волонтерок або медичних працівників. Під час перетину кордону жінка з дитиною викликає менше підозр, ніж чоловік аналогічного віку. Волонтерка, яка організовує евакуацію цивільних, може насправді вербувати жертв торгівлі людьми. Благодійний фонд допомоги біженцям може слугувати інструментом відмивання злочинних коштів. Ці механізми маскування ускладнюють виявлення жіночих злочинних мереж традиційними оперативно-розшуковими методами.

Торгівля людьми стала однією з найприбутковіших сфер жіночої організованої злочинності. Стаття 149 КК України передбачає відповідальність за купівлю-продаж людини або вчинення іншої незаконної угоди, пов'язаної з передачею людини [1]. Організовані групи, очолювані жінками, використовують довіру потенційних жертв. Вербувальниця знайомиться з жінкою у пункті гуманітарної допомоги, пропонує допомогу з працевлаштуванням за кордоном або безпечну евакуацію. Створюється довірливе середовище, жертву переконують у щирості намірів. Соціальні мережі стали основним каналом пошуку жертв – групи для ВПО, волонтерські спільноти, оголошення про працевлаштування. Транснаціональний характер цих злочинів вимагає координації з правоохоронними органами країн ЄС, куди потрапляють жертви.

Шахрайські схеми з використанням статусу внутрішньо переміщених осіб набули масштабного характеру. Статті 190 та 358 КК України

встановлюють відповідальність за шахрайство та підроблення документів [1]. Організовані групи створюють мережі фіктивних ВПО для отримання державної допомоги, гуманітарної допомоги, житлових субсидій. Жінки виступають координаторками цих схем, оскільки саме вони частіше звертаються до соціальних служб і викликають менше підозр у працівників. Один координатор може контролювати десятки фіктивних реєстрацій. Гроші, отримані від держави та міжнародних організацій, розподіляються всередині злочинної мережі. Виявлення таких схем ускладнюється легальністю формальних процедур реєстрації.

Незаконне переміщення через державний кордон організовується жінками як бізнес-послуга. Стаття 332 КК України криміналізує незаконне переправлення осіб через державний кордон України [1]. Основні клієнти – чоловіки призовного віку, які намагаються уникнути мобілізації. Організаторки створюють канали виїзду через сусідні країни, використовуючи підроблені документи або схеми легального перетину кордону з подальшим зникненням. Жінка з дітьми, яка супроводжує групу "родичів", викликає значно менше підозр прикордонників. Вартість послуг коливається від 5 до 15 тисяч доларів США. Злочинні групи мають розгалужену мережу у прикордонних регіонах та контакти з корумпованими посадовими особами.

Формування державної інформаційної стратегії вимагає комплексного підходу. Аналітична складова передбачає створення міжвідомчої системи моніторингу жіночої організованої злочинності. Інтеграція баз даних Національної поліції, СБУ, Державної прикордонної служби, органів соціального захисту дозволить виявляти аномальні паттерни поведінки. Моніторинг соціальних мереж та месенджерів необхідний для виявлення вербувальників та організаторів злочинних схем. Алгоритми машинного навчання можуть ідентифікувати підозрілу активність серед реєстрацій ВПО, звернень за гуманітарною допомогою, фінансових транзакцій благодійних організацій.

Превентивна робота спрямована на інформування населення та захист

вразливих категорій. Інформаційні кампанії через соціальні мережі, таргетована реклама з попередженнями про типові схеми шахрайства та торгівлі людьми. Навчання працівників соціальних служб, пунктів гуманітарної допомоги, прикордонників розпізнавати ознаки діяльності організованих груп. Створення безпечних каналів повідомлення про підозрілу діяльність – гарячі лінії, онлайн-платформи, чат-боти. Робота з громадами внутрішньо переміщених осіб для підвищення їх обізнаності про загрози.

Розслідування злочинів жіночих організованих груп потребує спеціальних підходів. Традиційні методи роботи з чоловічими злочинними організаціями не завжди ефективні. Жіночі злочинні мережі базуються на неформальних зв'язках – родинних, дружніх, земляцьких. Структура менш ієрархічна, рішення приймаються колективно або консенсусом. Комунікація відбувається через месенджери з наскрізним шифруванням, особисті зустрічі замасковані під дружні чи родинні. Негласні слідчі дії, передбачені статтями 246-271 Кримінального процесуального кодексу України, мають застосовуватися з урахуванням цієї специфіки [3]. Аудіо- та відеоконтроль, зняття інформації з транспортних телекомунікаційних мереж, контроль за вчиненням злочину дозволяють документувати злочинну діяльність.

Міжнародне співробітництво є критично важливим елементом стратегії. Конвенція ООН проти транснаціональної організованої злочинності передбачає механізми взаємної правової допомоги [4]. Жіночі організовані групи діють транснаціонально – вербування відбувається в Україні, експлуатація жертв у країнах ЄС, фінансові операції через офшорні зони. Координація з Європолом та Інтерполом необхідна для викриття цих мереж. Створення спільних слідчих груп з правоохоронними органами Польщі, Німеччини, Чехії, де перебуває найбільша кількість українських біженців. Обмін оперативною інформацією в режимі реального часу через канали міжнародної поліцейської співпраці.

Кваліфікація злочинів вимагає встановлення всіх елементів складу. Стаття 255 КК України передбачає відповідальність за створення злочинної

організації – стійкого ієрархічного об'єднання трьох або більше осіб [1]. Доведення стійкості зв'язків у жіночих групах ускладнюється їх неформальним характером. Судова практика повинна враховувати, що стійкість може виражатися не лише у формальній ієрархії, а й у тривалості функціонування групи, систематичності зв'язків, розподілі ролей. Кваліфікація за сукупністю злочинів – створення злочинної організації плюс конкретні злочини (торгівля людьми, шахрайство, легалізація доходів) – повинна відображати повний обсяг злочинної діяльності.

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.

Список використаних джерел:

1. Кримінальний кодекс України: Закон України від 05.04.2001 № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14.

2. Про організаційно-правові основи боротьби з організованою злочинністю: Закон України від 30.06.1993 № 3341-XII. URL: https://zakon.rada.gov.ua/laws/show/3341-12.

3. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17.

4. Конвенція ООН проти транснаціональної організованої

злочинності від 15.11.2000. URL: https://zakon.rada.gov.ua/laws/show/995_789.

САЙЧУК Дмитро
курсант 2 курсу Навчально-наукового інституту № 2 Харківського національного університету внутрішніх справ
рядовий поліції

Науковий керівник:
ГРІДІНА Наталія
Доцент кафедри адміністративної діяльності курсу Навчально-наукового інституту № 3 Харківського національного університету внутрішніх справ

ЗАБЕЗПЕЧЕННЯ ПРАВ І СВОБОД ГРОМАДЯН ПІД ЧАС РЕАЛІЗАЦІЇ ПОЛІЦЕЙСЬКИХ ПОВНОВАЖЕНЬ ЩОДО ПРОТИДІЇ ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ В УМОВАХ ЗБРОЙНОГО КОНФЛІКТУ

Сучасний етап розвитку Української держави характеризується складними викликами, пов’язаними з веденням збройного конфлікту та необхідністю забезпечення національної безпеки. У цих умовах особливої актуальності набуває проблема ефективної протидії організованій злочинності при одночасному неухильному дотриманні прав і свобод громадян. Організовані злочинні угруповання, використовуючи дестабілізацію суспільно-політичної ситуації, активізують свою діяльність, що створює додаткові загрози для громадської безпеки та правопорядку [5].

Національна поліція України в умовах збройного конфлікту стикається з необхідністю вирішення складного завдання: забезпечити ефективну протидію організованій злочинності, яка часто використовує воєнний стан для

розширення своїх злочинних схем, водночас неухильно дотримуючись європейських стандартів захисту прав людини. Це завдання ускладнюється тим, що традиційні методи роботи поліції потребують адаптації до умов воєнного стану, коли частина правових механізмів може бути обмежена або змінена.

Правове регулювання поліцейської діяльності з охорони громадянських прав у процесі боротьби з організованою злочинністю ґрунтується на ключових міжнародно-правових документах, до найважливіших з яких належать: Резолюція Парламентської асамблеї Ради Європи № 690 (1979) «Декларація про поліцію», Рекомендація Комітету Міністрів Ради Європи Rec (2001) 10 для держав-членів «Щодо Європейського кодексу поліцейської етики», Резолюція Генеральної Асамблеї ООН 34/169 «Кодекс поведінки службових осіб правоохоронних органів», разом з Основоположними принципами використання сили та вогнепальної зброї службовими особами правоохоронних органів, затвердженими восьмим Конгресом ООН з попередження злочинності [1].

Принцип поваги до прав людини та основних свобод, що становить основу комплексу європейських стандартів професійної діяльності поліцейських, набуває особливого значення в контексті протидії організованій злочинності в умовах збройного конфлікту. Цей принцип вимагає від працівників поліції дотримання найвищих стандартів професійної етики навіть у найскладніших оперативних ситуаціях, коли необхідно протидіяти добре організованим та озброєним злочинним угрупованням.

Для з’ясування особливостей функціонування поліцейських структур під час воєнних дій ключове значення мають норми Декларації Ради Європи № 690 «Про поліцію» від 1979 року, які окремо визначають алгоритм дій державних органів та співробітників поліції в період війни та іноземної окупації. Відповідно до цих норм, працівник поліції зобов’язаний продовжувати виконання своїх основних функцій із захисту населення та охорони власності навіть в умовах військового конфлікту та окупації ворогом,

діючи в інтересах цивільного населення. При цьому поліцейський не отримує статусу «комбатанта» і на нього не поширюються норми Третьої Женевської конвенції стосовно режиму військовополонених [4].

Організована злочинність в умовах збройного конфлікту демонструє підвищену суспільну небезпечність, оскільки злочинні угруповання можуть використовувати хаос воєнного стану для розширення своїх сфер впливу, контрабанди зброї, торгівлі людьми, незаконного обігу наркотичних засобів та інших тяжких злочинів. При цьому вони можуть маскувати свою діяльність під видом патріотичних ініціатив або волонтерських організацій, що значно ускладнює їх виявлення та документування злочинної діяльності.

Європейський кодекс поліцейської етики формулює конкретні стандарти використання правоохоронних повноважень, які зберігають свою дієвість і під час протидії організованій злочинності в умовах воєнних дій. Насамперед, Кодекс зобов'язує працівників поліції шанувати право кожної людини на життя, використовувати примус виключно за умов крайньої потреби і лише в межах, потрібних для досягнення правомірної цілі. Дані засади отримують надзвичайну важливість під час здійснення спеціальних заходів щодо організованих кримінальних формувань, коли зростає вірогідність застосування озброєння та фізичного впливу [3].

Заборона тортур та негуманного чи принижуючого ставлення, закріплена у переважній більшості міжнародних угод регіональних механізмів правозахисту, зокрема в Європейській Конвенції із захисту прав людини та основних свобод 1950 року, є безумовною навіть щодо підозрюваних у зв'язках з організованою злочинністю. Ніякі умови, враховуючи воєнний стан чи потребу здобуття відомостей про терористичні небезпеки, не здатні виправдати використання тортур або інших різновидів жорстокого ставлення [3].

Особливої уваги заслуговує дотримання процесуальних прав підозрюваних у справах про організовану злочинність. Право на справедливий суд, презумпція невинуватості та право на захист повинні неухильно

дотримуватися навіть щодо лідерів злочинних угруповань. Воєнний стан може обумовлювати певні особливості процедури, але не може бути підставою для ігнорування основних прав обвинувачених.

Застосування спеціальних засобів розвідки при протидії організованій злочинності потребує особливого правового регулювання для захисту приватності громадян. Використання технічних засобів спостереження та прослуховування повинно здійснюватися виключно на підставі судових рішень з дотриманням принципів необхідності, пропорційності та тимчасовості.

Міжнародне співробітництво у боротьбі з організованою злочинністю в умовах конфлікту набуває особливого значення через транснаціональний характер злочинних мереж. Обмін інформацією з іноземними органами та видача злочинців повинні здійснюватися з дотриманням міжнародних стандартів захисту прав людини та урахуванням ризиків для безпеки співпрацюючих осіб.

Контроль за дотриманням прав людини при протидії організованій злочинності повинен здійснюватися на кількох рівнях: внутрішньовідомчий, прокурорський, судовий та громадський. Кожен механізм має свою специфіку і повинен функціонувати навіть в умовах війни, хоча з певними адаптаціями до воєнного стану [4].

Підготовка персоналу поліції до роботи в умовах збройного конфлікту при дотриманні європейських стандартів захисту прав людини потребує спеціальних освітніх програм та тренінгів. Поліцейські повинні володіти не лише професійними навичками виявлення та розслідування злочинів організованих угруповань, а й глибоко розуміти принципи поваги до прав людини та вміти застосовувати ці принципи в складних оперативних ситуаціях.

Психологічні аспекти діяльності поліцейських в умовах збройного конфлікту також впливають на якість дотримання прав громадян. Підвищений стрес, постійна загроза життю, необхідність приймати рішення в умовах

невизначеності можуть негативно впливати на професійну поведінку поліцейських. Тому система психологічної підтримки та реабілітації персоналу є невід'ємною частиною забезпечення дотримання європейських стандартів поліцейської діяльності.

Громадський контроль за діяльністю поліції в умовах збройного конфлікту стикається з обмеженнями через необхідність збереження конфіденційності та безпеки операцій. Водночас принципи відкритості та підзвітності повинні зберігатися максимально, що потребує збалансованих рішень між вимогами безпеки та демократичного контролю [6].

Європейські стандарти професійної діяльності поліції щодо протидії організованій злочинності в умовах збройного конфлікту забезпечують: дотримання прав людини в складних оперативних умовах; підвищення ефективності міжнародного співробітництва; удосконалення правової системи з урахуванням воєнного стану; зміцнення довіри населення до правоохоронних органів; формування професійної культури, орієнтованої на повагу до людської гідності.

Реалізація цих стандартів у діяльності Національної поліції України сприятиме збалансованому підходу до протидії організованій злочинності, забезпечуючи ефективність правоохоронної роботи та дотримання прав громадян. Це критично важливо для збереження демократичних цінностей і верховенства права в умовах конфлікту, а також для євроінтеграції України [2].

Впровадження європейських стандартів у діяльність поліції щодо протидії організованій злочинності в умовах збройного конфлікту залишається стратегічним завданням, виконання якого забезпечить не лише ефективність правоохоронної системи, а й сприятиме утвердженню України як правової, демократичної держави, здатної захищати права та свободи своїх громадян навіть у найскладніших історичних умовах.

Список використаних джерел:

1. Європейський Кодекс поліцейської етики. Рекомендація (2001) 10, ухвалена Комітетом міністрів Ради Європи 19 вересня 2001 р. Та Пояснювальний меморандум. URL: https://hrea.org/wp-content/uploads/2021/02/Recommendation-Rec200110_European-Code-of-Police-Ethics_Ukrainian.pdf

2. Про Національну поліцію : Закон України від 02 липня 2015 року № 580-VIII. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text

3. Конвенція про захист прав людини і основоположних свобод від 04 листопада 1950 року. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text

4. Барба В. Забезпечення Національною поліцією прав і свобод громадян. *Південноукраїнський правничий часопис*. 2024. № 2. С. 145-148.

5. Поліцейська діяльність: адміністративно-правове регулювання : навчальний посібник / Ю. А. Хатнюк, О. Б. Мороз, В. В. Бондар, М. Ю. Самченко, С. С. Гнатюк, Є. В. Кобко ; за ред. Ю. С. Назара. Львів : Львівський державний університет внутрішніх справ, 2023. 640 с.

6. Драган О. В. Щодо повноважень Національної поліції України в умовах воєнного стану. *Адміністративне право і процес; фінансове право; інформаційне право*. 2024. № 1. С. 376-379.

САМОЙЛЕНКО Олена
професор кафедри оперативно-розшукової та поліцейської діяльності, Національний університет «Одеська юридична академія», доктор юридичних наук, професор

ПРОБЛЕМИ ПРОТИДІЇ ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ: АНАЛІТИЧНИЙ ОГЛЯД ТА ВИСНОВКИ

Протидія організованій злочинності залишається одним із ключових завдань правоохоронних органів в умовах збройного конфлікту. Її рівень безпосередньо впливає на стан національної безпеки, стабільність суспільства та ефективність правоохоронної системи. Показники статистики Державної судової адміністрації України дають змогу оцінити реальні тенденції розгляду кримінальних проваджень, що стосуються злочинів, учинених організованими групами та злочинними організаціями.

Аналізуючи динаміку судового розгляду кримінальних проваджень щодо злочинів, учинених організованими групами та злочинними організаціями (2023–2024 рр.) [1; 2], можна вдатись до прогнозування наслідків сучасної протидії кримінальним правопорушенням. Наведемо ці показники.

Так, в 2024 році в судах першої інстанції перебувало 1642 кримінальних провадження щодо злочинів, учинених організованими групами. Це на 242 провадження більше, ніж у 2023 році (тоді цей показник становив 1400 од.). Проте збільшення кількості розглянутих справ не супроводжувалося підвищенням ефективності їх завершення: на кінець звітного року нерозглянутими залишилося 1292 провадження, тоді як у 2023 році таких було 1086. Аналогічна тенденція простежується і щодо кількості осіб, стосовно яких провадження не були завершені. Якщо у 2023 році таких осіб налічувалося 3533, то в 2024 році їх кількість зросла до 4061. Така динаміка є невтішною та свідчить про зростання навантаження на судову систему та певне уповільнення в цілому реагування держави на подібні виклики організованої злочинності. Піднімаючи також звітну статистику Національної поліції України, можна підсумувати, що вищенаведені показники, з одного боку, пов’язані із збільшенням обсягу зареєстрованих кримінальних правопорушень, учинених організованими групами, з іншого – із кадровим дефіцитом у судах та складністю доказової бази у справах про організовану злочинність. Ускладнення самої структури злочинності через інтеграцію організованих груп у кіберпростір, інтенсифікація використання криптовалют,

мережевих схем зв'язку призводить до нестачі спеціалізованих слідчих та суддів, надмірного навантаження останніх в процесах розслідування та судового розгляду, необхідності проведення складних та фінансово затратних експертиз.

Схожі процеси спостерігаються і стосовно злочинів, учинених злочинними організаціями – більш складного, часто транснаціонального, рівня організованої злочинності. Так, в 2024 році на розгляді в судах першої інстанції перебувало 302 кримінальних провадження цієї категорії, що майже на 25 % більше, ніж у 2023 році (241 провадження). Водночас кількість нерозглянутих справ також зросла – з 203 до 241 одиниці, а кількість осіб, щодо яких провадження не були завершені, – з 805 до 1049. Отже, темпи їх фактичного розгляду залишаються нижчими за темпи надходження, що свідчить не тільки про фактично накопичення нерозглянутих проваджень та потенційно ризики порушення розумних строків судового розгляду, гарантованих ст. 6 Конвенції про захист прав людини і основоположних свобод, а й створює передумови для подальшої кримінализації суспільних відносин.

Довготривалий судовий розгляд справ, пов'язаних з організованими злочинними групами, зумовлює адаптацію цих структур до слідчих і судових методів роботи, пристосування схем злочинної діяльності до триваючих процесів слідства, напрацювання механізмів впливу на правоохоронну та судову системи держави. В умовах війни такий стан боротьби з організованою злочинністю та фактично «безкарність конкретної особи» підриває довіру громадян до правоохоронної системи та органів державної безпеки, впливає на зниження рівня правомірної поведінки останніх.

Разом із тим зростання кількості окремих видів кримінальних проваджень (наприклад за 2024 рік у звіті Національної поліції вказано, що кіберполіція направила до суду кримінальні провадження щодо протиправної діяльності 46 організованих груп і злочинних організацій, порівняно в 2023 роком – 42 групи [3]) свідчить про певний ступінь активізації діяльності

правоохоронних органів у сфері виявлення організованих злочинних угрупувань, що є позитивним показником у контексті протидії цьому виду злочинності. Ми вважаємо, що такий показник не може оцінюватися лише за кількістю справ. Головним критерієм має бути результативність їх завершення, винесення вироків і реальне знешкодження організованих злочинних груп. Більшість організованих груп функціонують за принципом ієрархічності та підпорядкованості керівнику/лідеру, тому некараність останніх або основних ланок системи (координаторів) сприяє інституціоналізації злочинності, коли організована група починає діяти за аналогією до легальних організацій, із власними нормами поведінки та системами контролю.

Отже, рівень фактичного розгляду справ щодо злочинів, учинених організованими групами та злочинними організаціями, негативно впливає на активізацію боротьби з організованими формами злочинності. Досягнення реальної ефективності протидії організованій злочинності можливе за умови зміцнення кадрового потенціалу судів, удосконалення процесуальних механізмів реагування та міжвідомчої взаємодії. Однією з основних передумов зниження рівня організованої злочинності можна вважати справедливе, невідворотне і своєчасне покарання її представника.

Список використаних джерел:

1. Звіт судів першої інстанції про розгляд матеріалів кримінального провадження № 1-К. 2023 URL: https://court.gov.ua/inshe/sudova_statystyka/zvit_dsau_2023.

2. Звіт судів першої інстанції про розгляд матеріалів ккримінального провадження № 1-К. 2024 URL: https://court.gov.ua/inshe/sudova_statystyka/zvit_dsau_2024.

3. Звіт про результати роботи Департаменту кіберполіції Національної поліції України у 2023 році. URL: https://cyberpolice.gov.ua/news/zvit-pro-rezultaty-roboty-departamentu-kiberpolicziyi-naczionalnoyi-policziyi-ukrayiny-u--

roczi-4792/?utm_source=chatgpt.com .

ТАТАРЕНКО Світлана
доцент кафедри оперативно - розшукової діяльності та інформаційної безпеки навчально-наукового інституту підготовки фахівців для підрозділів кримінальної поліції імені Е.О. Дідоренка Донецького державного університету внутрішніх справ, доктор філософії в галузі Право

ВЕРГУН Дмитро
курсант 3-го курсу кафедри оперативно - розшукової діяльності та інформаційної безпеки навчально-наукового інституту підготовки фахівців для підрозділі в кримінальної поліції імені Е.О. Дідоренка Донецького державного університету внутрішніх справ

АКТУАЛЬНІ ПИТАННЯ ЩОДО НЕОБХІДНОСТІ ВНЕСЕННЯ ЗМІН ДО КРИМІНАЛЬНОГО ПРОЦЕСУАЛЬНОГО КОДЕКСУ УКРАЇНИ СТОСОВНО ПРОВЕДЕННЯ ОКРЕМИХ СЛІДЧИХ (РОЗШУКОВИХ) ДІЙ

З 20 лютого 2014 року триває збройна агресія російської федерації проти нашої держави за цей час вдосконалено та змінено чимало законів, підзаконних актів та інструкцій, які регламентують права і свободи громадян нашої держави [1].

Зокрема, хочеться торкнутись теми безвісти зниклих громадян нашої держави, адже доля багатьох українців та українок наразі залишається невідомою. І це стосується не тільки військових, які зникли безвісти за особливих обставин, а і цивільних громадян, які зникли безвісти внаслідок збройного конфлікту

Так безумовно, закон України «Про правовий статус осіб, зниклих безвісти за особливих обставин» від 14.04.2022 надає певний алгоритм дій правоохоронних органів з цією категорією громадян нашої держави [2].

На нашу думку, для своєчасного та якісного збору, фіксації та документуванні інформації, яка надалі слугуватиме доказом у кримінальному провадженні, при розслідуванні даної категорії злочинів потребують змін і деякі статті кримінально процесуального кодексу України .

Зокрема, згідно з ч. 2 ст. 159 КПК тимчасовий доступ до речей і документів здійснюється на підставі ухвали слідчого судді, суду [3] .

Вважаємо за доцільне доповнити статтю стаття 159 частиною 3, в якій необхідно вказати, що при наявності заяви про розшук особи, зниклої безвісти за особливих обставин, яка згідно з статтею 18 Закон України «Про правовий статус осіб, зниклих безвісти за особливих обставин» може бути подана : «родичем такої особи, представником військового формування, органом державної влади, органом місцевого самоврядування, громадським об'єднанням або будь-якою іншою особою, якій стало відомо про зникнення» [2], та внесених відомостей до Єдиного реєстру досудових розслідувань [3], слідчий, у провадженні якого знаходиться дане кримінальне провадження, виносить постанову, погоджену прокурором, про тимчасовий доступ до речей і документів , а саме - абонентського номеру та мобільного терміналу вказаного у заяві, яким безвісти зниклий мав у користуванні на момент зникнення « зняття копії інформації, що міститься в таких електронних інформаційних системах, комп'ютерних системах або їх частинах, мобільних терміналах систем зв'язку, без їх вилучення» [3], тобто отримання інформації у операторів - провайдерів мобільного зв'язку України, про реєстрацію абонентського номеру та терміналу безвісти зниклого за особливих обставин на момент зникнення, згідно з вказаною інформацією у ЄРДР, з метою отримання інформації, що може сприяти розшуку особи, зниклої безвісти за особливих обставин не потребує ухвали слідчого судді.

Отримання такої інформації від операторів стільникового зв'язку

України по постанові слідчого дасть змогу своєчасно та швидко встановити обставини, які передували зникненню особи, та встановленню можливих осіб, причетних до зникнення особи.

Фіксації випадків використання абонентських номерів та терміналів безвісти зниклої особи за особливих обставин особами, які причетні до їх утримання або загибелі, у подальшому дасть можливість використання цієї інформації як доказу злочинної діяльності російської федерації у відношенні громадян України у цьому збройному конфлікті .

Реалізація запропонованих змін сприятиме: підвищенню ефективності досудового розслідування, забезпеченню швидкого реагування правоохоронних органів на випадки зникнення осіб з особливих обставин, зміцненню доказової бази у справах, пов'язаних із воєнними злочинами, створенню додаткових правових підстав для документування злочинної діяльності збройних формувань російської федерації проти громадян України.

Список використаних джерел:

1. Постанова Верховної Ради України Про Заяву Верховної Ради України "Про відсіч збройній агресії Російської Федерації та подолання її наслідків" від 21.04.2015 Відомості Верховної Ради (ВВР), 2015, № 22, ст.153 URL: https://zakon.rada.gov.ua/laws/show/337-19#Text .

2. Закон України «Про правовий статус осіб, зниклих безвісти за особливих обставин» від 14.04.2022 Відомості Верховної Ради (ВВР), 2018, № 38, ст.280 URL: https://zakon.rada.gov.ua/laws/show/2505-19#Text (дата звернення: 12.10.2025).

3. Кримінальний процесуальний кодекс України від 13.04.2012 Відомості Верховної Ради України (ВВР), 2013, № 9-10, № 11-12, № 13, ст.88 URL:https://zakon.rada.gov.ua/laws/show/4651-17?find=1&text=%D0%B3%D0%BB%D0%B0%D0%B2%D0%B0+15#w (дата звернення: 12.10.2025).

ТОКАР Петро
начальник Головного управління Національної поліції в Харківській області, кандидат юридичних наук; старший викладач кафедри юридичних дисциплін Сумської філії ХНУВС (за сумісництвом).

КРІЦАК Іван
Т.в.о. помічник начальника Головного управління Національної поліції в Харківській області кандидат юридичних наук, доцент,

ІСТОРИКО-ЕТНО-КУЛЬТУРНІ ТА МІЖНАРОДНІ АСПЕКТИ ПРОБЛЕМИ ОРГАНІЗОВАНОЇ ЗЛОЧИННОСТІ: НА ПРИКЛАДІ ХАРКІВСЬКОГО РЕГІОНУ

Кримінотеологічні наративи з практики І. В. Кріцака, що можуть бути корисними в сьогоднішніх реаліях російсько-української війни. *Впродовж останніх років ми досліджуємо не лише кримінологію зла, але й кримінологію Добра, яка неабияк важлива у правоохоронній практиці з багатьох мотивів. Страшною є статистика, коли нинішні молоді люди близько 80% не вірять у Бога. Понад 5500 років людство чекало Рождество Божої Матері, свято якої ми нещодавно відзначили. Зерно жінки зітре главу змія (Пс. 39:7). Це свідчить про те, як ми повинні почитати Божу Матір, а в її обличчі й кожну жінку, яка живе у цьому світі. Створимо людину за образом нашим і подобою нашою (Буття 1:26). Цим сам підтверджується троїчна сутність Бога. Важливо, щоб сьогодні жіноча половина людства не спотворювала образу жінки, її прекрасної красоти. Згадаємо, як виглядала*

Божа Матір, яка народила Спасителя і Месію, – Господа, Бога і Спаса нашого Іісуса Христа у 14 років, а відійшла до Господа у 70-річному віці. За одним із стародавніх описів, вона була середнього або трохи вище середнього зросту, із золотоподібним волоссям, оливковими очима, продовгуватим носом і руками, а також з некруглим, але довгастим обличчям. Відомий святий недавнього часу Паісій Святогорець говорить, що Божа Матір є такою якою вона зображається на Ієрусалимській іконі. За переданнями, той, хто хоча б раз у житті бачив Божу Матір вже ніколи не забуде цього неземного стану. Від неї виходила особлива Божа сила, святість і благодать. Лише подумати: у віці трьох років вона сама піднімається по 15-ти великих ступенях Єрусалимського Храму і вводиться у Алтарь, – Святая Святих, куди первосвященик міг заходити лише один раз у рік. Одного разу Божа Матір заглибилася читанням в таємничі слова пророка Ісаї (7:14): «Се Діва в утробі прийме і народить Сина, і назвуть ім'я Йому Еммануїл, що означає «З нами Бог»... Вона міркувала про образ тієї, хто народить сина Божого. В цей час їй захотілося всіма силами стати хоча б служницею тієї Діви... І саме в цю хвилину і відбулося таїнство «Благовіщення», коли архангел Гавриїл промовив такі слова: «Радуйся, Благодатная: Господь з Тобою! Благословенна Ти в женах!»... Божа Матір велика труженица і молитвенниця за рід людський. Більшість часу вона займалася рукоділлям та молитвою. Чого сьогодні варта всесвітня святиня «Пояс Пресвятої Богородиці», що передав нам апостол Фома, який знову ж, як і з Воскресінням Христовим, запізнився на погребіння Божої Матері, земного тіла якої не побачив, а лежав лише Пояс Пресвятої Богородиці. Одному святому відкрилося небо, де він побачив сонм мучеників і великомучеників, багатьох святих і преподобних, однак Матері Божої він там не побачив. За священним переданням більшість свого часу вона проводить на Землі, між тими, хто її кличе на допомогу. Лише 2 рази в житті мені вдалось відчути присутність Божої Матері, коли до м. Івано-Франківська привезли чудотворну ікону «Призри на смирення» з Києва. Цього часу батьки прикладали дитину на інвалідному візку до святині. В цей час, як

ми протирали миром, чудотворну Ікону увесь народ Божий одночасно почав плакати. Була відчутна особлива неземна Сила Божа, яку не можна пояснити словами. Інший випадок, коли біля Харківського національного університету внутрішніх справ на перехрестку Аерокосмічного проспекту та Мереф'янського шосе, що біля Аеропорту, величезна кількість харків'ян зустрічали з живими квітами хресний хід, який йшов зі Свято-Борисо-Глібського жіночого монастиря до Благовіщенського Собору м. Харкова. Цим самим усі почали плакати, зустрічаючи великою кількістю народу святі ікони, які йшли у хресному ході. Можливо такі приклади в умовах нинішньої російсько-української війни, хоч якось підтримають нас, укріплять у вірі, щоб не впасти у відчай, коли здається сил далі не має йти. Саме тому так важливо у недільний день спішити до Храму Божого, як до колодязя/криниці живої води, адже не знаємо коли і в який час зможемо хоча б раз у житті відчути таку силу і Благодать. Хіба, коли велика спека ми будемо пити воду звідки завгодно. Ні звичайно. Ми шукатимемо джерело живої води, яким втамуємо свою спрагу. Храм Божий є таким живим колодязем, де можна почерпнути Живу воду про яку говорив Христос жінці Самарянці у Євангелії (Іоанна 4:7-29).

Важливі події недавнього часу. Неоціненний внесок у розвиток фундаментальної кримінології сьогодні робить видатний вчений української держави *М. Г. Колодяжний*, кількісно-якісна характеристика наукових праць якого вже давно дорівнює рівню професора. Вчений, безсумнівно, за словами Ю. В. Орлова написав найкращу наукову статтю Вісника кримінологічної асоціації України 2025. №2(35). Частина 1 на тему: «Проблема комплексності у кримінології: аналіз минулого, оцінка теперішнього, погляд у майбутнє», яка розміщена першою у загальному списку авторів, що свідчить про рівень визнання. Слід відзначити, що сферою наукових інтересів *М. Г. Колодяжного* є проблема комплексності (комплексного підходу) у кримінологічній науці. Справді, вчені наших земель споконвіку були космополітами, намагалися загально розуміти Всесвіт, подібно до лікаря, який лікує людину комплексно,

а не розбирається лише в одному органі. Цей підхід через бібліометрію ми також підтримаємо. Він, справді, дає комплексне бачення Всесвіту через біблеїстику та бібліотерапію, що є неабияк важливими для сфери «criminal», а особливо для здійснення ефективної кримінально-виконавчої політики української держави. Взагалі вважаємо, що кожна стаття повинна містити хоча б невеликий текст про Небесне. Адже без Бога, ані до порога. Марна наука без Бога.

У підтримку духовно-ціннісної концепції праворозуміння особливо знадобилися висловлювання М. Г. Колодяжного, як представника Науково-дослідного інституту вивчення проблем злочинності імені академіка В. В. Сташиса Національної академії правових наук України присвячені розмірковуванню про Земне і Небесне, що є неабияк важливими в умовах нинішньої російсько-української війни. Вчений зазначає, що навколишній світ та фактично усі напрями людської діяльності, включаючи сферу запобігання злочинності, пронизані комплексністю. Вона має багато граней, специфіка яких проявляється залежно від природи відповідного об'єкту, явища чи процесу, що описуються. Комплексність має дуже широку онтологічну палітру. Вона вказує на різнобічність й різносторонність нашого буття. Наприклад, у Новому Завіті зустрічається фраза «Альфа й Омега», які є, відповідно, першою й останньою буквами грецького алфавіту. Вказаний біблейський вислів символізує повноту речей і життя людей. Лише крізь призму комплексності можна пізнати всебічність, зміст і якість будь-яких об'єктів [1, с. 5–6]. Вважаємо, що сказане можна повністю адаптувати при здійсненні досліджень організованої злочинності.

Кримінологічна школа *Харківського національного університету внутрішніх* справ серед різноманітних підходів до розуміння злочинності відстоює інтегративний підхід. Щодо розуміння та визначення злочинності на користь *оперування інтегративним підходом*, як потенційно найбільш ефективним і у доктринальному, і в емпіричному, прикладному значеннях в різних варіаціях репрезентується працями А. Ф. Зелінського, В. В. Голіни, О.

М. Ігнатова, О. Г. Кальмана, О. Г. Кулика, О. М. Литвинова, Ю. В. Орлова, В. М. Поповича й деяких інших вчених. Виходячи з вказаного підходу, *злочинність* – це історично мінливий, статистично стійкий, релятивний соціальний феномен, що виражається у масових, інституційних, суспільно небезпечних практиках, форми прояву яких мають кількісно-якісний вираз у понадсумативній/понаднормативній сукупності злочинів, а також злочинній діяльності [2, с. 250; 3, с. 36].

Важливою подією взаємодії теоретиків і практиків у профілактиці та боротьбі зі злочинністю стало те, що 4 липня 2025 відбулася зустріч між керівництвом Головного управління Національної поліції в Харківській області та представниками Науково-дослідного інституту вивчення проблем злочинності імені академіка В. В. Сташиса Національної академії правових наук України. У заході взяли участь шеф поліції Харківщини Петро Токар, директорка Інституту Владислава Батиргареєва та завідувач відділу кримінологічних досліджень Максим Колодяжний. Під час зустрічі сторони обговорили актуальні проблеми профілактики кримінальних правопорушень у регіоні та визначили ключові напрями подальшої співпраці. Зокрема, йшлося про обмін науковими напрацюваннями, розробку ефективних практичних рішень у сфері запобігання та протидії злочинності, а також впровадження кращих європейських стандартів у правоохоронну діяльність. За підсумками зустрічі було підписано меморандум про співпрацю між Головним управлінням та Інститутом. Документ покликаний зміцнити взаємодію між наукою та практикою для підвищення ефективності роботи поліції на Харківщині [4].

Щодо поняття злочинність та організована злочинність. Організована злочинність – найбільш суспільно-небезпечна форма протиправної діяльності. Наявність організованої злочинності у суспільстві вкрай негативно впливає на його розвиток, деформуючи суспільні відносини. На сьогодні вже ні у кого не викликає сумнівів факт існування організованої злочинності в нашому суспільстві. Юристи, кримінологи, соціологи,

психологи намагаються знайти оптимальні шляхи подолання цього явища чи принаймні досягти звуження його впливу [5, с. 29]. Загалом поняття «злочинність» і «організована злочинність» перебувають у логічному зв'язку, відповідно як родове і видове поняття. Родове поняття «злочинність» в історико-правовому вимірі вказує на конкретно-історичний зміст злочинності як суспільно-небезпечного, історично-перехідного, мінливого соціально і кримінально-правового явища, її тенденції й закономірності з урахуванням минулого, сьогодення й майбутнього. Видове поняття «організована злочинність» в історико-правовому вимірі крім названих загальних родових властивостей злочинності вказує на специфічні, які виражаються у здатності цього системного протиправного явища в організаційний спосіб, завдяки корупції (мета корупційних діянь та діяльності – протиправним шляхом отримати доступ до влади й управління та насиллю ефективно протистояти єдиному державному механізму правової та інституційної протидії злочинності, використовуючи прогалини в кримінальному законодавстві та суперечності в системі правосуддя і кримінальної юстиції. Із застосуванням запропонованого поняття «організована злочинність» перспективним є вивчення причин виникнення, становлення, розвитку та трансформації організованої злочинності, які відбуваються у конкретному історичному, культурному і політичному середовищі [6, с. 72].

Щодо історії виникнення організованої злочинності. Злочинність існує у світі з найдавніших часів. Досить згадати історію зі Святого Писання про двох братів – Каїна і Авеля. Так само професійна злочинність існує з найдавніших часів – треба згадати грабіжницькі походи вікінгів та інших стародавніх народів у межах населеного світу (ойкумени) стародавніх часів. Деякі дослідники схильні вважати, що *організована злочинність* (у сучасному сенсі слова) народилася порівняно нещодавно. Вони вважають, що виникнення організованої злочинності – це якісно новий етап розвитку злочинного світу. Якщо «неорганізовані» злочинці є аутсайдерами суспільства, то діяльність сучасних мафіозі будується в основному по законах

бізнесу, і тому вони стали складовим елементом суспільної життєдіяльності. Загальновідомо, що головна мета злочинних організацій – отримання максимальної матеріальної вигоди. У зв'язку з цим доцільно пригадати концепцію М. Вебера про два принципово різних типи «жадання наживи». Авантюристське бажання збагачення (в тому числі шляхом грабежу і крадіжки) спостерігається з якнайдавніших часів. Однак, лише в умовах капіталістичного ладу складається відношення до багатства як до закономірного результату раціональної діяльності по виробництву споживчих благ. Проте насправді *організована злочинність* явище, яке теж існує з незапам'ятних часів. Досить згадати міжнародну работоргівлю, яка існувала аж до XIX ст. (Стародавня Греція, Стародавній Рим, Візантія, Османська імперія і т. д.), торгівлю наркотиками на державному рівні (опіумні війни в Китаї), торгівлю зброєю (існують згадки з часів Стародавньої Греції й Стародавнього Риму) і т. д. [7].

Міжнародні аспекти дослідження організованої злочинності. Сьогодні на пошуковій платформі Web of Science понад 7 тисяч наукових статей присвячених «organized crime» організованій злочинності. Окремі з них нами опрацьовані. Міркування іноземних авторів можуть бути корисними у здійсненні українських наукових досліджень та науково-педагогічній практиці при читанні лекцій чи проведенні семінарських занять.

Впродовж останніх 35 років відомий американський політичний економіст Томас К. Шеллінг стверджував, що організована злочинність – це суто монопольне підприємство. Його визначення цього явища залишається дуже впливовим і продовжує формувати основу багатьох визначень організованої злочинності й сьогодні [8]. Чеські дослідники на противагу конструктивістській традиції дослідження організованої злочинності (таким країнам як США, Велика Британія, Італія та Німеччина) наповнили цей напрям постсоціалістичним контекстом та виявили, що організована злочинність не набуває однієї єдиної форми, а радше складається з різних репрезентацій, які спираються на чотири основні типи дискурсу – юридичний, поліцейсько-

розвідувальний, кримінологічний та етнокультурний – що дозволяє тлумачити організовану злочинність як повсюдне явище [9]. Слід відзначити, що ми постійно акцентуємо на розробленні етнокультурного аспекту розроблення проблем злочинності. Звідси, нами пропонується створення науково-дослідних кримінологічних центрів на рівні окремих регіонів української держави (*див. наші наукові статті*) [10; 11].

Унікальністю нігерійської організованої злочинності є те, що глава держави веде свій народ, як бос мафіозної організації, а кожен уряд штату та кожен федеральний урядовий департамент діють як підрозділ мафіозної організації. Фактично, контроль над організованою злочинністю в Нігерії перетворюється на гонитву за власною тінню. Загалом, операції нігерійської організованої злочинності, здебільшого, зосереджені більше на сфері природних ресурсів та привласнення урядом національного пирога, ніж на бізнес-організованій злочинності. Слабкий уряд є способом дії організованої злочинності, і нігерійська організована злочинність вважає це доцільним [12].

Зосереджуючись на випадку Мексики, треба відзначити, що нездатність основних кримінологічних теорій пояснити значні аспекти організованої злочинності в цій країні пов'язана з їхньою недостатньо визначеною сферою застосування. Основні теорії аналізують організовану злочинність як явище, що виникає в суспільствах, що характеризуються високим рівнем внутрішнього миру, верховенством права та сильними державними інституціями. У Мексиці, країні, яка не дотримується цих умов, прояви організованої злочинності суперечать панівним теоретичним припущенням. Зібрані автором дані свідчать про те, що злочинні організації та поліцейські органи Мексики настільки взаємопов'язані, що їх неможливо відрізнити одну від одної. На жаль, загальноприйняті кримінологічні моделі дають мало уявлення про те, як інтерпретувати інформацію, зібрану в таких складних умовах. В країні, де змова поліції зі злочинними організаціями є правилом, чи повинні дослідники тлумачити розповіді поліцейських як розповіді упереджених «аутсайдерів»? [13].

Автори Я. Ескі та А Серджі наголошують, що концепція організованої злочинності динамічно розвивалася. Це соціальний конструкт або загальне поняття, що охоплює різні емпіричні прояви. Вчені часто пропонували класифікувати організовані злочинні групи на ті, що займаються «рекетом» або «управлінням», і ті, що займаються «транзитною злочинністю» або «торгівлею». Однак ці твердження ніколи не оцінювалися на рівні окремих кримінальних кар'єр. Автори розглядають дві основні мети: по-перше, перевірялися відмінності в кримінальних кар'єрах злочинців, що скоюють організовану злочинність, між історично різними контекстами організованої злочинності – порівнюючи Італію, яка насамперед відома рекетом організованої злочинності, з Нідерландами, які характеризуються більше транзитною злочинністю. Досліджувалися також відмінності між кримінальними кар'єрами злочинців, що скоюють організовану злочинність, народжених у різні десятиліття, що дозволяє виміряти відмінності в моделях правопорушень у змінних контекстах організованої злочинності через ширші соціальні зміни, враховуючи при цьому більш специфічні для кожної країни зміни в політиці правоохоронних органів та боротьби з організованою злочинністю [14].

Традиційні хронології історії організованої злочинності в Америці, як правило, зосереджуються на прибутті великої кількості італійських іммігрантів у 1890-х роках як каталізаторі організованої злочинності. Однак аналіз історії взаємодії між колоністами та корінними народами Північної Америки свідчить про набагато раніший початок організованої злочинної діяльності, що характеризується прибуттям різних груп іммігрантів, а саме голландських, французьких та британських колоністів на північний схід Америки [15].

Документування ОЗГ на території Харківського регіону за перше півріччя 2025 року у противазі з минулим роком. На 33,3% зменшилась кількість (з 18 до 12) організованих груп і злочинних організацій, діяльність яких припинено, при цьому на 100% більше (з 0 до 3) – з міжрегіональними

зв'язками, на 100% більше (з 0 до 3) – сформованих на етнічній основі, на 100% менше (з 1 до 0) – з корумпованими зв'язками. Виявлено на 16,7% більше (з 24 до 28) злочинів, учинених ОГ та ЗО у сфері обігу наркотичних засобів та психотропних речовин. Не направлялись до суду кримінальні провадження за ознаками ст. 255 КК України (створення злочинної організації) (минулого року – 1) та ст. 257 КК України (бандитизм) (як і торік). На 18,6% менше викрито учасників ОГ і ЗО (з 70 до 57), задокументовано скоєних ними злочинів на рівні 2024 року (з 93 до 93). Стосовно 9 (у 2024 році – 25) таких осіб застосовано запобіжний захід у вигляді тримання під вартою.

У рамках виконання ГУНП в Харківській області Комплексної регіональної Програми забезпечення публічної безпеки і порядку та протидії злочинності у першому півріччі 2025 р., слід відзначити, що керівництвом Головного управління Національної поліції в Харківській області постійно вживаються заходи з виконання Комплексної регіональної Програми забезпечення публічної безпеки і порядку та протидії злочинності на території Харківської області на 2020-2025 роки, затвердженої рішенням XXIII сесії Харківської обласної ради VII скликання від 27.02.2020 р. № 1199-VII (зі змінами).

Так, у першому півріччі 2025 р., з урахуванням дії на території області воєнного стану та виконання підрозділами поліції завдань із забезпечення його правового режиму, в рамках реалізації Програми в аспекті організованої злочинності здійснено наступні заходи:

Організувати розгляд стану протидії злочинності на координаційних нарадах та засіданнях міжвідомчих робочих груп правоохоронних органів у сфері реалізації кримінальної юстиції. Особливу увагу приділяти питанням протидії корупційним злочинам, злочинам, учиненим організованими групами, злочинам у сфері обігу наркотичних засобів; фактам порушення прав людини (п. 1.2 Програми).

30 квітня 2025 року керівництво ГУНП в Харківській області взяло участь у координаційній нараді керівників правоохоронних органів,

організованій Харківською обласною прокуратурою, з питань забезпечення законності та правопорядку в умовах воєнного стану. Створено постійно діючі міжвідомчі робочі групи з ключових напрямів: протидії організованій злочинності, торгівлі людьми, незаконному обігу наркотиків, злочинам проти активістів і журналістів, у бюджетній, земельній, господарській та екологічній сферах, а також злочинам із використанням зброї та вибухівки. Додатково налагоджено координацію щодо збереження речових доказів і арештованого майна.

Для ефективної протидії організованій злочинності вдосконалено штатну структуру ГУНП в Харківській області. У слідчому управлінні ГУНП створено відділ розслідування особливо тяжких злочинів та інших кримінальних правопорушень, що набули суспільного резонансу. З урахуванням завдань підрозділів поліції в умовах воєнного стану, у слідчому управлінні ГУНП також створено постійно діючу слідчо-оперативну групу з розкриття та розслідування злочинів, пов'язаних зі збройним конфліктом. Діє робоча група ГУНП зі збору інформації для здійснювання оцінювання загроз організованої злочинності та тяжких злочинів за методологією Європолу «SOCTA». У рамках антитерористичних заходів та заходів забезпечення правового режиму воєнного стану, для виявлення та затримання диверсійно-розвідувальних груп супротивника на території області встановлено 31 блокпост. За результатами вжитих заходів, направлено до суду 14 (у I-II кварталах 2024 року – 13) кримінальних проваджень відносно злочинних груп з ознаками організованості. Викриті угруповання діяли у сферах незаконного обігу наркотичних засобів, службової та господарської діяльності. Встановлено 72 (34) їх учасника, доведено їх участь в учиненні 148 (69) злочинів, з яких 128 (47) – тяжких та особливо тяжких, у тому числі: 38 наркозлочинів, 39 шахрайств, 1 крадіжка, 13 фактів привласнення або розтрати майна, 27 злочинів у сфері службової діяльності, у тому числі 14 фактів хабарництва, 5 злочинів у сфері господарської діяльності.

Сучасні пріоритети протидії організованій злочинності. С. В.

Безпалько, І. В. Кріцак, Д. М. Тимчишин, О. В. Маник відзначають, що аналіз значної кількості наукових джерел у сфері організованої злочинності дав змогу зосередитися на ідеологічних концептах цього феномена в українському науковому просторі. Автори підкреслюють потребу формування національних і транскордонних механізмів протидії, зокрема у сфері кібербезпеки, та наголошують на значенні виявлення злочинних доходів, латентних рівнів злочинності й узагальнення правової доктрини для вироблення стратегій боротьби. Корупція й організована злочинність у сучасних умовах становлять загрозу національним інтересам, а їх подолання можливе лише через комплексне поєднання зусиль державних органів, правоохоронних інституцій, громадянського суспільства та міжнародної спільноти [15].

Висновки. Дослідження історико-етно-культурних та міжнародних аспектів проблеми організованої злочинності на прикладі Харківського регіону свідчать, що це явище має глибоке історичне коріння та динамічно трансформується відповідно до соціально-економічних, політичних і культурних умов. Воно виявляється як у традиційних формах, так і в новітніх проявах, зокрема у сфері наркобізнесу, кіберзлочинності та корупційних практик. Комплексність організованої злочинності зумовлює необхідність багатовимірного підходу, що поєднує історико-правовий, етнокультурний та міжнародний контексти. Для Харківського регіону, який перебуває під особливим тиском війни, актуальним є інтегративний підхід, що ґрунтується на взаємодії науки й практики, координації правоохоронних органів, запровадженні європейських стандартів, а також урахуванні духовно-ціннісних засад кримінології. Досвід співпраці науковців і поліції, створення міжвідомчих робочих груп та використання інноваційних методик свідчить про реальну перспективу зміцнення національної та регіональної безпеки. Організована злочинність є глобальним викликом, що потребує об’єднання зусиль держав, інституцій та громадянського суспільства. Саме комплексність, яка поєднує правові, соціальні, культурні та духовні виміри, є ключем до формування ефективних стратегій протидії цьому феномену.

Список використаних джерел:

1. Колодяжний М. Г. Проблема комплексності у кримінології: аналіз минулого, оцінка теперішнього, погляд у майбутнє. *Вісник Кримінологічної асоціації України.* 2025. № 2 (35). С. 5–24.

2. Орлов Ю. В. Політико-кримінологічна теорія протидії злочинності : моногр. Харків : Діса Плюс, 2016. 655 с.

3. Кримінологія. Академічний курс / Кол. авторів ; за заг. ред. О. М. Литвинова. К.: Видавничий дім «Кондор», 2018. 588 с.

4. Поліція Харківщини та науковці підписали меморандум про співпрацю у сфері запобігання злочинності. 04 липня 2025 року. URL: https://hk.npu.gov.ua/news/politsiia-kharkivshchyny-ta-naukovtsi-pidpysaly-memorandum-pro-spivpratsiu-u-sferi-zapobihannia-zlochynnosti

5. Семикопний А. Д. Організована злочинність та організовані форми злочинності у науці й законодавстві сучасної України і УСРР доби непу: порівняльна характеристика. *Вісник Харківського національного університету внутрішніх справ.* 2009. № 44. С. 29–38.

6. Мельник П. О. Поняття «організована злочинність» у історико правовому вимірі. *Young Scientis. Юридичні науки.* 2018. № 4 (56). С. 69–73.

7. Організована злочинність. ВікіпедіЯ. URL: https://uk.m.wikipedia.org/wiki/%D0%9E%D1%80%D0%B3%D0%B0%D0%BD%D1%96%D0%B7%D0%BE%D0%B2%D0%B0%D0%BD%D0%B0_%D0%B7%D0%BB%D0%BE%D1%87%D0%B8%D0%BD%D0%BD%D1%96%D1%81%D1%82%D1%8C

8. Franț A. E. *The Difficulties in Regulating the Fight Against Transnational Organised Crime*. У *European Finance, Business and Regulation (EUFIRE 2020)*. 2020. Pp. 351–361. DOI: 10.17573/ipar.2013.1.a01

9. Střítecký V., Diviák T. From legal definitions to ethnic identities: Representations of organized crime in Czech policy documents. *Trends in Organized Crime. 2022. № 25* (1). pp. 63–85. https://doi.org/10.1007/s12117-021-

09434-4

10. Кріцак І. В. Формування кримінологічних інноваційних науково-дослідних центрів / лабораторій у практичних підрозділах Національної поліції України. Безпекова ситуація в Україні в умовах війни: стан, загрози, напрями забезпечення : зб. тез наук.-практ. кругл. столу (м. Київ, 26 вересня 2023 р.) / МВС України, ДНДІ МВС України, Н.-д. лаб. кримінол. дослідж. та проблем запобіг. злочинності. Київ, 2023. С. 274–281.

11. Лук'яненко С. В. Кримінолог правоохоронних органів – спеціаліст з питань запобігання та протидії злочинності. *Вісник Кримінологічної асоціації України*. 2024. № 33 (3). С. 135–142. https://doi.org/10.32631/vca.2024.3.11.

12. Ebbe O. N. I. Organized Crime in Nigeria. In D. Siegel & H. van de Bunt (Eds.), *Traditional Organized Crime in the Modern World: Responses to Socioeconomic Change* (Studies of Organized Crime. 2012. Vol. 11, pp. 169–188. Springer. https://doi.org/10.1007/978-1-4614-3212-8_9

13. Pereda V. *Why Global North criminology fails to explain organized crime in Mexico*. Theoretical Criminology. 2022. Vol. 26, Issue 4, pp. 620-640. DOI: 10.1177/13624806221104562

14. Eski Y., Sergi, A. August, Early Access). *Ethnic profiling of organised crime? A tendency of mafia-cation in the Netherlands*. Trends in Organized Crime. 2023. № 27(2), pp. 120–139. https://doi.org/10.1007/s12117-023-09502-4

14. Hobbs D., Antonopoulos G. A. The history of native Americans and the misdirected study of organised crime. *Global Crime. 2008. № 9* (1–2). Pp. 66–83. https://doi.org/10.1080/17440570701862774

15. Безпалько С. В., Кріцак І. В., Тимчишин Д. М., Маник О. В. Вироблення ефективної протидії / боротьби з організованою злочинністю: концептуальний аналіз. *Актуальні проблеми держави і права*. 2024. Вип. 101. С. 18–37. DOI: https://doi.org/10.32782/apdp.v101.2024.3.

ТУРЕНКО Олег
професор кафедри загальноправових дисциплін Донецького державного у ніверситету внутрішніх справ докт ор філософських наук, професор

НЕВИЗНАЧЕНІСТЬ ПОНЯТТЯ «ПРИМУС ДО ПРАЦІ» В ЗАКОНОДАВСТВІ УКРАЇНИ – ПОШУК ІНФОРМАЦІЙНО-НАУКОВИХ ДЕФІНІЦІЙ

Через рік після Помаранчевої революції Конституційний Суд України проголосив, що «Із конституційних принципів рівності і справедливості випливає вимога визначеності, ясності і недвозначності правової норми, оскільки інше не може забезпечити її однакове застосування, не виключає необмеженості трактування у правозастосовній практиці і неминуче призводить до сваволі» [1]. Через своє рішення, КСУ означив науково-інформаційну цінність й імперативність правових дефініцій в законодавчій техніки і застеріг, що недбала правова техніки може привести до соціального хаосу і кризи демократичних інституцій держави. Втім, як стверджує Олена Дашковська рівень легального визначення понять у вітчизняному законодавстві залишається низьким. «Заважає сприйняттю права як ефективного правового регулятора учасниками суспільних відносин і зайва доступність, що переходить у декларативність (малоінформативність) законодавчих дефініцій» [2, с. 18] – зауважує вчена. В своєму дослідженні вона надає визначення правової дефініції: «це нормативно-правовий припис, що розкриває зміст правового поняття шляхом указівки його основних юридично значущих ознак або елементів із метою забезпечення єдності правового регулювання» [Там само, с. 22]. Це визначення є відправним поняттям розвідки автора.

Можна констатувати, що в національному законодавстві дефінітивних прогалин існує доволі багато. Одним з кричущих прикладів є відсутність дефініції поняття статті 43 Конституції України заборони «примусу до праці» і подальше закріплення цієї норми в Кримінальному кодексі України (Ст. 172. «Грубе порушення законодавства про працю», Ст. 173. «Грубе порушення угоди про працю»[2]) та Кодексі Законів про Працю (Ст. 31. «Заборона вимагати виконання роботи, не обумовленої трудовим договором», Ст. 32. «Переведення на іншу роботу. Зміна істотних умов праці»).

У перерахованих нормативно-правових актах відсутнє визначення поняття «примус до праці» є суперечливим. Воно як поняття примусової чи обов'язкової праці надається в Конвенції Міжнародної організації праці №29 (1930 р.), яка в 1996 р. була підтверджена постановою №9 Пленума Верховного Суд України, – «термін примусова чи обов'язкова праця означає будь-яку роботу чи службу, що її вимагають від якої-небудь особи під загрозою якогось покарання і для якої ця особа не запропонувала добровільно своїх послуг» [3]. Конвенція також надає перелік п'яті випадків, які не включають в собі примусову працю: a) праця або служба, що вимагається за законами про обов'язкову військову службу; b) громадянська праця в межах цивільних обов'язків; c) праця по вироку суду; d) праця що виконується внаслідок надзвичайних обставин війни або лиха, або їх загрози; e) роботи громадського характеру, які виконуються на користь громади [Там само]. Слід зазначити, що дефініція Конвенції №29 є доволі поверховою і ймовірно мала на увазі процедуру первісного наймання працівника на роботу, прямолінійної

2 Цікаве також розглянути сенс терміну «грубе», адже виникає питання: А якщо Судом буде доведено що проступок не грубий, а делікатний, то визначена дія – порушення угоди законодавства про працю, не буде вважатися правопорушенням?

відкритості і примітивності намірів роботодавця. Таким чином, дефініцію Конвенції №29 можна вважати не повною і рудиментарною, той яка не враховує соціально-економічної, управлінської і правової динаміки,

багатоукладності соціально-економічних реалій, що не має комплексного підходу до вирішення можливих конфліктів.

Не співвідношення сенсів проголошених Конвенції №29 з новими соціально-економічними реаліями надала Загальна декларація прав людини Прийнятої і проголошеної резолюцією 217 А (III) Генеральної Асамблеї ООН від 10 грудня 1948 р. Декларація Ст. 23.п.3. затвердила, що «Кожний працюючий має право на справедливу і задовільну винагороду, яка забезпечує гідне людини існування, її самої та її сім'ї, і яка в разі необхідності доповнюється іншими засобами соціального забезпечення» [4]. Текст означив актуалізацію справедливої нагороди за працю яка не можлива в процесі примусу і визнав працю соціальною основою гідного життя.

В 1957 р. МОП випустила Конвенцію про скасування примусової праці N 105, яку було ратифіковано в 2000 р. Стаття 1 Конвенції додала до форм примусу наступні випадки: а) засобу політичного впливу чи виховання або як засобу покарання за наявність чи за висловлювання політичних поглядів, чи ідеологічних переконань, протилежних усталеній політичній, соціальній, чи економічній системі; б) як метод мобілізації і використання робочої сили для потреб економічного розвитку; в) як засіб підтримання трудової дисципліни; г) як засіб покарання за участь у страйках; д) як захід дискримінації за ознаками расової, соціальної і національної приналежності чи віросповідання [5]. Тобто Конвенція № 105 визнавала що одним з порушників заборони на примус праці є державні інституції та політичні організації, які дисциплінарно можуть впливати на переконання робітників, що є прямим посяганням на права і свободи людини. До цього визнавалось що примус до праці міг привести до рабства, боргової кабали і кріпацької залежності, тобто прирівнюється до «злочинів проти людяності» (поневолення). Втім, не зважаючи на розширення обріїв загроз і актуалізації соціальних конфліктів нової дефініції «примусова праця» Конвенція №105 не надала.

Відтак, в національному законодавстві дефініція «примус до праці» залишається не чіткою, вона не розкриває всіх можливих механізмів примусу

і не з'ясовує поняття труд. Професійна кваліфікація КЗзПУ не визначає різноманітність видів, змісту, способу, характеру праці (найману та приватну, індивідуальну та колективну, фізичну та розумову, рівень кваліфікації, умови праці тощо) і є лише переліком занять. Тому певно таку масштабну роботу слід зробити. Що ж до поняття примусу, то частково це поняття включено в терміні «уразливий стан особи» (сукупність обставин: вік, стан здоров'я, психологічний стан тощо, які роблять людину більш підданою ризику вчинення щодо неї примушування, експлуатації, омани тощо). Але останнє поняття застосовується ККУ лише в обмеженій кількості статей і в змістовній формі теж потребує уточнення [6]. Ту ж характеристику заслуховує поняття «примус» яке сенсово вагається між термінами «примус», «примушування» та «насильство» [7]. Відтак, поняття «примус до праці» не має наукового визначеності й імовірніше є інформаційно-правовою метафорою, поняттям що є потенційною загрозою консолідації українського суспільства в стані війни.

Список використаних джерел:

1. Рішення Конституційного Суду України у справі за конституційним поданням 51 народного депутата України щодо відповідності Конституції України (конституційності) положень статті 92, пункту 6 розділу X «Перехідні положення» Земельного кодексу України (справа про постійне користування земельними ділянками) від 22 вересня 2005 року № 5-рп/2005. https://zakon.rada.gov.ua/laws/show/v005p710-05#Text

2. Дашковська О. Р. Правові дефініції як різновид нормативних приписів. Вісник Національної академії правових наук України. 2012. Вип. 3. С. 16–23. https://dspace.nlu.edu.ua/bitstream/123456789/3918/1/Dashkovska_16.pdf

3. Конвенція МОП про примусову чи обов'язкову працю : міжнародний документ від 28 червня 1930 р. № 29. URL: http://zakon4.rada.gov.ua/laws/show/993_136.

4. Загальна декларація прав людини. Прийнята і проголошена

резолюцією 217 А (III) Генеральної Асамблеї ООН від 10 грудня 1948 р. https://zakon.rada.gov.ua/laws/show/995_015#Text

5. Конвенцію про скасування примусової праці N 105 (993_013). URL: https://zakon.rada.gov.ua/laws/show/993_013#Text

6. Гайдулін О. О. Інтерпретація поняття «уразливий стан особи»: законодавчі визначення та сучасний правовий дискурс. Часопис Київського інституту права. 2018. №2. С. 40-44. https://kup.edu.ua/doc/chasopis/chasopis_2018_2.pdf

7. Собко Г.М. Психічне насильство: кримінологічні та кримінально-правові засади протидії: монографія. Херсон. : «Гельветика». 2020. 484 с.

УДОД Андрій
завідувач кафедри кримінального права та кримінології факультету підготовки фахівців для органів досудового розслідування Національної поліції України Донецького державного університету внутрішніх справ кандидат юридичних наук, доцент

ФОРМУВАННЯ СИСТЕМИ КРИМІНАЛЬНО-ПРАВОВОГО ЗАХИСТУ ОСІБ, ЯКІ ПОСТРАЖДАЛИ ВІД ЗБРОЙНОЇ АГРЕСІЇ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ

Повномасштабна збройна агресія рф проти України, що розпочалася 24 лютого 2022 року, спричинила безпрецедентні гуманітарні наслідки та поставила перед українською правовою системою низку викликів, пов'язаних із забезпеченням належного захисту прав і свобод мільйонів громадян, які постраждали від воєнних дій. Серед таких осіб – учасники бойових дій, ветерани війни, цивільні особи, які зазнали поранень, втратили житло чи майно, внутрішньо переміщені особи, родини загиблих захисників, а також

особи, які пережили окупацію, катування, депортацію та інші форми насильства з боку агресора. У цьому контексті формування ефективної системи кримінально-правового захисту постраждалих від збройної агресії набуває стратегічного значення не лише як інструмент відновлення справедливості, а й як необхідна умова збереження соціальної стабільності, довіри до держави та гарантування гідного життя для тих, хто відстоює незалежність України або став жертвою воєнних злочинів.

Перш за все, варто визначити коло суб'єктів, які потребують особливого кримінально-правового захисту в умовах збройного конфлікту. Відповідно до чинного законодавства України, до них належать військовослужбовці Збройних Сил України, Національної гвардії, інших військових формувань, які брали безпосередню участь у бойових діях та отримали статус учасника бойових дій або ветерана війни; особи, які проходили альтернативну службу в зоні бойових дій; цивільні особи, які постраждали внаслідок обстрілів, бомбардувань, мінування територій; внутрішньо переміщені особи, які були змушені залишити місця свого постійного проживання; члени сімей загиблих або зниклих безвісти захисників України; особи, які перебували в полоні, піддавалися катуванням, депортації або примусовій мобілізації на окупованих територіях [3]. Кожна з цих категорій має специфічні потреби у правовому захисті, що обумовлює необхідність диференційованого підходу при формуванні відповідних кримінально-правових механізмів та практики правозастосування.

Аналіз чинного законодавства України свідчить про наявність певних правових підстав для посиленого захисту постраждалих від збройної агресії, проте існуюча система є фрагментарною і потребує суттєвого вдосконалення. Кримінальний кодекс України передбачає кваліфікуючі ознаки для окремих складів злочинів, вчинених щодо військовослужбовців або осіб, які мають особливий статус, однак відсутні спеціальні норми, які б комплексно врегульовували кримінальну відповідальність за злочини, спрямовані проти ветеранів війни, цивільних постраждалих, родин загиблих захисників [4].

Закон України "Про статус ветеранів війни, гарантії їх соціального захисту" встановлює широкий перелік пільг та гарантій, проте механізми кримінально-правової відповідальності за порушення цих прав є недостатньо розробленими [3]. Окрему проблему становить необхідність повноцінної імплементації норм міжнародного гуманітарного права, зокрема положень Женевських конвенцій 1949 року та Римського статуту Міжнародного кримінального суду, які передбачають покарання за серйозні порушення прав цивільного населення під час збройних конфліктів [1].

Практика застосування кримінального законодавства в умовах війни виявила низку типових злочинів, які вчиняються щодо осіб, що постраждали від збройної агресії. Серед них особливе місце посідають шахрайські схеми, пов'язані з незаконним заволодінням коштами, призначеними для виплати допомоги постраждалим, привласнення гуманітарної допомоги, використання підроблених документів для отримання пільг та компенсацій. Нерідкими є випадки вчинення насильницьких злочинів, зокрема побоїв, погроз, умисних тілесних ушкоджень щодо ветеранів війни або членів їхніх сімей. Окремої уваги потребують злочини, пов'язані з порушенням трудових прав ветеранів, дискримінацією за ознакою участі в бойових діях, незаконним звільненням з роботи осіб, які мають пільги відповідно до законодавства. Крім того, поширеними є корупційні діяння посадових осіб органів влади та місцевого самоврядування, які перешкоджають реалізації прав постраждалих або зловживають своїм службовим становищем під час розподілу матеріальної допомоги, надання житла, оформлення документів. Усі ці злочини не лише завдають шкоди конкретним особам, а й підривають довіру суспільства до держави, послаблюють моральний дух нації та створюють передумови для соціальної напруженості.

У цьому контексті важливим є звернення до досвіду інших держав у формуванні систем захисту осіб, які постраждали від збройних конфліктів. Зокрема, досвід Ізраїлю демонструє ефективність створення спеціалізованих органів, які займаються розслідуванням злочинів проти ветеранів та

постраждалих, а також передбачає підвищену відповідальність за злочини щодо осіб, які мають статус захисників держави. Хорватія після завершення війни за незалежність запровадила спеціальні програми захисту прав внутрішньо переміщених осіб і ветеранів, включаючи механізми кримінального переслідування за військові злочини та злочини проти цивільного населення. Досвід країн-членів НАТО свідчить про важливість інтеграції психологічної підтримки ветеранів у систему правосуддя, зокрема шляхом урахування посттравматичного стресового розладу як пом'якшуючої обставини при призначенні покарання, а також створення спеціалізованих судів, які враховують специфіку психологічного стану учасників бойових дій. Такий підхід дозволяє не лише забезпечити справедливе покарання, а й сприяти соціальній реабілітації та реінтеграції ветеранів у суспільство [1].

Окрему увагу слід приділити проблемі балансу між кримінально-правовим захистом постраждалих від збройної агресії та забезпеченням справедливої кримінальної відповідальності самих ветеранів війни, які можуть вчиняти правопорушення під впливом посттравматичного стресового розладу, адаптаційних розладів або інших психологічних наслідків участі в бойових діях. З одного боку, держава має гарантувати особливий захист тим, хто ризикував життям заради національної безпеки, з іншого – не може допустити безкарності за вчинення тяжких злочинів. У цьому контексті доцільним є запровадження спеціальних механізмів оцінки психічного стану ветеранів на момент вчинення злочину, обов'язкового призначення судово-психіатричної експертизи у справах за участю осіб, які мають статус учасника бойових дій, а також розширення можливостей для застосування примусових заходів медичного характеру, альтернативних покарань, пробаційних програм, орієнтованих на реабілітацію. Важливо також передбачити у Кримінальному кодексі України окрему пом'якшуючу обставину – вчинення злочину особою, яка перебуває у стані психологічної дезадаптації внаслідок участі в бойових діях, що дозволить суддям більш гнучко підходити до призначення покарання з урахуванням індивідуальних обставин справи.

З урахуванням викладеного, формування ефективної системи кримінально-правового захисту осіб, які постраждали від збройної агресії, потребує комплексного підходу та внесення змін до кримінального законодавства України. По-перше, доцільно запровадити до Кримінального кодексу окрему кваліфікуючу ознаку – вчинення злочину щодо учасника бойових дій, ветерана війни, внутрішньо переміщеної особи або члена сім'ї загиблого захисника України, що передбачатиме посилення відповідальності за такі діяння. По-друге, необхідно криміналізувати окремі форми зловживань, пов'язаних із незаконним заволодінням коштами та майном, призначеними для допомоги постраждалим від війни, шляхом введення спеціальних складів злочинів або посилення санкцій за існуючі злочини проти власності та у сфері службової діяльності. По-третє, слід передбачити спеціальні норми, які регулюють кримінальну відповідальність за дискримінацію ветеранів війни у сфері праці, освіти, охорони здоров'я, надання соціальних послуг. По-четверте, важливо продовжити імплементацію норм міжнародного гуманітарного права щодо захисту цивільного населення під час збройних конфліктів та забезпечити ефективне розслідування і покарання за воєнні злочини [2]. По-п'яте, необхідно створити спеціалізовані підрозділи в органах досудового розслідування та прокуратури, які займатимуться виключно справами про злочини проти постраждалих від збройної агресії, забезпечити їх належною матеріально-технічною базою, кваліфікованими кадрами та можливостями міжнародної співпраці для притягнення винних до відповідальності навіть за межами України.

Загалом, формування системи кримінально-правового захисту осіб, які постраждали від збройної агресії Російської Федерації, є не лише юридичною, а й морально-етичною та політичною необхідністю. Кримінальне право в цьому контексті виступає не просто інструментом покарання, а механізмом відновлення справедливості, засобом соціальної підтримки та символом визнання подвигу і страждань мільйонів українців. Лише за умов системного підходу, міжвідомчої координації, запозичення найкращих

міжнародних практик, постійного моніторингу ефективності законодавства та його своєчасного вдосконалення можливе створення дієвої системи кримінально-правового захисту, яка не лише каратиме винних, а й відновлюватиме порушені права, сприятиме реінтеграції постраждалих у суспільство та зміцнюватиме віру громадян у справедливість і силу української держави.

Список використаних джерел:

1. Пінчук Р. С., Письменна О. П. Правовий захист учасників бойових дій та ветеранів війни. *Актуальні проблеми держави і права : зб. наук. пр. Вип. 83.* Одеса : Гельветика, 2019. С. 175--183.

2. Мартинюк О. В., Ципцюра В. В., Безносюк А. І. Щодо правового захисту цивільного населення під час збройного конфлікту у світлі імплементації норм міжнародного гуманітарного права. *Науковий вісник Ужгородського національного університету. Серія: Право. 2025. Вип. 88.* С. 82--89.

3. Про статус ветеранів війни, гарантії їх соціального захисту : Закон України від 22.10.1993 № 3551-XII. *Відомості Верховної Ради України.* 1993. № 45. Ст. 425.

4. Кримінальний кодекс України : Закон України від 05.04.2001 № 2341-III. *Відомості Верховної Ради України.* 2001. № 25--26. Ст. 131.

ФЕДОРЧАК Ірина
старший викладач кафедри кримінального права та кримінології факультету підготовки фахівців для органів досудового розслідування Національної поліції України Донецького державного університету внутрішніх справ

СНІЖКО Софія

курсантка факультету підготовки фахівців для органів досудового розслідування Національної поліції України Донецького державного університету внутрішніх справ

ЗАКОНОДАВЧЕ РЕГУЛЮВАННЯ ДОСТУПУ ДО ІНФОРМАЦІЙНИХ РЕСУРСІВ У КОНТЕКСТІ ПРОТИДІЇ ЗЛОЧИННОСТІ

У сучасних умовах глобалізації та збройного конфлікту інформаційна сфера стає одним із ключових полів протидії організованій злочинності. Доступ до інформаційних ресурсів для правоохоронних органів виступає стратегічним інструментом, адже саме інформація дозволяє виявляти злочинні мережі, відстежувати фінансові потоки, контролювати переміщення зброї та інших заборонених предметів. Однак ефективність цього процесу безпосередньо залежить від того, наскільки чітко і збалансовано врегульовані правові засади доступу до таких даних.

Українське законодавство формує багаторівневу систему регулювання доступу до інформації. На конституційному рівні визначено право кожного на захист особистих даних та гарантії недоторканності приватного життя [1]. Разом із тим Конституція України покладає на державу обов'язок забезпечувати громадську безпеку та протидіяти злочинності, що створює правову основу для спеціальних механізмів доступу до інформаційних ресурсів у правоохоронних цілях.

Базовими законами в цій сфері є Закон України «Про інформацію» [2], який визначає загальні принципи доступу та обмеження щодо інформації, Закон України «Про доступ до публічної інформації» [3], що регламентує прозорість діяльності органів влади, а також Закон України «Про захист персональних даних» [4], який встановлює вимоги до обробки чутливої інформації про фізичних осіб. Окреме місце займають норми Кримінального

процесуального кодексу України [5], де закріплено інструменти тимчасового доступу до речей і документів, можливості вилучення електронних носіїв, здійснення негласних слідчих (розшукових) дій.

Закон України «Про Національну поліцію» [6] та Закон України «Про оперативно-розшукову діяльність» [7] визначають межі повноважень правоохоронних органів у сфері збору інформації. Важливим є також міжнародний вимір: Україна імплементує стандарти Європейської конвенції з прав людини та керується практикою ЄСПЛ, що вимагає суворої відповідності принципам законності, необхідності й пропорційності у втручанні в приватне життя.

В умовах збройного конфлікту роль інформаційних ресурсів зростає в рази. Схеми організованої злочинності стають більш мобільними, використовують транскордонні канали, криптовалютні транзакції, а також приховані мережі комунікацій. Це зумовлює необхідність оперативного доступу до різних видів інформації — від телекомунікаційних даних і фінансових звітів до митних реєстрів і даних про переміщення транспортних засобів. Затримка у кілька днів може нівелювати результативність розслідування, адже злочинні угруповання швидко змінюють маршрути, канали чи фінансові інструменти.

Разом із тим розширення доступу до інформаційних ресурсів супроводжується серйозними ризиками. Порушення таємниці приватного життя, зловживання з боку посадових осіб, несанкціонований обмін даними або витоки можуть мати не лише правові, а й політичні та соціальні наслідки. Тому законодавче регулювання має передбачати надійні механізми контролю. Йдеться про багаторівневу систему запобіжників: внутрішній контроль у правоохоронних структурах, прокурорський нагляд, судовий дозвіл на доступ до певних категорій інформації, а також парламентський і громадський контроль.

Окремим завданням є розбудова міжвідомчих платформ обміну інформацією. В Україні вже запроваджуються елементи інтегрованих баз

даних між поліцією, прикордонною службою, митницею та фінансовим моніторингом. Проте законодавство має більш чітко врегулювати питання рівнів доступу, розмежування компетенцій та захисту даних. Ідеальною моделлю є створення єдиного інформаційного середовища з прозорими процедурами авторизації та відповідальності за зловживання.

Міжнародний досвід (зокрема ЄС та США) показує, що ефективне законодавче регулювання поєднує два елементи: високий рівень цифрової інтеграції інформаційних систем і жорсткий механізм демократичного контролю. Україна поступово наближається до таких стандартів, проте війна висуває додаткові виклики. Це вимагає внесення змін до чинних законів, які б дозволили діяти швидко, не виходячи за межі міжнародних зобов'язань у сфері прав людини.

Отже, законодавче регулювання доступу до інформаційних ресурсів у протидії злочинності має ґрунтуватися на трьох ключових принципах: оперативність прийняття рішень, правова визначеність і прозорість процедур та надійний захист прав людини. Саме таке поєднання забезпечить ефективність боротьби з організованою злочинністю, особливо в умовах збройного конфлікту, коли національна безпека потребує максимально злагоджених і легітимних дій держави.

Список використаних джерел:

1. Конституція України від 28 червня 1996 р. № 254к/96-ВР // URL https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text (дата звернення: 26.09.2025).

2. Закон України «Про інформацію» від 2 жовтня 1992 р. № 2657-XII // URL https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 26.09.2025).

3. Закон України «Про доступ до публічної інформації» від 13 січня 2011 р. № 2939-VI // URL https://zakon.rada.gov.ua/laws/show/2939-17#Text (дата звернення: 26.09.2025).

4. Закон України «Про захист персональних даних» від 1 червня 2010 р. № 2297-VI // URL https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 26.09.2025).

5. Кримінальний процесуальний кодекс України від 13 квітня 2012 р. № 4651-VI // URL https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 26.09.2025).

6. Закон України «Про Національну поліцію» від 2 липня 2015 р. № 580-VIII // URL https://zakon.rada.gov.ua/laws/show/580-19#Text (дата звернення: 26.09.2025).

7. Закон України «Про оперативно-розшукову діяльність» від 18 лютого 1992 р. № 2135-XII // URL https://zakon.rada.gov.ua/laws/show/2135-12#Text (дата звернення: 26.09.2025).

ФІГУРА Віталій
ад'юнкт відділу ад'юнктури і докторантури Національної академії Державної прикордонної служби України імені Богдана Хмельницького

API/PNR, ЯК ОДНЕ З ТЕХНОЛОГІЧНИХ РІШЕНЬ У СИСТЕМІ ПРОТИДІЇ ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ

Застосування технологічних рішень у протидії організованій злочинності є міждисциплінарною проблемою, розв'язанню якої присвячено роботи дослідників - фахівців різних галузей наук. Елементи цифрової трансформації і модифікації форм діяльності організованої злочинності, поза сумнівом, обумовлюють необхідність пошуку та впровадження нових технологічних рішень запобігання та протидії цьому виду злочинності.

Нами досліджується одне з них - це система попередньої інформації про пасажирів (API) та реєстраційних записів пасажирів (PNR) (далі - система

API/PNR).

16 вересня 2020 року розпорядженням Кабінетом Міністрів України схвалено Стратегію боротьби з організованою злочинністю» [1]. Діяльність Державної прикордонної служби, як державного органу, що бере участь у боротьбі з організованою злочинністю в межах виконання інших основних функцій у контексті даного документу підлягає відповідному інформаційно-аналітичному забезпеченню. Елементом такого забезпечення є розроблення та впровадження єдиної захищеної інформаційної системи, що забезпечить оперативний доступ суб'єктів боротьби з організованою злочинністю до державних баз даних, відповідний обмін даними. У межах міжнародного співробітництва у сфері боротьби з організованою злочинністю передбачене здійснення спільних оперативних заходів і транскордонних операцій щодо припинення організованої злочинної діяльності та запобігання їй.

Водночас, відповідно до ст.19 Закону України «Про організаційно-правові основи боротьби з організованою злочинністю» з метою вирішення завдань боротьби з організованою злочинністю правом збирати, накопичувати і зберігати інформацію про події і факти, що свідчать про організовану злочинну діяльність, її причини та умови, про осіб, які беруть участь в організованій злочинній діяльності наділені підрозділи Служби безпеки України та підрозділи органів Національної поліції. З цією метою в Міністерстві внутрішніх справ України і Службі безпеки України створюються централізовані банки даних [2].

В умовах війни та у післявоєнний період державна політика інформаційного забезпечення протидії організованій злочинності повинна включати комплекс заходів, методів, засобів та різноманітних технологічних рішень щодо створення, функціонування та використання інформаційних систем.

З урахуванням цього постає питання, в межах яких норм законодавства буде здійснюватися збирання, обробка, зберігання та аналіз великих масивів даних API/PNR для більш ефективної протидії організованій злочинності.

В контексті вищевикладеного, відповідь на це питання полягає у нормативному закріпленні права Державної прикордонної служби України на використання даних API/PNR на рівні окремого закону. Подальша інституціоналізація державної політики у сфері застосування інформаційного забезпечення протидії організованій злочинності може виглядати наступним чином - окреслення цілей і принципів, де інструментами реалізації виступатиме:

законодавство (закони, міжнародні угоди та договори);

інститути (Міністерство внутрішніх справ України, Служба безпеки України, Державна прикордонна служба України);

міжнародні організації на кшталт (EUROPOL, ICPO, ICAO, FRONTEX та інші);

інформаційно-аналітичні системи (національні та міжнародні) [3].

Відповідно до міжнародних домовленостей дана система API/PNR повинна була розпочати своє функціонування в міжнародних авіаційних пунктах пропуску. Основною метою впровадження даної системи є результативна протидія організованій транскордонній злочинності на державному кордоні, зокрема виявлення потенційних терористів, осіб, що нелегально переправляються через державний кордон, наркокур'єрів та інших причетних до протиправної діяльності осіб. Даною системою користуються більше 50 країни світу на різних континентах і вона вже продемонструвала свою високу ефективність.

API/PNR виступає у ролі одного з ефективних технологічних рішень і у сфері авіаційної безпеки і у сфері прикордонної безпеки. Її повноцінне функціонування також дозволить правоохоронним органам відстежувати транскордонні переміщення і формувати профілі ризиків для проведення превентивних заходів.

Актуальність даної системи з часом тільки зростає, адже організовані злочинні угрупування в більшості взаємодіють зі терористичними структурами; виникає гостра необхідність міжвідомчої взаємодії, координації

і міжнародний обмін даними.

На нашу думку сама суть поєднання інструментів державної політики у тісній взаємодії з технологічними можливостями системи API/PNR забезпечить абсолютно новий рівень аналітичної підтримки правоохоронних органів України.

Саме такі технологічні рішення, побудовані на інтеграції національних і міжнародних інформаційних ресурсів та раціональному використанні системи API/PNR, забезпечать ефективність протидії організованій злочинності.

Список використаних джерел:

1. Про організаційно-правові основи боротьби з організованою злочинністю : Закон України від 30.06.1993 р. № 3341-XII. URL: https://zakon.rada.gov.ua/laws/show/3341-12#Text (дата звернення: 10.09.2025).

2. Про схвалення Стратегії боротьби з організованою злочинністю : розпорядженням Кабінету Міністрів України від 16.09.2020 р. № 1126-р. URL: https://zakon.rada.gov.ua/laws/show/1126-2020-р#Text (дата звернення: 10.09.2025).

3. Філіппов С.О. Протидія транскордонній злочинності: глобальний контекст і реалії України. Одеса. Фенікс. 2019. С. 384

ШЛЯХОВИЙ Ярослав
курсант 2 курсу Навчально-наукового інституту №2 Харківського національного університету внутрішніх справ, рядовий поліції

Науковий керівник:
ГРІДІНА Наталія
доцент кафедри адміністративної діяльності курсу Навчально-наукового

інституту № 3 Харківського національного університету внутрішніх справ доктор філософії

ЗАБЕЗПЕЧЕННЯ ПРАВ ЛЮДИНИ В АДМІНІСТРАТИВНІЙ ПРАКТИЦІ ПОЛІЦІЇ ПРИ ВПРОВАДЖЕННІ ІННОВАЦІЙНИХ ЗАСОБІВ КОНТРОЛЮ ТА МОНІТОРИНГУ В УМОВАХ ВОЄННОГО СТАНУ

Впровадження інноваційних засобів контролю та моніторингу мають, в першу чергу,забезпечувати безпеку громадян в будь-яких обставинах. Сучасні виклики безпеки, спричинені збройною агресією проти України. Тому впровадження засобів контролю і моніторингу,зокрема систем відеоспостережень,біометричної ідентифікації, безпілотних літальних апаратів та інших інновації є необхідним заходом сьогодення. У таких умовах особливо важливим стає завдання ефективно поєднати такі заходи та гарантування прав і свобод людини і громадянина.

Положення, які є незмінними і непорушними навіть в умовах воєнного стану, закріплює Конституція України,а саме в статті 64. Європейська Конвенція про захист прав людини і основоположних свобод 1950 року (ст. 15) передбачає можливість тимчасового обмеження окремих прав задля захисту національної безпеки та громадського порядку. Це створює складну колізію між необхідністю оперативного реагування на загрози та збереженням демократичних стандартів [2].

Зокрема,у Верховній Раді був зареєстрований законопроект №11031,що включає в себе ключову ініціативу запровадження єдиної системи відеомоніторингу безпекової ситуації.У законопроекті запропоновано встановити єдині стандарти побудови та функціонування систем відеомоніторингу стану публічної безпеки центрального, регіонального та місцевого рівнів, порядок доступу до інформації, а також складу відеоданих,

метаданих, аналітичних даних, відеоархівів, сигналів тривог, що створюються ними. Забезпечення єдиних правил інформаційного обміну та захисту персональних даних на державному, регіональному та місцевому рівнях через єдиний інформаційний простір з урахуванням розмежування прав доступу до інформації. Саме такі кроки допомагають знайти компроміси для вирішення таких питань [1].

Так в період дії воєнного стану поліція, з урахуванням досвіду, має право і буде здійснювати посилений нагляд, контроль, профілактичні заходи. Використання нових технологій, наприклад систем відеоспостереження зі скануванням облич, аналітичних платформ – тільки посилює її можливості. І одночасно наражає на небезпеку права людей на приватне життя, на рівність, на недопущення зловживання.

Адміністративно-правові засоби забезпечення прав людини у цьому контексті мають включати: обов'язкову фіксацію підстав для застосування інноваційних засобів. Універсальним інститутом захисту законодавчо закріплених прав та інтересів громадян є адміністративне судочинство. Серед інструментів,які допомагаю громадянам відстоювати свої права у разі їх порушення є адміністративне оскарження. Перевагами адміністративного порядку оскарження, порівняно з оскарженням у судовому порядку, є спрощена процедура подання адміністративної скарги та оперативний розгляд скарги, що в кінцевому результаті повинно спростити комунікацію з органами державної влади для гарантування прав і свобод громадян [4].

Прикладом таких інновацій можна навести системи відеоспостереження з використанням штучного інтелекту. Такі дані можуть бути використані у кримінальному та адміністративному судочинстві. Штучний інтелект може швидко проаналізувати відео- чи аудіоматеріали та надати свою оцінку, визначивши, що саме відбулося й чи є задокументована подія порушенням закону. Теоретично це може зекономити час на ведення слідства та зменшити ризик людського суб'єктивізму. Зокрема, прецедент розгортання технологій масового відеоспостереження із ШІ мав місце у Франції напередодні Літніх

Олімпійських ігор 2024 року в Парижі [3] .

Також не слід нехтувати ризиками через використання ШІ. Вони також присутні у сфері предиктивної аналітики. Системи відеоспостереження на базі ШІ також можуть страждати від упередженості до деяких етнічних груп, ідентифікуючи їх на відео та некоректно інтерпретуючи їх поведінку. В технологіях ШІ існують проблеми упереджень та точності щодо нерепрезентативних даних, у такий спосіб створюючи прецеденти для посилення дискримінаційних ризиків. Хоча зібрані такими системами дані ШІ може систематизувати у базу даних й використовувати їх як для самонавчання та самовдосконалення, так і для ідентифікації суб'єктів, що вже раніше порушували закон. Таким чином, використання ШІ у системах відеоспостереження є корисним для розвитку предиктивної аналітики.

Список використаних джерел:

1. Міністерство внутрішніх справ України. У Верховній Раді зареєстровано законопроект № 11031 «Про відеомоніторинг стану безпеки», розроблений МВС України. URL: https://mvs.gov.ua/news/u-verxovnii-radi-zarejestrovano-zaknoprojekt-11031-pro-videomonitoring-stanu-bezpeki-rozroblenii-mvs-ukrayini

2. Legal Development Network. Які права можуть і НЕ можуть бути обмежені під час воєнного стану. 21.05.2025. URL: https://ldn.org.ua/consultations/yaki-prava-mozhut-i-ne-mozhut-buty-obmezheni-pid-chas-voiennoho-stanu/

3. Центр Дністрянського. Штучний інтелект та відеоспостереження: як запобігти ризикам в Україні. 24.09.2024. URL: https://dc.org.ua/news/shtuchnyy-intelekt-ta-videosposterezhennya-yak-zapobigty-ryzykam-v-ukrayini

4. Мельниченко Б. Адміністративно-правові засоби захисту прав, свобод та інтересів приватних осіб у сфері публічного управління // Вісник Національного університету "Львівська політехніка". Серія: Юридичні науки.

— 2022. — № 2 (34). — С. 64-75.

СЕКЦІЯ 2.
РОЛЬ КРИМІНАЛЬНОГО АНАЛІЗУ У ПРОТИДІЇ ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ ПІД

ЧАС ЗБРОЙНОГО КОНФЛІКТУ.

ГОРОЦЮК Юлія
курсант 1 групи 3 курсу факультету №2 Львівського державного університету внутрішніх справ

Науковий керівник:
МОВЧАН Анатолій
професор кафедри оперативно-розшукової діяльності Львівського державного університету внутрішніх справ доктор юридичних наук, професор

ВИКОРИСТАННЯ КРИМІНАЛЬНОГО АНАЛІЗУ ДЛЯ ВИЯВЛЕННЯ ТА ДОКУМЕНТУВАННЯ ОРГАНІЗОВАНИХ ЗЛОЧИННИХ УГРУПОВАНЬ

Організована злочинність є одним із найнебезпечніших явищ сучасного суспільства, адже поєднує високий рівень конспірації, стійкі внутрішні зв'язки та систематичну злочинну діяльність, що завдає шкоди громадянам і державі. Традиційні методи розслідування не завжди дозволяють своєчасно виявляти такі структури, оскільки вони відзначаються мобільністю, адаптивністю та використанням складних схем ухилення від відповідальності.

У цих умовах кримінальний аналіз виступає ефективним інструментом протидії організованій злочинності. Це система методів збору, узагальнення й інтерпретації даних про злочини, осіб та їхні зв'язки, що ґрунтується на поєднанні інформації з оперативних джерел, відкритих даних (OSINT), статистики, експертиз і баз даних. Його перевага полягає у здатності виявляти приховані закономірності, аналізувати фінансові та комунікаційні зв'язки й відстежувати рух ресурсів, що дозволяє ефективно викривати діяльність організованих злочинних груп [1, с. 235].

У практичній діяльності кримінального аналізу вирізняють кілька

ключових завдань. По-перше, він застосовується для виявлення ознак існування злочинної мережі в тих випадках, коли окремі правопорушення здаються випадковими й не пов'язаними між собою: аналітичне дослідження дозволяє виявити взаємозв'язки та закономірності, що вказують на наявність стійкої організованої структури. По-друге, кримінальний аналіз є ефективним інструментом документування злочинної діяльності, оскільки дає змогу систематизувати докази, підтвердити їхню взаємну узгодженість і обґрунтовано встановити організований характер злочинів. По-третє, він дозволяє прогнозувати подальші дії угруповання, виявляти його вразливі точки та планувати заходи з нейтралізації.

Водночас організовані злочинні угруповання зазвичай мають складну ієрархічну структуру з чітким розподілом функцій між учасниками. Одні відповідають за фінансування, інші – за силовий захист, контроль каналів постачання чи відмивання коштів. Для належного документування діяльності таких угруповань недостатньо лише зафіксувати факт окремого злочину. Необхідно зібрати докази, що свідчать про системний характер їхньої діяльності, наявність керівного центру, координацію дій та підпорядкованість учасників. У цьому контексті кримінальний аналіз є незамінним інструментом, адже дає змогу поєднати розрізнені фрагменти інформації в цілісну аналітичну картину.

Особливу роль у кримінальному аналізі відіграють методи соціальних та мережевих досліджень. Використання графічних моделей для відображення зв'язків між особами дозволяє наочно показати структуру угруповання, виявити центральні фігури та визначити ступінь їхнього впливу на інші ланки. Такі методи широко застосовуються в міжнародній практиці та показують високу ефективність у боротьбі з організованою злочинністю. Окрім того, кримінальний аналіз активно інтегрує інформаційні технології, серед яких програмні комплекси для обробки великих масивів даних, системи штучного інтелекту для виявлення закономірностей, а також інструменти цифрової криміналістики [2, с. 100].

В Україні застосування кримінального аналізу стає дедалі актуальнішим у зв’язку з інтеграцією до європейського правового простору. Зокрема, у структурі Національної поліції створені підрозділи кримінального аналізу, які спеціалізуються на зборі та систематизації інформації про кримінальні процеси. У цьому контексті важливим є не лише технічне забезпечення, а й підготовка фахівців, які володіють аналітичними методиками та здатні мислити комплексно. Адже саме від рівня професіоналізму аналітиків залежить якість отриманих висновків і здатність правоохоронних органів своєчасно реагувати на загрози [3, с. 135].

Кримінальний аналіз відіграє важливу роль і у сфері міжнародного співробітництва. Організована злочинність не має кордонів, адже поширюється через фінансові транзакції, інтернет-простір, нелегальну торгівлю та міграційні процеси. Саме тому обмін аналітичною інформацією між правоохоронними органами різних держав є ключовим чинником ефективної протидії транснаціональним злочинним мережам. Європол, Інтерпол та інші міжнародні організації активно застосовують методи кримінального аналізу, а досвід співпраці з ними має важливе значення і для України.

Вагомою перевагою кримінального аналізу є його здатність працювати не лише з уже наявними фактами, а й у сфері прогнозування. Завдяки аналізу динаміки злочинності, поведінки підозрюваних, а також економічних і соціальних процесів, стає можливим передбачення появи нових злочинних угруповань, прогнозування напрямів їхньої діяльності та запобігання злочинам ще до їх фактичного вчинення. Такий підхід перетворює кримінальний аналіз на ключовий елемент сучасної концепції превентивної діяльності правоохоронних органів [4, с. 107].

Водночас застосування кримінального аналізу супроводжується низкою викликів. Серед основних проблем – обмежений доступ до необхідної інформації, вимоги щодо збереження конфіденційності даних, недосконаліть законодавства у сфері захисту персональної інформації, а також

нерівномірний рівень технічного забезпечення між регіональними підрозділами. Подолання цих труднощів є необхідною передумовою ефективної боротьби з організованою злочинністю, яка постійно вдосконалює свої методи та адаптується до нових умов.

Отже, у сучасних реаліях кримінальний аналіз постає одним із найважливіших інструментів виявлення та документування діяльності організованих злочинних угруповань. Він дає змогу не лише розкривати окремі злочини, а й формувати системне розуміння функціонування кримінальних мереж, визначати їхню структуру, керівників, а також фінансові й інформаційні зв'язки. Завдяки цьому правоохоронна діяльність переходить від реактивного до проактивного формату: аналітичні методи дозволяють передбачати потенційні загрози та запобігати злочинам ще до їхнього вчинення.

Ефективне використання кримінального аналізу потребує належного правового регулювання, високого рівня професійної підготовки кадрів, доступу до сучасних технологій і тісної міжнародної співпраці. В умовах глобалізації злочинності та зростання соціально-економічних викликів кримінальний аналіз стає ключовим елементом формування національної системи безпеки. Лише комплексний підхід, що поєднує правові, організаційні та технічні інструменти, дає змогу досягти реальних результатів у боротьбі з організованою злочинністю, забезпечити захист прав громадян і зміцнити засади правопорядку в Україні.

Список використаних джерел:

1. Шинкаренко І.Р. Проблеми запровадження кримінального аналізу в діяльність підрозділів кримінальної поліції: теоретико-історичне підґрунтя. *Науковий вісник Дніпропетровського державного університету внутрішніх справ.* 2017. № 1. С. 233–242.

2. Богатирчук О.М. Можливості кримінального аналізу в протидії організованій екологічній злочинності. *Європейський правничий часопис*.

2024. Вип. 3. С. 96–101.

3. Білоус Р.В., Василинчук В.І., Таран О.В. Використання методів кримінального аналізу під час оперативного провадження та досудового розслідування. *Науковий вісник Національної академії внутрішніх справ*. 2021. № 1. С. 131–137.

4. Олійничук Р.П. Роль та значення кримінального аналізу в управлінні правоохоронною діяльністю. *Актуальні проблеми правознавства*. 2023. Вип. 4. С. 104–108.

ГАШЕНКО Сергій
старший викладач кафедри загальновійськових дисциплін Військово-юридичного інституту Національного юридичного університету імені Ярослава Мудрого,
підполковник

ГРІДІНА Анастасія
курсантка 2 групи 2 курсу, здобувачка першого (бакалаврського) рівня вищої освіти Військово-юридичного інституту Національного юридичного університету імені Ярослава Мудрого

ВОГНЕВА ПІДГОТОВКА ТА ЇЇ ВПЛИВ НА ДІЯЛЬНІСТЬ ОРГАНІЗОВАНИХ ЗЛОЧИННИХ ГРУП У ЗОНІ КОНФЛІКТУ

Вогнева підготовка організованих злочинних груп у зоні збройного конфлікту є критичною складовою їхньої оперативної та тактичної діяльності, що значно підвищує загрози безпеці громадян, місцевих громад та держави загалом [14, с. 112–120; 15, с. 89–97]. Високий рівень навичок поводження зі стрілецькою зброєю, тренування в умовах стресу та бойових ситуацій, а також відпрацювання взаємодії між учасниками угруповань дозволяють злочинним

структурам ефективно здійснювати рейди, засідки та інші насильницькі акти, що ускладнює діяльність правоохоронних органів та підсилює соціально-економічні ризики у регіонах конфлікту. Центральну роль у протидії цим загрозам відіграють державні та правоохоронні органи, які не лише здійснюють контроль над обігом стрілецької зброї, а й розробляють стратегічні концепції боротьби з озброєними організованими угрупованнями [1; 2; 3; 4; 5], впроваджують стандарти професійної підготовки особового складу та адаптують систему реагування до динаміки та специфіки бойових дій.

У межах міжнародної співпраці Україна активно інтегрує передовий досвід партнерів НАТО та ЄС [7; 8; 9] у сфері підготовки силових структур, розвитку тактичних навичок особового складу та комплексного аналізу діяльності організованих злочинних угруповань. Цей досвід охоплює методики тренування в умовах бойових дій, стандарти поводження зі стрілецькою та спеціальною зброєю, а також системи збору й обробки оперативної інформації для виявлення та нейтралізації загроз. Рекомендації Альянсу [7], стратегічні документи партнерів [8] та національні програми з безпеки [4] стали орієнтирами для формування сучасної державної політики, спрямованої на контроль над обігом зброї, підвищення професійного рівня військових і правоохоронців, а також моніторинг і прогнозування діяльності організованих груп у зоні конфлікту.

Пріоритетом державної політики України є забезпечення оперативного та ефективного реагування на загрози з боку озброєних організованих злочинних структур. Це включає широкий спектр заходів: від систематичного збору та аналізу оперативної інформації про діяльність злочинних угруповань до розробки превентивних стратегій і безпосереднього запобігання злочинам із застосуванням стрілецької та спеціальної зброї. Для реалізації цих завдань задіяні ключові державні органи, зокрема Служба безпеки України [3], Національна поліція [2], військові підрозділи та спеціальні аналітичні центри, які здійснюють координацію своєї діяльності відповідно до стратегічних

документів [4] та міжнародних домовленостей [7; 8]. Координація передбачає обмін оперативною інформацією, узгодження методик аналізу, планування спільних операцій, навчання персоналу та підвищення рівня вогневої підготовки, що дозволяє формувати ефективні превентивні та оперативні заходи.

У межах державної політики України щодо протидії організованій злочинності із застосуванням стрілецької зброї визначено комплекс механізмів, що забезпечують ефективну взаємодію державних структур та підвищують рівень безпеки громадян і стабільності регіонів конфлікту. До ключових заходів належить інтеграція вогневої підготовки та кримінального аналізу [12, с. 45–53; 13] у загальну систему національної безпеки та оборони шляхом координації між правоохоронними органами, військовими підрозділами та спеціальними аналітичними центрами; розвиток міжвідомчої та міжнародної співпраці для обміну досвідом щодо навчання персоналу та протидії озброєним групам; створення спеціалізованих аналітичних центрів та тренувальних платформ для моделювання дій злочинних угруповань і підвищення рівня підготовки власного персоналу; запровадження обов'язкових програм навчання правоохоронців і військових у сфері тактики застосування зброї, кримінального аналізу та превентивних заходів; забезпечення належного кадрового потенціалу у структурах, що відповідають за контроль зброї та аналітичне забезпечення діяльності організованих груп; а також активну участь у міжнародних навчаннях, дослідженнях та обміні досвідом [9; 10; 11; 15] щодо протидії озброєним злочинним структурам у зонах конфлікту.

Державні органи відіграють провідну роль у забезпеченні безпеки України, формуючи стратегічні напрями розвитку, впроваджуючи інноваційні підходи до протидії загрозам та координуючи взаємодію з міжнародними партнерами. Завдяки комплексному підходу Україна поступово трансформується з об'єкта загроз у активного суб'єкта протидії озброєним організованим структурам, здатного ефективно прогнозувати їхні дії,

нейтралізувати ризики та підтримувати стабільність у регіонах конфлікту [10; 11].

Це досягається через поєднання високого рівня вогневої підготовки силових підрозділів, застосування сучасних методів кримінального аналізу, інтеграцію міжнародного досвіду та участь у спільних навчаннях і аналітичних проектах [12; 13; 15]. Такий підхід дозволяє підвищити оперативну спроможність правоохоронних органів і військових підрозділів, посилює здатність держави захищати громадян і критичну інфраструктуру, а також створює основу для розвитку довгострокових стратегій національної безпеки, які відповідають сучасним викликам та умовам збройного конфлікту [4; 7; 9].

Список використаних джерел:

1. Кримінальний кодекс України: Закон України від 05.04.2001 № 2341-III // Відомості Верховної Ради України. – 2001. – № 25–26. – Ст. 131. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text

2. Про Національну поліцію: Закон України від 02.07.2015 № 580-VIII // Відомості Верховної Ради України. – 2015. – № 40–41. – Ст. 379. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text

3. Про Службу безпеки України: Закон України від 25.03.1992 № 2229-XII // Відомості Верховної Ради України. – 1992. – № 27. – Ст. 382. URL: https://zakon.rada.gov.ua/laws/show/2229-12#Text

4. Стратегія національної безпеки України: Указ Президента України від 14.09.2020 № 392/2020. – Київ, 2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text

5. Концепція боротьби з організованою злочинністю: Схвалена розпорядженням Кабінету Міністрів України від 21.07.2021 № 752-р. URL: https://zakon.rada.gov.ua/laws/show/1126-2020-р#Text

6. Доктрина інформаційної безпеки України: Указ Президента України від 25.02.2017 № 47/2017. – Київ, 2017. URL:

https://zakon.rada.gov.ua/laws/show/47/2017#Text

7. NATO Standardization Office. Allied Joint Doctrine for Countering Improvised Explosive Devices (AJP-3.15). – Brussels: NATO HQ, 2019. URL: https://assets.publishing.service.gov.uk/media/5aa10fe1e5274a7bd3417176/doctrine_nato_countering_ied_ajp_3_15.pdf

8. NATO. Building Integrity and Reducing Corruption Risk in Defence Sector: Compendium of Best Practices. – Brussels: NATO HQ, 2020. URL: https://www.dcaf.ch/sites/default/files/publications/documents/Compendium_Building_Integrity_and_Reducing_Corruption_in_Defence.pdf

9. European Union Agency for Law Enforcement Training (CEPOL). Firearms Trafficking and Organized Crime: Training Materials. – Budapest: CEPOL, 2021. URL: https://www.cepol.europa.eu

10. Europol. Serious and Organised Crime Threat Assessment (SOCTA) 2021. – The Hague: Europol, 2021. URL: https://www.europol.europa.eu/cms/sites/default/files/documents/socta2021_1.pdf

11. United Nations Office on Drugs and Crime (UNODC). Global Study on Firearms Trafficking 2020. – Vienna: UNODC, 2020. URL: https://www.unodc.org/documents/data-and-analysis/Firearms/2020_REPORT_Global_Study_on_Firearms_Trafficking_2020_web.pdf

12. Колб О. В. Кримінальний аналіз як інструмент у протидії організованій злочинності // Вісник кримінології. – 2021. – № 2. – С. 45–53.

13. Бандурка О. М., Шрамко С. В. Протидія організованій злочинності: правові та організаційні аспекти. – Харків: Право, 2019. – 312 с.

14. Стадник В. І. Вогнева підготовка як елемент професійної діяльності правоохоронних органів у зоні збройного конфлікту // Право і безпека. – 2022. – № 3. – С. 112–120.

15. Шумило М. О. Міжнародний досвід протидії організованій злочинності у період воєнних конфліктів // Науковий вісник ДДУВС. – 2020. – № 4. – С. 89–97.

ДЗЮБА Нікіта
здобувач 1 курсу факультету підготовки фахівців для підрозділів кримінальної поліції Національної поліції Дніпровського державного університету внутрішніх справ

Науковий керівник:
ВАЛЄЄВ Руслан
доцент кафедри адміністративного права і процесу ННІ ПППД НПУ Дніпровського державного університету внутрішніх справ кандидат педагогічних наук

АНАЛІЗ КРИМІНАЛЬНИХ ЗАГРОЗ: НЕЗАКОННИЙ ОБІГ НАРКОТИКІВ У ПЕРІОД ЗБРОЙНОЇ АГРЕСІЇ

Аналіз кримінальних загроз, пов'язаних з незаконним обігом наркотиків у період збройної агресії є вкрай актуальним питанням для сучасної України. Умови війни значною мірою змінюють характер злочинності, її динаміку та масштаби. Військовий стан, руйнація економічних зв'язків, втрата роботи, психологічна напруга серед населення та загальне відчуття нестабільності створюють сприятливий ґрунт для зростання як попиту, так і пропозиції на наркотичному ринку. При цьому незаконний обіг наркотиків стає не лише кримінальною проблемою, а й серйозною загрозою національній безпеці, оскільки він руйнує соціальну структуру суспільства, підриває здоров'я нації та може бути інструментом гібридних атак з боку агресора, у тому числі шляхом пропаганди та збуту наркотичних засобів серед військових.

Незаконний обіг наркотичних засобів у воєнний час має низку специфічних рис. По-перше, зростає мобільність кримінальних угруповань, які використовують хаос і проблеми з контролем на кордонах для

налагодження нових каналів постачання наркотиків. Збройна агресія призводить до послаблення традиційних механізмів державного контролю, а переміщення військових, біженців і переселенців створює додаткові можливості для маскування незаконних перевезень. По-друге, на тлі воєнних дій формується сприятливе середовище для тіньової економіки, де наркобізнес стає одним із найбільш прибуткових напрямів. По-третє, наркотики все частіше використовуються злочинними угрупованнями як джерело фінансування незаконної діяльності, включно з тероризмом та диверсіями проти держави [1].

Окремим аспектом є поширення наркотиків серед військовослужбовців. Умови бойових дій, колосальні психологічні та фізичні навантаження, постійний ризик для життя сприяють зростанню ризику вживання психоактивних речовин для зняття стресу чи втечі від реальності. Це створює загрозу боєздатності армії, підриває дисципліну та може використовуватися ворогом для ослаблення українських оборонних сил. Таким чином, незаконний обіг наркотиків у період війни є не лише соціальною, а й військово-стратегічною проблемою.

З точки зору суспільної безпеки, наркотики становлять багаторівневу загрозу. На індивідуальному рівні вони руйнують здоров'я людини, призводять до деградації особистості та зростання злочинності, пов'язаної з потребою у коштах для придбання наркотиків. На рівні суспільства наркотизація населення сприяє криміналізації середовища, підвищує рівень насильницьких злочинів, поглиблює соціальну маргіналізацію. На державному рівні незаконний обіг наркотиків підриває економіку, посилює корупційні ризики в правоохоронних органах, створює ґрунт для міжнародної злочинної співпраці, яка може мати антидержавний характер. Усі ці фактори у воєнний час лише загострюються, адже загальна нестабільність підсилює вразливість суспільства до кримінальних викликів.

Міжнародний досвід свідчить, що у конфліктних зонах наркобізнес часто використовується як джерело фінансування незаконних збройних

формувань. Приклади Афганістану, Колумбії чи Сирії демонструють, що наркотрафік здатний виступати стратегічним ресурсом для терористичних і сепаратистських рухів. Для України цей ризик є надзвичайно високим, оскільки російська агресія ведеться не лише військовими засобами, а й методами гібридної війни, де поширення наркотиків може розглядатися як спосіб деморалізації суспільства та знищення його людського потенціалу [2]. Таким чином, боротьба з незаконним обігом наркотиків у період збройної агресії є невід'ємною частиною забезпечення національної безпеки.

Правоохоронні органи України сьогодні стикаються з подвійним завданням: з одного боку – забезпечення оборони та протидія терористичним загрозам, з іншого – боротьба з кримінальними проявами, серед яких наркозлочинність займає провідне місце. Система блокпостів, що діє в умовах воєнного стану, значно допомагає виявляти незаконне перевезення наркотиків, проте цього недостатньо. Потрібні комплексні заходи, зокрема створення сучасних баз даних, інтеграція з міжнародними системами моніторингу наркотрафіку, посилення роботи кіберпідрозділів, оскільки значна частина збуту наркотиків перемістилася у віртуальний простір.

Важливою складовою державної політики має бути профілактика та просвітницька робота. В умовах війни зростає кількість людей у стані посттравматичного стресу, що підвищує ризик наркотизації. Своєчасна психологічна допомога, реабілітаційні програми для військовослужбовців і цивільних, соціальна підтримка вразливих категорій населення – усе це знижує вразливість суспільства до наркотичних загроз [3].

Невикористаним резервом попередження вживання наркотичних засобів у період воєнного часу на нашу думку залишається взаємодія поліції і громадськості, що є обов'язковою характеристикою моделі поліцейської діяльності, орієнтованою на громаду [4]. Іноді цю модель трактують як збільшення функцій поліції, її орієнтація на підвищення якості життя громадян. Проте така взаємодія передбачає і можливість залучення поліцією ресурсів громади на ті проблеми, які визнавались раніше суто поліцейськими.

У контексті нашого дослідження – це співпраця з організації психологічної допомоги, підтримки та реабілітації військовослужбовцям.

Таким чином, аналіз кримінальних загроз незаконного обігу наркотиків у період збройної агресії дозволяє зробити висновок, що ця проблема має комплексний характер і потребує багаторівневого підходу. Незаконний обіг наркотиків підсилює інші загрози національній безпеці, включаючи тероризм, корупцію, соціальну дестабілізацію та руйнацію людського потенціалу країни. Для України протидія наркозлочинності у воєнний час повинна стати частиною загальної стратегії безпеки, яка поєднує правоохоронні, соціальні, медичні та інформаційні заходи. Тільки системна та скоординована політика держави за підтримки міжнародної спільноти здатна мінімізувати ці загрози й забезпечити захист суспільства в умовах збройної агресії.

Список використаних джерел:

1. Про затвердження Порядку встановлення особливого режиму в'їзду і виїзду, обмеження свободи пересування громадян, іноземців та осіб без громадянства, а також руху транспортних засобів в Україні або в окремих її місцевостях, де введено воєнний стан: Постанова від 29.12.2021 № 1455. URL: https:// zakon.rada.gov.ua/laws/show/1455-2021-%D0%bf#Text.

2. Про введення воєнного стану в Україні: Указ Президента Украї ни від 24.02.2022 № 64/2022. URL: https://www.president.gov.ua/ documents/642022-41397.

3. Вознюк А. А. Злочини проти громадської безпеки та інші протиправ ні діяння, передбачені Особливою частиною КК України: актуальні питан ня розмежування. *Актуальні проблеми досудового розслідування : тези доп. IV Всеукр. наук.-практ. конф. (м. Київ, 1 лип. 2015 р.).* Київ : Нац. акад. внутр. справ, 2015. С. 281–287.

4. Валєєв Р.Г. Поліцейська діяльність, орієнтована на громаду, як складова соціального розвитку держави. *Сучасні проблеми правового, економічного та соціального розвитку держави : тези доп. XII Міжнар. наук.-*

практ. конф. (м. Вінниця, 1 груд. 2023 р.) / МВС України, ХНУВС, Наук. парк «Наука та безпека»; КМЄС. – Вінниця : ХНУВС, 2023. – С. 128 – 130.

ДРОБЕНКО Діна
викладач кафедри кримінального процесу та криміналістики факультету підготовки фахівців для органів досудового розслідування Національної поліції України Донецького державного університету внутрішніх справ

СНІЖКО Софія
курсантка факультету підготовки фахівців
для органів досудового розслідування
Національної поліції України
Донецького державного
університету внутрішніх справ

ЗАСТОСУВАННЯ КРИМІНАЛЬНОГО АНАЛІЗУ ДЛЯ ВИЯВЛЕННЯ СХЕМ НЕЛЕГАЛЬНОГО ОБІГУ ЗБРОЇ

Застосування кримінального аналізу для виявлення схем нелегального обігу зброї є одним із найважливіших інструментів протидії, особливо в умовах збройного конфлікту, коли традиційні контролюючі механізми часто виявляються ослабленими або паралізованими. Кримінальний аналіз не обмежується лише збором і перерахунком фактів — це системний процес перетворення розрізнених відомостей у зрозумілу модель поведінки злочинних мереж, яка дозволяє передбачати їхні кроки, виявляти вразливі місця логістики і фінансування та планувати цілеспрямовані операції з нейтралізації каналів постачання. У практиці аналітика це означає синтез оперативних повідомлень, результатів експертиз, митних і логістичних реєстрів, фінансових транзакцій, метаданих зв’язку, відкритих джерел

інформації та спостережень на місцях — кожен фрагмент допомагає заповнити картину схеми [1; 2].

На початковому етапі аналітичної роботи формується гіпотеза щодо механізму постачання: чи йдеться про прямий імпорт з-за кордону, контрабандні коридори через суміжні території, внутрішню реквізицію чи легалізацію через підставні фірми. Для перевірки гіпотез збираються і систематизуються дані — телефонні метадані та переговори, які можуть виявити мережеві зв'язки; фінансові сліди, що вказують на канали оплати; записи перевезень і логістики; результати балістичних досліджень, що дозволяють зв'язати окремі одиниці зброї з певними партіями; а також інформація з відкритих джерел: оголошення, соціальні мережі, супутникові знімки. Саме кореляція цих різнорідних даних, а не кожен окремий індикатор, створює доказову базу, яка дає змогу вивести на центральні вузли мережі — координаторів, посередників, постачальників і фінансових операторів [3].

Методи лінк-аналізу та візуалізації мереж дозволяють виявити ключові вузли та «білі плями» у схемі. Часто з одного на перший погляд незначного елементу — наприклад, регулярних дрібних грошових переказів на рахунки підставних компаній або повторюваних маршрутів транзиту вантажів через певні перевалочні пункти — випливає підтвердження існування складної логістичної структури. Геопросторовий аналіз, який поєднує дані GPS, супутникові знімки та повідомлення з місць, дозволяє картографувати маршрути та виявляти склади й перевалочні пункти. У конфліктних зонах, де доступ команд слідства може бути обмежений, такі віддалені методи стають стратегічно важливими для ідентифікації «гарячих» точок, які потім виводяться на операційне реагування.

Фінансовий трасінг відіграє роль «чутного» сліду, який часто веде до організаторів. Аналіз платіжних потоків — від офіційних банківських транзакцій до готівкових переказів і систем обміну валют — дозволяє встановити, які суб'єкти отримують кошти та яким чином вони легалізуються через бізнес-структури. Саме тут поєднання традиційної фінансової

криміналістики та алгоритмів виявлення аномалій у великих даних дає змогу виявити нетипові схеми, наприклад ланцюги між кількома країнами з підставними фірмами, або використання криптовалют і платіжних сервісів для маскування джерела коштів. Поєднання фінансових доказів із фізичними — вилученою зброєю, балістичними експертизами або записами переміщень — створює комплексну картину, придатну для судових процесів [4].

Технічні засоби і сучасні технології значно розширюють можливості кримінального аналізу. Бази даних балістичних відповідностей, системи розпізнавання серійних номерів, платформи для аналізу соціальних мереж, інструменти для обробки великих обсягів метаданих — все це дозволяє автоматизувати рутинні операції і зосередити увагу аналітика на інтерпретації складних патернів. Дрони і супутникові сервіси дають можливість моніторити віддалені райони та виявляти склади, навіть коли доступ наземних сил обмежений. Машинне навчання допомагає виявляти аномалії у фінансових потоках або в поведінці онлайн-оголошень, що раніше могли залишатися непоміченими.

Разом із тим робота аналітика стикається з численними обмеженнями. У зоні бойових дій інформація часто фрагментована та суперечлива: джерела можуть бути упередженими або свідомо фальсифікувати дані. Корупція і місцева колаборація іноді роблять певні коридори недоступними для контролю, а використання шифрованих каналів зв’язку і анонімних платіжних послуг ускладнює трасінг. Юридичні бар’єри — обмежений доступ до персональних даних, необхідність дотримання процесуальних норм при перехопленні комунікацій — вимагають від аналітиків високого рівня правової грамотності, щоб зібрані докази були прийнятними в суді. Етичні міркування — захист приватності цивільних, уникнення помилкових звинувачень і забезпечення безпеки інформаторів — також мають стояти на першому місці при плануванні аналітичних заходів.

Щоб підвищити ефективність кримінального аналізу, необхідна системна міжвідомча й міжнародна кооперація. Обмін даними між поліцією,

прикордонною службою, митницею, розвідувальними органами та фінансовими регуляторами створює умови для комплексної картини та синергетичного реагування. Стандартизація форматів даних і створення захищених каналів комунікації спрощують обмін розвідданими і скорочують час реагування. Важливими є також інвестиції в кадри — цілеспрямовані тренінги з фінансової криміналістики, балістики, OSINT та цифрової аналітики, а також постійне оновлення технічних засобів для обробки великих обсягів даних.

На операційному рівні аналітичні висновки мають трансформуватися у конкретні дії: планування контрольованих закупівель, блокування маршрутів, арешти ключових координаторів, блокування фінансових рахунків і вилучення товарів. Критично важливо, щоб такі дії були скоординовані і ґрунтувалися на міцній доказовій базі — інакше ризик провалу операції або юридичної дискредитації зростає. Післяопераційний аналіз також має стати регулярною практикою: вивчення причин успіхів і поразок, адаптація інструментів і процедур відповідно до нових схем контрабанди.

Таким чином, кримінальний аналіз виступає не просто як набір технік, а як стратегічний підхід до руйнування логістики й фінансування нелегального обігу зброї. У складних умовах збройного конфлікту його роль особливо вагома: тільки через системну аналітичну роботу можливо перейти від реагування на поодинокі інциденти до проактивного руйнування мереж і мінімізації загроз для цивільного населення та національної безпеки [1–4].

Список використаних джерел:

1. Кримінальний кодекс України від 05.04.2001 № 2341-III // URL https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 26.09.2025).

2. Закон України «Про Національну поліцію» від 02.07.2015 № 580-VIII // URL https://zakon.rada.gov.ua/laws/show/580-19#Text (дата звернення: 26.09.2025).

3. Наказ Міністерства внутрішніх справ України «Про затвердження

Інструкції про порядок виготовлення, придбання, зберігання, обліку, перевезення та використання вогнепальної, пневматичної, холодної і охолощеної зброї, пристроїв вітчизняного виробництва для відстрілу патронів, споряджених гумовими чи аналогічними за своїми властивостями метальними снарядами несмертельної дії, та патронів до них, а також боєприпасів до зброї, основних частин зброї та вибухових матеріалів» від 21.08.1998 № 622 // URL https://zakon.rada.gov.ua/laws/show/z0637-98#Text (дата звернення: 26.09.2025).

4. Наказ Міністерства внутрішніх справ України «Про затвердження Порядку декларування вогнепальної зброї і боєприпасів до неї» від 18.11.2024 № 768 // URL https://zakon.rada.gov.ua/laws/show/z1739-24#Text (дата звернення: 26.09.2025).

КАРПЕНКО Артем
а'дюнкт 4 курсу Дон ДУВС

Науковий керівник:
НАЗИМКО Єгор
доктор юридичних наук,
професор

СТРАТЕГІЧНИЙ АНАЛІЗ ЗЛОЧИННОЇДІЯЛЬНОСТІ ОРГАНІЗОВАНИХ ЗЛОЧИННИХ ГРУП ТА ЗЛОЧИННИХ УГРУПУВАНЬ, ЩО ВЧИНЯЮТЬ ЗЛОЧИНИ У СФЕРІ ОБІГУНАРКОТИЧНИХ ЗАСОБІВ.

Вдалим є визначення запропоноване Білоусом Р.В., Василинчуком В.І., Тараном О.В., що у межах наданих повноважень підрозділи кримінальної поліції здобувають достатній масив інформації про злочинну діяльність, зокрема про представників організованої злочинності. Тому, надважливим завданням є застосування інструментів, які надали б можливість опрацьовувати значні обсяги наявних даних. Одним із таких інструментів у діяльності оперативних підрозділів НПУ є кримінальний аналіз – специфічний

вид інформаційно-аналітичної діяльності, що полягає в ідентифікації та якомога точнішому визначенні внутрішніх зв'язків між інформацією (відомостями, даними), що стосуються злочину, і будь-якими іншими даними, отриманими з різних джерел, їх використанням в інтересах ведення оперативно – розшукової та слідчої діяльності, їх аналітичної підтримки [1, с. 131].

Слушно зауважив т. в. о. начальника Управління кримінального аналізу НПУ В. Єрофєєв, що кримінальний аналіз – це ефективна робота поліції та безпеки громадян. Він акцентував, що підрозділ аналітики Національної поліції орієнтований на проведення оперативного, тактичного та стратегічного аналізу. Стратегічний аналіз спрямований на аналіз діяльності організованих злочинних груп, а відтак – і на перспективу в роботі по боротьбі з ними [2]. Збір інформації, її класифікація та стратегічний аналіз допоможе виявляти злочини у сфері обігу наркотичних засобів, що скоєні організованими злочинними групами та злочинними організаціями та встановлювати учасників даних груп.

Як зазначають Самойленко О.А., Тіщенко В.В., Цехан Д.М. найпоширенішими у практиці інструментами стратегічного аналізу є: SWOT-аналіз; PEST-аналіз, SOCTA та OSINT (аналіз інформації з відкритих джерел); аналіз ризиків; аналіз злочинних моделе та профілів; аналіз тенденцій; аналіз географічних профілів; ситуаційний аналіз [3 , с. 19].

В свою чергу Федчак І.А. зазначає, що предметом стратегічного аналізу є слабкі місця та загрози, стратегічні переваги та потенціал об'єкта дослідження, які при певному поєднанні з іншими факторами внутрішнього й зовнішнього середовища формують альтернативні напрями дій, що сприяють досягненню стратегічних цілей та є комплексним дослідженням, спрямованим на майбутнє, з розробкою стратегічних управлінських рішень та опрацюванням концепцій у сфері боротьби зі злочинністю. Стратегічний аналіз широко використовується у довгостроковій перспективі (від 1 до 10 років), застосовує багато елементів, таких як політичні, демографічні,

економічні, соціальні, технологічні, географічні криміногенні фактори, та чимало інших видів даних[4, с. 201 - 202].

Так формування та ведення автоматизованої інформаційної підсистеми «SOCTA» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України», призначеної для забезпечення формування поліцією інформаційних ресурсів з обліку організованих груп або злочинних організацій, злочинних спільнот та сфер злочинної діяльності законодавчо закріплено в Інструкції з формування та ведення інформаційної підсистеми «SOCTA» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України» у 2023 р. Інформаційними ресурсами ІП «SOCTA» є задокументовані одиниці інформації щодо організованих груп та/або злочинних організацій, злочинних спільнот та сфер злочинної діяльності, які ґрунтуються на здобутій оперативній інформації та матеріалах, отриманих під час проведення досудового розслідування, та матеріалах закритих кримінальних проваджень [5].

За період з 2019 – 2021 рр. засуджено 96 осіб (2019 - 33; 2020 - 35; 2021 - 28); за період з 2022 – 2024 рр. засуджено 125 осіб (2022 - 37 ; 2023 - 38; 2024 - 50), що скоїли у складі організованої групи та злочинної організації кримінальні правопорушення за ст. 305 – 310 та 313 – 320 КК України [6]. Як бачимо, кількість учасників ОГ та ОЗУ, що скоюють вищевказані кримінальні правопорушення під час воєнного стану в Україні збільшилась.

Аналізуючи офіційні статистичні дані, Назимко Є.С., Пономарьова Т.І., Семенишина – Фіголь Б.М., вчені отримали наступні результати щодо частки ОГ та ОЗ у сфері обігу наркотичних засобів та психотропних речовин відносно частки ОГ та ОЗ у загальній злочинності по країні: 2019 р. – 30, 3 %; 2020 р. – 32,7 %; 2021 р. – 29,5 %; 2022 р. – 41 %; 2023 р. – 25 % [7, с. 193 - 194]. Як бачимо частка ОГ та ЗО, що скоюють наркозлочини є значною, що викликає інтерес кримінального аналізу.

Зокрема Бурангулов В.А. вважає, що стратегічний кримінальний аналіз забезпечує прийняття рішень, розробку політики планування та визначення

пріоритетів; розподіл ресурсів поліції; та із врахуванням видів злочинності, визначає відповідний підхід діяльності поліції [8, с. 203].

Отже, застосування стратегічного аналізу у довгостроковій перспективі відносно ОГ та ЗО є ефективним інструментом, що дає можливість встановити лідерів та найближчого оточення з подальшим припиненням їх діяльності. Отримуючи необхідну інформацію з різних джерел, що полягає у ідентифікації та представленому моделюванні внутрішніх зв'язків ОГ та ЗО, що скоюють злочини у вищевказаній сфері, працівники оперативних підрозділів НПУ у подальшому можуть використати її у оперативно – розшуковій та слідчій діяльності. Дана інформація дає можливість врахувати відповідний підхід реалізації, що сприяє ефективній протидії організованій наркозлочинності.

Список використаних джерел:

1. Білоус Р.В., Василинчук В.І., Таран О.В. Використання методів кримінального аналізу під час оперативного провадження та досудового розслідування. Науковий вісник Національної академії внутрішніх справ. 2021. № 1 (118). С. 131 – 137.

2. Кримінальний аналіз – це ефективна робота поліції та безпека громадян. Міністерство внутрішніх справ України: веб – портал. URL: https://mvs.gov.ua/uk/presscenter/news/Kriminalniy_analiz____ce_efektivna_robota_policii_ta_bezpeka_gromadyan_FOTO_10309 (дата звернення 05.10.2025).

3. Самойленко О.А., Тіщенко В.В., Цехан Д.М. Кримінальний аналіз і стратегічне прогнозування в правоохоронних органах України : метод. вказ. Національний університет «Одеська юридична академія». Одеса : Фенікс, 2023. .116 с.

4. Федчак І.А. Основи кримінального аналізу: навчальний посібник. Львів : Львівський державний університет внутрішніх справ, 2021. 288 с.

5. Про затвердження Інструкції з формування та ведення інформаційної підсистеми «SOCTA» інформаційно-комунікаційної системи «Інформаційний

портал Національної поліції України». Наказ МВС від 08.11.2023 р. № 902. Верховна Рада України: веб – сайт. URL: https://zakon.rada.gov.ua/laws/show/z2041-23#Text (дата звернення 05.10.2025).

6. Судова влада України . Офіційний веб- портал. URL: https://court.gov.ua/.

7. Назимко Є.С., Пономарьова Т.І., Семенишина – Фіголь Б.М. Організована злочинність як феномен кримінології постмодерну. Правова позиція. 2023. № 1 (38). С. 190 – 194.

8. Бурангулов В.А. Кримінальний аналіз у правоохоронній діяльності: : дис. …д-ра філ./ Одеса, 2024. 231 с.

КОБИЛИНСЬКИЙ Дмитро
курсант ФПФ ПКП НПУ Дніпровського державного університету внутрішніх справ

Науковий керівник:
ВАЛЄЄВ Руслан
доцент кафедри адміністративного права і процесу ННІ ПФППД НПУ Дніпровського державного університету внутрішніх справ кандидат педагогічних наук

МІСЦЕ ТА РОЛЬ КРИМІНАЛЬНОГО АНАЛІЗУ У ПРОАКТИВНІЙ ПОЛІЦЕЙСЬКІЙ ДІЯЛЬНОСТІ

Кримінальний аналіз сьогодні визнається одним із центральних елементів інноваційного розвитку поліцейської діяльності. Його суть полягає у глибокому вивченні даних про злочинність, їх інтерпретації та перетворенні на практично значиму інформацію. Саме завдяки аналізу правоохоронні органи можуть переходити від реагування на злочини до їхнього випереджального попередження.

У свою чергу, проактивність поліцейської діяльності є неодмінною

характеристикою нового підходу до її організації, що отримав назву community policing [1]. При цьому традиційна (чи професійна) модель роботи поліції отримує у сучасних дослідженнях характеристику «реактивної», оскільки передбачає втручання вже після скоєння правопорушення. Натомість сучасні виклики – організована злочинність, кіберзлочини, тероризм – вимагають іншого підходу. У цих умовах проактивна діяльність, підкріплена кримінальним аналізом, стає необхідністю для ефективного захисту суспільства.

М. Корнієнко вказує, що основне завдання кримінального аналізу полягає у зборі, систематизації та перетворенні різнорідних даних у цілісну систему знань. До уваги беруться як офіційні статистичні матеріали, так і відомості з оперативних джерел, відкритих баз даних, технічних засобів спостереження. Це дозволяє поліції бачити не окремі інциденти, а загальну картину криміногенної ситуації [2, с.63].

Важливою функцією аналізу є виявлення закономірностей у злочинній поведінці. Аналітики досліджують, які категорії осіб вчиняють злочини, у яких районах вони зосереджуються, які фактори підвищують ризик правопорушень. Така інформація формує основу для розробки адресних заходів протидії.

Значну роль у сучасному кримінальному аналізі, на думку О. Дуфенюк, відіграє прогнозування. Застосування математичних моделей, методів статистики, а також картографування злочинності дозволяє виявляти так звані «гарячі точки». Це дає змогу поліції завчасно посилювати патрулювання чи проводити профілактичні заходи у визначених районах [3, с.995].

Кримінальний аналіз виступає і як інструмент раціонального використання ресурсів. В умовах обмеженого кадрового та матеріального забезпечення поліція повинна діяти максимально ефективно. Саме завдяки аналітичним даним можна обґрунтовано визначати, де потрібна найбільша присутність сил і засобів.

Особливе значення кримінальний аналіз має у боротьбі з організованими

злочинними угрупованнями. Їхня діяльність зазвичай характеризується складними зв'язками, багаторівневою структурою та прихованістю. Аналітичні методи дозволяють виявляти ці зв'язки, відстежувати фінансові потоки та прогнозувати подальші дії злочинців.

У проактивній поліцейській діяльності важливо своєчасно виявляти фактори ризику. Кримінальний аналіз допомагає встановлювати соціальні, економічні та психологічні чинники, які сприяють зростанню злочинності. Це дає можливість не лише реагувати, але й спільно з іншими державними інституціями впливати на причини злочинної поведінки [4, с.106].

Значна увага приділяється інформаційним технологіям. Використання систем штучного інтелекту, великих даних та алгоритмів машинного навчання розширює можливості кримінального аналізу. Технології дозволяють обробляти величезні масиви даних у короткі терміни та робити точні прогнози.

Кримінальний аналіз сприяє і підвищенню прозорості діяльності поліції. Коли рішення щодо розподілу ресурсів чи заходів безпеки базуються на об'єктивних даних, зростає довіра громадян. Це є важливим чинником формування партнерських відносин між поліцією та суспільством.

Важливо підкреслити, що аналітична робота не є самоціллю. Вона має сенс лише тоді, коли її результати інтегруються у практичні дії поліцейських підрозділів. Для цього необхідна тісна взаємодія між аналітиками та оперативними працівниками, що забезпечує ефективне використання напрацьованої інформації [5, с.23].

Кримінальний аналіз також виконує навчальну та виховну функцію у структурі поліції. Аналізуючи допущені помилки, неефективні тактики або недооцінені ризики, правоохоронці підвищують свій професійний рівень. Це сприяє формуванню культури постійного вдосконалення.

Слід зазначити, що роль кримінального аналізу особливо актуальна у період трансформації української правоохоронної системи. В умовах війни та післявоєнної відбудови очікується зростання кримінальних ризиків – від незаконного обігу зброї до організованих схем економічних злочинів.

Аналітичний підхід стане ключовим інструментом у попередженні таких загроз.

Впровадження кримінального аналізу в практику української поліції вимагає розвитку спеціалізованих підрозділів та підготовки кадрів. Необхідно формувати систему професійного навчання аналітиків, забезпечувати їх доступом до сучасних технологій та міжнародних методик. Це дозволить інтегрувати національний досвід у світовий контекст.

Отже, кримінальний аналіз є не лише допоміжним інструментом, а фундаментальною основою проактивної поліцейської діяльності. Він забезпечує випереджальний характер реагування, дозволяє ефективно управляти ресурсами та будувати довіру з громадськістю. У перспективі саме розвиток кримінального аналізу визначатиме спроможність поліції забезпечувати безпеку в умовах складних суспільних викликів.

Список використаних джерел:

1. Валєєв Р.Г. Поліцейська діяльність, орієнтована на громаду (community policing) як передумова сталого розвитку соціуму. *Механізми управління розвитком територій: зб. наукових праць у 2 ч. Ч. 1.* Житомир: Поліський нац. ун-т, 2023. 216 с. С. 22 – 26

2. Корнієнко М.В. Кримінальний аналіз у діяльності Національної поліції України: стан і перспективи. *Право і суспільство*. 2024, № 1. С. 62-75.

3. Дуфенюк О.М. «Невирішені проблеми та нові виклики використання кримінального аналізу оперативними підрозділами Національної поліції». *Аналітичний вісник*. 2025. № 02. С. 993-1000.

4. Олійничук Р.П. Роль та значення кримінального аналізу в управлінні правоохоронною діяльністю. Актуальні проблеми правознавства. 2023. Вип. 4. С. 104–108.

5. Кисельов А. О., Копилов Е. В., Худенко Д. М. *Основи кримінального аналізу: навчальний посібник*. Дніпро: Дніпропетровський державний університет внутрішніх справ, 2023. 152 с.

ЛУНГОЛ Ольга
завідувач кафедри оперативно-розшукової діяльності та інформаційної безпеки ННІПФПКП ім. Е.О. Дідоренка Донецького державного університету внутрішніх справ, кандидат педагогічних наук, доцент

ШЕВЧЕНКО Андрій
здобувач вищої освіти 2 курсу ННІПФПКП ім. Е.О. Дідоренка Донецького державного університету внутрішніх справ

КРИМІНАЛЬНИЙ АНАЛІЗ ЯК ІНСТРУМЕНТ ВИЯВЛЕННЯ ОРГАНІЗОВАНИХ ЗЛОЧИННИХ УГРУПОВАНЬ В УМОВАХ ЗБРОЙНОГО КОНФЛІКТУ

В умовах дії правового режиму воєнного стану в Україні, криміногенна ситуація країни суттєво трансформується. Зростає не тільки загальна кількість злочинів, але й з’являються нові їхні види, зокрема пов’язані з тероризмом, саботажем, шпигунством і мародерством. Особливо небезпечною є діяльність організованих злочинних угруповань [1; 2], які активно використовують умови нестабільності у країні для інтеграції в нелегальні фінансові потоки, контрабанду, участі у воєнних діях, збагачуючись за рахунок конфлікту тощо.

У зв’язку з цим, ефективна протидія організованій злочинності вимагає від правоохоронних органів використання надійних та інноваційних інструментів. Одним із таких ключових інструментів є кримінальний аналіз (КА), який в умовах воєнного стану дозволяє адаптувати методи

роботи правоохоронних органів до нових викликів [3; 4]. Ефективність КА безпосередньо залежить від комплексного підходу, що поєднує традиційні методи збору та аналізу інформації з інноваційними технологіями, що, зокрема, включає використання Big Data, алгоритми штучного інтелекту та машинного навчання.

Успішність застосування КА для виявлення та нейтралізації організованих злочинних угруповань в умовах збройного конфлікту вимагає активної міжвідомчої та міжнародної співпраці. Спільна робота з військовими формуваннями, спецслужбами та міжнародними організаціями (Інтерпол, Європол) дозволяє забезпечити швидкий обмін інформацією та координувати зусилля в боротьбі з транснаціональною злочинністю. КА в умовах воєнного стану має бути орієнтований не лише на традиційні злочини, а й на злочини, що мають геополітичний характер, включаючи виявлення злочинних схем, пов'язаних із підривною діяльністю та впливом міжнародних сил.

КА у боротьбі з організованою злочинністю в умовах воєнного стану реалізується через такі напрями, як прогнозування та запобігання, розвідку на основі відкритих джерел інформації та аналіз Big Data. Використання методів інтелектуального аналізу даних та машинного навчання вже сьогодні дозволяє прогнозувати злочини ще до їхнього вчинення. Це допомагає правоохоронним органам швидше та точніше виявляти й запобігати злочинній діяльності. Застосування технологій Big Data дозволяє обробляти та аналізувати величезні обсяги інформації з різних джерел, таких як соціальні мережі, фінансові транзакції, комунікаційні канали та інші цифрові платформи, допомагаючи виявляти закономірності та аномалії, що свідчать про підготовку або вчинення злочину.

Для ефективної роботи фахівці КА повинні володіти не лише технічними, а й аналітичними та комунікаційними компетентностями. В гармонійному поєднанні це формує здатність у фахівця швидко

адаптуватися до мінливих умов сьогодення, робити обґрунтовані висновки та ефективно взаємодіяти з іншими підрозділами.

Отже, КА є важливим інструментом у протидії організованій злочинності в умовах воєнного стану. Його ефективність залежить від інтеграції новітніх технологій, таких як аналіз Big Data, ШІ, 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 КА 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.

Список використаних джерел:

1. Войтович Н.Ф. Організована злочинність в умовах воєнного стану: сучасні виклики та наукові орієнтири. Успіхи і досягнення у науці. № 19, 2025. С. 50-61.

2. Коваль А., Плютенко Я. Актуальні проблеми боротьби з організованою злочинністю: український та міжнародний досвід. Могилянські читання – 2024 : досвід та тенденції розвитку суспільства в Україні : глобальний, національний та регіональний аспекти. Право : XXVII Всеукр. наук.-практ. конф. : 6–10 листоп. 2024 р., м. Миколаїв: Вид-во ЧНУ ім. Петра Могили, 2024. С. 103-107.

3. Lysenko O.V., Haborets O.A., Lunhol O.M. Law enforcement information and analytical support. Current issues in modern science. Issue, (3), 2023. Pp. 281-291.

4. Луговцов Д.С. Роль кримінального аналізу у протидії організованій злочинності. Наукові тренди постіндустріального суспільства: збірник наукових праць з матеріалами VI Міжнародної наукової конференції, м. Івано-Франківськ, 26 квітня, 2024 р. /

Міжнародний центр наукових досліджень. Вінниця: ТОВ УКРЛОГОС Груп, 2024. С. 145-147.

МАКАРЕВИЧ Владислав
Курсант 302/23КР-(ПД)-Бк ННІ ФПФ ПКП ДонДУВС

Науковий керівник:
ГАБОРЕЦЬ Ольга
Доцент кафедри оперативно-розшукової діяльності та інформаційної безпеки навчально-наукового інституту підготовки фахівців для підрозділів кримінальної поліції імені Е.О. Дідоренка Донецького державного університету внутрішніх справ, доктор філософії, доцент

ЗАСТОСУВАННЯ КРИМІНАЛЬНОГО АНАЛІЗУ В ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ У ПЕРІОД ЗБРОЙНОЇ АГРЕСІЇ

Збройна агресія проти України докорінно змінила умови функціонування правоохоронних органів, поставивши перед ними завдання швидкого реагування та ефективного протидіяння злочинності в особливо складних умовах. Традиційні методи збору й обробки даних часто виявляються малоефективними, що зумовлює необхідність використання комплексних інструментів кримінального аналізу. У цьому контексті особливого значення набуває системне застосування аналітичних технологій, які дозволяють інтегрувати інформацію з різних джерел, перевіряти її достовірність та формувати висновки, релевантні реаліям воєнного часу.

Кримінальний аналіз передбачає використання широкого спектра інструментів: від базових методів просторово-часового аналізу злочинності,

що дозволяють виявляти закономірності у часі та місці вчинення правопорушень, до соціально-мережевого аналізу, який допомагає простежити структуру злочинних угруповань і канали їхньої комунікації. Важливим є застосування геоінформаційних систем для відображення криміногенних процесів у конкретних територіях, а також використання технологій аналізу цифрових доказів і спеціалізованого програмного забезпечення на зразок i2 Analyst's Notebook чи Maltego, що дозволяє обробляти великі масиви даних та будувати візуальні моделі зв'язків. У сучасних умовах активно застосовуються і можливості OSINT для збору інформації з відкритих джерел, а також інструменти прогнозного аналізу, що допомагають визначати ймовірні сценарії розвитку злочинної активності та своєчасно вживати превентивних заходів.

Застосування таких інструментів набуває особливої ваги у протидії воєнним злочинам, які характеризуються високим рівнем латентності та складністю процесу доказування. Вони дозволяють не лише встановлювати осіб, причетних до злочинів, а й виявляти приховані зв'язки між окремими епізодами злочинної діяльності, виявляти закономірності її розвитку та будувати прогностичні моделі. Важливу роль у підвищенні ефективності кримінального аналізу відіграють законодавчі зміни останніх років, які посилили правові механізми притягнення до відповідальності за воєнні злочини та оптимізували процес доказування.

У воєнний час особливого значення набуває стратегічний кримінальний аналіз, що забезпечує довгострокове планування оперативно-розшукових заходів, зокрема негласних слідчих дій. Використання сучасних інструментів аналізу у поєднанні з належним правовим регулюванням дозволяє правоохоронним органам ефективно реагувати на виклики воєнного стану, своєчасно виявляти загрози та приймати обґрунтовані рішення.

Отже, 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.

Список використаних джерел:

1. Реалізація філософії «Intelligence-led Policing» в системі кримінального аналізу Національної поліції України: монографія / Користін О., Швець Д., Бутко Б., Денисенко Б. та ін., за заг. ред. Користіна О. Є. – Київ: «ВАІТЕ», 2024. 444 с.

МАКАРЕНКОВ Олексій
науковий співробітник Юридичного інституту Університету Портукаленсе (Порто, Португалія), доктор юридичних наук, професор

КРИМІНОЛОГІЧНИЙ АНАЛІЗ КОРЕКЦІЙ ПІДКУПІВ ЧИНОВНІКІВ ЗІ ЗЛОЧИНАМИ ПРОТИ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ПІД ЧАС ВІЙНИ ІЗ ЗОВНІШНІМИ АГРСОРОМ

Припускаємо, що урахування взаємозв’язків підкупу і подальшого вчинення злочину проти фундаментальних цінностей національної безпеки дозволяє здійснювати своєчасну профілактику їхнього вчинення, своєчасно нейтралізуючи потенційних виконавців цих злочинів на етапі їхнього мотивування через неправомірну вигоду. Особу підкупають з метою її мотивування до вчинення неправомірних дій. Відповідно підкуп («неправомірна вигода», «хабар» та інші семантичні варіації) передує вчиненню іншого злочину, що сукупно означає появу трьох складів злочину: 1) парний злочин – неправомірні дії хабародавця і хабаротримувача;

2) кримінального правопорушення, за вчинення якого (дію або бездіяльність) було надано і отримано хабар.

Підкуп вид майнової корупції, де службова особа ставить за мету отримання матеріальної вигоди для задоволення власного приватного інтересу на шкоду публічному інтересу, який в сфері національної безпеки складає широкий спектр національних інтересів. Наприклад, на відміну Закону України «Про національну безпеку України» від 21.06.2018 № 2469-VIII, у законах Португальської Республіки виокремлено зовнішній і внутрішній виміри національної безпеки: 1) «національна оборона» - гарантування (garantir) суверенітету держави, національної незалежності і територіальної цілісності Португалії, а також забезпечення (assegurar) свободи та безпеки населення та захист основоположних цінностей конституційного ладу від будь-якої зовнішньої агресії чи загрози; дотримання міжнародних зобов'язань держави у військовій сфері відповідно до національних інтересів (ст. 1); 2) «внутрішня безпека» (a segurança interna) – це діяльність, що здійснюється державою для гарантування громадського порядку, безпеки та спокою, захисту людей та майна, запобігання та припинення злочинності, а також сприяння забезпеченню нормального функціонування демократичних інституцій, регулярного здійснення основних прав, свобод та гарантій громадян, а також поваги до демократичної законності (ч. 1 ст. 1) [1; 2].

Компаративно-правовий аналіз норм-дефініцій про однакові правові феномени виявив, що має сенс розрізняти національну безпеку у внутрішньому і зовнішньому вимірах. Визначення місця походження небезпеки для національних інтересів дозволяє підібрати підходящий організаційний засіб протидії. У випадку внутрішніх посягань на національну безпеку ефективним залишаються органи внутрішніх справ, національна гвардія, служба національної безпеки, а також їхні міжвідомчі групи зі службою військової розвідки тощо. Руйнування основ національної безпеки ззовні й тим більш через завчасно корупційним чином замотивованих громадян є гібридною формою війни, які, як відомо, можуть набувати форм

терористичних актів з перекладанням відповідальності на чинні органи публічної влади, провокацій цієї влади на насильство тощо.

Протидія такій гібридній агресії вимагає гласного і негласного збору соціологічних даних, використання інформації в порядку конфіденційного співробітництва (ст. 275 КПКУ), з відкритих джерел (OSINT), розвідданих, відомостей від країн-партнерів тощо. Наприклад, категорію допустимості розвідданих ab initio, зокрема й отриманих в результаті перехоплення службою національної безпеки і тому подібними органами, та результатів їхнього аналізу як належних доказів у судовому процесі з надійних джерел здійснює тільки суд, відповідно до національних правил визначення допустимості доказів (згідно з численними висновками про це ЄСПЛ), за дотримання режиму нерозголошення громадськості методів і способів отримання цих даних, інакше в подальшому злочинців стане складно викривати. Такі практики типові для юрисдикцій Австралії, США [3, с. 409-410].

Достатні дані і вірна оцінка дозволяють вміло використовувати такі адміністративні і силові ресурси, потужність яких дозволить забезпечити недоторканність конституційного ладу. В обставинах викликів гібридних агресій щонайменше постійним залишається запит на безперервну ідеологічну і роз'яснювальну роботу з боку публічної адміністрації та відкритих розвитку на засадах конституційних цінностей представників громадянського суспільства. Застосування силового ресурсу цілком може перевершувати потенціал органів внутрішньої безпеки та вимагати своєчасного долучення військових, сил самооборони територіальних громад і тому подібних структур, відповідно до завчасно розроблених процедур національного законодавства.

За умови стабільно високого рівня сприйняття корупції, високими залишаються ризики викривлення будь-якої інформації, зловживання цим в інтересах внутрішніх і зовнішніх злочинних груп, зокрема й в урядах іноземних держав, міжнародних організацій, транснаціональних корпорацій.

Наприклад, в Україні цей рівень долається тільки на 35 балів зі 100, що визначає 105 місце серед 180 країн. Усунення міжнародної корупції (підкупів національних чиновників з-за меж країни) на рівні з топ-корупцією амбітні цілі, якими переймається Українська нація, поступово запроваджуючи систему відповідних інноваційних норм про наступне, а саме: 1) протидію впливу олігархів на загальнонаціональну і муніципальні політики у вересні 2021 р.; 2) антикорупційну стратегію у червні 2022 р.; 3) інститут лобіювання у лютому 2024 р.; 4) дефініцію «дружніх країн» та інші умови для інституту множинного громадянства у червні 2025 р. тощо.

Логіка системи цього юридичного інструментарію демонструє побудову матриці для верифікації груп ризиків чиновників та інших осіб не тільки за ознаками невідповідності доходів витратам, але й через реєстраційні дані прозорості впливів на правотворчу та правозастовчу політики, бенефіціарів прибутків підприємств і/або реалізації публічно-владних рішень, зв'язки з економічним та політичними відносинами в межах юрисдикцій зовнішнього агресора і його союзників, а також інших зарубіжних країн тощо. Дані про нон-комплайнс у цих сферах стають ресурсом для реагування з боку органів кримінальної юстиції і сил оборони на виклики для національної безпеки, що діють в межах національного правового простору, з-за кордону та їхні комбіновані гібридні варіанти агресії.

Цифровий формат даних про вищезазначені ризики для національної безпеки і оборони, детерміновані підкупами, у роботі публічної влади стає запорукою належного реагування на них. Наприклад, згорткова нейронна мережа як особливий тип штучної нейронної мережі генерує запитувану інформацію за рахунок фільтрації вхідних даних через ітераційні шари вже наявних даних, які при необхідності згортаються і потім, за потреби, знову використовуються, в рамках отримання відповіді на запитані дані [4, с. 6].

Навчання штучних нейромереж на цих даних та використання їхніх ресурсів на постійній основі передбачає не тільки створення інфраструктури у вигляді достатньої кількості процесорів, модулів пам'ять, плат і тому

подібного апаратного забезпечення, але й піклування про збереження цих даних у безпеці від кібератак, шпигунства, викривлення, знищення тощо.

Отже, перманентне кримінологічне взяття до уваги кореляцій підкупу з подальшим вчиненням підкупленою особою злочину проти основ національної безпеки покликане забезпечити формування належної (своєчасної і повноцінної) реакції органів кримінальної юстиції на ці злочини. Фактично реагування на один завершений злочин (підкуп) елімінує підготовку, замах на вчинення і/або власне вчинення наступного злочину, що спрямований на завдання масштабних негативних наслідків, оскільки зачіпає інтереси усіх – цілої нації. Така профілактика тим більш важлива для забезпечення правопорядку і національної безпеки, якщо врахувати, що такі посягання у вигляді підкупів опосередковуються участю спеціальних служб з-за меж країни й відображають одночасно реальні загрози посягання на конституційні цінності держави. Ці ініціативи органів кримінальної юстиції є формою протистояння гібридній війні та посилення спроможностей сил оборони України у їхній роботі з успішної нейтралізації зовнішнього військового агресора

Підкуп особи з метою її спонукання до вчинення злочину проти національної безпеки є корупційним злочином, який доцільно кваліфікувати в межах окремо сформульованої статті відповідного розділу «про злочини проти основ національної безпеки» кримінального кодексу. Відповідно склад і санкції за вчинення злочинів, які описані у цьому розділі, з корисливих мотивів доцільно визначити в межах окремих частин його відповідних статей, за зразком ч. 3 ст. 110-2 і 114-2, а також ч. 3 ст. 431 ККУ.

Список використаних джерел:

1. Lei de Defesa Nacional nº 31-A/2009 de 7 de julho de 2009. A Assembleia da República Portuguesa. Diário da República n.º 138/2009, Série I de 2009-07-20.

2. Lei de Segurança Interna n.º 53/2008 de 29 de Agosto de 2008. A Assembleia da República Portuguesa.Diário da República n.º 167/2008, Série I de

2008-08-29.

3. Walker C. Intelligence and anti-terrorism legislation in the UK. Crime, Law & Social Change. 2005. Vol. 44. P. 387-422. doi:10.1007/s10611-006-9030-8

4. Artificial Intelligence: Machine Learning, Convolutional Neural Networks and Large Language Models. Edit by Deligiannidis, L., Dimitoglou, G., Arabnia, H. Berlin: Walter de Gruyter GmbH. 2024. 442 p.

МАРЖАН Єлизавета
інспектор відділу організації служби освітньої безпеки ГУНП в Кіровоградський області лейтенант поліції

Науковий керівник:
ПЕКАРСЬКИЙ Сергій
доцент кафедри оперативно-розшукової діяльності та інформаційної безпеки Навчально-наукового інституту підготовки фахівців для підрозділів кримінальної поліції імені Е. О. Дідоренка Донецького державного університету внутрішніх справ, кандидат юридичних наук, доцент

КРИМІНАЛЬНИЙ АНАЛІЗ ЯК ІНСТРУМЕНТ ВИЯВЛЕННЯ ТА РОЗСЛІДУВАННЯ ВОЄННИХ ЗЛОЧИНІВ

З 24 лютого 2022 року Україна перебуває в умовах правового режиму воєнного стану. Акцентуючи увагу на факти вчинених росією воєнних злочинів на тимчасово окупованих та деокупованих Україною територіях, постає потреба у залученні підрозділів кримінального аналізу для більш глибокого з’ясування обставин вчинених представниками країни-агресорки

кримінальних правопорушень.

Відповідно до статті 438 КК України, воєнні злочини відносяться до особливо тяжких кримінальних правопорушень та включають в себе: жорстоке поводження з військовополоненими або цивільним населенням, вигнання цивільного населення для примусових робіт, розграбування національних цінностей на окупованій території, застосування засобів ведення війни, заборонених міжнародним правом, незаконне переміщення або депортація дитини, невиправдана затримка репатріації дитини, вербування або використання дитини для участі у збройному конфлікті, воєнних (бойових) діях, інші порушення законів та звичаїв війни, що передбачені міжнародними договорами, згода на обов'язковість яких надана Верховною Радою України, а також віддання наказу про вчинення таких дій [1].

Тому, на основі подій сьогодення, постає необхідність залучення підрозділів кримінального аналізу Національної поліції України для повного та всебічного з’ясування деталей вчинених кримінальних правопорушень ворогом. Вищезгаданий підрозділ кваліфікується на систематизації, співставленні й узагальненні даних, отриманих із різноманітних джерел – слідчих, оперативних, відкритих та спеціальних. За допомогою проведення аналітичної роботи співробітниками кримінального аналізу можуть не лише встановлювати осіб, причетних до воєнних злочинів, а й виявляти взаємозв’язки між окремими епізодами злочинної діяльності, визначати закономірності та прогнози щодо потенційних загроз. У воєнний час цей інструмент набуває ще більшого значення, оскільки забезпечує оперативне ухвалення рішень і дозволяє правоохоронним органам діяти на випередження [2, с. 216].

Активна робота з удосконалення кримінального законодавства, запровадження сучасних методів аналізу й адаптація правоохоронної системи до викликів воєнного часу дозволяють сформувати потужний інструментарій у боротьбі з безкарністю. Важливо, аби ці зусилля були синхронізовані з міжнародними ініціативами щодо переслідування злочинців, аби забезпечити

справедливість не лише в межах національної юрисдикції, а й у рамках міжнародного кримінального правосуддя [3, с. 65].

Протягом збройного конфлікту постала значна проблема, яка пов'язана з незаконною депортацією та русифікацією українських дітей. Неповнолітніх та малолітніх дітей вивозять за межі, непідконтрольні Україні, позбавляють рідного житла, батьків тощо. З метою встановлення місцезнаходження дітей підрозділи кримінального аналізу проводять моніторинг телеграм-каналів, російських новин, соціальних мереж та відкритих баз даних, аби мати можливість встановити якомога більшу кількість викрадених дітей. Вищевказаний інструментарій з недавнього часу отримав свою назву – OSINT (Open Source Intelligence). Наукові джерелах зазначають, що OSINT це – діяльність по отриманню розвідувальної інформації з відкритих джерел кіберпростору [4].

В умовах, у яких знаходиться наша країна на сьогоднішній день одержання достовірної інформації в найкоротші терміни є важливим та необхідним не тільки для Збройних сил України, але й для підрозділів кримінальної поліції та Національної поліції в цілому, для Служби безпеки України та інших підрозділів, які здійснюють підслідність. Саме тому все частіше зустрічаємо інформацію, що правоохоронні органи використовують різні технологічні методи збору інформації, а також методи OSINT в своїй службовій діяльності.

Відповідно до статті 1 Закону України «Про інформацію» інформація являє собою будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [5]. Отже, таким чином законодавець відносить до суті інформації «відомості та/або дані», що представляють собою саме інформацію, перероблену в певну форму представлення, тобто, вищезазначені дані або відомості, а не інформація як знання про різні факти, події та речі, які, у свою чергу, не є інформацією в чистому вигляді [6].

Діяльність OSINT також дає можливість отримувати доступ до

електронних даних, таких зокрема як, листування, документи або ж інші електронні записи, які в свою чергу можуть становити доказову базу в кримінальному провадженні, щодо воєнних злочинів. Крім того, за допомогою методів OSINT можна фіксувати та ідентифікувати самих суб'єктів вчинення злочинів, та в результати мати змогу притягнути їх до відповідальності. OSINT відноситься до процесу збору інформації з загальнодоступних джерел, насамперед таких як соціальні медіа, різноманітні агентства новин, урядові записи та супутникові знімки.

Отже, висновуємо що найвідомішими та найбільш необхідними базами даних, якими користуються підрозділи кримінального аналізу у своїй повсякденній діяльності для розслідування воєнних злочинів є:

1. Maltego – це багатофункціональна платформа розвідки з відкритим кодом, створена для оптимізації та прискорення розслідувань;
2. Spiderfoot – це відкритий інструмент який дозволяє здійснювати збір і аналіз даних, таких як, IP-адреси, діапазони CIDR, домени та субдомени, ASN, електронні адреси, телефонні номери, імена, імена користувачів, адреси BTC та багато іншого;
3. Lampyre – це комерційне програмне забезпечення, орієнтоване на OSINT, що надає потужні інструменти для перевірки контрагентів, аналізу кіберзагроз, розслідування злочинів та фінансової аналітики;
4. Recon-ng – завдяки його функціоналу користувачі мають змогу здійснювати ідентифікацію вразливостей веб-ресурсів, проводити аналіз GeoIP, вивчати DNS-записи та здійснювати сканування відкритих портів, а також для виявлення конфіденційних файлів тощо.

Список використаних джерел:

1. Кримінальний кодекс України від 5 квітня 2001 року № 2341-III. Дата оновлення: 17 липня 2025 року. *Вебпортал Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2341-14#n1716.
2. Іваненко Г. Є. Проведення оперативного аналізу в умовах воєнного

стану. *Актуальним є характеристика оперативного аналізу в умовах воєнного стану*: матеріали міжнар. наук.-практ. конф., м. Київ, 11 серп. 2022 р. Київ. 2022. С. 216-218.

3. Кисельов А. О. Особливості здійснення кримінального аналізу на прикладі складання аналітичного звіту (за матеріалами УКА ГУНП в Дніпропетровській області). Бюлетень з обміну досвідом роботи № 228/2021. РВВ ДНДІ. К. 2021. С. 63-67.

4. Минько О. В., Іохов О. Ю., Оленченко В. Т., Власов К. В. Використання технологій OSINT для отримання розвідувальної інформації. *Експерт: парадигми юридичних наук і державного управління*. 2019. № 4(6). С. 201–208.

5. Про інформацію: Закон України від 2 жовтня 1992 року № 2657-XII. Дата оновлення: 14 червня 2025 року. *Вебпортал Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text.

6. Бакумов О.С., Марчук М.І., Гудзь Т.І., Венглінський О.О. Інформація: до питання про змістову еволюцію терміна. *Право і безпека – Law and Safety*. 2021. № 3 (82). С. 19-28.

СЛАВІНСЬКА Аліна
курсант ННІ ПФП КП ім. Е.О. Дідоренка
Донецького державного університету внутрішніх справ
рядовий поліції

Науковий керівник:
ГАБОРЕЦЬ Ольга
доцент кафедри оперативно-розшукової діяльності та інформаційної безпеки ННІ ПФП КП ім. Е.О. Дідоренка, доктор філософії, доцент Донецького

державного університету внутрішніх справ

ЗАСТОСУВАННЯ КРИМІНАЛЬНОГО АНАЛІЗУ У БОРОТЬБІ З ОРГАНІЗОВАНОЮ ЗЛОЧИННІСТЮ В УМОВАХ ЗБРОЙНОГО КОНФЛІКТУ

Збройний конфлікт на території України створює сприятливе середовище для активізації організованої злочинності, що вимагає посилення аналітичної складової у діяльності правоохоронних органів. У таких умовах особливої ваги набуває кримінальний аналіз як ключовий інструмент виявлення, прогнозування та нейтралізації злочинних загроз. Він дозволяє системно обробляти, узагальнювати та інтерпретувати інформацію про злочинну діяльність, виявляти тенденції, зв'язки між суб'єктами та формувати прогнози щодо розвитку криміногенної ситуації.

Кримінальний аналіз являє собою специфічний різновид інформаційно-аналітичної діяльності, спрямованої на виявлення, оцінювання, інтерпретацію та прогнозування взаємозв'язків між даними про злочинну діяльність та іншими інформаційними елементами, що потенційно можуть бути з нею пов'язані. Зазначений вид аналізу використовується для забезпечення ефективності досудового розслідування, реалізації оперативно-розшукових заходів, а також для формування тактичних і стратегічних рішень у сфері протидії злочинності. [4, с. 16]. Він є складовою аналітичної роботи оперативних і слідчих підрозділів, що прямо передбачено ст. 23 Закону України «Про Національну поліцію» [1]. Згідно з Постановою КМУ № 877 від 28.10.2015 року, аналітична функція визначається як ключова для забезпечення ефективного управління в умовах загроз національній безпеці [2].

Залежно від рівня аналітичного продукту існують три види кримінального аналізу:

- Операційний кримінальний аналіз - це форма інформаційно-аналітичної діяльності, що здійснюється у межах конкретних кримінальних

проваджень та охоплює обробку інформації, яка становить оперативний інтерес для кримінальної поліції або органів досудового розслідування. Така інформація стосується осіб, об’єктів, організованих груп чи злочинних організацій, а також ознак і характеристик, що дозволяють ідентифікувати їхню діяльність та сприяють ефективному розслідуванню кримінальних правопорушень. Проводиться аналіз тенденцій злочинності, встановлюються зони підвищеної концентрації кримінальних правопорушень, а також формується узагальнений профіль ймовірного підозрюваного та потерпілого. Зазначені заходи здійснюються з метою обґрунтування управлінських рішень щодо оптимального розподілу сил і засобів, а також для проведення ефективного операційного аналізу;

- Тактичний кримінальний аналіз - це вид аналітичної діяльності, що передбачає дослідження злочинності та окремих злочинів, скоєних на визначеній території протягом короткого проміжку часу. Аналіз здійснюється за конкретними видами кримінальних правопорушень або протиправної діяльності певних груп з метою розроблення тактичних заходів щодо затримання правопорушників, виявлення потенційних ризиків та запобігання конкретним злочинам.
- Стратегічний кримінальний аналіз - це процес ідентифікації та оцінювання криміногенних загроз, що спрямовані проти особи, суспільства або держави, з метою виявлення вразливих елементів правоохоронної системи чи соціального середовища. Такий аналіз передбачає вивчення тенденцій, закономірностей і прогнозування розвитку виявлених загроз у довгостроковій перспективі, що слугує основою для прийняття управлінських рішень, спрямованих на запобігання кримінальним правопорушенням та ефективну протидію злочинності [4, с. 29].

Особливістю організованої злочинності в умовах війни є її здатність до швидкої адаптації, використання корупційних механізмів, легальних бізнес-

структур, фіктивних підприємств, а також залучення до незаконного обігу зброї, наркотиків, товарів подвійного призначення. За даними Європолу, ключовими ознаками сучасної ОЗУ є високий рівень конспірації, використання цифрових технологій, криптовалют, а також проникнення у державні та комерційні структури [3]. Кримінальний аналіз дозволяє виявляти такі загрози, систематизувати дані про злочинні схеми, виявляти нові форми злочинної діяльності - зокрема шахрайство з гуманітарною допомогою, незаконне використання військової логістики, фальсифікацію документів для переміщення осіб та вантажів. Він також сприяє координації між правоохоронними органами - Національною поліцією, СБУ, ДБР, прокуратурою - та міжнародними партнерами, зокрема Європолом та Інтерполом. Водночас існують такі суттєві виклики:

- обмежений доступ до інформації в зоні бойових дій;
- фрагментарність баз даних та відсутність єдиної аналітичної платформи;
- недостатній рівень технічного оснащення аналітичних підрозділів;
- потреба у впровадженні сучасних технологій - штучного інтелекту, геоаналітики, автоматизованих систем прогнозування.

Перспективним напрямом є інтеграція національних інформаційних систем («Аркан», «ІТС», «Рубіж», «Гарпун») з міжнародними базами даних, а також розвиток міжвідомчого обміну інформацією в режимі реального часу. Важливо також забезпечити належну підготовку аналітиків, впровадити стандарти кримінального аналізу, адаптовані до умов воєнного стану.

Значення кримінального аналізу зростає пропорційно до складності викликів, які постають перед державою: від трансформації організованих злочинних угруповань до їхньої інтеграції у воєнну економіку, корупційні схеми та міжнародні кримінальні мережі. Ефективне застосування кримінального аналізу дозволяє не лише оперативно реагувати на загрози, а й формувати превентивні заходи, прогнозувати динаміку злочинності, оптимізувати розподіл ресурсів та забезпечити міжвідомчу координацію.

Таким чином, кримінальний аналіз у період збройного конфлікту має розглядатися як невід'ємна частина державної політики у сфері безпеки, що потребує системного розвитку, інтеграції з міжнародними практиками та адаптації до реалій воєнного часу. Його подальше вдосконалення є запорукою ефективної протидії організованій злочинності та стабілізації криміногенної ситуації в Україні.

Список використаних джерел:

1. Закон України «Про Національну поліцію» від 02.07.2015 № 580-VIII. [Електронний ресурс] - https://zakon.rada.gov.ua/laws/show/580-19#n162

2. Постанова Кабінету Міністрів України № 877 «Про затвердження Положення про Національну поліцію» від 28.10.2015. [Електронний ресурс] - https://zakon.rada.gov.ua/laws/show/877-2015-%D0%BF#Text

3. Europol. Serious and Organised Crime Threat Assessment (SOCTA) 2021. [Електронний ресурс] - https://www.europol.europa.eu/socta-report

4. Навчальний посібник Федчак І.А. «Основи кримінального аналізу». С. 16-30

СНІЖКО Софія
курсантка факультету підготовки фахівців для органів досудового розслідування Національної поліції України Донецького державного університету внутрішніх справ

Науковий керівник:
ДРОБЕНКО Діна
викладач кафедри кримінального процесу та криміналістики факультету підготовки фахівців для органів досудового розслідування Національної поліції України Донецького державного університету внутрішніх справ

ЗАСТОСУВАННЯ КРИМІНАЛЬНОГО АНАЛІЗУ ДЛЯ ВИЯВЛЕННЯ СХЕМ НЕЛЕГАЛЬНОГО ОБІГУ ЗБРОЇ

Застосування кримінального аналізу для виявлення схем нелегального обігу зброї є одним із найважливіших інструментів протидії, особливо в умовах збройного конфлікту, коли традиційні контролюючі механізми часто виявляються ослабленими або паралізованими. Кримінальний аналіз не обмежується лише збором і перерахунком фактів — це системний процес перетворення розрізнених відомостей у зрозумілу модель поведінки злочинних мереж, яка дозволяє передбачати їхні кроки, виявляти вразливі місця логістики і фінансування та планувати цілеспрямовані операції з нейтралізації каналів постачання. У практиці аналітика це означає синтез оперативних повідомлень, результатів експертиз, митних і логістичних реєстрів, фінансових транзакцій, метаданих зв’язку, відкритих джерел інформації та спостережень на місцях — кожен фрагмент допомагає заповнити картину схеми [1; 2].

На початковому етапі аналітичної роботи формується гіпотеза щодо

механізму постачання: чи йдеться про прямий імпорт з-за кордону, контрабандні коридори через суміжні території, внутрішню реквізицію чи легалізацію через підставні фірми. Для перевірки гіпотез збираються і систематизуються дані — телефонні метадані та переговори, які можуть виявити мережеві зв'язки; фінансові сліди, що вказують на канали оплати; записи перевезень і логістики; результати балістичних досліджень, що дозволяють зв'язати окремі одиниці зброї з певними партіями; а також інформація з відкритих джерел: оголошення, соціальні мережі, супутникові знімки. Саме кореляція цих різнорідних даних, а не кожен окремий індикатор, створює доказову базу, яка дає змогу вивести на центральні вузли мережі — координаторів, посередників, постачальників і фінансових операторів [3].

Методи лінк-аналізу та візуалізації мереж дозволяють виявити ключові вузли та «білі плями» у схемі. Часто з одного на перший погляд незначного елементу — наприклад, регулярних дрібних грошових переказів на рахунки підставних компаній або повторюваних маршрутів транзиту вантажів через певні перевалочні пункти — випливає підтвердження існування складної логістичної структури. Геопросторовий аналіз, який поєднує дані GPS, супутникові знімки та повідомлення з місць, дозволяє картографувати маршрути та виявляти склади й перевалочні пункти. У конфліктних зонах, де доступ команд слідства може бути обмежений, такі віддалені методи стають стратегічно важливими для ідентифікації «гарячих» точок, які потім виводяться на операційне реагування.

Фінансовий трасінг відіграє роль «чутного» сліду, який часто веде до організаторів. Аналіз платіжних потоків — від офіційних банківських транзакцій до готівкових переказів і систем обміну валют — дозволяє встановити, які суб'єкти отримують кошти та яким чином вони легалізуються через бізнес-структури. Саме тут поєднання традиційної фінансової криміналістики та алгоритмів виявлення аномалій у великих даних дає змогу виявити нетипові схеми, наприклад ланцюги між кількома країнами з підставними фірмами, або використання криптовалют і платіжних сервісів для

маскування джерела коштів. Поєднання фінансових доказів із фізичними — вилученою зброєю, балістичними експертизами або записами переміщень — створює комплексну картину, придатну для судових процесів [4].

Технічні засоби і сучасні технології значно розширюють можливості кримінального аналізу. Бази даних балістичних відповідностей, системи розпізнавання серійних номерів, платформи для аналізу соціальних мереж, інструменти для обробки великих обсягів метаданих — все це дозволяє автоматизувати рутинні операції і зосередити увагу аналітика на інтерпретації складних патернів. Дрони і супутникові сервіси дають можливість моніторити віддалені райони та виявляти склади, навіть коли доступ наземних сил обмежений. Машинне навчання допомагає виявляти аномалії у фінансових потоках або в поведінці онлайн-оголошень, що раніше могли залишатися непоміченими.

Разом із тим робота аналітика стикається з численними обмеженнями. У зоні бойових дій інформація часто фрагментована та суперечлива: джерела можуть бути упередженими або свідомо фальсифікувати дані. Корупція і місцева колаборація іноді роблять певні коридори недоступними для контролю, а використання шифрованих каналів зв’язку і анонімних платіжних послуг ускладнює трасінг. Юридичні бар’єри — обмежений доступ до персональних даних, необхідність дотримання процесуальних норм при перехопленні комунікацій — вимагають від аналітиків високого рівня правової грамотності, щоб зібрані докази були прийнятними в суді. Етичні міркування — захист приватності цивільних, уникнення помилкових звинувачень і забезпечення безпеки інформаторів — також мають стояти на першому місці при плануванні аналітичних заходів.

Щоб підвищити ефективність кримінального аналізу, необхідна системна міжвідомча й міжнародна кооперація. Обмін даними між поліцією, прикордонною службою, митницею, розвідувальними органами та фінансовими регуляторами створює умови для комплексної картини та синергетичного реагування. Стандартизація форматів даних і створення

захищених каналів комунікації спрощують обмін розвідданими і скорочують час реагування. Важливими є також інвестиції в кадри — цілеспрямовані тренінги з фінансової криміналістики, балістики, OSINT та цифрової аналітики, а також постійне оновлення технічних засобів для обробки великих обсягів даних.

На операційному рівні аналітичні висновки мають трансформуватися у конкретні дії: планування контрольованих закупівель, блокування маршрутів, арешти ключових координаторів, блокування фінансових рахунків і вилучення товарів. Критично важливо, щоб такі дії були скоординовані і ґрунтувалися на міцній доказовій базі — інакше ризик провалу операції або юридичної дискредитації зростає. Післяопераційний аналіз також має стати регулярною практикою: вивчення причин успіхів і поразок, адаптація інструментів і процедур відповідно до нових схем контрабанди.

Таким чином, кримінальний аналіз виступає не просто як набір технік, а як стратегічний підхід до руйнування логістики й фінансування нелегального обігу зброї. У складних умовах збройного конфлікту його роль особливо вагома: тільки через системну аналітичну роботу можливо перейти від реагування на поодинокі інциденти до проактивного руйнування мереж і мінімізації загроз для цивільного населення та національної безпеки [1–4].

Список використаних джерел:

1. . Кримінальний кодекс України від 05.04.2001 № 2341-III // URL https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 26.09.2025).

2. Закон України «Про Національну поліцію» від 02.07.2015 № 580-VIII // URL https://zakon.rada.gov.ua/laws/show/580-19#Text (дата звернення: 26.09.2025).

3. Наказ Міністерства внутрішніх справ України «Про затвердження Інструкції про порядок виготовлення, придбання, зберігання, обліку, перевезення та використання вогнепальної, пневматичної, холодної і охолощеної зброї, пристроїв вітчизняного виробництва для відстрілу патронів,

споряджених гумовими чи аналогічними за своїми властивостями метальними снарядами несмертельної дії, та патронів до них, а також боєприпасів до зброї, основних частин зброї та вибухових матеріалів» від 21.08.1998 № 622 // URL https://zakon.rada.gov.ua/laws/show/z0637-98#Text (дата звернення: 26.09.2025).

4. Наказ Міністерства внутрішніх справ України «Про затвердження Порядку декларування вогнепальної зброї і боєприпасів до неї» від 18.11.2024 № 768 // URL https://zakon.rada.gov.ua/laws/show/z1739-24#Text (дата звернення: 26.09.2025).

ШЕВЦОВА Анастасія
курсант 1 групи 3 курсу факультету №2 Львівського державного університету внутрішніх справ

Науковий керівник:
МОВЧАН Анатолій
професор кафедри оперативно-розшукової діяльності Львівського державного університету внутрішніх справ доктор юридичних наук, професор

РОЛЬ КРИМІНАЛЬНОГО АНАЛІЗУ У ПРОТИДІЇ ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ ПІД ЧАС ЗБРОЙНОГО КОНФЛІКТУ

Сучасні суспільства стикаються з численними викликами безпеки, серед яких особливе місце посідає організована злочинність – явище, що діє системно, координовано та у широких масштабах. Вона проявляється у різних формах – від фінансових махінацій до насильницьких дій – і в умовах збройного конфлікту набуває ще більшої небезпеки. Використовуючи хаос, ослаблення державних інститутів і зниження рівня контролю, злочинні угруповання отримують можливість діяти з мінімальним ризиком.

У таких умовах протидія організованій злочинності потребує нових

підходів, серед яких ключову роль відіграє кримінальний аналіз. Він дає змогу визначати структуру злочинних мереж, встановлювати їхні зв'язки та прогнозувати потенційні загрози для суспільства. Тому особливо актуальним є дослідження ролі кримінального аналізу у протидії організованій злочинності в умовах збройного конфлікту, що має безпосереднє значення для сучасної війни росії проти України.

Кримінальний аналіз у контексті збройного конфлікту передбачає систематичне дослідження кримінальної інформації, опрацювання великих масивів даних і формування прогнозів щодо діяльності організованих злочинних угруповань. Він охоплює збір відомостей з оперативних джерел, баз даних правоохоронних органів, відкритих ресурсів та соціальних мереж, що дає змогу виявляти закономірності у поведінці злочинних структур. Особливу увагу аналітики приділяють встановленню лідерів угруповань, каналів фінансування, способів координації дій і методів впливу на суспільство. В умовах війни ці аспекти набувають особливого значення, адже організована злочинність нерідко поєднує свою діяльність із незаконною торгівлею зброєю, контрабандою ресурсів та експлуатацією вразливих груп населення [1, с. 63].

У практичному вимірі кримінальний аналіз дозволяє правоохоронним органам ефективно планувати операції, мінімізувати ризики для цивільного населення та сил безпеки, а також раціонально використовувати обмежені ресурси в умовах кризи. Завдяки аналітичним методам можна встановлювати причинно-наслідкові зв'язки між злочинними діями та військовими подіями, прогнозувати можливі сценарії діяльності угруповань і запобігати загрозам ще до їхньої реалізації. Крім того, кримінальний аналіз сприяє систематизації доказів для судових проваджень, що має вирішальне значення для забезпечення верховенства права навіть у періоди нестабільності.

Науковці підкреслюють важливість застосування методів мережевого аналізу, які дозволяють візуалізувати взаємозв'язки між учасниками злочинних структур, визначати ключові ланки та контролювати інформаційні потоки. В умовах збройного конфлікту такі підходи стають ефективним інструментом

для відстеження руху фінансів, зброї, контрабанди та інших ресурсів. Використання сучасних технологій – зокрема систем обробки великих даних і штучного інтелекту – дає змогу аналізувати тисячі подій, моделювати поведінку злочинних мереж і прогнозувати потенційні ризики для безпеки держави та суспільства [2, с. 109].

Не менш важливим напрямом кримінального аналізу є його психологічний аспект, який зосереджується на розумінні мотивації учасників організованих злочинних угруповань, їхньої здатності до адаптації, стратегічного мислення та використання вразливостей державних і суспільних структур. Аналіз психологічних характеристик злочинців дає змогу визначити рушійні чинники їхньої поведінки – від прагнення матеріальної вигоди до бажання влади, контролю чи належності до групи.

В умовах війни цей аспект набуває особливої ваги, оскільки соціальні інститути перебувають під тиском, ресурси обмежені, а рівень суспільної напруги зростає. У таких обставинах злочинні угруповання часто використовують страх, невизначеність і дезінформацію для посилення власного впливу. Аналіз поведінкових патернів дозволяє не лише ідентифікувати ключових учасників злочинних мереж, а й прогнозувати їхні подальші дії, враховуючи емоційні, соціальні та ситуативні чинники.

Завдяки цьому кримінальний аналіз перетворюється на інструмент не лише виявлення, а й попередження злочинів. Розуміння психологічних механізмів, що лежать в основі рішень злочинців, дає змогу планувати превентивні заходи, формувати ефективну комунікаційну політику правоохоронних органів і, зрештою, забезпечувати вищий рівень безпеки для цивільного населення навіть у надзвичайних умовах.

В умовах повномасштабної війни росії проти України роль кримінального аналізу стає особливо актуальною. Створення аналітичних підрозділів у Національній поліції, інтеграція з міжнародними організаціями та обмін інформацією з партнерами дозволяють підвищити ефективність протидії організованій злочинності. У воєнний час такі підходи набувають

стратегічного значення для національної безпеки, адже контроль над кримінальною діяльністю і попередження масштабних злочинів зменшують соціальні втрати та підтримують функціонування державних структур.

Таким чином, кримінальний аналіз виступає не лише інструментом розкриття злочинів, а й механізмом стратегічної протидії організованій злочинності в умовах збройного конфлікту. Він забезпечує комплексне уявлення про структуру угруповань, їхні дії та наслідки, дозволяє планувати превентивні заходи та систематизувати докази для подальших судових процедур.

Отже, роль кримінального аналізу у протидії організованій злочинності під час збройного конфлікту є ключовим елементом ефективної системи національної безпеки. Він дозволяє виявляти структури та взаємозв'язки угруповань, прогнозувати їхню поведінку, оптимізувати використання ресурсів і мінімізувати ризики для цивільного населення. У воєнний час кримінальний аналіз виступає не лише інструментом розкриття злочинів, а й важливим компонентом стратегічного планування та захисту національних інтересів.

Застосування кримінального аналізу забезпечує баланс між превентивними заходами, оперативним реагуванням і правовим забезпеченням, сприяє відновленню стабільності та зміцненню правопорядку навіть у кризових умовах. Ключове значення має усвідомлення того, що ефективна аналітика стає запорукою збереження соціальної цілісності, безпеки громадян та розвитку держави навіть у періоди масштабних військових конфліктів.

Список використаних джерел:

1. Ченцова А., Гусєва С., Кисельов А. Кримінальний аналіз в умовах воєнного стану. *UNIVERSUM*. Лютий 2024, 5, 2024. С. 62–66.

2. Кримінологія: підручник. За ред. В.Ю. Голубовського, Є.В. Кунц. М.: Юрлітінформ, 2020. 264 с.

СЕКЦІЯ 3.
РОЗВИТОК ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ОПЕРАТИВНО-РОЗШУКОВОЇ ТА КРИМІНАЛЬНОЇ ПРОЦЕСУАЛЬНОЇ ДІЯЛЬНОСТІ В УМОВАХ ВОЄННОГО СТАНУ.

АНДРУХ Віталій
старший викладач кафедри кримінального процесу та криміналістики Донецького державного університету внутрішніх справ доктор філософії в галузі права

ЩОДО ОСКАРЖЕННЯ НЕДОТРИМАННЯ РОЗУМНИХ СТРОКІВ У ДОСУДОВОМУ КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

Типовим порушенням норм кримінального процесуального закону, що має системний характер, є недотримання слідчим, дізнавачем чи прокурором розумних строків досудового розслідування. Така практика призводить до ситуацій, коли особа тривалий час перебуває у стані правової невизначеності, не маючи змоги реалізувати свої процесуальні права.

Варто зазначити, що існуючий механізм оскарження недотримання розумних строків суб'єктами сторони обвинувачення у досудовому кримінальному провадженні передбачає можливість безпосереднього звернення до прокурора вищого рівня (ст. 308 КПК України) [1]. Однак подібний механізм не може вважатися ефективним засобом правового захисту, оскільки не забезпечує незалежного та безстороннього розгляду скарги.

Причини неефективності існуючого порядку оскарження недотримання розумних строків до прокурора мають як правову, так і інституційну природу.

По-перше, відомчий характер прокурорського контролю зумовлює конфлікт інтересів, адже прокурор є представником сторони обвинувачення, яка підтримує державне обвинувачення у кримінальному провадженні. Обвинувальна спрямованість прокурора не дозволяє йому виступати незалежним та неупередженим арбітром у питаннях, що стосуються будь-яких зволікань у провадженні. Тобто прокурор не може одночасно виступати процесуальним керівником досудового розслідування і суб'єктом, що оцінює його ефективність та правомірність дотримання строків.

По-друге, ієрархічна підпорядкованість прокурора негативно впливає на об'єктивність розгляду скарг. Прокурор вищого рівня, до якого подається скарга, розглядає її не з позиції захисту прав особи, а переважно з позиції виправдання правомірності дій або бездіяльності підпорядкованих йому осіб. У результаті така процедура нерідко перетворюється на формальний розгляд без реального впливу на прискорення досудового розслідування. Прокурор як зацікавлений учасник кримінального судочинства не може забезпечити ефективний, неупереджений та незалежний контроль за дотриманням розумних строків досудового кримінального провадження.

Враховуючи зазначене, серед науковців дедалі більше утверджується думка про необхідність передачі компетенції щодо розгляду скарг про недотримання розумних строків від прокурора вищого рівня до слідчого судді [2, с. 128]. Слідчий суддя є саме тим процесуальним суб'єктом, який здатен забезпечити незалежний, неупереджений і об'єктивний розгляд скарг, оскільки він не має процесуальної зацікавленості у результатах розслідування, адже виступає представником судової гілки влади. Судовий розгляд таких скарг сприятиме дотриманню балансу між публічним інтересом держави у забезпеченні виконання завдань кримінального провадження та приватним інтересом особи щодо реалізації права на розгляд справи у розумний строк.

Роль слідчого судді у механізмі контролю за дотриманням розумних строків є ключовою, оскільки тільки суд може забезпечити незалежну оцінку обставин затягування розслідування, встановити об'єктивність причин

бездіяльності органів досудового розслідування та зобов'язати усунути виявлені порушення. Крім того, практика ЄСПЛ переконливо свідчить, що виключно судовий контроль може відповідати критеріям ефективного засобу правового захисту у розумінні ст. 13 Конвенції про захист прав людини і основоположних свобод [3; 4].

Разом з тим, необхідно зазначити, що у випадку унормування порядку оскарження недотримання розумних строків до слідчого судді постає потреба у подальшому вдосконаленні процесуального механізму контролю за дотриманням розумних строків вже слідчим суддею. Зокрема, має бути передбачена можливість оскарження недотримання розумних строків слідчим суддею до суду апеляційної інстанції. Такий підхід узгоджується із загальними принципами побудови судової системи та гарантіями доступу до правосуддя на всіх без виключення стадіях кримінального судочинства.

Отже, правова регламентація оскарження недотримання розумних строків у досудовому кримінальному провадженні до прокурора вищого рівня виглядає дефектною. Такий порядок є протилежним принципу ефективного захисту прав людини, оскільки прокурор має обвинувальну функціональну спрямованість та не може забезпечити неупереджений розгляд скарги. Внаслідок цього, зі змісту кримінального процесуального закону доречно вилучити положення, які передбачають оскарження недотримання суб'єктами сторони обвинувачення розумних строків у досудовому кримінальному провадженні до прокурора вищого рівня. Натомість важливо унормувати порядок звернення із такими скаргами безпосередньо до слідчого судді, наділивши останнього процесуальними повноваженнями здійснювати незалежний судовий контроль за дотриманням розумних строків, що забезпечить реальне, а не декларативне дотримання стандартів ефективного засобу правового захисту.

Список використаних джерел:

1. Кримінальний процесуальний кодекс України. Закон України від 13

квіт. 2012 р. № 4651-VI. *Голос України*. 2012. №№ 90-91. URL: https://zakon.rada.gov.ua/laws/show/4651-17 (дата звернення: 10.09.2025).

2. Москаленко О. В., Півненко Л. В. Щодо змісту засади розумних строків у кримінальному судочинстві. *Збірник наукових праць Харківського національного педагогічного університету імені Г. С. Сковороди. Право.* 2015. Вип. 23. С. 124-128.

3. Case of Kudła v. Poland, № 30210/96, 26.10.2000. URL: https://hudoc.echr.coe.int/eng#{%22sort%22:[%22kpdate%20Descending%22],%22itemid%22:[%22001-58920%22]} (дата звернення: 10.09.2025).

4. Case of Akdivar and others v. Turkey, № 21893/93, 19.09.1996. URL: https://hudoc.echr.coe.int/eng#{%22sort%22:[%22kpdate%20Descending%22],%22itemid%22:[%22001-58062%22]} (дата звернення: 10.09.2025).

АФАНАСЬЄВА Валерія
здобувачка вищої освіти 410-го навчального взводу Одеського державного університету внутрішніх справ

Науковий керівник:
ЯНКОВИЙ Микола
професор кафедри кримінального процесу та криміналістики Одеського державного університету внутрішніх справ, кандидат юридичних наук, професор

OSINT ЯК КРИМІНАЛІСТИЧНИЙ ІНСТРУМЕНТ ДОКУМЕНТУВАННЯ ВОЄННИХ ЗЛОЧИНІВ: ПЕРЕВАГИ ТА ОБМЕЖЕННЯ

У контексті сучасних збройних конфліктів дедалі більшого значення набуває застосування інструментів відкритої розвідки (Open Source Intelligence, OSINT) для документування та доказування воєнних злочинів. Традиційні

методи криміналістичного розслідування часто є ускладненими через недоступність місця події, руйнування інфраструктури, загрозу безпеці слідчих і свідків. У цих умовах OSINT виступає як потужний допоміжний інструмент для фіксації подій, збору доказів і підтвердження фактів порушення Міжнародного гуманітарного права.

OSINT - це процес збору, обробки, аналізу та інтерпретації інформації, яка знаходиться у відкритому доступі. Це можуть бути публікації у соціальних мережах, супутникові знімки, фото- і відеоматеріали з відкритих джерел, медіа-ресурси, блоги, бази даних та офіційні документи. У криміналістиці OSINT використовується як інструмент верифікації фактів, встановлення особи підозрюваних, хронології подій та збору доказів для подальшої юридичної оцінки [1].

OSINT дозволяє отримувати великі обсяги даних без необхідності фізичної присутності на місці події. Зокрема, зображення зі супутників або відеозаписи із соціальних мереж дають змогу зафіксувати руйнування об’єктів, використання забороненої зброї або присутність військових формувань.

На думку Д.О. Коновалової, і ми з нею погоджуємося, збір інформації, що була виявлена у ході OSINT-дослідження, може здійснюватись будь-якими методами залежно від її доказової сили (скріншот, визначення хеш-суми тощо). Аналітики OSINT можуть у реальному часі відстежувати розвиток подій, що дає можливість оперативно фіксувати факти, які можуть бути втрачені або знищені пізніше [2, с. 460].

Інструменти машинного навчання і штучного інтелекту можуть автоматично виявляти візуальні аномалії, ідентифікувати об’єкти, обличчя, місцевість тощо, значно спрощуючи процес аналізу великих масивів даних. Проте, відкриті джерела не завжди є надійними. Фейкові відео, дезінформація, змонтовані записи можуть вводити в оману слідчих. Тому OSINT, як справедливо зазначається у відповідній літературі, вимагає ретельної верифікації за допомогою інших джерел або експертизи [3, с. 78].

OSINT-дані зазвичай не визнаються як самодостатній доказ у

міжнародному кримінальному процесі. Вони можуть виступати як допоміжний матеріал, що потребує підтвердження іншими засобами доказування. Використання особистих даних, відеозаписів без згоди осіб, навіть у воєнний час, викликає дискусії щодо конфіденційності, згоди та прав людини.

У зонах бойових дій часто спостерігається нестача інтернету, блокування інформаційних каналів, цензура. Це обмежує повноцінний доступ до даних у режимі реального часу. Bellingcat — одна з найвідоміших OSINT-організацій, яка розслідувала інцидент з MH17, застосовуючи супутникові знімки, відео з You Tube і геолокацію. Conflict Intelligence Team — документує воєнні злочини, здійснені в Україні після повномасштабного вторгнення росії, збираючи цифрові докази для подальшої передачі в Міжнародний кримінальний суд. Ukrainian Witness — ініціатива збору відео з місць подій громадянами з метою фіксації руйнувань, стратифікації злочинів проти мирного населення [4, с. 167].

Таким чином, застосування OSINT як криміналістичного інструменту у документуванні воєнних злочинів має суттєвий потенціал, особливо в умовах гібридних конфліктів, коли традиційні методи збору доказів обмежені. Його переваги – швидкість, доступність, незалежність і масштабність – дозволяють розширити горизонти кримінального розслідування. Водночас OSINT не позбавлений ризиків, пов’язаних із достовірністю джерел, правовими обмеженнями та необхідністю верифікації. Отже, він повинен використовуватись як частина комплексного підходу до збору доказів, інтегрованого з традиційною криміналістикою, судовою експертизою та міжнародним правом.

Список використаних джерел:

1. Закон України «Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам». URL: https://zakon.rada.gov.ua/laws/show/2137-20#Text.

2. Коновалова Д.О. Особливості використання розвідки на основі

відкритих джерел (OSINT) у кримінальному провадженні. *Юридичний науковий електронний журнал.* 2024. № 11. С. 459-462.

3. Латиш К. Особливості використання цифрових даних OSINT у міжнародній практиці. *Сучасні реалії протидії воєнним злочинам: набутий досвід та погляд в майбутнє* : матеріали панельної дискусії VII Харківського Міжнародного юридичного форуму, м. Харків, 25 верес. 2023 р. С. 77-81.

4. Торбас О.О. OSINT при розслідуванні кримінальних правопорушень : підручник. Одеса : Юридика, 2024. 180 с.

БОЙЧУК Владислав
здобувач вищої освіти факультету службово-бойової діяльності НГУ Київського інституту Національної гвардії України

Науковий керівник:
БЕЙКУН Андрій
доцент кафедри правового забезпечення та правоохоронної діяльності факультету забезпечення державної безпеки Київського інституту Національної гвардії України кандидат юридичних наук, доцент

ТЕНДЕНЦІЇ ПРАВОВОГО РЕГУЛЮВАННЯ КІБЕРПРОСТОРУ ЯК ФІЗИЧНОГО ПРОСТОРУ ТЕАТРУ ВОЄННИХ ДІЙ

Наприкінці четвертого року від початку повномасштабної збройної агресії, російська федерація залишається основним джерелом загроз національній та міжнародній кібербезпеці, яка активно реалізує концепцію інформаційного протиборства, базовану на поєднанні деструктивних дій у кіберпросторі та інформаційно-психологічних операцій, механізми якої

активно застосовуються у війні проти України. Така деструктивна активність створює реальну загрозу реалізації наявних можливостей відбиття актів кібертероризму та кібердиверсій стосовно національної інформаційної інфраструктури.

Ще задовго до повномасштабного вторгнення росія посилила кібератаки на державні органи, оборонно-промисловий комплекс, інфраструктурні об’єкти, ІТ-мережі та ЗМІ в Україні. Кіберборотьба й кіберзахист стали одними із ключових елементів війни. Наші фахівці та хакери-волонтери не лише успішно протистоять нападам, а й завдають дошкульних ударів у відповідь. За оцінками керівника служби з питань інформаційної безпеки та кібербезпеки Апарату РНБО, Україна – єдина держава, яка змогла здобути перевагу у протистоянні кібератакам та інформаційній агресії російської федерації. Проте маємо усвідомлювати: про остаточну перемогу наразі не йдеться. Ворог також удосконалюється. Нинішній тренд – інтелектуальні атаки задля виявлення слабких місць в інфраструктурі. І світовий досвід доводить: надійна робота систем кіберзахисту залишатиметься актуальною і у мирний час [1].

Кіберпростір разом з іншими фізичними просторами де-юре визнано і фактично є одним з театрів воєнних дій. Набирає сили тенденція зі створення кібервійськ, до завдань яких належить не лише забезпечення захисту національної критичної інформаційної інфраструктури від кібератак, а й проведення превентивних наступальних операцій у кіберпросторі, що включає виведення з ладу критично важливих об'єктів інфраструктури противника шляхом руйнування інформаційних систем, які управляють такими об'єктами.

У зв’язку з триваючою повномасштабною війною, рядом дослідників, зокрема, А. Савчуком, А. Жариковою, О. Радутним, прогнозується подальше зростання інтенсивності міждержавного протиборства і розвідувально-підривної діяльності у кіберпросторі. Розширюється коло структур, які намагаються сформувати власну кіберрозвідку, оволодіти сучасними технологіями розвідувально-підривної діяльності у кіберпросторі, посилюють

державний контроль за національними сегментами мережі Інтернет. При цьому поширюється інструментарій, що передбачає накопичення великих масивів інформації щодо поведінки людини, соціальних груп та використання сучасних досягнень у сфері штучного інтелекту. Посилюється тенденція здійснення розвідувально-підривної діяльності у кіберпросторі шляхом залучення спецслужбами російської федерації, міжнародних хакерських угруповань для реалізації кібервпливу [2, с. 27].

Як зазначає експерт А. Жарикова, російська агресія на Україну не обмежилася лише збройними протистояннями. Агресія в кіберпросторі була і раніше, але, починаючи з 2022 року, вона набрала відкритих форм. Разом з тим, перед початком відкритої російської агресії було здійснено низку шпигунських операцій, які мали на меті збір інформації, насамперед, з установ суб'єктів оборонно-безпекового сектору, а також потужних суб'єктів підприємництва. Це надавало можливість владі російської федерації будувати певну стратегію подальших дій, відповідно до відомих планів української сторони. Доречі, найбільшим джерелом хакерських атак протягом 2022-2024 років у світі стає саме російська федерація, яка здійснює більш ніж половину усіх злочинних дій у цій сфері на міжнародному рівні – 58%. За нею КНДР, на яку припадає 23%. Україна займає перше місце серед тих, проти кого вони спрямовані. На Україну припадає 19% усіх світових кібератак. Для контрасту: відсоток кібератак на Бельгію, Японію та Німеччину не перевищує 3% від загальної світової кількості [3].

Слід, як вбачається, погодитись з поглядами Л.Ю. Веселової та В.В. Зуя, що й досі, не дивлячись на суворі реалії повномасштабної війни, наразі існує проблема недосконалості законодавства у сфері кібербезпеки, застарілість інформаційно-правових норм, недостатній рівень стягнень за інформаційні правопорушення, повільна та несистемна інтеграція положень європейського законодавства в окреслену сферу [4, с. 18; 5, с. 231].

Варто зазначити, що проблематика кібернетичної безпеки та державної політики, спрямованої на її забезпечення, виступає предметом наукових

досліджень багатьох вчених, насамперед, фахівців у галузі адміністративного, кримінального права, а також права інтелектуальної власності, зокрема: І.В. Арістової, І.Л. Бачило, О.Д. Довганя, Р.О. Додонова, І.М. Дороніна, В.В. Зуй, Л.В. Кузенка, О.Є. Кутафіна, В.Л. Манілова, О.В. Нестеренка, Г.В. Падалки, В.Л. Сидоренка, О.Ю. Синявської, С.Г. Стеценка, С.С. Теленика, М.М. Тищенка, Ю.П. Тихомірова, О.М. Шевчука, І.О. Харитоненка та інших.

Водночас, аналіз чинного законодавства вказує на те, що існує ряд недоліків щодо регулювання питання кібербезпеки (оборони), які потребують негайного формування пропозицій щодо шляхів вирішення існуючих проблем як з урахуванням потреб забезпечення національної безпеки в умовах повномасштабної війни, так і необхідності європейської інтеграції національного законодавства в цілому.

У цьому контексті слушно зважує С.С. Теленик на те що, держава має виступити ініціатором та гарантом ефективного розвитку і використання інформаційного простору України, особливо в оборонній сфері. Система кібербезпеки повинна бути багаторівневою і надійною, тобто такою, що унеможливить отримання несанкціонованого доступу до відомостей військового характеру, даних, що складають державну таємницю. У зв'язку з цим ряд авторів, зокрема, В.В. Зуй та С.С. Теленик пропонують створити Інформаційний кодекс України, що систематизував би інформаційно-правові норми та, зокрема, більш чітко, детально і змістовно регулював би питання забезпечення кібербезпеки. Погодимося, що наразі існує проблема недосконалості законодавства у сфері кібербезпеки, застарілість інформаційно-правових норм, недостатній рівень стягнень за інформаційні правопорушення, повільне застосування положень європейського законодавства в даній сфері. Пропонується також формування уніфікованого понятійно-термінологічного апарату у сфері кібербезпеки, а також його узгодження з термінологією чинного українського законодавства та міжнародних актів з питань кібернетичної безпеки [5, с. 233; 6].

Оновлення та розвиток чинного інформаційного законодавства вимагає,

на погляд дослідників у сфері кіберзахисту, насамперед, О.М. Суходолі, комплексного підходу, який повинен ґрунтуватись на таких засадах:

1. Розроблення та впровадження регуляторних механізмів щодо ефективного функціонування нормативного масиву з питань кібербезпеки.

2. Співпраця з стратегічними союзниками з обміну інформацією, найкращими практиками та ресурсами для забезпечення кібербезпеки.

3. Розвиток національних засобів захисту інформаційного простору та електронних ресурсів.

4. Підготовка та реагування на кібератаки, що повинно включати в себе: ідентифікацію, захист, виявлення, реагування та відновлення.

5. Впровадження загальнодержавної програми забезпечення кібер-освіти та підвищення обізнаності громадян та юридичних осіб з питань кібербезпеки.

6. Комплексність підходу до кіберзагроз та міжсекторіальне співробітництво.

7. Постійне оновлення Стратегії забезпечення державної безпеки, Стратегії кібербезпеки та інших галузевих стратегій з метою своєчасного визначення та окреслення механізму реагування на нові виклики у галузі кібернетичної загрози тощо [7].

Отже, як вбачається, особлива увага забезпечуючих структур повинна приділятись розробкам стратегічних нормативів з питань кібербезпеки, їх регулярному оновленню та контролю виконання відповідного плану заходів реалізації на основі оцінки ефективності та спроможностей. Для своєчасного поновлення таких нормативів, в Україні необхідно розробити критерії оцінки стану кібербезпеки в державі, особливо в умовах особливих правових режимів, а після проведення відповідного правового аналізу, - визначити ключові напрями формування нової Стратегії кібербезпеки України, що розраховуватиметься на період після 2025 року. Враховуючи міжнародний досвід, включно з фундаментальними рекомендаціями та директивами НАТО та ЄС, основний стратегічний напрям діяльності суб'єктів національної

системи кібербезпеки повинен бути спрямований на кіберзахист критичної інформаційної інфраструктури.

Таким чином, вирішення питань інформаційної та кібернетичної безпеки, насамперед, пов'язане із необхідністю захисту національного інформаційного простору та розвитку інформаційно-комунікаційної системи для забезпечення державної інформаційної політики, у тому числі, в умовах ескалації зовнішніх загроз та небезпек для держави до критичного рівня.

Список використаних джерел:

1. Кириченко Анастасія. Кібербезпека в Україні: шляхи розвитку та можливості. *Укрінформ.* 07 січня 2024. URL: https://www.ukrinform.ua/rubric-technology/3704093-kiberbezpeka-v-ukraini-slahi-rozvitku-ta-mozlivosti.html (дата звернення: 09.10.2025).
2. Савчук А.В. Кібербезпека в системі національної безпеки України. *Кваліфікаційна (бакалаврська) робота*. 58 с. ДоНУ імені Василя Стуса, Вінниця, 2022. URL: https://jarch.donnu.edu.ua/article/ view/12715/1261883.pdf (lsej.org.ua) (дата звернення: 09.10.2025).
3. Жарикова Анастасія. Кількість кібератак у 2023 році зросла на 16 % – Держспецзв'язку. *Українська правда*. Розділ: Економічна правда. 31 січня 2024. [Інформаційний портал]. URL: https://www.epravda.com.ua/news/2024/01/31/709355 (дата звернення: 09.10.2025).
4. Веселова Л.Ю. Адміністративно-правові основи кібербезпеки в умовах гібридної війни: *автореф. дис. докт. юр. наук*: 12.00.07; Одеський державний університет внутрішніх справ, 2021. 38 с.
5. Зуй В.В. Актуальні проблеми кібербезпеки в Україні з урахуванням європейської інтеграції. *Південноукраїнський правничий часопис*. Правове забезпечення адміністративної реформи. 4-2022, Ч.1. С. 231-235. URL: http:// www.sulj.oduvs.od.ua/archive/2022/4/part_1/35.pdf (дата звернення: 09.10.2025).
6. Теленик С.С. Державна система захисту критичної

інфраструктури України: концептуальні засади адміністративно-правового регулювання. *Монографія.* URL: https://jurkniga.ua/contents/derzhavna-sistema-zakhistu-kritichnoi-infrastrukturi-ukraini-kontseptualni-zasadi-administrativno-pravovogo-regulyuvannya.pdf?srsltid=AfmBOopbP3IBUus1V-aeQGzd7p8muhVRxx5YrBm WgRWWbAIcVnT7JDmq (дата звернення: 09.10.2025).

7. Державна система захисту критичної інфраструктури в системі забезпечення національної безпеки: *аналітична доповідь* / за ред. О.М. Суходолі. Київ: НІСД, 2020. 28 с.

БОНДАРЕНКО Артем
курсант 3-го курсу
Донецького державного
університету внутрішніх справ

Науковий керівник:
КВАШУК Олександр
старший викладач кафедри кримінального процесу та криміналістики факультету підготовки фахівців органів досудового розслідування Донецького державного університету внутрішніх справ, кандидат юридичних наук

ЗНАЧЕННЯ OSINT-ТЕХНОЛОГІЙ ДЛЯ КРИМІНАЛЬНОЇ ПРОЦЕСУАЛЬНОЇ ДІЯЛЬНОСТІ

В епоху цифрових технологій, коли інформація стає доступною з різних джерел, використання OSINT (Open Source Intelligence) інструментарію набуває важливого значення при розслідуванні кримінальних правопорушень.

OSINT – це процес збору, аналізу і використання інформації, яка перебуває у відкритому доступі. Ця інформація може бути отримана з різних

джерел, таких як вебсайти, соціальні мережі, публічні бази даних, новинні ресурси, блоги тощо. Основною метою упровадження методики OSINT є збирання релевантної інформації для подальшого аналізу і прийняття рішень.

Цей підхід застосовується в різних сферах, включаючи правоохоронну діяльність, розвідку, бізнес-аналітику, кібербезпеку та ін. У сучасних умовах, коли велика кількість інформації публікується онлайн, OSINT стає важливим інструментом для здійснення різних видів аналізу та досліджень [1].

Отже, OSINT – це сукупність способів і методів пошуку інформації у загальнодоступних джерелах, таких як: соціальні мережі та відкриті бази даних в Інтернеті. Основними перевагами OSINT є доступність джерел та економія матеріальних ресурсів для отримання такої інформації.

Використання можливостей OSINT для цілей досудового розслідування розширяє інструментарій слідчого, прокурора, дізнавача, оперативних підрозділів із отримання інформації, що має значення для виконання завдань кримінального провадження, дозволяючи встановити особу підозрюваного за фотографією, місцезнаходження особи, яка перебуває в розшуку – за допомогою соціальних мереж, зокрема особистих сторінок розшукуваної особи та кола її знайомих; встановити відомості про коло спілкування та інтереси особи тощо. Слід мати на увазі, що OSINT включає не лише процес пошуку інформації як такий, але передбачає і технологію збереження, відповідної обробки та порівняння з іншою інформацією з метою досягнення певного результату щодо встановлення обставин, що мають значення для кримінального провадження, висунення криміналістичних версій, планування процесу розслідування [2].

Основні напрямки використання OSINT у кримінальному провадженні передбачають: ідентифікацію та розшук (встановлення особистих даних, зв'язків, звичок та геолокації підозрюваних/обвинувачених, а також для розшуку прихованого майна та активів, що особливо актуально при розслідуванні економічних та корупційних злочинів); розслідування кіберзлочинів (OSINT слугує основою для відстеження цифрових слідів,

аналізу метаданих та ідентифікації джерел злочинної діяльності у кіберпросторі та даркнеті); документування воєнних злочинів (в умовах агресії OSINT став одним із ключових джерел інформації для документування подій, фіксації руйнувань та встановлення причетних осіб).

На сьогодні, за даними Офісу Генерального прокурора, зареєстровано понад 187 тис. воєнних злочинів, і від того, наскільки якісно будуть зафіксовані докази та встановлені обставини їх вчинення, напряму залежать шанси встановити справедливість і притягнути винних у їх вчиненні до передбаченої законом відповідальності. І попри значний обсяг справ цієї категорії мова йде не про далеке майбутнє – близько 3 тис. відповідних кримінальних проваджень національні суди вже розглянули, тож відповідна судова практика активно формується. У сучасних реаліях OSINT (розвідка на основі відкритих джерел) є одним із ключових джерел інформації, що широко використовується в процесі збору доказів щодо вчинення злочинів, зокрема воєнних. Така практика вимагає від національної правової системи не лише глибшого розуміння специфіки цифрових доказів, але й активного вивчення і впровадження найкращого міжнародного досвіду в цьому питанні [3].

Таким чином, OSINT-технологія є незамінним інструментом сучасної кримінальної процесуальної діяльності, який забезпечує швидкий та ефективний збір інформації для розслідування**.** Основна цінність методики полягає у здатності перетворювати величезні масиви публічних даних – від соціальних мереж і відкритих реєстрів до геоінформаційних систем – на оперативні орієнтири та потенційні електронні докази у широкому спектрі проваджень, включаючи кіберзлочини, економічні злочини, розшук активів тощо.

Головною проблемою використання цього інструменту є забезпечення процесуальної достовірності та допустимості отриманих результатів, що має привернути увагу законодавця до необхідності удосконалення нормативного забезпечення процедур роботи із цифровими доказами на рівні КПК, продовження відповідних досліджень та розробки науково обґрунтованих

рекомендацій із урахуванням сучасного практичного досвіду пошуку, виявлення та фіксації відомостей про кримінальні правопорушення та осіб, які їх вчинили.

Список використаних джерел:

1. OSINT: технологія збору та аналізу даних з відкритих джерел. 2022. URL: https://softlist.com.ua/articles/osint-tekhnologiya-sbora-i-analiza-dannyh-iz-otkrytyh-istochnikov/ .

2. Ліхтанська, А. П., Михайлов, В. О. (2024). Використання OSINT в кримінальному праві України. Dictum factum, *№ 1*, С. 105–111. URL: https://df.duit.in.ua/index.php/dictum/article/view/319/286.

3. OSINT як доказ у розслідуванні воєнних злочинів: представники ВС взяли участь у тематичному семінарі. URL: https://supreme.court.gov.ua/supreme/pres-centr/news/1883443.

ВИНОГРАДОВА Ксенія
Курсант 3 курсу Дніпровського державного університету внутрішніх справ

Науковий керівник:
ВАРАВА Володимир
доцент кафедри ОРД Дніпровського державного університету внутрішніх справ

СУЧАСНІ ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ ОПЕРАТИВНО-РОЗШУКОВОЇ ДІЯЛЬНОСТІ В УКРАЇНІ

Дослідження сучасних проблем та перспектив розвитку оперативно-розшукової діяльності в Україні є надзвичайно актуальним з низки об’єктивних

причин, зумовлених як загальними глобальними викликами, так і специфічними умовами української дійсності.

Оперативно-розшукова діяльність - це система гласних і негласних пошукових та контррозвідувальних заходів, що здійснюються із застосуванням оперативних та оперативно-технічних засобів [1].

ОРД є ключовим інструментом протидії диверсійно-розвідувальній діяльності, тероризму, шпигунству та кіберзагрозам, які є невід'ємними складовими гібридної війни. В умовах воєнного стану значно зростає роль ОРД у виявленні та нейтралізації агентурного впливу, вербування та діяльності проросійських елементів.

Серед сучасних проблем ОРД є недостатність кваліфікованих фахівців, спеціалізованого програмного забезпечення та технічних засобів для ефективного розслідування кіберзлочинів, також слід зазначити прогалини у законах, а саме у Законі України "Про оперативно-розшукову діяльність". Норми цього закону застарілі та не враховують сучасні реалії, зокрема щодо використання новітніх технологій. Також варто враховувати відсутність єдиної інформаційної бази та ефективного механізму обміну інформацією між СБУ, Національною поліцією, ДПСУ, Бюро економічної безпеки призводить до дублювання функцій і зниження загальної ефективності. Ще не менш важливим є високе навантаження, небезпечні умови праці, особливо в умовах війни, недостатнє фінансове та соціальне забезпечення, що призводять до відтоку досвідчених кадрів.

Серед перспектив розвитку ОРД в Україні є насамперед оновлення та вдосконалення нормативно-правової бази, адже законодавство часто вважають таким, що не повністю відповідає сучасним викликам, особливо в сфері кіберзлочинності, загроз національної безпеки, нових технологій [2].

Модернізація технологій та інформаційно-аналітичного забезпечення також має значення для вдосконалення. Використання єдиних інформаційно-аналітичних систем, які дозволяють збирати, систематизувати, обробляти дані оперативно та з високою якістю підвищує ефективність ухвалення рішень

підрозділами, які здійснюють ОРД [3].

Умови воєнного стану показали, що існують нормативні та організаційні перепони, які уповільнюють застосування ОРД заходів, коли швидкість має критичне значення. Також важливою є потреба в процедурах, які дозволяють оперативно реагувати, але при цьому захищають права людини, а розробка особливих правових та організаційних механізмів дозволяють ефективно здійснювати ОРД в умовах воєнного стану, коли треба балансувати між безпекою та правами людини [4].

Отже, майбутнє оперативно-розшукової діяльності в Україні визначатиметься здатністю держави модернізувати її правові, організаційні й технологічні засади, що забезпечить ефективність у протидії злочинності та відповідність демократичним цінностям.

Список використаних джерел:

1. Про оперативно-розшукову діяльність : Закон України від 18.02.1992 № 2135-XII : станом на 9 серп. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/2135-12#Text (дата звернення: 23.09.2025).
2. Туз О. С., Тищук В. В. Сутність оперативно-розшукової діяльності // Науковий вісник Ужгородського національного університету. Серія: Право. – 2025. – № 24(3). – С. 115–120. – Режим доступу: https://visnyk-juris-uzhnu.com/wp-content/uploads/2025/03/24-3.pdf (https://visnyk-juris-uzhnu.com/wp-content/uploads/2025/03/24-3.pdf?utm_source=chatgpt.com) (дата звернення: 23.09.2025).
3. Білецький В. Сучасні виклики та напрями розвитку оперативно-розшукової діяльності в Україні // ResearchGate. – 2024. – Режим доступу: https://www.researchgate.net/publication/389870822 (дата звернення: 23.09.2025).
4. Єрьоменко В. О. Особливості оперативно-розшукової діяльності в умовах воєнного стану // Вісник ДДУВС. — 2024. — № 4. — С. 100–110. — Режим доступу: https://visnik.dduvs.edu.ua/index.php/visnyk/article/view/673

(https://visnik.dduvs.edu.ua/index.php/visnyk/article/view/673?utm_source=chatgpt.com)(дата звернення: 23.09.2025).

ВІННІЧЕНКО Іуліанія
курсантка 4-го курсу факультету підготовки фахівців для органів досудового розслідування Національної поліції України Донецького державного університету внутрішніх справ

Науковий керівник:
ПЕКАРСЬКИЙ Сергій
доцент кафедри оперативно-розшукової діяльності та інформаційної безпеки Навчально-наукового інституту підготовки фахівців для підрозділів кримінальної поліції імені Е. О. Дідоренка Донецького державного університету внутрішніх справ, кандидат юридичних наук, доцент

ОПЕРАТИВНО-РОЗШУКОВА ПРОТИДІЯ ПІДРОЗДІЛАМИ КРИМІНАЛЬНОЇ ПОЛІЦІЇ ВЧИНЕННЮ ТЕРОРИСТИЧНИХ АКТІВ

Протидія тероризму є одним з пріоритетних завдань нашої держави та набуває критичного значення для підрозділів кримінальної поліції. Терористичні акти несуть пряму загрозу життю громадян, стабільності суспільства, а також державній та національній безпеці [1]. А отже підрозділи кримінальної поліції, використовуючи гласні та негласні методи оперативно-розшукової діяльності, мають забезпечити негайне виявлення, документування та припинення підготовчої діяльності терористичних груп на ранніх етапах, що являється способом запобігти невиправним наслідкам та мінімізувати потенційну суспільну шкоду. Відповідно пошук і фіксація фактичних даних про розвідувально-підривну діяльність спеціальних служб іноземних держав та організацій, а також отримання інформації в інтересах безпеки громадян, суспільства і держави є завданням оперативно-розшукової

діяльності [2, ст. 1].

Кримінальним кодексом України (далі КК України – прим. автора) передбачено кримінальну відповідальність за діяння, пов'язані з терористичними актами. Відповідно до положень статті 258 КК України під терористичним актом слід розуміти застосування зброї, вчинення вибуху, підпалу чи інших дій, які створювали небезпеку для життя чи здоров'я людини або заподіяння значної майнової шкоди чи настання інших тяжких наслідків, якщо такі дії були вчинені з метою порушення громадської безпеки, залякування населення, провокації воєнного конфлікту, міжнародного ускладнення, або з метою впливу на прийняття рішень чи вчинення або невчинення дій органами державної влади чи органами місцевого самоврядування, службовими особами цих органів, об'єднаннями громадян, юридичними особами, міжнародними організаціями, або привернення уваги громадськості до певних політичних, релігійних чи інших поглядів винного (терориста), а також погроза вчинення зазначених дій з тією самою метою [3].

Своєю чергою, стаття 258-1 КК України передбачає підстави кримінальної відповідальності за втягнення особи у вчинення терористичного акту або примушування до вчинення терористичного акту з використанням обману, шантажу, уразливого стану особи, або із застосуванням чи погрозою застосування насильства [3].

Окрім того, чинний КК України передбачає підстави кримінальної відповідальності за:

- публічні заклики до вчинення терористичного акту [3, ст. 258-2];
- створення терористичної групи чи терористичної організації [3, ст. 258-3];
- сприяння вчиненню терористичного акту, проходження навчання тероризму [3, ст. 258-4];
- фінансування тероризму [3, ст. 258-5].

В сучасних умовах для підрозділів кримінальної поліції Національної поліції України та Служби безпеки України викликом стало вербування, через

соціальні мережі, представниками країни-агресорки українських дітей та молоді для вчинення терористичних актів. Саме тому ефективна оперативно-розшукова протидія вчиненню терористичних актів базується на системному, міжвідомчому та прогностичному підході. Це сприяє своєчасності виявлення латентних ознак підготовки до теракту та оперативній нейтралізації терористичних осередків і мереж, особливо у просторах Інтернету. Основною метою стає оперативно-розшукове запобігання вчиненню злочину, що досліджується. Це вимагає зусиль для збору та аналізу фактичних даних про злочинні наміри, джерела фінансування, канали комунікації та потенційні об'єкти терористичних актів, а також проведення відповідної роз'яснювальної роботи серед різних верств населення. Під час проведення роз'яснювальної роботи необхідно звернути увагу громадян на те, що згідно чинних норм звільняється від кримінальної відповідальності за діяння особа, крім організатора і керівника терористичної групи чи терористичної організації, яка добровільно повідомила правоохоронний орган про відповідну терористичну діяльність, сприяла її припиненню або розкриттю злочинів, вчинених у зв'язку із створенням або діяльністю такої групи чи організації, якщо в її діях немає складу іншого злочину [2, ст. 258-3].

Окрім того, необхідно вказати на те, що в сучасних умовах розвитку інформаційно-комунікативних технологій, більшість складових вчинення терористичних актів відбувається у кіберпросторі, і тому, важливим для оперативно-розшукової протидії злочинним викликам є застосування спеціалізованих оперативно-розшукових заходів та слідчих (розшукових) дій. Такими заходами є:

- моніторинг різних Інтернет-платформ та месенджерів;
- ідентифікація осіб, причетних до поширення та здійснення вербування (особливо щодо дітей та молоді);
- збір фактичних даних з подальшим забезпеченням процесуальної належності, допустимості, достовірності доказів [3, ст. 94].

Відповідно оперативно-розшукова діяльність підрозділів кримінальної

поліції спрямовується на протидію розвідувально-підривній діяльності спеціальних служб країни-агресорки. А подальший кримінальний аналіз зібраних оперативних даних, перетворює їх на прогностичну модель загроз та сценаріїв дій терористів. Своєчасне встановлення моделі загроз, на нашу думку, сприятиме координації всіх сил та засобів, а також забезпечить протидію вчиненню терористичного акту.

Проведений нами теоретичний аналіз дозволяє дійти висновку, згідно до якого оперативно-розшукова протидія вчиненню терористичних актів підрозділами кримінальної поліції є ключовим аспектом системи національної та державної безпеки в умовах повномасштабної агресії росії проти України.

Список використаних джерел:

1. Про національну безпеку України: Закон України від 21 червня 2018 року № 2469-VIII. Дата оновлення: 05 жовтня 2025 року. *Вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text.

2. Про оперативно-розшукову діяльність: Закон України від 18 лютого 1992 року № 2135-XII. Дата оновлення: 09 серпня 2024 року. *Вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/2135-12#Text.

3. Кримінальний кодекс України від 5 квітня 2001 року № 2341-III. Дата оновлення: 17 липня 2025 року. *Вебпортал Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2341-14#n1716.

4. Кримінальний процесуальний кодекс України від 13 квітня 2012 року № 4651-VI. Дата оновлення: 01 серпня 2025 року. *Вебпортал Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text.

ГОЛОВКІН Сергій

доцент кафедри кримінального процесу та криміналістики факультету підготовки фахівців для органів

досудового розслідування Національної поліції України Донецького державного університету внутрішніх справ, кандидат юридичних наук, доцент

ДЕЯКІ ОСОБЛИВОСТІ ПРОВЕДЕННЯ СЛІДЧИХ (РОЗШУКОВИХ) ДІЙ ПРИ РОЗСЛІДУВАННІ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, ВЧИНЕНИХ ОРГАНІЗОВАНИМИ ГРУПАМИ

Організована злочинність сьогодні залишається однією з найсерйозніших загроз національній безпеці. Її характерною рисою є високий рівень координації, планування та професіоналізму злочинців. Саме тому розслідування кримінальних правопорушень, вчинених організованими групами, потребує від слідчих підвищеної обережності, тактичної гнучкості й тісної взаємодії з оперативними підрозділами. Слідчий огляд та обшук є слідчими (розшуковими) діями, які спрямовані перш за все на виявлення, фіксацію та вилучення криміналістично значущої інформації з матеріальних об'єктів та мають суттєве значення в розслідуванні кримінальних правопорушень, вчинених організованими групами.

Огляд місця події є першочерговою слідчою (розшуковою) дією, що закладає основу для подальшого доказування. Водночас кримінальні правопорушення, вчинені організованими групами, мають низку особливостей, які значною мірою впливають на зміст, послідовність і тактику проведення огляду.

Традиційно огляд місця події, як і будь-яка інша слідча (розшукова) дія, охоплює три етапи: 1) підготовчий; 2) робочий; 3) заключний. Підготовчий етап має ключове значення, адже саме він визначає якість отриманих доказів. Перед виїздом на місце події слідчий повинен отримати актуальну інформацію про можливу діяльність організованої групи; оцінити потенційні ризики – збройний опір, наявність вибухонебезпечних предметів тощо; забезпечити

необхідний склад слідчо-оперативної групи, включаючи спеціалістів-криміналістів, вибухотехніків, ІТ-фахівців тощо; підготувати засоби фіксації – фото-, відеоапаратуру, дрони, 3D-сканери.

Проведення огляду місця події в кримінальних провадженнях даної категорії відзначається наступними особливостями:

- організовані групи можуть використовувати кілька локацій – місце підготовки, місце вчинення кримінального правопорушення, місце зберігання знарядь чи викраденого. Тому доцільно проводити координовані або одночасні огляди на різних об’єктах;

- внаслідок ретельного планування кримінальних правопорушень основні сліди можуть бути відсутні. Значення набувають опосередковані ознаки – запахові сліди, мікросліди, частинки ґрунту, фрагменти упаковок тощо;

- організовані групи на місці вчинення кримінальних правопорушень часто створюють обстановку, яка не відповідає дійсності. Особливу увагу при проведенні огляду слід приділяти виявленню негативних обставин, що дозволить встановити інсценування кримінального правопорушення з метою приховання організованої злочинної діяльності;

- в процесі огляду важливо виявляти не лише предметні сліди, але й ознаки спільної діяльності – кількість і типи слідів, способи комунікації, знаки умовних позначень, внутрішню логістику дій злочинців;

- оскільки кримінальні правопорушення, вчинені організованими групами нерідко супроводжуються спробами знищення доказів, важливо забезпечити повну, безперервну та детальну фіксацію кожного етапу огляду;

- під час огляду місця події нерідко виявляються відомості, що потребують негайного реагування - проведення обшуків, затримань, виявлення спільників. Тому слід забезпечити координацію між слідчим та оперативними працівниками, щоб результати огляду оперативно використовувалися для подальших слідчих (розшукових) дій.

Ретельний, тактично правильний і своєчасний огляд дозволяє не лише

встановити обставини події, але й розкрити структуру організованої групи, характер її діяльності та роль кожного учасника. Саме тому удосконалення практики проведення цієї слідчої (розшукової) дії є важливим напрямом підвищення ефективності боротьби з організованою злочинністю.

Для розслідування кримінальних правопорушень, вчинених організованими групами суттєве значення має обшук, який є однією з найважливіших і найрезультативніших слідчих (розшукових) дій, спрямованих на виявлення й вилучення предметів, документів, цінностей, знарядь кримінального правопорушення, а також осіб, що переховуються від органів досудового розслідування.

При розслідуванні кримінальних правопорушень, вчинених організованими групами, обшук набуває особливої складності, адже злочинці діють злагоджено, конспіративно та, як правило, мають високий рівень підготовки до протидії слідству. Організовані групи зазвичай заздалегідь готуються до можливих обшуків – облаштовують схованки, знищують або переміщують докази, використовують охоронні системи, паролі, кодові замки, камери відеоспостереження, спеціальні шифри. З огляду на це, перед проведенням обшуку в тісній координації з оперативними підрозділами необхідно:

- отримати достовірну інформацію про місцезнаходження доказів і осіб;

- визначити усі можливі об’єкти обшуку (житло, офіси, транспорт, склади, електронні носії, сервери);

- підготувати резервні групи для одночасних або послідовних дій;

- забезпечити охорону учасників обшуку у разі можливого збройного опору.

З метою мінімізації витоку інформації та забезпечення раптовості, обшуки при розслідуванні кримінальних правопорушень, вчинених організованими групами часто проводяться одночасно за кількома адресами (житлові приміщення, місця зустрічей, офіси, склади, транспортні засоби). При проведенні одночасних обшуків доцільним є створення єдиного

координаційного центру, що буде здійснювати управління діями кількох груп обшуку, забезпечувати синхронність та оперативний обмін інформацією.

Члени організованих груп зазвичай демонструють агресивну поведінку, узгоджені лінії захисту або імітують непоінформованість. Слідчий повинен вміти оперативно реагувати, дотримуючись законності та прав людини. Важливо забезпечити нейтралізацію психологічного впливу злочинців, роз'єднати їх під час проведення обшуку, мінімізувати їхню комунікацію між собою.

Метою обшуку є не лише вилучення речових доказів, але й встановлення зв'язків між членами організованої групи, виявлення:

- спільних планів, схем, фінансових документів;
- засобів зв'язку (телефони, комп'ютери, месенджери);
- списків учасників, контактів, адрес, паролів.

Результати обшуку часто є ключовими доказами існування організованої групи та розподілу ролей.

Проведення обшуку при розслідуванні кримінальних правопорушень, вчинених організованими групами, характеризується не тільки підвищеним рівнем підготовки злочинців до протидії, але й необхідністю попереднього планування та координації між підрозділами, масштабністю, багатолокаційністю та технологічним забезпеченням, потребою у злагодженій роботі фахівців різних напрямів, суворим дотриманням процесуальної форми для забезпечення допустимості доказів.

Таким чином, ефективність обшуку при розслідуванні кримінальних правопорушень, вчинених організованими групами, визначається поєднанням оперативної раптовості, правової бездоганності, технічного оснащення та високої професійної підготовки учасників цієї слідчої (розшукової) дії.

ДЕРЕВ'ЯНЧЕНКО Юрій
начальник УКР Головного управління Національної поліції

в Кіровоградській області,
полковник поліції
аспірант Донецького державного університету внутрішніх справ

ПІДСТАВИ РОЗШУКУ ОСІБ, ЗНИКЛИХ БЕЗВІСТИ ЗА ОСОБЛИВИХ ОБСТАВИН

Складність здійснення пошукових заходів та слідчих (розшукових) дій щодо встановлення місцезнаходження осіб, зниклих безвісти за особливих обставин обумовлюється наявними проблемами правового регулювання організаційного та тактичного забезпечення даного напрямку діяльності підрозділів Національної поліції. Натепер актуалізувалися питання щодо своєчасного отримання інформації, що може сприяти розшуку особи, взаємодії зі слідчими підрозділами та судово-медичними установами при ідентифікації тіл та проведенні репатріаційних заходів. У зв'язку з цим, неабиякої актуальності набуває питання правового, організаційного та тактичного забезпечення розшуку осіб, зниклих безвісти за особливих обставин, встановлення їхнього місцезнаходження чи місця поховання.

Основоположною базою для дослідження розшуку осіб, зниклих безвісти за особливих обставин є праці таких вітчизняних науковців, як: І. В. Басиста, Б. І. Бараненко, О. В. Бочковий, В. І. Галаган, В. Г. Дрозд, М. І. Єрофеєв, О. С. Закальський, С. В. Зеленцов, О. М. Калачова, О. В. Ковальова, Л. О. Кожура, С. А. Комісаров, М. В. Кривонос, Л. М. Максимів, М. М. Перепелиця, С. В. Терешонок та ін.

Водночас, незважаючи на наявні праці вчених, в теорії оперативно-розшукової діяльності відсутні комплексні дослідження, пов'язані з проблематикою розшуку осіб, зниклих безвісти за особливих обставин, а тому дослідження цього аспекту видаються необхідними для можливого удосконалення відповідних суспільних відносин відповідно до положень міжнародного гуманітарного права, у тому числі визначення підстав розшуку осіб, зниклих безвісті за особливих обставин.

Відповідно до статті 4 Конвенції «Про захист цивільного населення під час війни», особами, що перебувають під захистом цієї конвенції, є ті, хто в будь-який момент та за будь-яких обставин опиняються, у разі конфлікту чи окупації, під владою сторони конфлікту або окупаційної держави, громадянами яких вони не є [1]. Положення щодо ідентифікації таких осіб та надання інформації їх найближчим родичам передбаченні у статтях 122 та 123 Женевської конвенції «Про поводження з військовополоненими» [2]. Крім того, положення, спрямовані на ідентифікацію та реєстрацію поранених і загиблих осіб, передбачені у статтях 15 – 17 Конвенції «Про поліпшення долі поранених і хворих у діючих арміях» [3]. Відповідно в статтях 19, 20 Конвенції «Про поліпшення долі поранених, хворих та осіб, які зазнали корабельної аварії, зі складу збройних сил на морі» [4] регламентується порядок встановлення долі зниклих безвісти, які померли.

У 2009 році Міжнародний комітет Червоного Хреста прийняв «Керівні принципи/Типовий закон про зниклих безвісти» відповідно до якого, зникла безвісти особа – це особа, місцезнаходження якої невідоме і яка – на основі достовірної інформації – була оголошена зниклою безвісти відповідно до національного законодавства у зв'язку зі збройним конфліктом і внутрішнім насильством, стихійними лихами чи будь-якою іншою ситуацією, що може вимагати втручання державного органу [5].

У 2018 році Верховна Рада України ухвалила Закон «Про правовий статус осіб, зниклих безвісти». Базою для його ухвалення став Типовий закон про зниклих безвісти Міжнародного комітету Червоного Хреста, але реалізувати на практиці його було дуже складно. Тому в 2022 році в умовах правового режиму воєнного стану були внесені зміни щодо розшуку осіб, зниклих безвісти за особливих обставин. Особливими обставинами законодавчий акт визнає збройний конфлікт, воєнні дії, тимчасову окупація частини території України, надзвичайні ситуації природного чи техногенного характеру [6]. Особа набуває статусу такої, що зникла безвісти за особливих обставин, з моменту внесення про неї відомостей, що містяться у заяві про

факт зникнення, до Єдиного реєстру осіб, зниклих безвісти за особливих обставин та вважається такою, що зникла безвісти за особливих обставин, з моменту подання заявником заяви про факт зникнення особи [6].

Заява про розшук особи, зниклої безвісти за особливих обставин, подається до відповідного територіального органу Національної поліції України та може бути подана родичами такої особи, представником військового формування, органом державної влади, органом місцевого самоврядування, громадським об'єднанням або будь-якою іншою особою, якій стало відомо про зникнення, а також Уповноваженим з питань осіб, зниклих безвісти за особливих обставин, якщо зазначені родичі звернулися до нього з повідомленням про зникнення особи [6]. У заяві про розшук особи, зниклої безвісти за особливих обставин, зазначається інформація, що може сприяти розшуку такої особи. Відомості, зазначені у заяві про розшук особи, зниклої безвісти за особливих обставин, підлягають внесенню до Реєстру в порядку, передбаченому Законом України «Про правовий статус осіб, зниклих безвісти за особливих обставин», протягом 24 годин після отримання Уповноваженим від Національної поліції України інформації про зникнення особи за особливих обставин або інформації про отримання заяви про розшук такої особи [6].

Відповідно до пп. 2 п. 4 розділу XI Інструкції з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні, яка затверджене наказом МВС України від 7 липня 2017 року № 575, у разі подання заяви, а саме повідомлення про безвісне зникнення особи, за обставин, що свідчать про можливість учинення стосовно неї злочину, протягом 24 год. обов'язково вносять до ЄРДР відомості про вчинення кримінального правопорушення з попередньою кваліфікацією умисного вбивства, уживають усіх передбачених КПК України заходів для всебічного, повного та неупередженого дослідження обставин кримінального провадження [7].

Одним із нововведень, щодо розшуку осіб, зниклих безвісти за особливих обставин є введення в дію наказу МВС від 05.07.2023 № 553 «Про затвердження Положення про інформаційну підсистему «Електронна розшукова справа» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України», який передбачає мету, структуру та функції інформаційної підсистеми «Електронна розшукова справа» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України», а також порядок її використання органами (підрозділами) поліції в розшуковій роботі [8]. Сам алгоритм організації розшуку осіб, зниклих без вісти за особливих обставин відображено у відомчому наказі МВС, який містить інформацію з обмеженим доступом і використовується виключно співробітниками які мають доступ до такої інформації.

Підсумовуючи викладене, треба відмітити, що на сьогодні в Україні існує позитивна динаміка врегулювання питань пов'язаних розшуком осіб, зниклих безвісти за особливих обставин. Законодавство України розвивається

відповідно до норм міжнародного права, збалансовуючи систему понять та створення відповідних органів та процедур для пошуку зниклих безвісти в умовах ведення воєнних дій на території України.

Список використаних джерел:

1. Про захист цивільного населення під час війни : Конвенція від 12 серпня 1949 р. URL: https://zako№.rada.gov.ua/laws/show/995_154#Text.

2. Про поводження з військовополоненими : Конвенція від 12 серпня 1949 р. URL: https://zako№.rada.gov.ua/laws/show/995_153#Text.

3. Про поліпшення долі поранених і хворих у діючих арміях : Конвенція від 12 серпня 1949 р. URL: https://zako№.rada.gov.ua/laws/show/995_151#Text.

4. Про поліпшення долі поранених, хворих та осіб, які зазнали корабельної аварії, зі складу збройних сил на морі : Конвенція від 12 серпня

1949 р. URL: https://zako№.rada.gov.ua/laws/show/995_152#Text.

5. ICRC, Advisory Service on International Humanitarian Law, 'Guiding Principles/Model Law on the Missing', 28 Feb. 2009. URL: https://www.icrc.org/en/document/guiding-principles-model-law-missing-model-law.

6. Про правовий статус осіб, зниклих безвісти за особливих обставин: Закон України URL: https://zakon.rada.gov.ua/laws/show/2505-19#Text.

7. Інструкція з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні: затв. наказом МВС України від 7.07.2017 р. № 575. URL: http://zakon2.rada.gov.ua/laws/show/z0937-17/page.

8. Положення про інформаційну підсистему «Електронна розшукова справа» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України»: затв. наказ МВС від 05.07.2023 № 553. URL: https://zakon.rada.gov.ua/laws/show/z1504-23#Text.

ДОРОШЕНКО Ростислав
курсант другого курсу Навчально-наукового інституту підготовки фахівців для підрозділів кримінальної поліції імені Е. О. Дідоренка Донецького державного університету внутрішніх справ

Науковий керівник:
ПЕКАРСЬКИЙ Сергій
доцент кафедри оперативно-розшукової діяльності та інформаційної безпеки Навчально-наукового інституту підготовки фахівців для підрозділів кримінальної поліції імені Е. О. Дідоренка Донецького державного університету внутрішніх справ,

кандидат юридичних наук, доцент

ОСОБЛИВОСТІ ПРОТИДІЇ ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ, ПОВ'ЯЗАНОЇ З ОБІГОМ НЕБЕЗПЕЧНИХ МАТЕРІАЛІВ

В умовах повномасштабної збройної агресії проти України проблематика радіаційного, хімічного та біологічного захисту набуває особливої актуальності та визначає нові пріоритети державної політики у сфері національної безпеки. Наслідки воєнних дій створюють комплексні ризики для навколишнього природного середовища, здоров'я населення та стабільного функціонування об'єктів критичної інфраструктури. Прикладом цього є події навколо Чорнобильської АЕС, Запорізької АЕС тощо.

У структурі сил безпеки та оборони вагоме місце посідає діяльність Національної поліції України, яка, поряд із забезпеченням правопорядку, виконує завдання з реагування на надзвичайні ситуації, документування воєнних злочинів, а також забезпечення міжвідомчої взаємодії з іншими суб'єктами сектору безпеки та оборони. В системі підрозділів кримінальної поліції функціонує Департамент забезпечення діяльності, пов'язаної з небезпечними матеріалами [1]. Основним завданням діяльності Департаменту є попередження, виявлення та припинення кримінальних правопорушень, пов'язаних з радіоактивними, хімічними, біологічними та ядерними матеріалами (РХЯ), відходами або іншими речовинами та матеріалами, які за своїми властивостями можуть створити або створюють небезпеку для життя, здоров'я людей чи для довкілля (далі – небезпечні матеріали) [1].

У сучасних умовах України загроза радіаційних, хімічних або біологічних інцидентів є реальною через техногенні аварії, обстріли та інші військові дії, а також через дії злочинних спільнот, які пов'язані з незаконним поводженням із небезпечними речовинами. Інструкція про порядок дій органів (підрозділів) поліції в разі виявлення радіоактивних, хімічних та ядерних матеріалів або отримання інформації про порушення правил чи незаконне поводження з ними, яка затверджена наказом МВС України від 06 вересня

2017 роки № 754 визначає що при отриманні повідомлення про порушення правил або незаконне поводження з РХЯ матеріалами чи безпосередньому виявленні підозрюваного об’єкта поліцейські зобов’язані негайно вжити заходів щодо забезпечення індивідуальної та публічної безпеки, недопущення подальшого контакту людей та тварин з ними, та в обов’язковому порядку повідомити оперативного чергового по органу (підрозділу) поліції про цей факт [2].

Поліцейські СОГ при виїзді на зазначені повідомлення обов’язково повинні бути екіпіровані комплектом спеціального одягу та засобів індивідуального захисту у складі: засобів захисту шкіри, органів дихання та зору (халат, бахіли, респіратор (протигаз) або одноразова марлева маска, гумові рукавички, окуляри відкритого і закритого типу тощо), спеціальними приладами для виявлення та попередньої ідентифікації РХЯ матеріалів, індивідуальними дозиметрами, радіометричними та дозиметричними приладами, експрес-тестами для визначення небезпечних речовин, сертифікованими у відповідному порядку [2]. При цьому перед початком огляду місця події старший СОГ інструктує фахівців заінтересованих органів державної влади про вжиття заходів щодо збереження слідів для криміналістичного дослідження (відбитки папілярних візерунків пальців рук, сліди ніг (взуття), транспортних засобів, біологічні залишки слини, волосся, крові тощо) [2].

СОГ здійснює огляд місця події виключно в присутності фахівців заінтересованих органів державної влади. Вилучення підозрюваного об’єкта здійснюється в присутності інспектора-криміналіста фахівцями, екіпірованими засобами індивідуального захисту, відповідно до повноважень одного із заінтересованих органів державної влади чи іншого суб’єкта, до сфери повноважень якого належить питання поводження з відповідним РХЯ матеріалом [2].

Основними завданнями поліції є забезпечення охорони публічного порядку, допомога в евакуації населення, перекриття доступу на заражені

території та фіксація можливих злочинів, пов’язаних із застосуванням небезпечних речовин. Відповідно, діяльність поліцейських не обмежується суто реагуванням на надзвичайну ситуацію, а має стратегічне значення для подальшої кримінально-правової кваліфікації подій та формування доказової бази. Для прикладу стаття 265 Кримінального кодексу України визначає підстави кримінальної відповідальності за незаконне поводження з радіоактивними матеріалами, під яким розуміємо придбання, носіння, зберігання, використання, передача, видозмінення, знищення, розпилення або руйнування радіоактивних матеріалів (джерел іонізуючого випромінювання, радіоактивних речовин або ядерних матеріалів, що перебувають у будь-якому фізичному стані в установці або виробі чи в іншому вигляді) без передбаченого законом дозволу [3].

Отже, у разі виявлення ознак кримінального правопорушення, пов’язаного з незаконним поводженням із радіоактивними, хімічними чи біологічними матеріалами, поліція ініціює досудове розслідування, організовує діяльність слідчо-оперативної групи, документує подію, здійснює збір доказів та проводить процесуальні дії у взаємодії з СБУ, ДСНС та іншими уповноваженими суб’єктами.

Узагальнюючи, можна стверджувати, що ефективність діяльності кримінальної поліції щодо протидії організованій злочинності в умовах РХБ-загроз визначається комплексністю підходу, який поєднує технічні засоби контролю, правове регулювання, організаційні заходи та психологічну стійкість особового складу. Саме така інтегрована модель дозволяє гарантувати належний рівень захисту населення і критичної інфраструктури, сприяє збереженню громадського порядку та формує довіру суспільства до правоохоронної системи в умовах сучасних воєнних і техногенних викликів.

Список використаних джерел:

1. Департамент забезпечення діяльності, пов’язаної з небезпечними матеріалами. Офіційний вебпортал Національної поліції України. URL:

https://npu.gov.ua/pro-policiyu/struktura-nacionalnoyi-policiyi/departament-zabezpechennya-diyalnosti-povyazanoyi-z.

2. Інструкція про порядок дій органів (підрозділів) поліції в разі виявлення радіоактивних, хімічних та ядерних матеріалів або отримання інформації про порушення правил чи незаконне поводження з ними: затв. наказом МВС України від 06 вересня 2017 роки № 754. URL: https://zakon.rada.gov.ua/laws/show/z1240-17#Text.

3. Кримінальний кодекс України від 5 квітня 2001 року № 2341-III. Дата оновлення: 17 липня 2025 року. *Вебпортал Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2341-14#n1716.

ЄМЕЛЬЯНОВ Роман
доцент кафедри оперативно-розшукової діяльності та інформаційної безпеки навчально-наукового інституту підготовки фахівців для підрозділів кримінальної поліції імені Е.О. Дідоренка ДонДУВС, доктор філософії

ЩОДО ПИТАННЯ УЧАСТІ ОПЕРАТИВНИХ ПРАЦІВНИКІВ ПІД ЧАС РОЗКРИТТЯ ТА РОЗСЛІДУВАННЯ ЗЛОЧИНІВ ВЧИНЕНИХ ОРГАНІЗОВАНИМИ ГРУПАМИ

Взаємодію підрозділів кримінальної поліції з органами досудового розслідування під час документування кримінальних правопорушень можна трактувати як здійснюваний відповідно до чинного законодавства суб’єктами оперативно-розшукової діяльності, кримінального процесу й інших галузей права спільний процес збирання, систематизації, перевірки та оцінювання фактичних даних, необхідних для доказування в кримінальному провадженні,

виконання інших завдань кримінального судочинства й оперативно-розшукової діяльності з подальшою їх перевіркою та закріпленням у визначеному КПК порядку, що супроводжується обміном інформацією, консультаціями та наданням іншої допомоги з урахуванням суб'єктивних особливостей і ресурсних можливостей кожного із суб'єктів [1, с.52].

Оскільки організовані злочинні групи характеризуються високим рівнем конспірації, розподілом ролей, стійкістю зв'язків, наявністю матеріально-технічної бази та фінансових ресурсів, а також здатністю впливати на посадових осіб або свідків, протидія та документування таких видів злочинів є не аби якою складною. Це зумовлює необхідність комплексного підходу, що включає застосування оперативно-розшукових, аналітичних, криміналістичних і процесуальних засобів.

Досліджуючи питання злочинів, що вчиняються організованими групами й злочинними організаціями, які сформовані на етнічній основі В.Г. Северук стверджує, що взаємодія оперативних підрозділів правоохоронних органів МВС, СБУ, ДФСУ, ДПСУ, ДПтСУ між собою, здійснюється в таких формах: обмін інформацією в питаннях протидії незаконному обігу наркотичних засобів (90%); сумісні виїзди в регіони для проведення узгоджених дій, перевірок і надання допомоги місцевим правоохоронним органам у боротьбі з незаконним обігом наркотичних засобів, вивчення та поширення позитивного досвіду (34,5%); створення сумісних слідчо-оперативних груп для розслідування конкретних злочинів (18,3%); проведення сумісних цільових заходів для виявлення та припинення злочинів, а також усунення причин та умов, які сприяють їх здійсненню (28,4%); взаємне використання можливостей правоохоронних органів для підвищення кваліфікації працівників, проведення сумісних семінарів, конференцій (11,2%); надання взаємної допомоги силами й засобами в процесі протидії організованій наркозлочинності (22,6%); видання сумісних наказів, вказівок, інших організаційно-розпорядливих документів (12,3%); випуск сумісних бюлетенів (збірок) та інших інформаційних видань (9,4%) [2, с.189].

У документуванні та розслідування злочинів вчинених організованими групами оперативні підрозділи виконують ключову роль, яка полягає у зборі первинної інформації про діяльність організованих груп, документуванні злочинної діяльності, встановленні структури угруповання, каналів фінансування та зв'язків з іншими злочинними формуваннями.

Проведеним Р. Велієвим дослідження підстав для початку розслідування незаконного обігу зброї, учиненого організованими злочинними групами, встановлено, що у 40 % випадків такими підставами є рапорти працівників оперативних підрозділів про виявлення ознак, що свідчать про вчинення досліджуваних нами кримінальних правопорушень [3, с.286].

Первинна інформація, зокрема щодо діяльності організованих злочинних груп, що вчиняють розбої в умовах воєнного стану, здобувається підрозділами кримінальної поліції багатьма способами та методами, одним з яких є оперативний пошук. Досліджуючи проблемні питання розбоїв, вчинюваних організованими злочинними групами в умовах воєнного стану, І.В. Жук стверджує, що процес оперативного пошуку ознак досліджуваного ним виду злочинів, має специфічні ознаки, які відокремлюють його від інших форм оперативно-розшукової діяльності. При цьому, відомостями, які встановлюються під час оперативного пошуку є: склад організованої злочинної групи, розподіл ролей; наявність зброї; факти готування і вчинення злочину; знаряддя та сліди готування до вчинення; сліди, залишені на місці вчинення; знаряддя вчинення; інші речі, що мають значення для встановлення учасників організованих злочинних груп, що вчиняють розбої в умовах воєнного стану; викрадені предмети і речі тощо [4, с.33].

Значну роль у встановленні факту вчинення економічних злочинів організованими групами відіграє оперативна інформація, що отримується в ході проведення оперативними працівниками оперативно-розшукових заходів. Як правило, оперативна інформація містить відомості не лише про факти групових злочинів та осіб, які їх учинили, а й про потерпілих, свідків і всіх тих, хто причетний до скоєння злочину [5, с.275].

Більш складніше, на думку А.В. Крижевського, зібрати інформацію про лідерів організованих злочинних об’єднань. Він зазначає, що в основному, така інформація отримується оперативним шляхом, тому потребує конспірації та захищеності від витоків [6, с.734].

На стадії досудового розслідування оперативні працівники забезпечують пошукову та аналітичну підтримку досудового розслідування, ініціюють та проводять негласні слідчі (розшукові) дії та передають їх результати слідчому для використання в доказуванні.

Практична діяльність як оперативних працівників, так і слідчих свідчить про те, що встановлення, зокрема, факту вчинення групових злочинів багато в чому залежить від позиції потерпілих, від уміння співробітників правоохоронних органів спонукати потерпілих до подачі заяви про вчинений злочин і дачі правдивих показань. При цьому слідчі та оперативні працівники повинні мати відповідну психологічну підготовку, ураховувати психологічний стан і мотивацію поведінки потерпілого, тактично правильно сформувавши його тверду позицію на дачу правдивих показань [5, с.274].

Варто особливо відзначити, що передача частини оперативно-розшукової інформації слідчим органам не повинна припиняти розвідувальну роботу або знижувати її темпи. Цей збір повинен тривати до кінця слідства, а іноді збір інформації доцільно продовжувати й у ході досудового розслідування (особливо коли організована група ще продовжує функціонувати). Відомості про організовані групи повинні накопичуватися постійно, щоб свого часу вони могли бути затребувані в процесі розслідування [5, с.274].

Отже, сучасні виклики криміногенного середовища, зокрема активізація діяльності організованих злочинних груп, зумовлюють необхідність удосконалення системи взаємодії між різними структурними елементами правоохоронних органів. Саме синергія зусиль дозволяє досягати результативності у викритті, документуванні та притягненні до відповідальності членів організованих злочинних угруповань.

Список використаних джерел:

1. Саковський А.А., Жижин А.В. Взаємодія підрозділів кримінальної поліції та органів досудового розслідування в документуванні кримінальних правопорушень. *Науковий вісник Національної академії внутрішніх справ.* 2019. №2 (111). С. 49-54
2. Северук В.Г. Взаємодія органів національної поліції України з іншими підрозділами правоохоронних органів під час протидії злочинам, що вчиняються організованими групами й злочинними організаціями, які сформовані на етнічній основі. *Актуальні проблеми держави і права.* 2021. С. 186-197
3. Велієв Р.Е. Особливості початкового етапу розслідування незаконного обігу зброї, учиненого організованими злочинними групами. *Вісник кримінологічної асоціації України*.2024.№2(32). С. 283-294
4. Жук І.В. Оперативний пошук у протидії організованим злочинним групам, що вчиняють розбої в умовах воєнного стану. *Південноукраїнський правничий часопис*. 2025. С. 32-36
5. Юрченко А., Рачок І. Проблемні питання встановлення факту вчинення економічних злочинів організованими групами. *Підприємництво, господарство і право.* №12. 2020. С. 272-277
6. Крижевський А.В. Особливості допиту учасників організованих злочинних об'єднань, підозрюваних у вчиненні шахрайств. *Електронне наукове видання «Аналітично-порівняльне правознавство».* Випуск 2025. № 01. С. 731-737. URL: https://app-journal.in.ua/wp-content/uploads/2025/02/124.pdf

КИРИЛЬЧУК Анна
здобувач ступеня вищої освіти бакалавра
Донецького державного університету

внутрішніх справ

Науковий керівник:
ЄМЕЛЬЯНОВ Роман
доцент кафедри оперативно - розшукової діяльності та інформаційної безпеки навчально-наукового інституту підготовки фахівців для підрозділів кримінальної поліції імені Е.О. Дідоренка Донецького державного університету внутрішніх справ, доктор філософії в галузі «Право»

ЗАГАЛЬНІ ЗАСАДИ ОПЕРАТИВНО-РОЗШУКОВОЇ ДІЯЛЬНОСТІ В УКРАЇНІ: СУТНІСТЬ ТА СУЧАСНІ ВИКЛИКИ

Оперативно-розшукова діяльність (ОРД) є важливою складовою системи забезпечення національної безпеки, боротьби зі злочинністю, тероризмом та іншими загрозами. Повномасштабна війна, розв’язана Російською Федерацією проти України, докорінно змінила всі сфери суспільного життя, зокрема — діяльність правоохоронних органів. Оперативні підрозділи, які раніше працювали в умовах мирного часу, тепер зіштовхуються з безпрецедентними викликами, що вимагають не лише гнучкої адаптації, а й переосмислення методів роботи. Серед найбільш актуальних проблем – обмеження доступу до тимчасово окупованих територій, ризики для життя працівників та складність документування злочинів.

Оперативно-розшукова діяльність є різновидом правоохоронної діяльності, яка має виключно державний характер. Вона законодавчо визначена і санкціонована державою, здійснюється обмеженим колом спеціальних суб’єктів, що діють від імені держави, в порядку і в межах, визначених і обмежених законом, підконтрольна державним органам, спрямована на захист держави, суспільства, людини специфічними засобами і методами.

Перш за все дамо визначенню поняттю «оперативно-розшукова діяльність». Відповідно до ст. 2 Закону України «Про оперативно-розшукову діяльність» - оперативно-розшукова діяльність - це система гласних і негласних пошукових та контррозвідувальних заходів, що здійснюються із застосуванням оперативних та оперативно-технічних засобів.

Оперативно-розшукова діяльність як найбільш дієвий і ефективний механізм в профілактиці і розкритті злочинів має певний перелік завдань, принципів та правову основу.

Отже, завданням оперативно-розшукової діяльності є пошук і фіксація фактичних даних про протиправні діяння окремих осіб та груп, відповідальність за які передбачена Кримінальним кодексом України, розвідувально-підривну діяльність спеціальних служб іноземних держав та організацій з метою припинення правопорушень та в інтересах кримінального судочинства, а також отримання інформації в інтересах безпеки громадян, суспільства і держави (ст. 1 ЗУ «Про ОРД»).

У найзагальнішому розумінні принципи оперативно-розшукової діяльності (ОРД) – це основоположні правила, яких мають дотримуватись оперативні працівники у своїй щоденній роботі. Вони відображають політичні та соціальні особливості розвитку суспільства, а також ґрунтуються на моральних і правових уявленнях громадян про суть, мету, завдання та порядок здійснення ОРД. Законом визначено перелік принципів оперативно-розшукової діяльності:

1) верховенство права
2) законності
3) дотримання прав і свобод людини.

Правова основа оперативно-розшукової діяльності визначена в ст. 3 ЗУ «Про оперативно-розшукову діяльність».

Повномасштабна військова агресія Російської Федерації, що розпочалася 24 лютого 2022 року, зумовила введення воєнного стану на всій території України Указом Президента України № 64/2022. З початком війни

кардинально змінились умови функціонування правоохоронної системи.

Правове регулювання цього специфічного виду діяльності згадується в ст. 10 ЗУ «Про правовий режим воєнного стану», де вказано на неприпустимість припинення повноважень органів державної влади, до яких в тому числі відносять органи, що здійснюють оперативно-розшукову діяльність. Оперативні підрозділи вимушені адаптувати свою діяльність до реалій воєнного часу, що супроводжується рядом специфічних викликів:

1) обмеження доступу до тимчасово окупованих територій: одним із найсуттєвіших викликів є відсутність фізичного доступу до тимчасово окупованих територій. Це унеможливлює оперативне реагування на злочини, збір первинної інформації, проведення слідчих дій і свідчить про значне обмеження суверенітету держави в цих регіонах. В умовах окупації фіксація злочинів часто можлива лише за допомогою непрямих джерел: показань свідків, супутникових знімків, перехоплень тощо. Це суттєво ускладнює не лише встановлення істини, а й доведення вини винних осіб.

2) ризики для життя працівників оперативних підрозділів: ще одним викликом є постійна загроза життю та здоров'ю працівників оперативних підрозділів. Робота в зоні бойових дій передбачає перебування під обстрілами, мінну небезпеку, ризик потрапляння в полон або загибелі. У таких умовах необхідно не лише зберігати професіоналізм, а й приймати швидкі, життєво важливі рішення. Тому в умовах воєнного стану важлива спеціальна підготовка оперативних працівників, спрямована на надання першої домедичної допомоги та психологічної допомоги.

3) складна процедура документування злочинів: воєнний час породжує нові злочини — військові злочини, геноцид, злочини проти людяності, документування яких вимагає точності. Через небезпеку та обмежений доступ до місць подій збір доказів часто є фрагментарним. Незважаючи на це, оперативні підрозділи спільно з військовими, медиками й міжнародними спостерігачами працюють над фіксацією кожного злочину.

4) необхідність взаємодії з міжнародними організаціями: оперативні

дані часто потребують міжнародної правової підтримки, а результати ОРД можуть використовуватись як докази у міжнародних провадженнях щодо воєнних злочинів і злочинів проти людяності.

Варто зазначити проблематику функціонування ОРД в умовах воєнного стану, це здебільшого включає такі проблеми:

1) обмежений судовий контроль за негласними заходами: відповідно до Закону України «Про оперативно-розшукову діяльність» (ст. 8), негласні заходи можуть проводитися лише за рішенням суду. Проте у воєнний час реалізація повноцінного судового контролю ускладнена через: обмежене функціонування судів у зоні бойових дій; проблеми з дотриманням строків розгляду клопотань, а також можливі випадки фактичного проведення негласних заходів без належного судового рішення. Це створює ризики порушення ст. 8 Європейської конвенції з прав людини щодо права на повагу до приватного життя.

2) відсутність чітких критеріїв законності та допустимості результатів ОРД як доказів у кримінальному провадженні: Кримінальний процесуальний кодекс України допускає використання результатів ОРД як доказів за умови належного процесуального оформлення. Проте під час воєнного стану бракує чітких стандартів фіксації, оцінки допустимості та розмежування матеріалів ОРД і слідства, що часто призводить до визнання таких доказів недопустимими у суді.

3) дотримання права на приватність: ст. 32 Конституції України гарантує право кожного на недоторканність приватного життя, листування, телефонних розмов, іншої кореспонденції. Проведення ОРД, особливо в умовах воєнного стану, часто межує з втручанням у приватне життя, що вимагає: обґрунтованості заходів, мінімізації ризиків зловживань та чіткого контролю за збереженням отриманої інформації.

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 ОРД 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.

Список використаних джерел:

1. Конституція України : закон від 28 черв. 1996 р. № 254к/96-ВР. Відомості Верховної Ради України. 1996. № 30. Ст. 141.
2. Кримінальний процесуальний кодекс України : закон України від 13 квіт. 2012 р. № 4651-VI. Відомості Верховної Ради України. 2013. № 9–10, № 11–12, № 13. Ст. 88.
3. Закон України «Про оперативно-розшукову діяльність» : Закон України від 18 лют. 1992 р. № 2135-XII. Відомості Верховної Ради України. 1992. № 22. Ст. 303.
4. Про затвердження Указу Президента України «Про введення воєнного стану в Україні» : Закон України від 24 лют. 2022 р. № 2102-IX. Офіційний вісник України. 2022. № 17. Ст. 879.
5. Про правовий режим воєнного стану : Закон України від 12 трав. 2015 р. № 389-VIII. Відомості Верховної Ради України. 2015. № 28. Ст. 250.
6. Європейська конвенція про захист прав людини і основоположних свобод від 4 листоп. 1950 р. Офіційний вісник України. 1998. – № 13. Ст. 52.

КОВАЛЬ Микита
курсант 2-го курсу факультету підготовки фахівців
для підрозділів кримінальної поліції
Національної поліції України
Дніпровського державного
університету внутрішніх справ

Науковий керівник:
ВАЛЄЄВ Руслан
доцент кафедри адміністративного права і процесу Дніпровського державного університет

НАПРЯМИ РОЗВИТКУ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ПОЛІЦЕЙСЬКОЇ ДІЯЛЬНОСТІ В УМОВАХ ВОЄННОГО ЧАСУ

У сучасних умовах воєнного стану, який триває в Україні у зв'язку зі російською збройною агресією, перед усіма державними інституціями постали безпрецедентні виклики, в першу чергу щодо забезпечення не лише національної безпеки, а й правопорядку.

Однією з ключових структур, відповідальних за внутрішню безпеку, громадський порядок, протидію злочинності та стабільність у тилу, є Національна поліція України. В умовах становлення інформаційної цивілізації, стрімкого розвитку технологій, у тому числі штучного інтелекту, в умовах війни, інформаційне забезпечення поліцейської діяльності має вийти на новий стратегічний рівень. Саме ефективна організація інформаційних потоків, оперативний обмін даними, захищеність інформації, аналітична обробка даних і використання сучасних технологій стають вирішальними чинниками в забезпеченні ефективної діяльності поліції як інструменту державної влади та громадської безпеки.

В умовах воєнного стану змінюється сам характер поліцейської функції. Якщо в мирний час акцент робився на протидії правопорушенням загального кримінального характеру, забезпеченні безпеки дорожнього руху, контролі за дотриманням адміністративного законодавства, то в умовах війни зростає роль поліції у сфері контррозвідки, протидії диверсіям, боротьбі з мародерством, організації евакуації населення, захисту стратегічних об'єктів, співпраці з військовими підрозділами, гуманітарною допомогою. Така трансформація

функцій вимагає не лише перегляду нормативно-правової бази, а й докорінного оновлення системи інформаційного забезпечення, яке повинно бути не просто інструментом підтримки рішень, а активним фактором забезпечення оперативної переваги [1, с. 25].

У цьому контексті особливо важливим є розвиток інтегрованих інформаційних систем, які об’єднують у собі бази даних про злочини, правопорушників, транспортні засоби, зброю, зниклих безвісти, підозрілих осіб, переміщення на території країни. У критичних ситуаціях, коли рішення необхідно приймати негайно, навіть секунда затримки може коштувати життя. Тому доступ до актуальної, перевіреної та повної інформації стає критично необхідним. Українська поліція вже має певний досвід у цій сфері, зокрема через Єдину інформаційну систему МВС, але в умовах війни виникає потреба у її радикальному вдосконаленні, розширенні функціоналу, захисті від кібератак, підвищенні мобільності й автономності.

Крім доступу до внутрішніх баз даних, надзвичайно важливим є налагодження обміну інформацією з іншими структурами – Збройними силами України, СБУ, ДСНС, Держприкордонслужбою, органами місцевого самоврядування, міжнародними партнерами. Лише через синергію зусиль і об’єднання інформаційних ресурсів можна досягти належного рівня ситуаційної обізнаності. Зокрема, аналітичні центри при МВС повинні мати прямий доступ до супутникових даних, геолокаційної інформації, даних аеророзвідки, щоб прогнозувати загрози, виявляти місця скупчення ворога або незаконних формувань, запобігати провокаціям і вчасно організовувати заходи з ліквідації загроз [2, с.7].

Важливою сферою інформаційного забезпечення в умовах воєнного стану є кібербезпека. Сьогодні інформаційна війна є невід’ємною частиною гібридної агресії, і Україна постійно зазнає атак на державні реєстри, сайти органів влади, системи зв’язку та навіть критичну інфраструктуру. У таких умовах забезпечення надійного шифрування, резервного копіювання, швидкого відновлення інформаційних систем та захисту конфіденційної

інформації є не просто технічною задачею, а питанням національної безпеки.

Не менш важливим аспектом є інформаційна взаємодія з населенням. У час війни довіра громадян до поліції є фундаментом для збереження громадського порядку. Суспільство має отримувати достовірну, своєчасну та зрозумілу інформацію про поточну ситуацію, загрози, правила поведінки в надзвичайних умовах. У цьому контексті важливо забезпечити ефективну роботу пресслужб, офіційних каналів комунікації, мобільних додатків, чат-ботів, а також гарячих ліній для звернень громадян. Поліція має не лише інформувати, а й активно слухати суспільство, оперативно реагувати на звернення, поширювати контент, що формує єдність, мотивацію до взаємодопомоги та підтримує моральний дух населення.

Окрему увагу слід приділити персоналу поліції, який безпосередньо працює в зоні бойових дій або на прифронтових територіях. Інформаційне забезпечення в таких умовах має включати мобільні засоби зв'язку, автономні канали передачі даних, захищені пристрої, доступ до систем супутникової навігації, цифрових карт місцевості, баз даних про ймовірних злочинців чи ворожих агентів. Важливо, щоб працівники поліції були навчені не лише користуватися технічними засобами, а й розуміли основи інформаційної безпеки, вміли виявляти дезінформацію, використовувати аналітичні інструменти для оцінки ризиків. Тому питання підготовки кадрів, створення спеціалізованих підрозділів інформаційної підтримки та постійного підвищення кваліфікації набуває пріоритетного значення [3, с.200].

Особливого значення набуває також проблема обліку внутрішньо переміщених осіб, зниклих безвісти, ідентифікації тіл загиблих, документування воєнних злочинів, а також створення безпечного освітнього середовища в умовах війни, бо життя, здоров'я та освіта наших дітей – майбутнє українського суспільства [4]. Усі ці напрями потребують високого рівня автоматизації, систематизації даних, міжвідомчої взаємодії та цифрової трансформації.

Загалом, розвиток інформаційного забезпечення поліцейської діяльності

в умовах воєнного стану – це не просто технічне вдосконалення чи цифрова модернізація, а питання стратегічної оборони та національного виживання. Сучасна війна ведеться не лише на фронті, а й в інформаційному просторі, в кіберпросторі, в мізках людей. І поліція, як інституція, що стоїть між державою та суспільством, повинна бути максимально готовою до нових викликів, адаптованою до високих стандартів оперативності, точності, захищеності та аналітичності. Лише за умов системного підходу, міжвідомчої координації, інституційної пам'яті, впровадження інновацій і постійного навчання можливе формування ефективної, сучасної та мобільної системи інформаційного забезпечення, яка дозволить поліції України виконувати свою місію навіть в умовах найбільшого випробування – повномасштабної війни.

Список використаних джерел:

1. Доценко О.С. Процес стратегічного управління в Національній поліції України. *Південноукраїнський правничий часопис. 2021. № 3. Ч.1* С.21–25.

2. Охріменко І.М. Стратегія розвитку правоохоронних органів України в сучасних умовах. *Управління освітнім процесом галузевого ВНЗ МВС України: матеріали круглого столу (Київ, 12 трав. 2017 р.).* К.: НАВС, 2017. С. 7–11.

3. Медведенко С.В., Медведенко Н.В. Засади стратегічного управління в умовах воєнного стану в органах та підрозділах національної поліції України. *Південноукраїнський правничий часопис. 2022. № 1–2.* С. 200–206

4. Валєєв Р.Г. Роль поліції у забезпеченні безпечного освітнього середовища в умовах воєнного стану. *Міжнародна та національна безпека: теоретичні і прикладні аспекти : матер. VIII Міжнар. наук.-практ. конф. (м. Дніпро, 15 бер. 2024 р.)*; у 2-х ч. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2024. Ч. І. 740 с. С. 400 – 403.

КОВТУНЕНКО Станіслав

слухач кафедри підготовки офіцерів запасу ВЮІ НЮУ ім. Ярослава Мудрого

Науковий керівник:
ПУГАЧ Вячеслав
викладач кафедри підготовки офіцерів запасу ВЮІ НЮУ ім. Ярослава Мудрого

OSINT ЯК ІНСТРУМЕНТ В РОЗСЛІДУВАННІ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ

З розвитком інформаційно-телекомунікаційних технологій повсякденне життя людей стало нерозривно пов'язано з діяльністю в мережі Інтернет. Нині значний масив інформації є у вільному доступі, через що її пошук з відкритих джерел став доволі поширеним явищем. Саме на це спрямований Open source intelligence, який перекладається з англійської як «розвідка з відкритих джерел». Повномасштабна агресія росії проти України стала каталізатором його розвитку: значна кількість журналістів-розслідувачів та правоохоронців виявляла воєнні злочини, вчинені російськими військовими, використовуючи OSINT. Проте, він дозволяє фіксувати не лише воєнні злочини, а й інші кримінальні правопорушення, що є актуальним у сучасних умовах.

Серед науковців немає єдності щодо визначення OSINT, проте загалом його можна окреслити як певну послідовність дій, спрямовану на пошук, збір та аналіз інформації з загальнодоступних джерел з подальшим формуванням висновків щодо неї [2, с. 125]. Варто зазначити, що існує підвид «розвідки з відкритих джерел» – ГЕО-OSINT, що спеціалізується на аналізі геопросторових даних. Ці дані можуть бути отримані з супутникових знімків (Landsat, Maxar), цифрових карт (Google Maps, Bing Maps), соціальних медіа з геолокацією, відкритих баз геоінформаційних систем та інших. Сутність цього напряму полягає у встановленні просторових зв'язків між діями, подіями та об'єктами на основі часу фіксації та місцезнаходження. Завдяки цій течії стає можливим ідентифікація місць, де було вчинено правопорушення,

відстеження маршрутів підозрюваних, відновлення хронології подій за геоданими, верифікації свідчень, моделювання сценаріїв правопорушень у просторі та часі тощо. Цей різновид є актуальним для розслідування багатьох видів кримінальних правопорушень [5, с. 87-89].

З метою підвищення ефективності цієї діяльності було розроблено багато інструментів, серед яких можна виділити:

Maltego – платформа з відкритим кодом, яка надає доступ до 58 джерел даних та бази, що містить понад 1 мільйон об'єктів. Крім того, має засоби візуалізації, завдяки чому користувачі можуть швидко формувати результат розслідування, зручний для аналізу та сприйняття [2, с. 223] [6, с. 907];

Spiderfoot – має відкритий вихідний код із різноманітними функціями, включаючи можливість отримувати та аналізувати IP-адреси, адреси електронної пошти, номери телефонів, імена та імена користувачів, адреси BTC та інше. Має вбудований веб-сервер та зручний інтерфейс користувача [2, с. 224] [6, с. 907];

Lampyre – комерційне програмне забезпечення, створене спеціально для OSINT, має велику базу даних та зрозумілий інтерфейс. Також містить засоби для перевірки контрагентів, виявлення кіберзагроз, кримінальних правопорушень та фінансової аналітики. Завдяки ній розслідування можна почати з базової точки даних – реєстраційний номер компанії, ім'я чи номер телефону [6, с. 908];

Як уже було зазначено, OSINT найбільше було використано при розслідуванні воєнних злочинів. Використовуючи його спеціалісти з фрагментів, що містяться у мережі збирають загальну картину, доповнюючи її даними, отриманими з допомогою ГЕО-OSINT [6, с. 908].

Також OSINT використовують і при розслідуванні корупційних кримінальних правопорушень. Співробітники антикорупційних органів зазначають, що інформацію можна знайти у відкритих джерелах шляхом аналізу постів у соціальних мережах та автоматизованого пошуку у реєстрах і

агрегаторах [2, с. 125]. Крім того, у вільному доступі існують спеціалізовані інтернет-платформи. Зокрема, YouControl, що надає можливість перевіряти зв'язки між посадовими особами та бізнесом. Поряд із цим функціонує Opendatabot, який об'єднує дані з державних реєстрів та судових рішень, що сприяє підвищенню прозорості в судовій системі. Окрім зазначених працює «Прозорро. Продажі», котрий має алгоритми, призначені для аналізу процесів продажу державного майна [3, с. 4-5].

OSINT може бути використаним і під час розслідування кримінальних правопорушень проти власності. Розроблено алгоритм, що складається з таких етапів – збір інформації, її фільтрування, аналіз, крос-перевірка і підтвердження, створення аналітичних звітів. Крім цього, під час роботи з допомогою OSINT науковці наголошують на необхідності дотримання протоколу Берклі – документа, що містить настанови щодо роботи з інформацією з відкритих джерел [2, с. 222-223].

Проте, науковці стверджують, що чинне кримінально-процесуальне законодавство має проблеми через повільне пристосування до технологічних змін. Крім того, деякі експерти відносять інформацію, отриману з відкритих джерел до «цифрових доказів», чим не погоджуються з судовою практикою, яка вважає їх «електронними доказами». Менше з тим, єдність думок існує лише щодо необхідності підкріплення таких доказів іншими, зібраними традиційним шляхом. Або використовувати виключно «електронні докази» у випадках, коли інші зібрати або перевірити у інший спосіб неможливо [1, с. 230-231; 2, с. 125].

Однак існують проблеми при застосуванні OSINT. По-перше, поширеність фейкових новин та дезінформації вимагає участі експертів. По-друге, в будь-якому випадку використання такого способу збору доказів існує ризик порушення приватного життя осіб.

Отже, OSINT може бути застосованим при розслідуванні майже будь-яких кримінальних правопорушень. Разом із тим варто пам'ятати, що задля ефективної роботи з джерелами варто залучати експертів. Крім того,

необхідно дотримуватись норм, як етичних, так і нормативних, зокрема – протоколу Берклі, з метою недопущення протиправного порушення приватного життя осіб та відповідності вимогам доказів, передбачених кримінально-процесуальним законодавством.

Список використаних джерел:

1. Басиста І.В., Гаврилюк Л. В., Гутник А. В., Хитра А. Я. Використання цифрових даних з відкритих джерел під час розслідування кримінальних правопорушень: окремі аспекти. *Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького: Журнал. Серія Право.* 2024. № 17 (29). С. 227-243.

2. Деревягін О. Використання OSINT інструментарію при розслідуванні кримінальних правопорушень проти власності. *СБУ в умовах війни в Україні: сучасні реалії та інноваційні стратегії забезпечення національної безпеки:* зб. тез доп. міжнар. наук.-практ. конф., м. Київ 4–5 липня 2024 року. Київ, 2024. С. 221-225.

3. Думчиков М.О. Використання OSINT технологій для виявлення корупційних правопорушень: сучасні підходи та виклики. *Академічні візії.* 2024. №36. С. 1-6.

4. Калінніков О. В. Перспективи подальшого використання OSINT у кримінальному провадженні. XXIV INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE TECHNOLOGIES OF SCIENTISTS AND IMPLEMENTATION OF MODERN METHODS. С. 124-129

5. Москаленко Я. С., Кривошея Д. Г., Дейкун О. С., Кисельов А. О. ГЕО-OSINT в кримінальному аналізі. *Modernization of today's science: experience and trends.* 2025. С.86-91.

6. Тома М.Г., Василова О.В. Інструменти OSINT: фіксація воєнних злочинів в Україні. *Електронне наукове видання «Аналітично-порівняльне правознавство».* 2025. №2. С. 905-909.

КОНОНЕНКО Віктор
здобувач вищої освіти факультету службово-бойової діяльності НГУ Київського інституту Національної гвардії України

Науковий керівник:
БЕЙКУН Андрій
доцент кафедри правового забезпечення та правоохоронної діяльності факультету забезпечення державної безпеки Київського інституту Національної гвардії України кандидат юридичних наук, доцент

ОРГАНІЗАЦІЙНО-ПРАВОВА ПРОБЛЕМАТИКА ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ У СИСТЕМАХ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ В УМОВАХ ПОВНОМАСШТАБНОЇ ЗБРОЙНОЇ АГРЕСІЇ

Беззаперечно, що кіберзагрози, які здатні порушити функціонування державних інститутів, систем забезпечення державної безпеки, критичної інфраструктури держави та загрожувати безпеці громадян, - стають одним із ключових факторів впливу на сучасні збройні конфлікти. Яскравим прикладом цього є російсько-українська війна, яка, не зважаючи на її повномасштабність, має класичний «гібридний» характер, тобто, країна агресор у збройному конфлікті застосовує широкий спектр «допоміжних засобів», зокрема, кібероперації та кібератаки на різноманітні об’єкти нашої держави: інформаційний простір, банківську та медійну сфери, системи зв’язку та управління, об’єкти критичної інфраструктури тощо. Відповідно, ці відносно нові виклики національній безпеці держави вимагають системного підходу до забезпечення кіберзахисту та розробки ефективних механізмів, (зокрема, організаційно-правового) протидії.

Кібербезпека, кібервійни, інформаційні війни, кіберзахист, кіберпростір

поняття, які останнім часом все більше наповнюються відповідним етимологічно-правовим змістом та слугують ключовими тригерами відповідного галузевого нормативного масиву, спрямованого, в першу чергу, на захист: сфери національної безпеки і оборони, національного суспільного простору, господарюючих суб'єктів, громад та окремого громадянина у цьому кібер-протистоянні.

Окресленій проблематиці приділяє увагу дедалі більше науковців, зокрема: Баранов О.А., Бєлєвцева В.В., Богуцький П.П., Веселова Л.Ю., Гаврильців М.Т., Горулько В.В., Діордіца І.В., Довгань О.Д., Золотар О.О., Козьміних А.В., Кундеус О.М., Леоненко Н.А., Настюк В.Я., Павленко В.С., Подорожна Т.С., Поступна О.В., Ткачук Т.Ю., Шемчук В.В. та інші.

Як вже широко відомо, і як наголошує Т.С. Подорожна, - дії сучасних терористів виходять за межі елементарних гуманітарних принципів (у цьому контексті про російську федерацію можна говорити як про найбільш небезпечного терориста сучасного періоду розвитку людства). Відбувається зневажання основ людяності. В умовах такої боротьби важко закликати до поваги прав людини, застосовувати цей посил до тих, хто повністю його ігнорує. Практично щодня потужним кібератакам із застосуванням просунутих інформаційних технологій піддаються державні установи, ЗМІ, об'єкти критичної інфраструктури, система життєзабезпечення. Усе це – частина скоординованої кібернетичної агресії проти України [1, с. 493].

Водночас, використання інформаційних технологій та телекомунікаційних систем, насамперед, у системах забезпечення національної безпеки і оборонній сфері, стає невід'ємною частиною повсякденного життя, і Збройні Сили, інші військові формування, правоохоронні, розвідувальні органи, органи державної влади тощо також позиціонуються і як суб'єкти використання ІТ та ТС, і як потенційні об'єкти кібероперацій. Застосовуючи телекомунікації та комп'ютерні мережі, необхідно усвідомлювати й ризики, які вони створюють. Сучасні хакерські атаки становлять загрозу не лише для окремих осіб, а й для цілих держав.

Кіберзброя, яка дедалі частіше прирівнюється до зброї масового ураження через свою ефективність і руйнівні наслідки, є ключовим фактором, що викликає занепокоєння. Чим швидше розвиваються інформаційні технології, тим більш актуальною стає проблема захисту інформаційно-телекомунікаційних систем нашої держави.

Варто підкреслити, що критичні вразливості в програмному забезпеченні та автоматизованих системах викликають серйозні побоювання, і урядові структури разом із суспільством постійно шукають ефективніші заходи для захисту інформації, Інтернет-ресурсів та програмного забезпечення від кіберзагроз. Підтвердженням актуальності цього питання стала зустріч на вищому рівні глав держав та урядів країн-членів НАТО у Варшаві 2016 року. Під час заходу було підписано історичну угоду між ЄС і НАТО про співпрацю у сфері безпеки, зокрема щодо гібридних загроз і кібератак. Таким чином, кіберпростір нормативно-декларативно на міжнародному рівні визнано новим оперативним середовищем поряд із сушею, морем, повітрям і космосом, а кібероперації стали невід'ємною частиною сучасних гібридних конфліктів [2].

Як підкреслює нам Л.Ю. Веселова, особливу увагу кібероперація приділяють провідні країни світу, такі як: США, Великобританія, Китай тощо. У цих державах виділяються значні бюджетні кошти на розвиток кібернетичної складової збройних сил, а також реалізуються масштабні програми для забезпечення національної безпеки, національної оборони й захисту об’єктів критичної інфраструктури від кібератак. Оскільки повністю захищені мережі наразі залишаються недосяжною метою, кібербезпека стала одним із ключових пріоритетів розвитку будь-якої сучасної армії [3, с. 131].

У наш час структури Збройних Сил України, інших суб’єктів сектору безпеки і сил оборони активно насичуються підрозділами кібербезпеки, стрімкий розвиток яких значною мірою спричинений повномасштабною війною, яку російська федерація веде проти нашої держави з 2022 року. Агресор активно використовує кіберпростір для реалізації своїх цілей не лише щодо України, а й стосовно інших держав, насамперед, стратегічних партнерів

України. Російська федерація нарощує масштаби кібершпіонажу та активно впливає на громадську думку, використовуючи неправдиву інформацію і пропаганду. Основною метою цих дій є дестабілізація ситуації всередині країни, поширення хаосу й паніки, спотворення свідомості громадян, що створює підґрунтя для досягнення стратегічних інтересів у повномасштабній загарбницькій «гібридній» війні.

Як зазначають нам дослідники Центру Разумкова, попри те, що гібридні війни, зазвичай, асоціюються із сучасними конфліктами, варто згадати і про історію Радянського Союзу як приклад класичного гібридного підходу до боротьби проти визвольних рухів колонізованих народів. «Громадянська війна» 1918–1921 років на території сучасної України, яка насправді була російсько-українським збройним конфліктом, стала одним із христоматійних прикладів гібридної війни. Її складовими були: масштабна пропаганда, створення сепаратистських територіальних утворень, масове збройне вторгнення, голодомори (1921–1922, 1932–1933, 1947 р.р.), етнічні чистки, переслідування дисидентів, «мовна війна», а також терор і нагнітання страху у суспільстві [4].

Аналізуючі події 2014-2021 років, Кундеус О.М. підкреслює, що прямому вторгненню на територію України передував великий підготовчий етап, що включав активну розбудову та накопичення військової сили агресора, втручання у внутрішні справи України, маніпуляції виборами, підбурювання до масових протестів, створення підривних організацій і, аксіомно, одне з найсуттєвіших: систематичну інформаційну обробку населення України та світової спільноти, а також масовані кібератаки на державну інфраструктуру напередодні повномасштабного вторгнення. Вторгнення стало лише завершальним актом цієї гібридної драми [5, с. 122].

Звісно, що цитований нами автор не міг у 2020 році знати про масовані кібератаки на сервери державних установ, насамперед, Міністерства оборони, Генерального штабу ЗСУ, урядових структур тощо за тиждень перед повномасштабним збройним вторгненням, проте, загальну аналітичну канву

гібридних прийомів, способів та засобів агресора, насамперед, широке застосування кібератак, він спрогнозував цілком точно.

Отже, можна зробити висновок, що в умовах відсічі повномасштабної збройної агресії, подальших геополітичних змін та комп'ютеризації усіх сфер життя суспільства, посилилися зовнішні виклики і загрози, а також ризики в інформаційному просторі. На сучасному етапі розвитку суспільства і держави серед найактуальніших загроз національній інформаційній безпеці, зважаючи на динамічність інформаційної сфери, можна виокремити: протиправний вплив на національні інформаційні ресурси, інформаційно-телекомунікаційні системи та інформаційну інфраструктуру; використання засобів та методів поширення недостовірної інформації для дезінформації людей, застосовуючи при цьому, зокрема, методи впливу на психіку людини для дезорганізації та придушення волі; несанкціоноване втручання в національний інформаційний простір; кібератаки на державні автоматизовані системи управління, зв'язку, банківську та промислову сфери, корпоративні та індивідуальні бази даних. З огляду на це, трансформація інформаційного та кібер- просторів в сучасних умовах існування нашої держави визначили новий вектор розвитку правового регулювання інформаційної безпеки в Україні з огляду на міжнародні стандарти у цій сфері.

Список використаних джерел:

1. Подорожна Т.С. Забезпечення інформаційної безпеки України в умовах сучасних викликів та загроз з боку РФ. *Аналітично-порівняльне правознавство*. 2023. № 6. С. 491–497. URL: https://app-journal.in.ua/wp-content/ uploads/2023/12/87.pdf (дата звернення: 07.10.2025).

2. НАТО та ЄС підписали угоду про співпрацю у сфері кіберзахисту. 10 лютого 2016. [Інформаційний портал: Європейська правда. Міжнародна безпека та євроінтеграція України]. URL: https:// www.eurointegration.com.ua/ news/2016/02/10/7044661/ (дата звернення: 07.10.2025).

3. Веселова Л.Ю. Кібербезпека в умовах гібридної війни:

адміністративно-правові засади / *Монографія*: «Видавничий дім Гельветика», 2021. 488 с. URL: https://oldiplus.ua/kibernetychna-bezpeka-v-umovah-gibrydnoyi-vijny-administratyvno-pravovi-zasady/?srsltid=AfmBOorK94nc2dFIrOen7mfFB0e2jNIS4ZjgA2Z_sBKccsce5vwJioPl (дата звернення: 07.10.2025).

4. «Гібридна» війна Росії – виклик і загроза для Європи. *Національна безпека і оборона*. № 9-10 (167-168). Український центр економічних і політичних досліджень імені Олександра Разумкова. 2016. URL: https://razumkov.org.ua/uploads/journal/ukr/NSD167-168_2016_ukr.pdf (дата звернення: 07.10.2025).

5. Кундеус О.М. Теоретичні аспекти гібридної війни РФ проти України / *Регіональні студії*. Ужгород, Видавничий дім «Гельветика». Вип. 20. 2020. С.120-124. URL: https://dspace.uzhnu.edu.ua/jspui/handle/lib/39665 (дата звернення: 07.10.2025).

КОРЕНСЬКОЙ Сергій
аспірант
(Донецький державний університет внутрішніх справ)

Науковий керівник:
ЛОСКУТОВ Тимур
головний науковий співробітник науково-дослідної лабораторії з проблем запобігання кримінальним правопорушенням
доктор юридичних наук, професор
(Донецький державний університет внутрішніх справ)

ЩОДО ОКРЕМИХ НЕДОЛІКІВ ПРОВЕДЕННЯ ОГЛЯДУ МІСЦЯ ПОДІЇ ПІД ЧАС РОЗСЛІДУВАННЯ ДОРОЖНЬО-ТРАНСПОРТНИХ ПРИГОД

Під час розслідування дорожньо-транспортних пригод (далі – ДТП) результати огляду місця події можуть відігравати вирішальне значення у ході доказування. Окремі недоліки процесуальної форми проведення огляду місця події за фактом вчинення ДТП можуть створювати невиправдані перешкоди в діяльності як стороні обвинувачення, так і інших учасників кримінального провадження.

Розглянемо окремі недоліки більш детально:

1. Не визнання особи учасником огляду місця події. Відповідно до положень КПК України огляд місця події, у невідкладних випадках, може бути проведений до внесення відомостей до Єдиного реєстру досудових розслідувань (далі ЄРДР). Сторона обвинувачення має вжити належних заходів для забезпечення присутності під час проведення слідчої (розшукової) дії осіб, чиї права та законні інтереси можуть бути обмежені або порушені [10]. На практиці мають місце ситуації, коли всупереч положенням ст. 223 КПК України у протоколі огляду місця події анкетні дані присутніх осіб (водіїв, власників транспортних засобів та інших осіб) не вказуються. Як наслідок, такі особи не можуть ознайомитись зі змістом протоколу огляду місця події та схеми ДТП, засвідчити правильність складання та факт ознайомлення з матеріалами оскільки формально не беруть участь у процедурі огляду.

О.А. Лучко пише, що при проведенні огляду можуть приймати участь особи, процесуальний статус яких у КПК України не визначений. Такими особами можуть бути: власник житла чи іншого володіння особи, у якому проводиться огляд; особа, у житлі якої проводиться огляд, яка на момент його проведення не є підозрюваною у розумінні ст. 42 КПК України; учасники ДТП (при проведенні огляду місця такої події), особа, що підлягає освідуванню, якщо вона не затримана і їй не повідомлено про підозру, представник установи зв'язку (при огляді кореспонденції) тощо [2, с. 113]. На наше переконання, учасники ДТП є особами, які вже мають процесуальний «статус» у кримінальному процесі. Це може бути особа, чиї права та законні інтереси

можуть бути обмежені чи порушені, або ж інша особа, права чи законні інтереси якої обмежуються під час досудового розслідування. Присутність даних осіб при огляді в обов'язковому порядку має бути відображена у протоколі огляду місця події, що в свою чергу, надає право на ознайомлення зі змістом останнього.

2. Збирання доказової інформації до внесення відомостей до ЄРДР. За загальним правилом здійснення досудового розслідування до внесення відомостей до ЄРДР або без такого внесення не допускається і тягне за собою відповідальність, окрім винятків встановлених кримінальним процесуальним законом. Так, огляд місця події є єдиною слідчою (розшуковою) дією, яку допускається здійснювати при розслідуванні злочинів до внесення відомостей до реєстру [1]. Під час проведення огляду місця події, до внесення відомостей до ЄРДР, стороною обвинувачення може бути вилучено (скопійовано) записи камер відеоспостереження, які розташовані біля місця скоєння ДТП. В більшості випадків такі «докази» мають сумнівне походження, оскільки останні не фіксуються в протоколі огляду місця події, та фактично отримуються стороною обвинувачення поза правовим полем. Також відеоматеріал, який добутий з портативного відео-реєстратора транспортного засобу, без згоди володаря (користувача) транспортного засобу вважається таким, що отримний з порушенням правил допустимості доказів та не може використовуватись у процесі доказування стороною обвинувачення.

Т.О. Лоскутов відзначає, що чинна редакція ст. 86 КПК України не регламентує жодних винятків із правила щодо законного порядку одержання доказу. Зміст цієї норми не містить ніяких вказівок на можливість використання доказу, що одержаний з якимось незначним або несуттєвим порушенням законного порядку. Навіть незначне порушення процесуальних положень щодо отримання доказу має призводити до його недопустимості, а отже, неможливості використання у ході доказування винуватості у вчиненні кримінального правопорушення. У такий спосіб може ігноруватися вагомість та важливість доказу для встановлення обставин вчиненого кримінального

правопорушення [3, с. 107].

Таким чином отримання доказів з істотним порушенням прав і свобод людини під час здійснення огляду місця події ДТП знижує ефективність проведення такої слідчої (розшукової) дії та у перспективі сковує доказовий потенціал сторони обвинувачення.

3. Обмеження права на свободу учасників ДТП. Відповідно до ч. 6 ст. 237 КПК України слідчий, прокурор має право заборонити будь-якій особі залишити місце огляду до його закінчення та вчинювати будь-які дії, що заважають проведенню огляду [1]. Ці дії формально співпадають з моментом кримінального процесуального затримання.

Такі заходи примусу треба розмежовувати беручи за основу наслідки їх застосування. Правий є М.М. Потоцький, який аналізуючи норми щодо заборони залишення місця огляду/обшуку вказує, що ззовні це може бути схоже на затримання, однак, підстави для затримання в даних випадках відсутні й правові наслідки від цих процесуальних дій відповідно будуть різні. З огляду на тривалість, спосіб утримання та наслідки, забезпечення перебування особи у певному місці під час здійснення огляду, за загальним правилом не може розцінюватись як затримання [4, с. 187]. На наше переконання, заборона слідчого будь-якій особі залишити місце огляду до його закінчення та вчинювати будь-які дії, що заважають проведенню огляду є законною лише у разі визнання особи учасником такого огляду. Зважаючи на процесуальні наслідки,вважається, що таку заборону не можна вважати кримінальним процесуальним затриманням.

З огляду на усе вищевказане слід підсумувати, що учасники ДТП є особами, які вже мають процесуальний «статус» у кримінальному процесі. Це може бути особа, чиї права та законні інтереси можуть бути обмежені чи порушені, або ж інша особа, права чи законні інтереси якої обмежуються під час досудового розслідування. Відзначимо, що збирання доказів стороною обвинувачення має відбуватись відповідно до законної процедури. Пропонуємо внести зміни до КПК України, якими надати дозвіл стороні

обвинувачення знімати показання технічних приладів та технічних засобів, що мають функції фото- і кінозйомки, відеозапису, чи засобів фото- і кінозйомки, відеозапису до внесення даних до ЄРДР, за аналогією з процедурою дізнання. Вважаємо, що заборона слідчого будь-якій особі залишити місце огляду до його закінчення та вчиняти будь-які дії, що заважають проведенню огляду є законною лише у разі визнання особи учасником такого огляду.

Список використаних джерел:

1. Кримінальний процесуальний кодекс України. Закон від 13.04.2012. № 4651-VI. URL : https://zakon.rada.gov.ua/laws/show/4651-17 (дата звернення: 10.09.2025).

2. Лучко О.А. Огляд у кримінальному досудовому провадженні: дис. … канд. юрид. наук: 12.00.09. Маріуполь, 2021. 269 с.

3. Лоскутов Т.О. Щодо критеріїв визначення допустимості доказів у кримінальному провадженні. *Вчені записки Таврійського національного університету імені В.І. Вернадського.* Серія: Юридичні науки. 2021. Т. 32(71), № 1. С. 106–110.

4. Потоцький М.М. Затримання особи за підозрою у вчиненні кримінального правопорушення: дис. … докт. філософії: 12.00.09. Кропивницький, 2022. 275 с.

КОСЯЧЕНКО Євгеній
курсант ФПФ ПКП НПУ Дніпровського державного університету внутрішніх справ

Науковий керівник:
ВАЛЄЄВ Руслан
доцент кафедри адміністративного права і процесу ННІ ПФППД НПУ Дніпровського державного університету внутрішніх справ

кандидат педагогічних наук

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ЯК ІНСТРУМЕНТ ПРОТИДІЇ ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ В УМОВАХ ЗБРОЙНОГО КОНФЛІКТУ

У період збройного конфлікту суспільство стикається з низкою специфічних викликів, які загострюють проблеми безпеки й створюють сприятливе середовище для діяльності організованих злочинних угруповань. Інформаційні технології водночас полегшують злочинну діяльність, але й відкривають нові можливості для правоохоронних органів. Тому потрібно проаналізувати інформаційні технології як інструмент протидії організованій злочинності в умовах збройного конфлікту.

Сучасні організовані злочинні групи діють за принципом мережевої організації, і інформаційні технології створюють інструментарій для комплексного аналізу таких мереж, дозволяючи переходити від фрагментарних даних до цілісних карт зв'язків і поведінкових моделей. Великі дані і методи їх обробки відкривають можливість інтеграції розрізнених джерел інформації, включно з телекомунікаційними метаданими, банківськими транзакціями, відкритими джерелами, соціальними мережами, супутниковими і геоданими [1, с. 323].

Аналітичні платформи з можливістю кореляції й агрегації цих даних здатні виявити аномалії, повторювані патерни і ключові вузли злочинних мереж, які були б недоступні при традиційному розслідуванні. Тезнології штучного інтелекту можуть здійснювати аналіз тональності повідомлень, частоти взаємодій і часових вікон, і навіть періоди активності, цикли прийняття рішень і, можливо, заплановані операції [2].

У свою чергу, геолокаційні технології й аналіз просторових даних допомагають відстежувати переміщення підозрілих конвоїв, локалізувати місця незаконного видобутку чи торгівлі та виявляти точки зосередження

нелегальної діяльності, а поєднання з історичними даними створює можливість прогнозування маршрутів і зон ризику. Автоматизація збору доказів і цифрова криміналістика значно підвищують якість доказової бази, а автоматизовані робочі процеси для обробки доказів, їх хешування й збереження ланцюга зберігання роблять матеріали прийнятними в суді та зменшують ризики процедурних помилок [2].

Водночас, поліцейських потрібно своєчасно готувати до ефективного використання інформаційних технологій. Чинником, який сприятиме підвищенню інформаційної компетентності поліцейських може стати впровадження ще на етапі підготовки курсантів віртуального освітнього середовища [3].

Штучний інтелект та машинне навчання дозволяють класифікувати й прогнозувати поведінку, виявляти нетипові шаблони фінансових операцій і визначати найімовірніші зв'язки між суб'єктами, хоча застосування цих технологій потребує уваги до якості даних і прозорості алгоритмів. Важливою є також взаємодія між державними органами, приватними провайдерами й громадянськими ініціативами, а платформи для обміну розвідданими і стандарти форматів даних підвищують оперативність реакції, проте потребують регуляторних і етичних механізмів для мінімізації ризиків зловживань [2].

Разом з тим, потрібно зазначити, що кіберзлочинність у контексті організованої злочинності і збройного конфлікту набуває множинного значення, від онлайн-шахрайств та злому інфраструктури до використання цифрових платформ для вербувань, координації та фінансування [4, с. 18].

Протидія цим явищам потребує як технічних, так і правових, організаційних заходів. Посилення кібербезпеки критичних інформаційних інфраструктур, таких як банківські системи, енергетика, телекомунікації та державні реєстри, захист від DDoS-атак, шифрування каналів зв'язку, сегментація мереж і використання систем виявлення вторгнень знижують вразливість інфраструктури, яку злочинні групи можуть використовувати для

підривних операцій або як джерело доходів. Відстеження й блокування каналів фінансування організованих груп через складні фінансові схеми, використання криптовалют, мультиплікаційні трансакції та фронт-компанії потребує інформаційних систем для аналізу фінансових потоків, автоматизованих тригерів підозрілих транзакцій і співпраці з фінансовими установами.

Підвищення кіберграмотності населення й бізнесу знижує вразливість до фішингових атак і соціальної інженерії, а міжнародна співпраця та гармонізація правових норм забезпечують ефективний обмін розвідданими, узгодження санкцій і координацію арештів та блокувань [4, с. 19].

Попри очевидні переваги, існують обмеження: проблеми з доступом до якісних даних і їхньою сумісністю між системами, ризики порушення прав людини й надмірного спостереження, вразливість технічних рішень до кібератак, брак кваліфікованих кадрів у сфері цифрової криміналістики та аналітики. Інформаційні технології надають потужний набір інструментів для виявлення, моніторингу і нейтралізації організованих злочинних мереж в умовах збройного конфлікту.

Таким чином, 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 ІТ 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.

Список використаних джерел:

1. Іванцов, В. О. Захист інформації в інформаційно-аналітичній діяльності правоохоронних органів у контексті протидії організованій злочинності. *Протидія організованій злочинності і корупції в умовах збройного конфлікту: досвід та перспективи з нагоди 5-річчя створення Департаменту стратегічних розслідувань НПУ: зб. матеріалів Міжнар. наук.-практ. конф. (м. Кропивницький, 04 жовт. 2024 р.).* Кропивницький: ДонДУВС, 2024. С. 321-324.

2. Зінченко Д.А, Висоцький М.О. Заходи забезпечення кібербезпеки в системах обміну інформацією правоохоронних органів. *Застосування інформаційних технологій у правоохоронній діяльності. Матеріали круглого стола 14 грудня 2023 року*. .Кропивницький: ДонДУВС, 2023. С. 98-100.

3. Валєєв Р.Г. Конструювання віртуального освітнього середовища при підготовці майбутніх поліцейських у ВНЗ. *Всеукраїнська наук.-практ. конф. «Національна поліція Донеччини: проблеми становлення та стратегія розвитку – 2016»: Зб. тез доповідей.* Маріуполь : ДВНЗ «ПДТУ». – С. 157-159.

4. Сащенко М.І. Проблемні аспекти запобігання кіберзлочинності в Україні. *Young Scientist.* 2022. № 1 (101). С. 17-20.

КРАВЧУК Дмитро
курсант 3 курсу
навчально – наукового інституту підготовки фахівців для підрозділів кримінальної поліції ім. Е.О.Дідоренка Донецького державного університету внутрішніх справ

Науковий керівник:
ДРОБЕНКО Діна
викладач кафедри кримінального процесу та криміналістики факультету підготовки фахівців для органів досудового розслідування Національної поліції України *Донецького державного університету внутрішніх справ*

Щодо єдиної системи електронного документообігу в Міністерстві внутрішніх справ (СЕД) : роль електронного документообігу в кримінальному процесі

Єдина система електронного документообігу в Міністерстві внутрішніх справ виконує декілька функцій йдеться про забезпечення комунікації між органами державної виконавчої влади, а також слугує єдиним реєстром документів в Міністерстві внутрішніх справ зокрема органів Національної поліції України. Кримінальне провадження включає в себе великий за обсягом документообіг, на кожному етапі якого здійснюється реєстрація великої кількості процесуальних документів і тому для зменшення навантаження на органи досудового розслідування та інші підрозділи Національної поліції України які беруть безпосередню участь в кримінальному процесі, було введено СЕД, що дає змогу здійснювати безпосередню міжвідомчу комунікацію між підрозділами та забезпечує прозорість при заповненні процесуальних документів.

Поняття СЕД сьогодні не закріплено Законом України «Про електронні документи та електронний документообіг», воно затверджено в одному із відомчих наказів МВС [2]. Щодо загального поняття електронного документообігу, то ми можемо дати йому наступне визначення - це сукупність процесів створення, оброблення, відправлення, передавання, одержання, зберігання, використання та знищення електронних документів, які виконуються із застосуванням перевірки цілісності та у разі необхідності з

підтвердженням факту одержання таких документів[2]. Також даний закон закріплює порядок проведення електронного документообігу, де йдеться про те, що фактично кожний орган державної влади, місцевого самоврядування і т.д. вирішує самостійно порядок проведення такого документування [2]. Самостійність у прийнятті таких рішень є важливим фактом, адже кожен державний орган має здійснювати документообіг відповідно до своєї компетенції та можливостей. З урахуванням цифрового та інформаційного розвитку суспільства нормативно-правова база потребує внесення змін з конкретизацією на окремі системам електронного документообігу. Щодо визначення СЕД системи МВС, можемо сказати, що це автоматизована система, призначена для документального забезпечення процесів управління та автоматизації діловодства та документообігу, здійснення контролю за виконавською дисципліною, забезпечення обробки електронних документів та, за необхідності, документів у паперовому вигляді в діяльності: апарату МВС та Головного центру з надання сервісних послуг, територіальних центрів з надання сервісних послуг, закладів, установ і підприємств, що належать до його управління; Національної гвардії України; центральних органів виконавчої влади, діяльність яких спрямовується і координується Кабінетом Міністрів України через Міністерство внутрішніх справ України [4]. Нажаль, правового регулювання застосування СЕД в діяльності Національної поліції України немає, але при цьому застосування даної системи відповідає загальним нормативно-правовим нормам.

Закріпленої норми Кримінального процесуального кодексу щодо електронного документу та загальних положень про електронний документообіг немає. Існують загальні положення про електронний документ в якості доказу, на прикладі ст. 99 Кримінального процесуального кодексу яка вказує, що оригіналом електронного документа являється його відображення, якому надається таке ж значення, як документу [1]. Як ми вже зазначали, що законодавство потребує змін з урахуванням цифрових нововведень таких як СЕД та інших.

Роль СЕД у кримінальному процесі є важливим фактором, оскільки кримінальний процес потребує в найкоротший строк розгляду та прийняття рішень щодо питань у кримінальних провадженнях. На це вказує і мета створення цієї системи яка зазначена в Наказі МВС України від 28.04.2017 року щодо «Вимог до створення і впровадження єдиної системи електронного документообігу в Міністерстві внутрішніх справ України та центральних органах виконавчої влади, діяльність яких спрямовується і координується Кабінетом Міністрів України через Міністра внутрішніх справ України», де вказано що однією із мети створення СЕД є забезпечення інформаційно-аналітичної підтримки діяльності системи МВС, якості і своєчасності прийняття управлінських рішень, взаємодії виконавців [4].

Враховуючи умови воєнного стану на території нашої держави, впровадження електронного документообігу в установах які входять до складу сил безпеки й оборони країни є критично важливим. Оскільки деякі з важливих документів через військову агресію були знищені або втрачені. Електронний документообіг дає змогу зберегти дані та інформацію яку містив той чи інший документ. Також важливим функціоналом є комунікація між центрами управління та районами доступ до яких через ведення бойових дій неможливий або ускладнений.

Наприклад, через запровадження електронного документообігу в Північно-Східне міжрегіональне управління юстиції (Полтавська, Сумська, Чернігівська області) вдалося забезпечити безперервність роботи обласних структур Міністерства юстиції та зберегти всю документацію під час тимчасової окупації частини Сумської області в 2022 році [3]. За підтримки проекту ЄС “Право-Justice”, який реалізується з 2019 року, було створено електронний архів і забезпечено належне зберігання Національного архівного фонду України, який на даний момент реалізували у своїй структурі Міністерство юстиції, Державна архівна служба та Міністерство цифрової трансформації [3].

В свою чергу Міністерством внутрішніх справ було введено СЕД МВС,

який реалізується з 2017 року але належне застосування саме в практичній діяльності набув пізніше, оскільки такі нововведення потребують належного правового регулювання. Дані нововведення як було зазначено в умовах воєнного стану створюють умови для зберігання документації та створення електронних-інформаційного архіву. Також важливе значення має відновлення вже втрачених документів в умовах ведення бойових дій.

Ми можемо підсумувати ,що впровадження електронного документообігу в МВС, зокрема органах Національної поліції України, потребує законодавчого врегулювання. Розвиток інформаційних технологій дещо випереджає законодавчу базу і це призводить до певних прогалин. СЕД безумовно потребує вдосконалення з урахуванням специфіки роботи певних органів та підрозділів МВС, але впровадження таких систем є кроком до підвищення ефективності діяльності органів державної влади та забезпечення безбар'єрної комунікації між собою та безпосередньо в середині установ.

Список використаних джерел:

1. Кримінальний процесуальний кодекс України : Закон України від 13 квіт. 2012 р. № 4651-VI // Законодавство України / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/4651-17 (дата звернення: 19.09.2025).

2. Про електронні документи та електронний документообіг : Закон України від 22 трав. 2003 р. № 851-IV // Законодавство України / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/851-15 (дата звернення: 19.09.2025).

3. Презентація пілотного проєкту електронного архівування, реалізованого за сприяння Про- єкту ЄС «Право-Justice». URL: https://www.pravojustice.eu/ua/post/vidbulasya-prezentaciya- pilotnogo-proyektu-elektronnogo-arhivuvannya-realizovanogo-za-spriyannya-proyektu-yes- pravo-justice (дата звернення: 19.09.2025).

4. Вимоги до створення і впровадження єдиної системи електронного документообігу (СЕД) в МВС : Наказ МВС України від 28 квіт. 2017 р. № 363.

URL: https://mvs.gov.ua (дата звернення: 19.09.2025).

КРИВИК Аліна
старший судовий експерт відділу судової експертизи (м. Мелітополь) Запорізького науково-дослідного експертно-криміналістичного центру МВС України, м. Запоріжжя, Україна

ДАКТИЛОСОКПІЧНИЙ ОБЛІК ЯК ОСНОВНЕ ДЖЕРЕЛО НАКОПИЧЕННЯ ТА ЗБЕРІГАННЯ ДАКТИЛОСКОПІЧНОЇ ІНФОРМАЦІЇ

У зв’язку з ростом злочинності, особливу роль відіграє інформація, яка характеризує різні сторони злочину, а також осіб, які його скоїли. Одним із засобів збору такої інформації виступає криміналістична реєстрація.

Одним із проявів криміналістичної реєстрації виступають криміналістичні обліки та удосконалення їх використання як різновид інформаційного забезпечення судово-експертної діяльності по боротьбі зі злочинністю [1, с.9].

В реаліях сьогодення одним із найбільш інформативним та результативним із криміналітичних обліків є дактилоскопічний облік.

В Україні дактилоскопічний облік функціонує на центральному (м. Київ) та обласному рівнях (наприклад, Харківська область, Львівська область), розпорядником якого є Державний науково-дослідний експертно-криміналістичний центр МВС України України (далі – ДНДЕКЦ МВС) та Науково-дослідні експертно-криміналістичні центри МВС України (далі – НДЕКЦ МВС) (Свідоцтво про Державну реєстрацію бази персональних даних України – Серія АА № 000267 від 15.09.2011 запис у Реєстрі № 249).

Дактилоскопічний облік складається з основного масиву

(дактилокартотек/слідотек) та архіву. Дактилокартотеки формуються з дактилокарт невпізнаних трупів, безвісно зниклих осіб та осіб, які були піддані дактилоскопіюванню, а слідотеки – з реєстраційних карт слідів рук, які вилучені під час оглядів місць подій за фактами нерозкритих злочинів та безвісного зникнення осіб [2].

У підрозділах експертної служби МВС облік здійснюється за допомогою автоматизованої дактилоскопічної ідентифікаційної системи (далі – АДІС).

Дактилоскопічний облік ведеться за допомогою ідентифікаційної системи, яка включає установчі дані та дактилоскопічну інформацію про криміногенних осіб, за допомогою такої системи: – забезпечується зберігання та облік, видача оперативно-довідкової інформації на певну категорію осіб (наприклад, що вчинили кримінальний злочин у межах території України тощо); – здійснюється ідентифікація осіб, що приховують від правоохоронних структур свої біографічно установчі дані; – здійснюється пошуковий процес злочинців за слідами, які були виявлені на місці події [3, с.179].

Правила збирання, накопичення, зберігання, використання та знищення біометричних даних розкриваються тільки в підзаконних нормативних актах. Так, в Інструкції «Про порядок функціонування дактилоскопічного обліку експертної служби МВС України» визначено що проводиться дактилоскопіювання осіб, які:– затримані за підозрою у вчиненні злочину;– взяті під варту;– обвинувачуються у вчиненні злочину;– піддані адміністративному арешту. Даною Інструкцією також регулюються строки зберігання дактилоскопічних карт та підстави їх вилучення з обліку до спливу строків зберігання [2].

Саме дактилоскопічний облік є важливою системою збору, зберігання та використання відбитків пальців для ідентифікації особи, яка використовується в криміналістиці для встановлення причетності осіб до злочину, розшуку безвісно зниклих осіб та ідентифікації невпізнаних трупів.

З метою постійного накопичення дактилоскопічної ідентифікаційної системи більш якісною інформацією (якісних дактилокарт) експертами

Державного та територіальних підрозділів науково-дослідних експертно-криміналістичних центрів МВС України (ДНДЕКЦ МВС України) між структурними підрозділами МВС України, Державної кримінально-виконавчої служби України (ДКВС) проводяться тренінги на тему «Дактилоскопіювання». Це важлива складова сучасних методів безпеки та ідентифікації осіб. Програми тренінгів включають основи дактилоскопії, техніку зняття відбитків пальців, обговорення типових помилок під час дактилоскопіювання та шляхи їх уникнення.

Окрім цього, з метою отримання якісної слідової інформації дактилоскопічного походження проводяться практичні навчання з метою оволодіння теоретичною базою і практичними навичками роботи зі слідовою інформацією під час проведення огляду місця події та інших слідчих (розшукових) дій. Це цілком природно, оскільки саме якісне та правильне дактилоскопійование особи та вилучення слідової інформації надає в подальшому проведення більш точного аналізу та порівняння в АДІС.

На теперішній час необхідним є також оновлення програмного забезпечення ідентифікаційних систем та правового регулювання дактилоскопічного обліку, так як під час воєнного стану стає поширеним способом ідентифікації особи невпізнаних трупів військовослужбовців дактилоскопіювання таких та занесення вказаної інформації до АДІС.

На думку деяких спеціалістів, потребують правового врегулювання не тільки питання дактилоскопічного обліку, але й інших біометричних даних. Це пропонується вирішити шляхом прийняття закону про біометричну реєстрацію, де були б визначені її види, порядок формування та використання, шляхом запозичення позитивного досвіду іноземних країн щодо створення єдиних надвеликих масивів дактилоскопічної інформації в центральних підрозділах. Наприклад, таким шляхом пішли Німеччина, Ізраїль, Швейцарія, Чехія, Словаччина, Казахстан та Угорщина. Важливим також буде удосконалення діючої системи автоматизованих дактилоскопічних обліків МВС України шляхом створення єдиного автоматизованого банку даних з

нарощуванням потужностей існуючих центральних, обласних програмно-технічних комплексів задля проведення перевірок у режимі реального часу та наданням авторизованого доступу до баз працівникам усіх правоохоронних органів [4, с.241].

Враховуючи те, що дактилоскопічний облік є одним із важливих джерел накопичення та зберігання інформації, яка допомагає в подальшому ідентифікувати особу, вважаємо за потрібне наголосити на тому, що вдосконалення та оновлення правового регулювання, програмного забезпечення та практичного досвіду є важливим для відповідності дактилоскопічного обліку міжнародним стандартним, а також безпосередньо відповідності функціональних вимог такого для отримання належних результатів.

Список використаних джерел:

1. А.В. Кофанов. Навчально-методичний комплекс «Криміналістичні обліки та удосконалення їх використання – Навчально-методичний комплекс. – Київ: КИЙ, 2009. – 55 с.

2. Інтернет ресурс: https://zakon.rada.gov.ua/laws/show/z1066-01#Text

3. Кажанов С.П. Використання автоматизованої інформаційної системи ідентифікації пальцевих відбитків в організації розкриття та розслідування злочинів // С.П. Кажанов. – К., 2016 - С.178-182.

4. Книженко С.О., Шарабан О.І. Дактилоскопічний облік в Україні: правове регулювання та тенденції розвитку// Науковий вісник Ужгородського Національного Університету, 2023, С. 237 - 242.

ЛЕЖЕНКО Олександр
курсант, Військово-юридичного інституту, Національного юридичного університету імені Ярослава Мудрого

Науковий керівник:
ГАШЕНКО Сергій
старший викладач кафедри загальновійськових дисциплін (Військово-юридичного інституту Національного юридичного університету імені Ярослава Мудрого) підполковник

РОЗВИТОК ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ОПЕРАТИВНО-РОЗШУКОВОЇ ДІЯЛЬНОСТІ В УМОВАХ ВОЄННОГО СТАНУ

Розвиток інформаційного забезпечення оперативно-розшукової діяльності в умовах воєнного стану є визначальним чинником у системі гарантування національної безпеки, протидії злочинності та викриття диверсійно-розвідувальних проявів противника. У період війни оперативні підрозділи працюють у надзвичайно динамічних і ризикованих умовах, що зумовлює потребу у вдосконаленні механізмів збору, накопичення, аналізу та застосування інформації [3. с.4]. Саме належний рівень інформаційного забезпечення дозволяє правоохоронним органам своєчасно виявляти загрози, запобігати злочинам, нейтралізовувати диверсійні групи, розкривати випадки шпигунства, колаборації та терористичної діяльності.

Актуальні виклики воєнного стану істотно трансформують характер оперативно-розшукової роботи. Посилення активності спецслужб противника, збільшення масштабів кібератак та інформаційно-психологічних операцій потребують упровадження нових методів роботи з даними та їхнього захисту. Вдосконалення інформаційного забезпечення оперативно-розшукової діяльності передбачає створення інтегрованих інформаційних систем та єдиних баз даних, що містять відомості про осіб, транспортні засоби, зброю та інші об’єкти оперативного інтересу. Важливим напрямом є цифровізація і автоматизація процедур: упровадження електронного документообігу, автоматизований аналіз телефонних з’єднань та поступове впровадження

штучного інтелекту. Значного значення набувають технології кіберрозвідки й цифрової криміналістики, включаючи моніторинг соціальних мереж і месенджерів, виявлення бот-мереж та протидію інформаційним впливам ворога.

Водночас дедалі ширше застосовуються сучасні технічні засоби – безпілотні літальні апарати, супутникові знімки, системи відеоаналітики та ідентифікації облич, геоінформаційні технології, що дозволяють відстежувати переміщення підозрілих осіб чи груп. Не менш важливим є зміцнення кіберзахисту, який базується на використанні криптографічних засобів, багаторівневих систем автентифікації та ефективних заходів запобігання витокам інформації.

Особливої актуальності в умовах війни набуває міжвідомча та міжнародна співпраця. Налагоджений обмін оперативними даними між українськими правоохоронними органами та силовими структурами, а також взаємодія з Інтерполом, Європолом і спецслужбами держав-партнерів створюють умови для оперативного виявлення та ліквідації транснаціональних загроз.

Перспективи розвитку інформаційного забезпечення ОРД полягають у формуванні єдиної національної системи збору й аналізу даних, упровадженні технологій штучного інтелекту та Big Data для встановлення прихованих зв’язків між об’єктами оперативного інтересу, посиленні кіберпідрозділів і вдосконаленні підготовки кадрів у сфері цифрової аналітики.

Україна, як і чимало інших держав, неодноразово переживала періоди, коли введення воєнного стану спричиняло надзвичайні виклики. Такі обставини, позначені постійною напругою та зростанням небезпек, висувають перед правоохоронними органами особливі вимоги – максимальної професійності, злагодженості та оперативності. В умовах війни провідна роль належить оперативно-розшуковій діяльності Національної поліції, адже саме вона забезпечує не лише охорону громадського порядку, а й захист прав, життя та майна громадян. У цей період завдання поліції значно ускладнюються: поряд

із боротьбою зі злочинністю необхідно гарантувати безпеку в умовах, де будь-яка помилка може мати критичні наслідки. Ефективність роботи визначається не лише суворим дотриманням законодавства, але й умінням швидко адаптуватися, застосовувати нові тактики та вибудовувати результативні стратегії реагування. Сучасні виклики, що поєднують у собі геополітичні та технологічні фактори, роблять оперативно-розшукову діяльність ще більш затребуваною. Стале оновлення методів роботи, аналіз ефективності дій, впровадження сучасних технологій і міжвідомча співпраця є необхідними для підтримання належного контролю за ситуацією та попередження злочинних проявів [4. с.90].

Закон України «Про оперативно-розшукову діяльність» визначає цю сферу як систему гласних і негласних заходів розвідувального, пошукового та контррозвідувального характеру, що здійснюються за допомогою оперативних і технічних засобів [1.с.3-4]. Її ключове завдання – своєчасне виявлення, припинення й розслідування злочинів, а також гарантування безпеки суспільства. В Україні до цієї діяльності залучені різні відомства: Національна поліція України – підрозділи кримінальної та спеціальної поліції, орієнтовані на боротьбу зі злочинністю та захист громадян; Державне бюро розслідувань – здійснює оперативні заходи й підтримує розслідування; Служба безпеки України – контррозвідка, підрозділи з протидії тероризму, організованій злочинності й корупції; Служба зовнішньої розвідки та розвідувальні органи МО України – відповідають за збір і аналіз зовнішньої інформації; Державна прикордонна служба України – реалізує оперативно-розвідувальні заходи для захисту кордону; НАБУ та БЕБ – здійснюють оперативну діяльність у сферах корупційних і економічних правопорушень [2.с. 52]

Оперативно-розшукова діяльність у період війни виходить на новий рівень складності. Вона охоплює не лише розкриття злочинів, а й протидію диверсійним і шпигунським загрозам, боротьбу з тероризмом та організованою злочинністю. Успішність такої роботи залежить від

координації між структурами, професійної підготовки кадрів, застосування спеціальних методів розслідування, а також від здатності балансувати між захистом прав людини та забезпеченням національної безпеки. Особливу роль у цьому процесі відіграють взаємодія між відомствами та військовими структурами для координації дій у надзвичайних ситуаціях, модернізація правового регулювання з урахуванням специфіки воєнного стану, зокрема щодо негласних заходів, забезпечення прозорості й правомірності дій правоохоронців для підтримання довіри суспільства, а також професійна підготовка кадрів – від оперативних навичок до знань у сфері кібербезпеки й надання першої допомоги.

Водночас міжнародний досвід та стандарти, зокрема положення Конвенції про захист прав людини і основоположних свобод (1950 р.), нагадують про неприпустимість нехтування правами людини навіть у час війни[3.с.5]. Це створює додатковий виклик для українських правоохоронних органів, які змушені одночасно реагувати на реальні загрози та дотримуватися принципів правової держави. Таким чином, оперативно-розшукова діяльність у період воєнного стану потребує гнучкості, високого рівня координації, удосконалення нормативної бази та зміцнення технічного й кадрового потенціалу. Вона стає ключовим інструментом збереження національної безпеки, правопорядку та довіри громадян до державних інституцій.

Список використаних джерел:

1. Закон України «Про оперативно-розшукову діяльність»

2. Зінченко, Данііл, Олена Джафарова. Соціальні мережі як інструмент оперативно-розшукової діяльності поліції під час воєнного стану в Україні. Видавництво Національної академії Державної прикордонної служби України імені Б. Хмельницького Свідоцтво суб’єкта видавничої справи ДКNo 3010 від 22.10. 2007, 2024.

3. Цифра Р.О. Дем’янець М.Р. Кисельов А.О. Оперативна розшуковадіяльність підрозділів національної поліції України в період

воєнного стану. 2024.

4. Шумейко Д.О. Фактори, що впливають на ефективність застосування засобів оперативнорозшукової діяльності в умовах воєнного стану. Актуальні питання та перспективи використання оперативно-розшукових засобів у розкритті злочинів в умовах воєнного стану: Збірник наукових праць. Національна академія внутрішніх справ. 2023.

ЛЄЙКО Міхаіл
Здобувач ступеня вищої освіти магістра Національної академії внутрішніх справ

ВИДИ НЕГЛАСНИХ СЛІДЧИХ (РОЗШУКОВИХ) ДІЙ

У сучасному кримінальному процесі України негласні слідчі (розшукові) дії (далі – НСРД) є одним із найефективніших інструментів отримання доказової та орієнтовної інформації про кримінальні правопорушення, які мають латентний характер. Їх застосування зумовлене необхідністю протидії тяжким та особливо тяжким злочинам, коли використання відкритих процесуальних дій є неможливим або неефективним.

Відповідно змісту п.1 ст.246 КПК України: негласні слідчі (розшукові) дії - це різновид слідчих (розшукових) дій, відомості про факт та методи проведення яких не підлягають розголошенню, за винятком випадків, передбачених цим Кодексом [1].

Правову основу проведення НСРД становлять положення Кримінального процесуального кодексу України, зокрема глава 21 (статті 246–275). Відповідно до п.2 ст. 246 КПК України, негласні слідчі (розшукові) дії проводяться у разі, якщо відомості про кримінальне правопорушення чи особу, яка його вчинила, неможливо отримати іншим способом [1]. Зазначені дії здійснюються з дотриманням принципів законності, пропорційності та судового контролю.

Залежно від характеру втручання у права і свободи людини НСРД можна

класифікувати на кілька основних видів. До першої групи належать негласні слідчі (розшукові) дії, пов'язані з втручанням у приватне спілкування. До них відносяться аудіо- та відеоконтроль особи, зняття інформації з транспортних телекомунікаційних мереж, а також зняття інформації з електронних інформаційних систем. Ці дії здійснюються виключно на підставі ухвали слідчого судді та характеризуються значним обмеженням конституційних прав, зокрема права на таємницю листування та приватного життя.

Другу групу становлять НСРД, не пов'язані безпосередньо з втручанням у приватне спілкування, але спрямовані на негласне отримання інформації про поведінку осіб, об'єкти або місця. До таких дій належать спостереження за особою, річчю або місцем, обстеження публічно недоступних місць, житла чи іншого володіння особи, а також встановлення місцезнаходження радіоелектронного засобу. Дані заходи дозволяють фіксувати фактичні дії підозрюваних осіб та їх зв'язки без розкриття факту здійснення негласних слідчих (розшукових) дій.

Окреме місце серед НСРД посідають дії, пов'язані з контролем за вчиненням злочину. До них належать контрольована поставка, контрольована та оперативна закупка, спеціальний слідчий експеримент, а також імітування обстановки злочину. Зазначені дії спрямовані на документування злочинної діяльності у реальному часі та широко застосовуються під час розслідування злочинів у сфері незаконного обігу наркотичних засобів, корупції та діяльності організованих злочинних угруповань.

Ще одним важливим видом НСРД є виконання спеціального завдання з розкриття злочинної діяльності організованої групи або злочинної організації. Така дія передбачає негласне проникнення уповноваженої особи в злочинне середовище з метою отримання інформації про структуру, керівників, фінансування та способи вчинення злочинів. Вказаний вид НСРД є одним із найбільш складних та ризикованих, але водночас ефективних у боротьбі з організованою злочинністю.

В свою чергу згідно змісту розділу 1 наказу «Про затвердження Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні» від 16.11.2012р.

№114/1042/516/1199/936/1687/5 наведена інша класифікація нс(р)д: до першого виду відносяться нс(р)д, які проводяться виключно у кримінальному провадженні щодо тяжких або особливо тяжких злочинів: (аудіо-,відео контроль особи(ст.260 КПК України); накладення арешту на кореспонденцію (ст.261 КПК України); огляд і виїмка кореспонденції(ст.262 КПК України); зняття інформації з транспортних телекомунікаційних мереж; зняття інформації з електронних інформаційних систем без відома її власника, володільця або утримувача (ст.264 КПК України); обстеження публічно недоступних місць, житла чи іншого володіння особи (ст.267 КПК України); спостереження за особою в публічно доступних місцях (ст.269 КПК України); аудіо-, відео контроль місця (ст.270 КПК України); негласне отримання зразків, необхідних для порівняльного дослідження (ст.274 КПК України); спостереження за річчю або місцем у публічно доступних місцях (ст.269 КПК України); контроль за вчиненням злочину (ст.271 КПК України); виконання спеціального завдання з розкриття злочинної діяльності організованої групи чи злочинної організації (ст.272 КПК України). Другий вид нс(р)д - проводяться незалежно від тяжкості злочину: зняття інформації з електронних інформаційних систем або її частини , доступ до яких не обмежується її власником, володільцем або утримувачем і не пов’язаний з подоланням системи логічного захисту (ч.2 ст.264 КПК України); установлення місцезнаходження радіоелектронного засобу (ст.268 КПК України)[2].

Особливістю проведення негласних слідчих (розшукових) дій є суворий судовий контроль та обмежений строк їх здійснення. Порушення порядку санкціонування або проведення НСРД тягне за собою визнання отриманих результатів недопустимими доказами у кримінальному провадженні, що неодноразово підтверджується судовою практикою.

Таким чином, негласні слідчі (розшукові) дії є важливим елементом механізму досудового розслідування, який дозволяє ефективно протидіяти тяжким і особливо тяжким злочинам. Водночас їх застосування потребує чіткого дотримання вимог кримінального процесуального законодавства та забезпечення балансу між інтересами правосуддя і правами людини.

Список використаних джерел

1. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 № 4651-VI.
2. Наказ «Про затвердження Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні» від 16.11.2012р. №114/1042/516/1199/936/1687/5

ЛОСКУТОВ Тимур
головний науковий співробітник науково-дослідної лабораторії з проблем запобігання кримінальним правопорушенням
доктор юридичних наук, професор
(Донецький державний університет внутрішніх справ)

ЩОДО НОРМАТИВНОГО ЗАБЕЗПЕЧЕННЯ ЗАСАДИ СПЕЦІАЛЬНОЇ ПРОПОРЦІЙНОСТІ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ В УМОВАХ ВОЄННОГО СТАНУ

1. Введення правового режиму воєнного стану в Україні пов’язано з встановленням різних юридичних обмежень для членів громадян. Задля гарантування соціальної безпеки та результативної боротьби зі злочинністю під час здійснення бойових дій державні органа вимушені унормовувати правообмеження. Водночас законодавчі обмеження не повинні бути свавільними, не прогнозованими. Правові обмеження в період воєнного стану мають відповідати вимозі пропорційності з урахуванням певного випадку небезпеки виконання воєнних дій та необхідності провести ефективне (результативне) розслідування обставин вчинення кримінального

правопорушення.

Нормативне забезпечення засади пропорційності у кримінальному процесуальному законі є важливим та потрібним у сьогоднішніх умовах дії правового режиму воєнного стану. Оскільки наразі досить швидко змінюються нормативні приписи процесуального законодавства, зміст котрих подекуди не узгоджується з фактичними реаліями проведення воєнних дій на території держави. Ситуація небезпеки у зв'язку з проведенням бойових дій значно перешкоджає забезпеченню процесуальних гарантій реалізації прав, свобод і законних інтересів суб'єктів кримінальних процесуальних відносин.

2. Під час здійснення кримінального провадження в обстановці виконання воєнних дій має нормативно забезпечуватися та реалізовуватися не лише загальна засада пропорційності, а й «спеціальна пропорційність» як окремий принцип кримінального процесу. Зміст останньої виявляється у співвідношенні небезпеки воєнної ситуації та необхідністю гарантування прав, свобод і законних інтересів осіб, які залучаються до сфери кримінального судочинства.

3. Норми кримінального процесуального закону не забезпечують належним чином спеціальну засаду пропорційності під час кримінального провадження в умовах воєнного стану. Вказаний недолік кримінального процесуального законодавства може негативно позначатися на забезпеченні прав, свобод і законних інтересів людини та на ефективності проведення кримінальної процесуальної діяльності в період воєнного стану.

4. Обстановка виконання воєнних дій обумовлює перевагу публічного інтересу у кримінальному провадженні, учасники якого можуть перебувати в небезпеці під час проведення процесуальних дій. Ця ситуація значно ускладнює реалізацію звичайного порядку (форми) кримінального процесу. У зв'язку з цим, державні органи вимушені проводити кримінальну процесуальну діяльність за правилами особливого (спеціального) порядку кримінального провадження, у межах якого оцінюється не тільки

співвідношення публічного та приватного (індивідуального) інтересу, а також пропорційність державного інтересу в умовах воєнного стану та приватного інтересу.

Враховуючи сьогоднішню ситуацію воєнного стану, наявність ризику завдання шкоди життю та здоров'ю людей під час виконання бойових дій, у змісті кримінального процесуального закону регламентуються правила особливого (спеціального) порядку кримінального процесу, що пов'язаний з розширенням процесуальної компетенції сторони обвинувачення та додатковим обмеженням прав, свобод і законних інтересів осіб, які залучаються до сфери кримінального судочинства (ст. 615 КПК України та інші нормативні приписи КПК України). У наведений спосіб нормативно забезпечується спеціальна засада пропорційності у кримінальному провадженні в період воєнного стану.

5. Зміст спеціальної засади пропорційності має стосуватися всіх потенційних випадків кримінального провадження в обстановці проведення бойових дій. Іншими словами, приписи КПК України мають врегульовувати спеціальну засаду пропорційності стосовно кожної ситуації відступу від загальної форми кримінальної процесуальної діяльності.

6. Нормативне забезпечення засади «спеціальної пропорційності» у кримінальному провадженні під час дії правового режиму воєнного стану уможливить вирішення проблем правового регулювання, що стосуються проведення слідчих (розшукових) дій, застосування заходів забезпечення кримінального провадження в обстановці виконання бойових дій.
Необхідність нормативного забезпечення спеціальної засади пропорційності в період воєнного стану у процесуальному законі зумовлюється дефектністю законодавчої термінології, що негативно вливає на результати тлумачення процесуальних норм під час правозастосування у перебігу кримінальному провадженні. Суб'єкти кримінального процесу в обстановці воєнного стану можуть вкладати різний зміст у поняття оціночних термінів, що

використовуються для визначення «спеціальної пропорційності» між державним (суспільним) інтересом та приватним (індивідуальним) інтересом у кримінальному судочинстві («наявності об'єктивних обставин, що унеможливлюють», «відсутня об'єктивна можливість», «неможливості розгляду», «в разі неможливості з об'єктивних причин», тощо). Це не сприяє ефективності кримінального провадження в умовах воєнного стану та гарантуванню прав, свобод і законних інтересів людини.

7. З метою покращення змісту процесуальних норм щодо нормативного регулювання кримінальної процесуальної діяльності в умовах воєнного стану слід регламентувати «спеціальну пропорційність» як окрему засаду кримінального провадження під час дії правового режиму воєнного стану. Комплексний та системний підхід до нормативного забезпечення спеціальної засади пропорційності у кримінальному провадженні в обстановці воєнного стану сприятиме забезпеченню ефективності кримінального процесу та справедливості обмеження прав, свобод і законних інтересів людини.

НУРГАЛІЄВ Едуард
здобувач вищої освіти 3 курсу ННІПФПКП ім. Е.О. Дідоренка Донецького державного університету внутрішніх справ

Науковий керівник:
ЛУНГОЛ Ольга
завідувач кафедри оперативно-розшукової діяльності та інформаційної безпеки ННІПФПКП ім. Е.О. Дідоренка Донецького державного університету внутрішніх справ, кандидат педагогічних наук, доцент

ЗНЯТТЯ ІНФОРМАЦІЇ З ЕЛЕКТРОННИХ КОМУНІКАЦІЙНИХ

МЕРЕЖ ЯК ВАЖЛИВИЙ ЗАСІБ ОПЕРАТИВНО-РОЗШУКОВОЇ ДІЯЛЬНОСТІ В УМОВАХ ВОЄННОГО СТАНУ

У сучасних умовах воєнного стану, спричиненого повномасштабною збройною агресією проти України, забезпечення державної безпеки через виявлення та нейтралізацію диверсійно-розвідувальних груп, протидію тероризму та інформаційно-психологічним операціям набувають першочергового значення. Одним з відповідних засобів, що використовується в оперативно-розшуковій діяльності, є законне перехоплення інформації (перехоплення електронних комунікацій) з мереж зв'язку [1 – 3]. В умовах активного використання цифрових технологій злочинцями, зазначений засіб дозволяє ефективно фіксувати комунікації, ідентифікувати учасників злочинної діяльності, встановлювати їхню роль, наміри та зв'язки.

Нормативно-правовою основою проведення заходів законного зняття інформації з електронних комунікаційних мереж виступають статті 263 та 264 Кримінального процесуального кодексу України [4], а також положення Закону України «Про оперативно-розшукову діяльність» та інші нормативні акти, зокрема спільний наказ СБУ і Держспецзв'язку «Про затвердження нормативного документа «Технічні засоби для здійснення уповноваженими органами оперативно-розшукових, контррозвідувальних, розвідувальних заходів та негласних слідчих (розшукових) дій в електронних комунікаційних мережах загального користування України. Загальні технічні вимоги» [5]. Законодавство визначає процедуру санкціонування, порядок звернення до суду, коло суб'єктів, які мають право ініціювати такі дії, а також місце операторів комунікацій у забезпеченні технічної можливості зняття інформації.

Згідно з положеннями статті 263 КПК України, зняття інформації з електронних комунікаційних мереж полягає у проведенні, із застосуванням відповідних технічних засобів спостереження, відборі та фіксації змісту

інформації, яка передається особою та має значення для досудового розслідування, а також одержанні, перетворенні й фіксації різних видів сигналів, що передаються каналами зв'язку. Йдеться, зокрема, про перехоплення голосових викликів, SMS/MMS-повідомлень, інтернет-трафіку, даних з VPN-з'єднань, месенджерів тощо. Це дає змогу не лише фіксувати зміст комунікації, а й отримувати метадані: час, тривалість, геолокацію, IP-адреси, тип послуги тощо. Така інформація має значну доказову цінність у справах, що стосуються терористичної діяльності, шпигунства, державної зради та колабораціонізму.

Відповідно до статті 264 КПК України, зняття інформації з електронних інформаційних систем дозволяє отримати доступ до даних, що зберігаються на комп'ютерах, серверах, у хмарних сховищах або автоматизованих інформаційних системах. Сюди можна віднести як активну інформацію (відкриті файли, листування, бази даних), так і дані, які були видалені або приховані. В умовах воєнного стану це дозволяє виявляти факти співпраці з окупаційними силами, підготовку терористичних актів, передавання даних ворогу, а також простежувати цифрові сліди злочинної діяльності.

Зняття інформації з електронних комунікаційних мереж (за ст. 263 КПК) та з електронних інформаційних систем (за ст. 264 КПК) може застосовуватися комплексно. Наприклад, у межах одного кримінального провадження правоохоронці можуть одночасно здійснювати прослуховування телефонних дзвінків, доступ до історії з'єднань через мобільні мережі, а також віддалено вивчати вміст комп'ютерного пристрою підозрюваного. Такий підхід дозволяє формувати повну картину цифрової активності об'єкта спостереження, документувати факти злочинної діяльності, збирати докази для судового розгляду.

Зняття інформації з електронних комунікаційних мереж в умовах збройного конфлікту є не лише технічно можливим, а й правомірним засобом забезпечення національної безпеки. Успішне його застосування потребує поєднання нормативно обґрунтованого процесу із високотехнологічною

підтримкою, а також глибокого розуміння функціонування комунікаційних систем. У контексті подальшого вдосконалення інституту негласних слідчих дій доцільним видається не лише адаптація законодавства до новітніх технологій, але й створення єдиної технічної платформи для взаємодії правоохоронних органів з провайдерами. Збереження балансу між ефективністю державної безпеки та дотриманням прав людини має залишатися пріоритетом у цій сфері.

Список використаних джерел:

1. Челпан Ю., Степанов В. Перехоплення інформації в мережах мобільного зв'язку покоління 5G. СБУ в умовах війни в Україні: сучасні реалії та інноваційні стратегії забезпечення національної безпеки: матеріали міжнародної науково-практичної конференції 4-5 липня 2024 року. Київ : Алерта, 2024. С. 263 – 265.
2. Челпан Ю.В., Степанов В.А. Законне перехоплення інформації в IP підсистемах мультимедійного зв'язку. Зв'язок. № 1, 2025. С. 17 – 22.
3. Степанов В.А., Челпан Ю.В. Аспекти законного перехоплення інформації в мережі мобільного зв'язку, яка одночасно використовує технології 4G, 5G та IMS. Телекомунікаційні та інформаційні технології. № 3. 2024. С. 69 – 76.
4. Кримінальний процесуальний кодекс України. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/4651-17#n2413 (Дата звернення: 01.10.2025).
5. Спільний наказ Служби безпеки України та Адміністрації Держспецзв'язку від 31.12.2021 № 460/781 «Про затвердження нормативного документа «Технічні засоби для здійснення уповноваженими органами оперативно-розшукових, контррозвідувальних, розвідувальних заходів та негласних слідчих (розшукових) дій в електронних комунікаційних мережах загального користування України. Загальні технічні вимоги». URL: https://surl.li/sqypqe (Дата звернення: 01.10.2025).

ОПАНАСЕНКО Олена
курсантка 3-го курсу *факультету підготовки фахівців для органів досудового розслідування Національної поліції України Донецького державного університету внутрішніх справ*

Науковий керівник:
ХИТРОВСЬКИЙ Дмитро
старший викладач кафедри загальноправових дисциплін факультету підготовки фахівців для органів досудового розслідування Національної поліції України Донецького державного університету внутрішніх справ

КІБЕРТЕРОРИЗМ ТА КІБЕРЗЛОЧИНИ: ЗАГРОЗИ В УМОВАХ ВІЙНИ

Сучасна війна виходить далеко за межі традиційного поля бою, охоплюючи інформаційний, економічний і цифровий простори. Особливістю сучасної кіберзлочинності є її тісна інтеграція з іншими формами організованої злочинності – фінансуванням тероризму, відмиванням коштів, незаконною торгівлею інформацією та зброєю. Україна, ставши об’єктом масштабної гібридної агресії, зіткнулася з безпрецедентним зростанням кіберзагроз, спрямованих на критичну інфраструктуру, органи державної влади, фінансову систему та інформаційні ресурси. Це зумовлює необхідність посилення національної та міжнародної співпраці у сфері кібербезпеки, удосконалення правових механізмів і створення ефективних систем обміну інформацією про кіберінциденти.

Національне законодавство визначає кіберзлочин (комп’ютерний злочин) як суспільно небезпечне та винне діяння, що здійснюється у кіберпросторі або з його використанням. Відповідальність за такі дії встановлена Кримінальним кодексом України та міжнародними договорами, ратифікованими нашою державою. Отже, кіберзлочинність можна розглядати

як сукупність злочинів, учинених у цифровому середовищі.

З кримінально-правової точки зору кіберзлочини охоплюють ті кримінальні правопорушення, які законодавець об'єднав у Розділі XVI Особливої частини Кримінального кодексу України. Це відокремлює їх від інших видів злочинів і визначає їхню належність до сфери кіберзлочинності.

Вирішальним чинником є спосіб учинення таких діянь – із використанням електронно-обчислювальних машин, телекомунікаційних систем, комп'ютерних мереж чи мереж електрозв'язку. Саме ця ознака надає кіберзлочинам їхню специфіку та визначає їх як окремий вид кримінальних правопорушень.

На сучасному етапі розвитку інформаційного суспільства кіберзлочини умовно поділяють на дві основні категорії – агресивні та неагресивні. До агресивних належать кібертероризм, погрози фізичної розправи, кіберпереслідування, кіберсталкінг. До неагресивних – кіберкрадіжка, кібершахрайство, кібервандалізм, кібершпигунство, розсилання спаму чи шкідливого програмного забезпечення. Такий поділ відображає як ступінь суспільної небезпеки, так і характер впливу злочину на особу чи інформаційне середовище.

При розгляді кіберзлочинності в умовах війни необхідно розглянути таке ключове поняття як кібертероризм.

За визначенням І.А. Білан, кібертероризм – це навмисні дії з використанням інформаційно-комунікаційних технологій, що здійснюються з політичною чи ідеологічною мотивацією з метою залякування населення, дестабілізації суспільства або порушення роботи критичних інформаційних систем[1].

Як зазначає В. Котляров, проблема кібертероризму носить глобальний характер і є надзвичайно актуальною в сучасному інформаційному суспільстві. За короткий проміжок часу кібератаки перетворилися з поодиноких випадків на одну з основних загроз інформаційній безпеці держав. Великі країни світу приділяють значну увагу захисту критично важливих

інформаційних ресурсів та розробці механізмів впливу на інформаційні системи інших держав [2].

В умовах глобалізації та поширення цифрової інформації зростають ризики інформаційного впливу на суспільство, особу та державу. Інформаційна епоха сприяє поширенню інформаційно-комунікаційних воєн, що призвело до виникнення кібертероризму – форми інформаційного тероризму, яка поєднує фізичні терористичні акти з операціями в кіберпросторі. Такі дії можуть призвести до підриву суверенітету, незалежності та територіальної цілісності держави [2].

Кіберпростір став ареною нової форми гібридної війни, де традиційні злочинні структури тісно переплітаються з воєнними та розвідувальними операціями. У цих умовах організована кіберзлочинність трансформується з економічного явища у стратегічний інструмент агресії. Саме тому розробка ефективних механізмів протидії вимагає комплексного підходу: удосконалення національного законодавства, розвитку цифрової грамотності, підготовки кіберспеціалістів і зміцнення міжнародної координації[3].

У сучасних умовах війни кіберзлочинність і кібертероризм виступають ключовими загрозами національній безпеці. Кіберзлочинність перетворюється на системну складову організованої злочинності з транснаціональним характером, високим рівнем анонімності та технологічною складністю, здатну завдавати шкоди державним інституціям, критичній інфраструктурі та суспільству. Кібертероризм поєднує інформаційні та фізичні атаки, спрямовані на дестабілізацію держави, підрив суверенітету та фінансування злочинних або воєнних операцій. Усе це підкреслює стратегічну небезпеку цих явищ і необхідність комплексних заходів протидії в умовах війни.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. **Білан І. А.** Кібертероризм як загроза національній безпеці України. Інформація і право. 2023. № 1. Режим доступу: https://il.ippi.org.ua/article/view/291584. (дата звернення 02.10.2025).

2. **Котляров В.О.** «Кібертероризм як загроза міжнародній безпеці». Наукові праці Міжрегіональної Академії управління персоналом. Політичні науки та публічне управління. 2023. № 5 (71). Режим доступу: https://journals.maup.com.ua/index.php/political/article/view/2981/3430 (дата звернення 02.10.2025).

3. **National Security and Defense Council of Ukraine (NSDC).** *Annual report on national security and cyber defence of Ukraine*. 2024. Режим доступу: https://www.rnbo.gov.ua (дата звернення 02.10.2025).

ОШЕДША Ангеліна
аспірантка відділу дослідження проблем кримінального процесу та судоустрою Науково-дослідного інституту вивчення проблем злочинності ім. акад. В.В. Сташиса НАПрН України

Науковий керівник:
ГЛИНСЬКА Наталія
доктор юридичних наук, професор, завідувачка відділом дослідження проблем кримінального процесу та судоустрою, Науково-дослідний інститут вивчення проблем злочинності імені академіка В.В. Сташиса НАПрН України

ЧАСОВІ МЕЖІ НАКЛАДЕННЯ АРЕШТУ НА МАЙНО У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ: ПРОБЛЕМИ ПРАВОВОЇ РЕГЛАМЕНТАЦІЇ

Відповідно до положень кримінального процесуального закону, накладення арешту на майно виконує важливу функцію у забезпеченні

дієвості кримінального провадження. Однак з огляду на чинне нормативно-правове регулювання арешту майна, практична реалізація цього заходу забезпечення кримінального провадження не вирізняється правовою визначеністю, насамперед у зв'язку з відсутністю вказівки на строк його тривалості. Така прогалина створює передумови для необмеженого у часі втручання у право особи на мирне володіння майном, що суперечить принципам кримінального судочинства.

Варто зазначити, що відповідно до ст. 170 КПК України накладення арешту на майно розглядається як тимчасове обмеження права на відчуження, розпорядження та/або користування майном [1]. Хоча арешт майна не означає його конфіскацію чи втрату права власності, однак тимчасове позбавлення можливості його реалізовувати є суттєвим втручанням сферу охоронюваних законом прав, свобод та законних інтересів людини. Саме тому дослідження дефектів правової регламентації строку дії арешту майна у кримінальному провадженні має фундаментальний правозахисний зміст і видається особливо актуальним.

У межах загального підходу до застосування заходів забезпечення кримінального провадження чітке визначення строків виступає важливим інструментом запобігання свавільному втручанню у права та свободи людини. Тобто в межах загального підходу законодавця до заходів забезпечення кримінального провадження, визначення строків є тією необхідністю, яка дозволяє уникнути довільного втручання у права та свободи людини та гарантувати дотримання процесуальної рівноваги між публічним інтересом і тимчасовим обмеженням прав і свобод осіб, щодо яких обрано той чи інший захід забезпечення кримінального провадження. Разом з тим, як нами було відзначено у попередньому дослідженні, відсутність нормативного регулювання строку дії ухвали про арешт майна вказує на існування необґрунтованого нормативного дефекту, коли захід забезпечення, що прямо впливає на обмеження права власності, може застосовуватись на невизначений або надмірний строк без необхідності періодичного перегляду

доцільності його продовження [2, с. 111].

Важливою ілюстрацією наслідків проблем правової регламентації часових меж накладення арешту на майно слугує Постанова Дніпровського районного суду м. Києва від 15 жовтня 2021 року (справа № 1-182/2011). Відповідно до змісту провадження початкове накладення арешту на грошові кошти заінтересованої особи відбулося 16 квітня 2008 року. Водночас питання про скасування арешту майно та повернення грошових коштів вирішено лише після спливу тринадцяти років. Строк дії арешту майна виявився настільки тривалим, що протягом цього періоду настала смерть підозрюваного у вчиненні кримінального правопорушення та сплинули строки давності притягнення до кримінальної відповідальності [3]. Наведений приклад наочно демонструє, як відсутність у кримінальному процесуальному законодавстві визначеної тривалості строку накладення арешту на майно призводить до ситуацій, коли тимчасовий захід фактично перетворюється на безстрокове обмеження права власності. Крім того, у практичному вимірі особа позбавлена ефективного засобу захисту для контролю за обґрунтованістю продовження накладеного арешту на майно. Подібні ситуації не лише не відповідають завданням кримінального провадження, але й суперечать практиці Європейського суду з прав людини, зокрема у справах «Pendov v. Bulgaria», «Rysovskyy v. Ukraine» тощо [4; 5].

Таким чином, нормативно-правова регламентація строку накладення арешту на майно є необхідною умовою для приведення норм кримінального процесуального законодавства у відповідність до принципу правової визначеності та забезпечення реального, а не декларативного змісту тимчасового характеру цього заходу забезпечення кримінального провадження. В такому контексті доцільним вбачається внесення до КПК України змін і доповнень, якими важливо передбачити конкретний та розумний строк накладення арешту на майно у кримінальному провадженні, після спливу якого питання щодо його подальшого застосування має вирішуватися з урахуванням наявності обґрунтованої потреби в такому

продовженні.

Список використаних джерел:

1. Кримінальний процесуальний кодекс України. Закон України від 13 квіт. 2012 р. № 4651-VI. *Голос України*. 2012. №№ 90-91. URL: https://zakon.rada.gov.ua/laws/show/4651-17 (дата звернення: 10.09.2025).

2. Ошедша А. Д. Щодо визначення строку накладення арешту на майно у кримінальному провадженні. *Прикарпатський юридичний вісник*. 2025. № 3. С. 110-115. DOI: https://doi.org/10.32782/pyuv.v3.2025.21

3. Постанова Дніпровського районного суду від 15 жовтня 2021 року. Справа № 1-182/2011. Провадження № 1/755/13/21. *Єдиний державний реєстр судових рішень.* URL: https://reyestr.court.gov.ua/Review/100346710 (дата звернення: 10.09.2025).

4. Case of Pendov v. Bulgaria, № 44229/11, 12.10.2020. URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-201890%22]} (дата звернення: 10.09.2025).

5. Rysovskyy v. Ukraine, № 29979/04, 20.10.2011. URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-107088%22]} (дата звернення: 10.09.2025).

ПАТРЕЛЮК Дмитро
докторант
кандидат юридичних наук
(Донецький державний університет внутрішніх справ)

ОКРЕМІ НАПРЯМИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ КРИМІНАЛЬНОГО ПЕРЕСЛІДУВАННЯ

Ефективність кримінального переслідуванняможна оцінювати за різними критеріям. Такими критеріями можуть бути досягнення мети,

розумний строк, рівень забезпечення прав, свобод і законних інтересів учасників кримінального провадження тощо. Дослідження шляхів підвищення ефективності кримінального переслідування є необхідним задля покращення дієвості органів кримінального переслідування та досягнення оптимального рівня забезпечення прав і свобод людини у перебігу кримінального провадження.

Надаючи визначення ефективності досудового розслідування О.О. Торбас відзначив, що це ознака досудового розслідування, яка може бути оцінена шляхом перевірки кількості проведених об'єктивно необхідних процесуальних дій, та оперативністю прийняття проміжних і кінцевих процесуальних рішень [1, с. 387-388]. Оцінюючи ефективність досудового розслідування автор взяв за основу такі критерії, як досягнення мети, кількість необхідних процесуальних дій та затрачений проміжок часу на прийняття проміжних та кінцевих рішень. Іншими словами, ефективність, в першу чергу, оцінюється досягненням головної мети, що є вірним, на наш погляд. Однак, на наше переконання, у даному визначені набір критеріїв щодо оцінки ефективності розслідування є неповним. Пропонуємо додати до переліку такий критерій як рівень забезпечення прав і свобод людини. Адже головну мету можна досягти використовуючи при цьому докази, які здобуті з порушенням прав людини, та які в подальшому будуть визнані судом недопустимими.

Розглянемо більш детально декілька напрямів підвищення ефективності кримінального переслідування, які на наш погляд є найбільш визначальними.

1. Деформалізація правовідносин між суб'єктами кримінального переслідування. Прокурор як процесуальний керівник перебуває в постійній взаємодії з органом досудового розслідування, яку потрібно розглядати як спільну діяльність указаних суб`єктів, що головним чином, спрямована на виконання завдань кримінального провадження. Така взаємодія може набувати як процесуальної, так і організаційної форми [2]. Вважається, що суб'єкти кримінального переслідування об'єднані єдиною спільною метою

обвинувальної спрямованості. Дану мету можна сформулювати наступним чином: пошук обвинувальних доказів для підтвердження фактів та обставин, які викривають конкретну особу у вчиненні кримінального правопорушення.

Т.О. Лоскутов пише, що відповідно до вимог спеціальнодозвільного типу регулювання органи кримінального судочинства уповноважені здійснювати правозастосовну діяльність лише на підставі, у межах і способами, чітко визначеними кримінальним процесуальним законодавством. Основою спеціальнодозвільної діяльності суб'єктів кримінального процесу є загальна заборона та чітко визначений дозвіл на обмеження прав людини. Науковець відзначає, що залежно від можливості обмеження прав, свобод і законних інтересів людини діяльність органів кримінального судочинства має регулюватися або за спеціальнодозвільним, або за загальнодозвільним типом правового регулювання [3, с. 172-175]. Відповідно, якщо окремі процесуальні дії органів кримінального переслідування не тягнуть за собою обмеження прав людини, то здійснювати такі дії допускається відповідно до загальнодозвільного типу правового регулювання, упускаючи зайвий формалізм. В той же час, у ситуаціях можливих обмежень прав і свобод людини – має переважати надлишковий формалізм у діяльності органів кримінального переслідування.

2. Удосконалення спеціалізації суб'єктів кримінального переслідування. Наявність спеціалізації у окремих суб'єктів кримінального переслідування є позитивним з точки зору ефективності. Такими прикладами можуть бути наявність Спеціалізованої антикорупційної прокуратури, Спеціалізованої прокуратури у сфері оборони, Спеціалізованої екологічної прокуратури, Бюро економічної безпеки України, наявність у структурі органів досудового розслідування Національної поліції слідчих у справах з розслідування дорожньо-транспортних пригод, у справах за участю дітей тощо.

В окремих структурних підрозділах прокуратури існує негласне правило про розподіл між прокурорами справ за типом правопорушень. За такий

негласний розподіл прокурорів відповідає керівник підрозділу. В окремих підрозділах прокуратури такий розподіл є гласним та оформлений наказом керівника про розподіл обов'язків [4, с. 90]. Такий, в більшості, неформальний поділ процесуальних керівників за спеціалізацією відповідним чином позитивно впливає на ефективність кримінального переслідування. Однак, на наше переконання, в структурі органів прокуратури мають бути офіційно закріплені напрями діяльності та відповідні прокурори, які повинні бути закріплені за такими напрямами.

На погляд В.І. Чечерського недоліки тематичної спеціалізації органів кримінального переслідування пов'язані з обмеженістю трудового ресурсу, що не дозволяє запровадити таку спеціалізацію на всіх без винятку напрямах. Крім того, необхідно докладати додаткові зусилля на швидке й оперативне оновлення правової компетентності прокурорів, які працювали за відповідною спеціалізацією, у випадку зміни покладених на них функцій і завдань [5, с. 124]. Запровадження тематичної спеціалізації у органах прокуратури доводить свою ефективність, оскільки на конкретному напрямку дозволяє комплексно вирішувати покладені на прокуратуру завдання у цій сфері. Завдяки їй замість реактивного ситуативного реагування на окремі факти порушень запроваджується проактивний проблемно-орієнтований та науково обґрунтований системний підхід, з визначенням пріоритетних напрямків, професійними та наближеними до людей і потреб суспільства прокурорами [5, с. 128].

Отже, впровадження окремих напрямів спеціалізації для суб'єктів кримінального переслідування підвищує ефективність розслідування в цілому, сприяє виробленню дієвих алгоритмів (планів) розслідування тих чи інших кримінальних правопорушень. Перспективним напрямом спеціалізації прокурорів-процесуальних керівників може бути напрям організованої злочинності.

Список використаних джерел:

1. Торбас О.О. Розсуд у кримінальному процесі України : дис. … д-ра. юрид. наук : 12.00.09. Одеса, 2021. 454 с.

2. Постанова Великої палати Верховного суду від 31.10.2024 р. Справа № 990/39/24. Провадження № 11-180заі24. URL: https://reyestr.court.gov.ua/Review/123313996 (дата звернення: 06.09.2025).

3. Лоскутов Т.О. Предмет регулювання кримінального процесуального права : монографія. Київ : Юридичний світ, 2016. 416 с.

4. Прокурор: керує? координує? наглядає? розслідує : Звіт за результатами дослідження «Роль прокурора на досудовій стадії кримінального процесу». Бєлоусов Ю., Венгер В., Мітько В., Орлеан А., Сущенко В., Яворська В. ; за заг. ред. Бєлоусова Ю. Київ : СТ-Друк, 2017. 268 с. URL : https://issuu.com/irf_ua/docs/prokuror_210_270 (дата звернення 17.09.2025).

5. Чечерський В.І. Ефективність впровадження спеціалізації прокурорів на прикладі спеціалізованих екологічних прокуратур. *Науковий вісник Ужгородського національного університету*. Серія : Право. 2023. Вип. 75 (3). С. 123-128.

ПЕРМЯКОВ Дмитро
здобувач вищої освіти факультету забезпечення державної безпеки Київського інституту Національної гвардії України

Науковий керівник:
БЕЙКУН Андрій
доцент кафедри правового забезпечення та правоохоронної діяльності факультету забезпечення державної безпеки Київського інституту Національної гвардії України,кандидат юридичних наук, доцент

ТРАНСФОРМАЦІЯ РОЗУМІННЯ ПРАВОВИХ КАТЕГОРІЙ У СФЕРІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ У СУЧАСНИХ РЕАЛІЯХ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ

Безумовно, що захист усіх об'єктів та елементів критичної інфраструктури від кіберзагроз в умовах повномасштабної збройної агресії російської федерації проти України вимагає комплексного підходу, що поєднує як технологічні рішення і організаційні заходи так і належне національне нормативно-правове забезпечення та міжнародну співпрацю.

Аксіомно, що захист інформаційних систем, персональних даних та національної інфраструктури від кіберзагроз вимагає не лише технічних рішень, але й ефективного правового регулювання. Розвиток інформаційно-телекомунікаційних систем, як відомо, впливає як на форми взаємодії у суспільстві, так і на потенційні можливості завдавати ураження об'єктам критичної інфраструктури. Не є таємницею, що російсько-українська війна характерна і численними кібер-атаками, якими обмінюються наші спеціальні підрозділи з ворогом. Об'єктами таких атак є: і електронні засоби управління, і засоби регулювання технологічних процесів, і засоби масової інформації та телекомунікації тощо. За таких умов особливого значення набуває гарантування інформаційної та кібернетичної безпеки держави, суспільства і окремої особистості, у тому числі і шляхом удосконалення відповідної нормативно-правової бази.

Як зазначено у Законі України «Про основні засади забезпечення кібербезпеки України», кібербезпека - захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [1].

З визначення ми бачимо, що складові інформаційної та кібернетичної

безпеки можна визначити наступним чином: безпека держави, безпека суспільства, безпека особи. При цьому безпека особи, суспільства та держави може забезпечуватися як на національному, регіональному, так і міжнародному рівні.

Разом з тим, комплексний аналіз сучасного правового поля у сфері кібербезпеки виявляє низку суттєвих проблем, які потребують вирішення.

По-перше, слід відзначити асинхронність розвитку законодавчої бази та технологічного прогресу, що призводить до утворення прогалин у правовому регулюванні новітніх форм кіберзагроз. Ця проблема посилюється транскордонним характером кіберпростору, який нівелює традиційні юрисдикційні межі та ускладнює застосування національного законодавства до злочинів, що мають глобальний масштаб.

По-друге, особливої уваги, навіть в умовах повномасштабної війни, заслуговує дилема балансування між посиленням заходів кібербезпеки та збереженням фундаментальних прав на приватність і свободу інформації. Ця проблема набуває особливої гостроти як в контексті зростаючої ролі цифрових технологій у повсякденному житті громадян, так і «природнім» обмеженням деяких прав і свобод громадян в умовах особливих правових режимів.

По-третє, варто визнати, що певна особливість національних підходів до правового регулювання кібербезпеки становить суттєву перешкоду для ефективного міжнародного співробітництва у цій сфері. Насамперед, відсутність уніфікованих стандартів та процедур ускладнює координацію зусиль різних держав, у першу чергу, союзників України у протидії кіберзагрозам глобального масштабу.

По-четверте, існує певна проблематика застосування термінологічного апарату національного законодавства. Так, зокрема, із термінами кібербезпека та кіберпростір тісно пов’язане поняття кіберправо. Наразі кіберправо позиціонується як уособлена галузь права, що постійно розвивається та формується у самостійну групу суспільних відносин. Кіберправо може бути як підгалуззю міжнародного права, так і самостійною внутрішньодержавною

галуззю. Якщо ж говорити про кіберправо та кібербезпеку, то слід вести мову про наднаціональний автономний правовий режим правового регулювання. Проблематика правового регулювання кібербезпеки в сучасних реаліях пов’язана із динамічністю цієї сфери міжнародного права, яка характеризується постійним розвитком, а також відсутністю досвіду комплексного правового регулювання багаторівневих транснаціональних відносин в Інтернеті.

Як вбачається, для подолання зазначених проблем необхідна оновлена комплексна стратегія вдосконалення правового регулювання кібербезпеки. Ключовим елементом такої стратегії має стати впровадження адаптивних правових механізмів, здатних миттєво реагувати на появу нових технологічних викликів. Це може бути реалізовано, як вбачає ряд дослідників, через використання інструментів т.з. «м'якого права», яке дозволяють експериментувати з новими підходами до регулювання без внесення радикальних змін до законодавства [2, с. 86-87].

Разом з тим, існують погляди щодо проблематики транскордонних інформаційних відносин, що унеможливлює суто національне правове регулювання і належне забезпечення означеної галузевої безпеки. Така «траскордонність» суспільних відносин у сфері гарантування інформаційної та кібернетичної безпеки є однією із проблемних аспектів, оскільки видається вкрай складним створення єдиних нормативних актів, до яких зможуть приєднатися більшість країн. Проблематикою правового регулювання кібербезпеки є також факт відсутності міжнародно-правових договорів між багатьма країнами-учасницями щодо врегулювання зазначеної сфери суспільних відносин [3].

Як акцентує ряд дослідників, впровадження принципу «безпека через дизайн» у розробку нових технологій та відповідне правове регулювання може стати превентивним заходом, що дозволить зменшити вразливість систем до кібератак ще на етапі їх проектування. Це вимагає тісної співпраці між законодавцями, технологічними компаніями та експертами з кібербезпеки [4].

Нарешті, розвиток державно-приватного партнерства на загальнодержавному рівні у сфері кібербезпеки та створення відповідних правових механізмів для його реалізації дозволить об'єднати ресурси та експертизу державного та приватного секторів для більш ефективного протистояння кіберзагрозам.

Таким чином, вдосконалення правового регулювання кібербезпеки вимагає системного підходу, що враховує технологічні, соціальні та міжнародні аспекти проблеми. Лише через комплексну реалізацію зазначених заходів можна створити ефективну правову базу для забезпечення кібербезпеки в умовах стрімкого розвитку цифрових технологій. Правове регулювання кібербезпеки є складним та динамічним процесом, який вимагає постійної адаптації до нових викликів цифрової епохи. Ефективне правове забезпечення кібербезпеки потребує комплексного підходу, що враховує технологічні, соціальні та міжнародні аспекти проблеми. Важливо також забезпечити баланс між заходами безпеки та захистом фундаментальних прав і свобод громадян. Лише через системний підхід до правового регулювання кібербезпеки можна створити надійний фундамент для захисту цифрового простору та забезпечення сталого розвитку інформаційного суспільства [5].

Безумовно, що кібероперації у російсько-українському збройному протистоянні фактично відкривають нову епоху у веденні війни, яка потребує переосмислення існуючих правових норм. І хоча міжнародне гуманітарне право і залишається актуальним засобом для регулювання кібероперацій, його адаптація до реалій цифрового світу є необхідною. Розробка технічної експертизи, міжнародна співпраця та інтеграція кіберзасобів у правові системи стають ключовими кроками на шляху до ефективного регулювання кібервійни. І досвід російсько-української війни у протидії та нейтралізації кіберзагроз слугує важливим прикладом для наших союзників, демонструючи необхідність системного підходу до вирішення цієї проблеми.

Список використаних джерел:

1. Закон України «Про основні засади забезпечення кібербезпеки

України», 2017. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 05.10.2025).

2. Новицький В. Я. Проблематика правового регулювання інформаційної та кібербезпеки в сучасній світовій політиці: міжнародно-правовий аспект. *Європейські перспективи*. № 2. 2021. С. 84-91. URL: https://ep.unesco-socio.in.ua/wp-content/uploads/2021/05/84-_Novyts-kyj.pdf (дата звернення: 05.10.2025).

3. Довгань О. Д. Правові аспекти забезпечення кібербезпеки об'єктів критичної інфраструктури: національний та міжнародний вимір. *Інформація і право*. № 4(51). 2024. URL: http://il.ippi.org.ua/article/view/317970 (дата звернення: 05.10.2025).

4. Бондар Г. Російські APT-групи продовжують атакувати Україну. (УНІАН, 31.01.2023). URL: https://www.unian.ua/techno/communications/rosiyski-apt-grupi-prodovzhuyut-atakuvati-ukrajinu-12128238.html (дата звернення: 05.10.2025).

5. Матеріали справи за фактом кібератаки на "Київстар" спрямують на розгляд МКС. (Укрінформ, 04.04.2024). URL: https://www.ukrinform.ua/rubric-ato/3848169-illa-vituk-nacalnik-departamentu-kiberbezpeki-sbu.html (дата звернення: 05.10.2025).

ПОНОМАРЕНКО Віктор
викладач кафедри адміністративного права та процесу навчально-наукового інституту права та соціального менеджменту Донецького державного університету внутрішніх справ

ВИКОРИСТАННЯ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ ФІКСАЦІЇ ТА ДОКАЗУВАННЯ ВОЄННИХ ЗЛОЧИНІВ

У контексті триваючої агресії російської федерації проти України, накопичення, збереження та використання доказів воєнних злочинів набуває

надзвичайної важливості. Сучасні інформаційні технології забезпечують можливість фіксації фактів порушень, які інакше могли б бути втрачені через хаос бойових дій, знищення документів чи поширення ворожої дезінформації. Застосування мобільних додатків, що забезпечують незмінність метаданих, таких як eyeWitness to Atrocities, дозволяє фіксувати фото, відео та аудіозаписи із вбудованою інформацією про час і місце зйомки, що вже використовуються у національних судах України для підтвердження фактів руйнувань і злочинів проти цивільного населення. Паралельно, супутникові знімки, зокрема з даних Sentinel-1 та інших SAR-датчиків, застосовуються для моніторингу масштабів руйнувань та перевірки їх кореляції з даними з місця подій [1]. Важливу роль відіграють і методи OSINT, які дозволяють на основі відео з соціальних мереж, геолокації, аналізу метаданих та архівів підтверджувати або спростовувати факти обстрілів та інші воєнні злочини.

Законодавче забезпечення цифрових доказів в Україні базується на положеннях Кримінального процесуального кодексу, де у статті 99 визначено статус електронних доказів як документів [2]. Судова практика підкреслює, що недопустимим є відхилення доказу лише на підставі його електронної форми, а копії або дублікати електронних документів, створені за участі спеціалістів, можуть визнаватися оригіналами. Верховний Суд також роз’яснив, що електронні докази, отримані через міжнародну правову допомогу, повинні відповідати не лише українським процесуальним нормам, але й міжнародним угодам, адже порушення процедури може призвести до їх недопустимості. У міжнародному контексті, прокурори України вже проходять навчання з питань відповідності електронних доказів міжнародним стандартам, зокрема положенням Будапештської конвенції та практики ЄСПЛ, що є вкрай важливим для майбутніх процесів у Міжнародному кримінальному суді.

Значну роль відіграють міжнародні проекти та форуми, де обговорюються питання використання електронних доказів та OSINT у документуванні злочинів, прикладом чого став Форум із цифрових доказів та

кібербезпеки, проведений у жовтні 2024 року за підтримки Національного координаційного центру кібербезпеки.

Переваги таких технологій очевидні: вони дають змогу швидко та об’єктивно фіксувати факти злочинів навіть за відсутності фізичного доступу до місця події, забезпечують можливість перевірки подій у ретроспективі завдяки супутниковим знімкам і архівам, підвищують прозорість і зменшують ризик маніпуляцій зі свідченнями. Разом з тим існують і суттєві виклики. Це необхідність гарантувати автентичність та цілісність цифрових доказів, уникати маніпуляцій і підробок, а також забезпечувати баланс між доказуванням злочинів і захистом права людини на приватність, особливо коли збір даних здійснюється через соціальні мережі чи месенджери. Проблемою залишаються і прогалини у законодавстві, адже статус скріншотів, копій чи даних з відкритих джерел досі чітко не врегульовано.

Для розвитку цієї сфери необхідним є подальше удосконалення законодавства шляхом уточнення визначень і процедур роботи з електронними доказами, стандартизація процесів збору та збереження даних, включаючи технічні методи хешування й контроль ланцюга зберігання. Важливим є системне навчання прокурорів, слідчих та суддів міжнародним стандартам та співпраця з експертами з кібербезпеки та OSINT-спільнотами. Також перспективним є використання алгоритмів штучного інтелекту для попередньої перевірки та класифікації великого обсягу цифрових матеріалів, проте за умови їх правової оцінки та захисту від потенційних порушень прав людини.

У підсумку можна стверджувати, що сучасні інформаційні технології є ключовим інструментом у процесі фіксації та доказування воєнних злочинів в Україні. Вони вже довели свою ефективність і дозволили зібрати значний масив доказів для національних та міжнародних судових процесів, але їхній повний потенціал буде реалізовано лише за умови вдосконалення правового регулювання, розвитку судової практики та забезпечення міжнародної співпраці у сфері доказування злочинів проти людяності та воєнних злочинів.

Список використаних джерел:

1. Dietrich, O., Peters, T., Sainte Fare Garnot, V., Sticher, V., Ton-That Whelan, T., Schindler, K., & Wegner, J. D. (2025). An open-source tool for mapping war destruction at scale in Ukraine using Sentinel-1 time series. Communications Earth & Environment, 6(1), 215. doi:10.1038/s43247-025-02183-7.

2. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 року № 4651-VI. *Відомості Верховної Ради України.* 2013. № 9-10. № 11-12. № 13. Ст. 88.

ПОТОЦЬКИЙ Мирослав
доцент кафедри кримінального процесу та криміналістики факультету підготовки фахівців для органів досудового розслідування НПУ
Донецький державний університет внутрішніх справ
доктор філософії за спеціальністю 081 «Право»

ОКРЕМІ ОСОБЛИВОСТІ КРИМІНАЛЬНОГО ПРОВАДЖЕННЯ В УМОВАХ ВОЄННОГО СТАНУ

Здійснення кримінального провадження в умовах воєнного стану характеризується застосуванням «особливих процедур», оскільки застосування «загальних процедур» може бути не ефективним, а в окремих випадках навіть неможливим.

Одним із викликів системи кримінальної юстиції в умовах війни є подекуди об'єктивна неможливість дотримання органами досудового розслідування, прокуратурою та судами строків, які встановлює Кримінальний процесуальний кодекс України (далі – КПК України). Це створює ситуацію загрози порушення прав учасників кримінального

провадження [1].

В.В. Топчій відзначає, що проведення бойових дій на окремих територіях ускладнює стандартні процедури фіксування процесуальних дій у кримінальному провадженні. Окупація частини територій робить неможливим проведення стандартного розслідування кримінальних правопорушень. У відповідь на таку ситуацію вносять зміни до чинного законодавства, які регулюють та спрощують процедури розслідування у кримінальних провадженнях. Ці зміни мають за мету забезпечити ефективне розслідування кримінальних правопорушень в умовах воєнного стану, з урахуванням особливостей і обмежень, що виникають у зв'язку з реаліями та умовами війни на території держави [2, с. 237].

Вбачається, що процедура кримінального провадження в умовах воєнного стану має характеризуватись спрощенням порядку такого провадження, при цьому об'єктивно враховуючи баланс сторін у можливостях реалізації їх прав та обов'язків. Однак, не кожен порядок проведення процесуальних дій в умовах воєнного стану відповідно до національного законодавства характеризується як спрощений та ефективний.

Так, порядок кримінального провадження в умовах воєнного стану, серед інших, містить такі «особливі процедури»: спрощена фіксація початку досудового розслідування, додаткові можливості щодо фіксації слідчих (розшукових) дій, розширення випадків проведення слідчих (розшукових) дій без участі понятих, покладення виконання окремих повноважень слідчого судді на відповідного прокурора, наявність розширених підстав для зупинення досудового розслідування, додаткові підстави для здійснення кримінального процесуального затримання, особливий порядок визначення підслідності кримінальних правопорушень, передбачених ст.ст. 407, 408 КК України, можливість продовження строку тримання під вартою до одного місяця керівником відповідного органу прокуратури, можливість продовження строку для вручення письмового повідомлення про підозру затриманій особі, додаткові можливість щодо дистанційної участі захисника у кримінальному

провадженні тощо.

Більш детально зупинимось на «регулюванні» строку досудового кримінального провадження через застосування інституту зупинення та відновлення досудового розслідування. Так, відповідно до положень ст. 6 Європейської конвенції з прав людини (далі – ЄКПЛ) кожен має право на справедливий і публічний розгляд його справи упродовж розумного строку незалежним і безстороннім судом, встановленим законом, який вирішить спір щодо його прав та обов'язків цивільного характеру або встановить обґрунтованість будь-якого висунутого проти нього кримінального обвинувачення. Згідно ст. 15 ЄКПЛ під час війни або іншої суспільної небезпеки, яка загрожує життю нації, будь-яка Висока Договірна Сторона може вживати заходів, що відступають від її зобов'язань за Конвенцією, виключно в тих межах, яких вимагає гострота становища, і за умови, що такі заходи не суперечать іншим її зобов'язанням згідно з міжнародним правом [3]. Отже можливість відступу від положень ст. 6 ЄКПЛ, в більшості, має залежить від гостроти становища, тобто від обстановки в конкретному місці і у визначений проміжок часу здійснення досудового кримінального провадження.

Ст. 280 КПК України містить перелік підстав, які надають право стороні обвинувачення зупинити досудове розслідування, тим самим зупинити відлік процесуальних строків. Так, досудове кримінальне провадження може бути зупинено за наявності об’єктивних обставин, що унеможливлюють подальше проведення досудового розслідування в умовах воєнного стану [4].

Т.О. Лоскутов наголошує, що правове регулювання зупинення досудового розслідування обумовлює ризик порушення права на розумні строки кримінального провадження (права на справедливий судовий розгляд) та ризик зниження ефективності кримінального процесу. Автор вважає врегулювання у кримінальному процесуальному законі зупинення та відновлення досудового розслідування в умовах воєнного стану недоцільним, оскільки, по-перше існує неабиякий ризик зниження ефективності досудового

розслідування та, по-друге, через необхідність виконання формальної роботи щодо складання процесуальних документів. Дослідник пропонує під час правового режиму воєнного часу регламентувати у законі винятково розумний строк для проведення досудового розслідування. Такий строк, на думку науковця, дозволить визначати ефективність досудового розслідування в умовах бойових дій шляхом урахування конкретних обставин здійснення кримінального провадження [5, с. 13-16].

Підтримуючи позицію з даного питання Т.О. Лоскутова вважається, що передбачення додаткових підстав для зупинення досудового кримінального провадження в умовах воєнного стану є обтяжуючим (з огляду на процесуальне оформлення такого рішення) для сторони обвинувачення та може негативно впливати на ефективність розслідування в цілому. Процесуальна форма розслідування в умовах воєнного стану має змінюватись у бік її спрощення. Отже, вважається, що строк досудового кримінального провадження має бути гнучким, тобто залежати від обставин провадження та бути поза обтяжливими процедурами фіксації прийняття рішення про його зупинення чи відновлення.

Список використаних джерел:

1. Строки у кримінальному процесі під час війни: у чому проблема?. *Justtalk.* URL : https://justtalk.com.ua/post/stroki-u-kriminalnomu-protsesi-pid-chas-vijni-u-chomu-problema (дата звернення: 10.10.2025).

2. Топчій В.В. Особливості здійснення та реалізації кримінального провадження в умовах воєнного стану. *Ірпінський юридичний часопис: науковий журнал*. 2024. Вип. 2 (15). С. 233-242.

3. Конвенція про захист прав людини і основоположних свобод від 4 листопада 1950 р. Рада Європи. URL: https://zakon.rada.gov.ua/laws/show/995_004 (дата звернення: 08.10.2025).

4. Кримінальний процесуальний кодекс України. Закон від

13.04.2012. № 4651-VI. URL : https://zakon.rada.gov.ua/laws/show/4651-17 (дата звернення: 07.10.2025).

5. Лоскутов Т.О. Правове регулювання строків досудового розслідування в умовах воєнного стану. *Правовий часопис Донбасу*. 2022. № 2. С. 11-18

ПРОЦЕНКО Олександра
курсантка 401 навчального взводу Факультету підотовки фахівців для органів досудового розслідування НПУ Донецького державного університету внутрішніх справ

Науковий керівник:
ГРУЗДЬ Олександр
завідувач кафедри кримінального процесу та криміналістики факультету підготовки фахівців для органів досудового розслідування Національної поліції України Донецького державного університету внутрішніх справ

СИНЕРГІЯ КРИМІНАЛЬНОГО АНАЛІЗУ ТА МІЖНАРОДНОГО СПІВРОБІТНИЦТВА У ПРОТИДІЇ ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ ПІД ЧАС ВІЙНИ

Сучасний етап еволюції української державності відзначається безпрецедентним рівнем системних викликів, детермінованих триваючою збройною агресією росії проти України. Вказані події зумовили суттєву трансформацію усіх сфер суспільного життя, породивши не лише загрози воєнного характеру, але й комплекс негативних криміногенних факторів, що безпосередньо впливають на стан національної безпеки. У контексті воєнних дій, які підривають обороноздатність держави, дестабілізують соціально-економічні процеси та ускладнюють функціонування системи публічного управління, спостерігається якісне і кількісне зростання криміногенних

ризиків. Війна виступає каталізатором деструктивних процесів у сфері безпеки, сприяючи руйнуванню інституційної спроможності держави, ерозії правових механізмів контролю та створенню сприятливого середовища для поширення організованої злочинності.

Беручи до уваги, що в умовах збройної агресії організована злочинність отримала нові імпульси для розвитку, зумовлені руйнуванням інституційної стабільності державного управління, формуванням тіньових економічних механізмів, ослабленням прикордонного контролю та зростанням корупційних ризиків, можна констатувати, що зазначені чинники об’єктивно сприяють активізації діяльності злочинних угруповань, які використовують хаотичність, соціально-економічну нестабільність і кризові процеси воєнного часу з метою незаконного збагачення та розширення сфер кримінального впливу. У науковому дискурсі цілком обґрунтованим постає питання про те, наскільки доцільним і ефективним є твердження, що в умовах зростання кількості випадків незаконного обігу зброї, активізації наркотрафіку, підвищення ризиків торгівлі людьми та інтенсифікації кіберзлочинності протидія цим явищам потребує системного, комплексного підходу, заснованого на тісній взаємодії суб’єктів безпеки як на національному, так і на міжнародному рівнях. [1].

Одним із найбільш ефективних інструментів протидії організованій злочинності, який довів свою результативність у практиці правоохоронної діяльності демократичних держав, виступає кримінальний аналіз як спеціалізована аналітико-інформаційна технологія в системі кримінальної юстиції. Його сутність полягає у цілеспрямованому, системному та багатоетапному процесі збору, верифікації, узагальнення, структуризації й інтерпретації інформаційно-аналітичних даних, що відображають динаміку, тенденції та закономірності функціонування злочинних угруповань. Кримінальний аналіз виступає інтеграційною складовою оперативно-розшукової, слідчої та стратегічної діяльності органів кримінального спрямування, забезпечуючи їхню спроможність до комплексного оцінювання

ситуацій, встановлення латентних взаємозв'язків між окремими суб'єктами та подіями злочинної діяльності, ідентифікації ключових осіб злочинних організацій, їх фінансово-економічних ресурсів та каналів взаємодії [2].

З теоретичного погляду, кримінальний аналіз є інструментом трансформації первинної оперативної інформації у стратегічні знання, що дозволяють приймати управлінські рішення, орієнтовані на упередження, локалізацію та нейтралізацію кримінальних загроз. Його функціональне призначення виходить за межі традиційного розуміння інформаційної підтримки досудового розслідування, оскільки він забезпечує прогнозування майбутніх тенденцій у злочинній діяльності, моделювання ризикових сценаріїв, а також оптимізацію використання ресурсів правоохоронних структур. Саме в умовах воєнного стану значення кримінального аналізу набуває особливої ваги, оскільки він стає одним із ключових інструментів забезпечення превентивного реагування на криміногенні процеси. Масове поширення незаконного обігу зброї, зростання рівня корупції, активізація тіньової економіки, а також посилення транснаціональних форм злочинності зумовлюють потребу в оперативному виявленні нових схем і тактик злочинних угруповань.

У цьому контексті аналітична діяльність набуває стратегічного значення для національної безпеки, адже дозволяє забезпечити системне прогнозування кримінальних загроз, формування адаптивних моделей криміногенної поведінки, а також підвищити ефективність міжвідомчої взаємодії у межах національної та міжнародної правоохоронної кооперації. Таким чином, кримінальний аналіз у сучасних умовах воєнного протистояння трансформується із допоміжного інструменту слідчо-оперативної діяльності у фундаментальний механізм стратегічного управління безпековою політикою держави [3].

Слід вважати, що, сучасний кримінальний аналіз характеризується високим рівнем технологічної інтегрованості та переходом до цифрової парадигми. Його методологія дедалі більше спирається на використання

інструментів відкритої розвідки (OSINT), аналізу великих даних (Big Data), штучного інтелекту та машинного навчання. Беручи до уваги сучасні виклики, особливе значення має аналіз цифрових слідів — даних із соціальних мереж, месенджерів, електронних платіжних систем. Це дозволяє точніше ідентифікувати учасників злочинних мереж, відстежувати незаконні фінансові потоки та виявляти приховані комунікації. Слід зазначити, що українське законодавство поки лише частково враховує потенціал таких технологій у кримінальному провадженні, що зумовлює правову невизначеність і знижує доказову цінність отриманих аналітичних даних [4].

Беручи до уваги сучасні тенденції розвитку злочинності, слід констатувати, що організована злочинність дедалі частіше набуває транснаціонального характеру, виходячи за межі окремих державних юрисдикцій. У глобалізованому середовищі злочинні мережі демонструють високий рівень адаптивності, використовуючи міжнародні фінансові системи, криптовалютні платформи, офшорні схеми, канали контрабанди та нелегальної міграції.

Звернемо увагу, що у таких умовах національні зусилля, навіть за умови їх високої ефективності, не можуть забезпечити належного рівня протидії організованим формам злочинності. Саме тому вважаємо за доцільне підкреслити ключову роль міжнародного співробітництва, яке охоплює обмін оперативною інформацією, координацію дій правоохоронних органів різних держав та проведення спільних розслідувань. Україна, будучи активним суб’єктом міжнародної правоохоронної взаємодії, бере участь у діяльності таких структур, як Інтерпол, Європол, SELEC, а також підтримує тісні контакти з правоохоронними органами держав-партнерів. Участь у спільних операціях, інтеграція до баз даних Інтерполу, обмін відомостями щодо переміщення підозрюваних і незаконних активів сприяють підвищенню якості кримінального аналізу та рівня аналітичної взаємодії.

Зазначимо, що міжнародні партнери часто надають доступ до передових технологічних платформ, здатних забезпечити оперативну обробку великих

масивів інформації, що значно перевищує можливості національних ресурсів. Водночас, інтегрованість українських систем кримінального аналізу до європейських та світових інформаційних мереж залишається частковою, що, на нашу думку, об'єктивно обмежує потенціал спільних дій у сфері протидії організованій злочинності [5].

Спільна стратегія кримінального аналізу та міжнародного співробітництва є багатовимірним і динамічним явищем. На нашу думку, її ефективність проявляється не лише у взаємному підсиленні ресурсів та компетенцій учасників, а й у здатності створювати якісно нові результати, які неможливо досягти окремо.

Враховуючи практичний досвід, дані, отримані від міжнародних партнерів, дозволяють українським аналітикам формувати більш точні прогнози щодо розвитку злочинної діяльності, моделювати потенційні сценарії та оцінювати ризики різних угруповань. У свою чергу, результати кримінального аналізу, проведеного вітчизняними фахівцями, стають підґрунтям для планування та реалізації спільних міжнародних операцій і спеціальних заходів.

Як приклад, у практиці вже зафіксовано успішні випадки взаємодії з Європолом у сфері протидії кримінальних проваджень за ст. 111-1 КК України, якою законодавець доповнив кодекс у 2022 році. Завдяки спільним операціям вдалося викрити масштабні злочинні мережі, що одночасно діяли в кількох країнах ЄС та в Україні, координували фінансові потоки та обмінювалися цифровими ресурсами для відмивання доходів. Цей кейс демонструє, що лише інтеграція ресурсів, інформаційних платформ і аналітичних компетенцій різних держав здатна забезпечити ефективний прорив у боротьбі з організованою злочинністю та транснаціональними загрозами [6].

Можна констатувати, що, як зазначають Іван та Андрій Богатирови, збройний конфлікт створює не лише загрози, а й нові можливості для протиправної діяльності, зокрема контрабанди через лінію фронту та

використання хаотичних умов для реалізації корупційних схем. Беручи до уваги їхні дослідження, можна констатувати, що ключовими проблемами залишаються недосконаліть законодавчої бази, високий рівень корупції у владних структурах та відсутність спеціалізованих методик дослідження організованої злочинності в умовах воєнного стану.

Очевидним є те, що, ці спостереження перегукуються з висновками інших дослідників, які наголошують на необхідності ґрунтовного кримінологічного аналізу, інтеграції сучасних технічних засобів контролю та запровадженні законодавчих обмежень для посадових осіб. Водночас автори підкреслюють важливість активізації участі громадян у співпраці з правоохоронними органами як додаткового механізму підвищення ефективності протидії організованій злочинності. [7].

Таким чином, організована злочинність у період війни виступає комплексною загрозою для національної та міжнародної безпеки. На нашу думку, її ефективне подолання можливе лише за умов системного розвитку кримінального аналізу та активної міжнародної взаємодії. Синергія цих напрямів дозволяє підвищити результативність протидії злочинності, формувати нову безпекову архітектуру та забезпечувати адаптацію системи кримінальної юстиції до викликів XXI століття. Перспективи полягають у створенні спільних аналітичних центрів, уніфікації стандартів збору та обробки даних, а також підготовці фахівців нового покоління, здатних поєднувати знання з кримінального аналізу, міжнародного права та сучасних інформаційних технологій.

Список використаних джерел:

1. Орлов Ю. В. злочинність і протидія їй в умовах війни: кримінально-правовий та кримінологічний виміри : монографія. Харків : Вид-во «Право», 2023. 252 с.

2. Федчак І. А. Основи кримінального аналізу : навч. посіб. Львів : Львів. держ. ун-т внутр. справ, 2021. 288 с.

3. Литвиненко В.І., Пригунов П.Я. Протидія організованій злочинності діяльності в Україні: крізь призму останніх правових новел (міжнародний та вітчизняний досвід). *Право.ua*. 2020. № 2. С. 54–63. URL: https://doi.org/10.32782/law.2020.2.8 (дата звернення: 16.09.2025).

4. Бєлова М. В., Бєлов Д. М., Рущак І. В. Штучний інтелект у досудовому розслідуванні кримінальних справ: окремі питання міжнародної практики. *Аналітично-порівняльне правознавство*. URL: https://app-journal.in.ua/wp-content/uploads/2025/02/138.pdf (дата звернення: 17.09.2025).

5. European Union Serious and Organised Crime Threat Assessment. *Europol*. URL: https://www.europol.europa.eu (дата звернення: 17.09.2025).

6. Богатирьов І., Богатирьов А. Організована злочинність в умовах воєнного стану: проблеми та шляхи їх подолання. *Law & Border*. 2024. Т. 3, № 1. С. 5–26. URL: https://doi.org/10.32453/law_border.v3i1.1637 (дата звернення: 20.09.2025).

7. Перегляд Штучний інтелект в кримінальному аналізі | UNIVERSUM. *Молодіжна наукова ліга | Архів*. URL: https://archive.liga.science/index.php/universum/article/view/2021/2049 (дата звернення: 20.09.2025).

РАЗУВАЄВА Альбіна
курсантка 2 групи 2 курсу,
здобувачка першого (бакалаврського) рівня вищої освіти
Військово-юридичного інституту
Національного юридичного університету імені Ярослава Мудрого

Науковий керівник:
ГАШЕНКО Сергій
старший викладач кафедри загальновійськових дисциплін
Військово-юридичного інституту
Національного юридичного

університету імені Ярослава Мудрого,
підполковник

РОЗРОБКА ІНТЕРАКТИВНИХ НАВЧАЛЬНИХ ПЛАТФОРМ ДЛЯ ВОГНЕВОЇ ПІДГОТОВКИ З УРАХУВАННЯМ ОПЕРАТИВНОЇ ІНФОРМАЦІЇ

Розвиток інтерактивних навчальних платформ для вогневої підготовки є одним із важливих факторів покращення бойової готовності та ефективності оперативно-розшукової діяльності [1, с. 77]. У контексті воєнного стану швидкий доступ до актуальних даних про озброєння, тактичні сценарії та результати навчальних вправ набуває критичного значення [2] для збереження життя і здоров’я персоналу, а також для вдосконалення процесу прийняття рішень в бойових і оперативних умовах. Окрім технічних і організаційних аспектів, невід'ємною складовою є запровадження системи оцінювання результативності навчання на основі ключових показників ефективності (KPI) та аналізу великих даних [5, с. 48]. Аналіз телеметрії стрільби, часу реагування, помилок у виконанні тактичних завдань і психологічних характеристик дозволяє формувати об'єктивні профілі компетентності особового складу.

Інтерактивні платформи забезпечують централізоване збирання, обробку та аналіз детальної інформації щодо стрілецької зброї, її технічного стану, боєприпасів і особистих показників стрільби, таких як час реакції, точність та аналіз розподілу помилок. Через інтеграцію симуляційних модулів, телеметричного запису та аналітичних алгоритмів ці системи створюють персоналізовані навчальні траєкторії. Це дозволяє скоротити витрати на боєприпаси і час для відпрацювання базових навичок, покращити якість інструктажу завдяки зворотному зв’язку в режимі реального часу та запровадити прозору і об’єктивну систему оцінювання рівня підготовки особового складу.

Інтерактивні платформи надають можливість централізовано збирати, обробляти та аналізувати дані про стрілецьку зброю, рівень її освоєння, а також результати індивідуальної та командної вогневої підготовки. Завдяки таким можливостям інструктори отримують чітке уявлення про сильні та слабкі сторони особового складу, можуть швидко коригувати навчальні задачі, мінімізувати витрати на боєприпаси та час на базові вправи.

Мета таких платформ полягає у поєднанні оперативної інформації з навчальними модулями для налаштування тренувань відповідно до реальних умов застосування зброї. Розробка та реалізація таких платформ природно випливає з концепції інтеграції оперативної інформації. Практично це включає формування централізованих реєстрів із детально прописаними протоколами телеметрії, форматами звітності та процедурами авторизації, розробку критеріїв сертифікації програмного забезпечення й контенту, а також впровадження механізмів тестування в пілотному режимі з подальшим поступовим масштабуванням ефективних рішень.

Систематичне підвищення кваліфікації кадрів є ключовим елементом ефективного впровадження. Інструктори та командири повинні проходити комплексні курси з використання цифрових інструментів, аналізу даних і адаптації сценаріїв до оперативних потреб. Також необхідно передбачити фінансові й інфраструктурні механізми — державні програми, міжнародну допомогу, державно-приватне партнерство та створення автономних локальних платформ для підрозділів з обмеженим доступом до зв'язку. Такий підхід гарантує стабільність, постійне оновлення та розширення функціональних можливостей платформи у довгостроковій перспективі.

У рамках міжнародного співробітництва Україна активізує процес впровадження передових практик НАТО та партнерських країн у сфері електронного навчання [3, p. 34], моніторингу й оцінки ефективності вогневої підготовки. Цей комплексний підхід охоплює такі ключові напрями: – використання інтерактивних симуляторів для створення реалістичних тактичних сценаріїв з метою вдосконалення як індивідуальних, так і

колективних навичок володіння стрілецькою зброєю; – застосування технологій віртуальної та доповненої реальності [6, p. 991], які моделюють складні бойові умови, що сприяє розвитку психологічної стійкості та оперативності дій військових; – адаптацію міжнародних стандартів підготовки персоналу до національних особливостей, з урахуванням специфіки використання зброї та вимог безпеки, притаманних Збройним Силам і правоохоронним органам України; – розвиток нормативно-правової бази для регулювання підготовки військових кадрів, безпечного поводження зі зброєю та інтеграції цифрових платформ у навчальні процеси; – покращення кваліфікації інструкторів і командирів шляхом підготовки до роботи з сучасними цифровими технологіями; – розширення міждержавної наукової і освітньої взаємодії задля формування спільних навчальних курсів.

Основним завданням державної політики в цій сфері є підвищення ефективності навчання військовослужбовців, зниження ризиків неправомірного використання зброї та забезпечення готовності підрозділів до виконання завдань [7, с. 15]. За даними досліджень Міністерства оборони України, інтеграція оперативної інформації в процес вогневої підготовки сприяє скороченню часу адаптації військових до нових умов бойових операцій [1, с. 80] та збільшенню точності застосування озброєння на 25–30%. Така тенденція суттєво впливає на загальну бойову ефективність підрозділів.

До 2030 року планується впровадження єдиної інтерактивної платформи, яка об'єднає навчальні модулі, інформацію про стрілецьку зброю, результати тренувань та аналітику з оперативних джерел. Інтеграція з оперативними системами дозволить своєчасно адаптувати тренувальні сценарії до актуальної обстановки, забезпечуючи відповідність навчання реальним викликам і потребам.

Досягнення цілей вимагає поетапного плану з визначенням джерел фінансування (держпрограми, міжнародна допомога, державно-приватне партнерство), пілотними проєктами в навчальних центрах та масштабуванням ефективних рішень з урахуванням автономної інфраструктури для підрозділів

з обмеженим зв’язком. Очікувані результати — підвищення бойової готовності та точності застосування озброєння, зниження витрат на тренування й боєприпаси, покращення оперативно-розшукової інформації та зміцнення безпеки особового складу.

Список використаних джерел:

1. Міністерство оборони України. Біла книга – 2022: Збройні Сили України. Київ : МОУ, 2023. 180 с.
2. Закон України «Про національну безпеку України» від 21.06.2018 № 2469-VIII. Голос України. 2018. № 122.
3. NATO Standardization Office. NATO Education and Training Network: Guidelines and Standards. Brussels : NATO, 2021. 95 p.
4. Руденко М. В. Інноваційні підходи до вогневої підготовки військовослужбовців. Військовий часопис. 2021. № 3. С. 45–52.
5. Koryagin A., Petrenko I. Virtual and Augmented Reality for Military Training: Experience of Ukraine and NATO Partners. Defence Technology. 2020. Vol. 16, № 4. P. 987–995.
6. Міністерство оборони України. Доктрина підготовки Збройних Сил України. Київ : МОУ, 2019. 72 с.

РОМАНОВ Віталій
доцент кафедри спеціальних поліцейських дисциплін та базової загальновійськової підготовки Сумської філії Харківського національного університету внутрішніх справ, кандидат юридичних наук

ДОСТУП ДО ІНФОРМАЦІЇ МОБІЛЬНИХ АБОНЕНТІВ: ПРАВОВІ ПРОБЛЕМИ ТА ШЛЯХИ ВДОСКОНАЛЕННЯ

У контексті воєнного стану та стрімкого розвитку цифрових технологій питання доступу до інформації мобільних абонентів набуває особливої актуальності. Дані, що зберігаються мобільними операторами, є критично важливими для ефективної роботи оперативно-розшукових органів, зокрема у протидії диверсіям, кіберзагрозам, терористичним актам та злочинам проти національної безпеки. Проте чинне законодавство України регулює цей процес лише частково, що створює правову невизначеність і ускладнює оперативне реагування в умовах надзвичайних ситуацій. Саме тому виникає потреба у комплексному перегляді нормативної бази, аби забезпечити баланс між захистом прав громадян і національною безпекою.

Чинне законодавство України регламентує це питання фрагментарно. Закон України «Про оперативно-розшукову діяльність» лише передбачає право звернення до суду, проте не встановлює чітких строків та форми клопотання [3]. Натомість Кримінальний процесуальний кодекс України визначає загальні правила тимчасового доступу до речей і документів, але не враховує специфіку оперативно-розшукової діяльності [2]. Це спричиняє виникнення правових прогалин, які ускладнюють своєчасне отримання інформації.

Додаткову колізію створює судова практика: слідчі судді першої інстанції не мають допуску до державної таємниці, тоді як судді апеляційних судів не уповноважені розглядати клопотання про доступ до даних операторів [4]. Такий стан справ блокує процес отримання критично важливих даних і знижує ефективність роботи правоохоронних органів.

Європейська конвенція про захист прав людини і основоположних свобод (ст. 8) встановлює, що втручання у сферу приватності можливе лише за умов законності, легітимної мети (національна безпека, запобігання злочинам) та пропорційності [3, с. 7]. Зарубіжний досвід підтверджує важливість чітких строків і прозорих процедур:

у Польщі суд розглядає клопотання протягом 24 годин, а оператор

зобов’язаний надати дані упродовж 48 годин [5];

у Німеччині доступ можливий лише за мотивованою ухвалою судді, із залученням захисника та парламентським контролем [6];

у Великій Британії використовується «fast track»-процедура із 24-годинним строком ухвалення рішення [7].

Аналіз наведених практик свідчить, що ефективна модель доступу до мобільних даних повинна включати:

уніфіковану форму клопотання;

жорсткі строки розгляду й виконання ухвал (24–48 годин);

визначений перелік інформації, до якої можливий доступ;

механізми контролю та гарантії захисту прав громадян.

З метою усунення колізій і забезпечення балансу між інтересами безпеки та приватності пропонується доповнити Закон України «Про оперативно-розшукову діяльність» новою статтею 8-1 «Тимчасовий доступ оперативних підрозділів до відомостей мобільних операторів та інших електронних ресурсів».

Основні положення статті передбачають:

подання уніфікованого клопотання керівником оперативного підрозділу, погодженого прокурором;

розгляд клопотання слідчим суддею апеляційного суду протягом 24 годин;

обов’язок операторів надати дані у строк до 48 годин;

обмеження переліку інформації, яка може бути запитана, з обґрунтуванням її значення для розслідування;

дотримання норм КПК України та гарантій захисту державної таємниці й конфіденційних відомостей.

Впровадження цих змін дозволить забезпечити швидке реагування правоохоронних органів, узгодженість процедур судового контролю, зменшити ризики зловживань та підвищити рівень довіри суспільства до правоохоронної системи. Це також наблизить українське законодавство до

європейських стандартів.

Чинне нормативне регулювання механізмів доступу до даних мобільних операторів в Україні є недостатньо визначеним і суперечливим. Запропоновані зміни спрямовані на створення чіткої процедури тимчасового доступу, що поєднує оперативність реагування з гарантіями захисту прав людини. Досвід Польщі, Німеччини та Великої Британії свідчить про ефективність формалізованих клопотань, обмежених строків і прозорих механізмів контролю. Запровадження аналогічних підходів в Україні сприятиме підвищенню правової визначеності, усуненню правових колізій та гармонізації з європейськими стандартами.

Список використаних джерел:

1. Конституція України: Закон України від 28 червня 1996 р. № 254к/96-ВР // Відомості Верховної Ради України. – 1996. – № 30. – Ст. 141.
2. Кримінальний процесуальний кодекс України: Закон України від 13 квітня 2012 р. № 4651-VI // Відомості Верховної Ради України. – 2013. – № 9–13. – Ст. 88, 138, 200.
3. Про оперативно-розшукову діяльність: Закон України від 18 лютого 1992 р. № 2135-XII // Відомості Верховної Ради України. – 1992. – № 22. – Ст. 303.
4. Лист Вищого Спеціалізованого суду України «Про деякі питання здійснення слідчим суддею суду першої інстанції судового контролю за дотриманням прав, свобод та інтересів осіб під час застосування заходів забезпечення кримінального провадження» від 05.04.2013 № 223-559/0/4-13.
5. Lewandowski M. Kodeks postępowania karnego: komentarz. – Wyd. 2. – Warszawa: C.H. Beck, 2022. – 336 s. – S. 212–215.
6. Schönke A., Schröder G. Strafprozessordnung – Kommentar zum StPO. – 31. Aufl. – München: C.H. Beck, 2023. – 784 S. – § 100g: S. 110–115.
7. Home Office. Investigatory Powers Act 2016: Acquisition of Communications Data – Code of Practice. – London: The Stationery Office, 2017.

– 128 p. – P. 93–98.

САГАЙДАК Мирослава
Здобувач ступеня вищої освіти магістра Національної академії внутрішніх справ

ОПЕРАТИВНО-РОЗШУКОВЕ ВИЯВЛЕННЯ ЗЛОЧИНІВ, ПОВ'ЯЗАНИХ З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ (DEEPFAKE, AI-ШАХРАЙСТВА)

Стрімкий розвиток технологій штучного інтелекту відкрив для суспільства безліч нових можливостей, але водночас створив і принципово нові загрози у сфері безпеки. Сучасні інструменти генерації контенту — зокрема deepfake-технології, алгоритми імітації голосу та інші системи автоматизованого створення даних — дедалі частіше використовуються злочинцями для шахрайства, маніпуляцій або приховування реальної особи під час вчинення правопорушень. Це формує цілу групу злочинів, які важко своєчасно ідентифікувати традиційними методами, адже цифрові сліди швидко змінюються, а самі технології стають доступними навіть користувачам без спеціальної підготовки.

У таких умовах оперативно-розшукова діяльність потребує переосмислення та адаптації. Перед правоохоронними органами постає завдання не лише відстежувати та фіксувати нові схеми зловживань, а й навчитися працювати з технологічно складними доказами, виявляти ознаки штучної генерації контенту та прогнозувати можливі ризики. Оперативне виявлення злочинів, пов'язаних із використанням штучного інтелекту, стає важливою умовою забезпечення кібербезпеки, захисту громадян та дотримання законності в інформаційному середовищі.

Саме тому дослідження особливостей оперативно-розшукового виявлення таких правопорушень є актуальним і практично значущим. Воно дає можливість

визначити інструменти, підходи та методи, які допоможуть підвищити ефективність роботи правоохоронців у боротьбі з новими цифровими формами злочинності.

Поява глибинних нейронних мереж, генеративних моделей та великих масивів навчальних даних суттєво змінила характер цифрової взаємодії. Сучасні системи здатні створювати фото, відео та аудіо, що практично не відрізняються від реальних, а також імітувати мовлення конкретної людини чи відтворювати її поведінкові патерни. Найбільш поширеними інструментами стали deepfake-технології та AI-інструменти для автоматичного створення тексту, голосу чи графічного контенту, що відкрили простір для нових видів шахрайства — від підміни особи до маніпулювання фінансовими операціями.

До найпоширеніших форм правопорушень, де застосовується генеративний ШІ, належать:

1) Deepfake-шахрайство. Створення фальшивих відеозвернень або відеодоказів, що імітують політиків, керівників компаній, відомих осіб чи навіть звичайних громадян. Такі матеріали використовуються для вимагання коштів, дестабілізації організаційної діяльності або маніпулювання суспільною думкою [3].

2) Голосові AI-шахрайства. Імітація голосу родичів, роботодавців чи посадовців із метою виманювання грошей або доступу до службової інформації. Цей тип злочинів особливо небезпечний через високу емоційну реактивність жертви [2].

3) Автоматизоване фінансове шахрайство. AI-боти здатні масово створювати шахрайські листи, підробляти цифрові підписи чи навіть обманювати системи біометричної аутентифікації [1].

4) Втручання в інформаційні та комунікаційні системи. ШІ використовується для автоматичного зламу паролів, аналізу вразливостей або створення шкідливого контенту, який адаптується під конкретну жертву [2].

Оперативно-розшукова діяльність у сфері AI-злочинів має низку відмінностей від традиційного виявлення кіберправопорушень [1]. Головна

проблема полягає в тому, що злочинці використовують ті самі технології, які застосовують правоохоронці, тільки з більшим 1рівнем анонімності та автономності.

По-перше, оперативники стикаються з нестачею технічних інструментів. Для виявлення deepfake потрібні спеціальні алгоритми детекції, здатні аналізувати мікродефекти генерації — рендеринг очей, нестійкість тіней, аномалії міміки. Більшість таких інструментів перебувають у стадії розробки, а технологія підробки розвивається швидше, ніж технологія захисту [3].

По-друге, ускладнюється збір доказової бази. Звичні цифрові сліди (метадані, журнали подій, IP-адреси) легко маскуються через VPN, TOR-мережі чи автоматичні боти. Крім того, deepfake-матеріали часто не містять явних ознак редагування, тому потребують комплексної експертизи із залученням фахівців з цифрової криміналістики [4].

По-третє, змінюється характер оперативного спостереження. Якщо раніше акцент робився на фізичну чи комунікаційну діяльність підозрюваного, то тепер у центрі уваги — його цифрові взаємодії, сліди роботи з генеративними моделями, використання спеціальних API чи інструментів автоматизації.

У практиці оперативно-розшукових підрозділів найбільш перспективними вважаються такі напрями [1]:

- Алгоритмічна детекція підробленого контенту. Використання моделей машинного навчання, що визначають аномалії у відео, аудіо або зображеннях.
- Моніторинг поведінкових ознак. AI-боти та deepfake-аватари часто не відтворюють справжніх мікрореакцій чи інтонацій, що може бути помітним при технічному аналізі.
- Цифрова криміналістика нового покоління. Робота з цифровими слідами генерації: аналіз структури нейромереж, виявлення повторюваних «артефактів» конкретної моделі.

- Співпраця з технологічними платформами. Компанії розробляють вбудовані маркери («watermarks»), які дозволяють відстежувати штучно створений контент.

Правове поле не встигає за технологіями. В Україні досі відсутнє чітке визначення deepfake-контенту як окремого об'єкта правопорушення, а докази, створені ШІ, часто викликають суперечки щодо їх допустимості у судовому процесі. Оперативним підрозділам також бракує законодавчо закріплених процедур доступу до логів та технічних слідів, які генерують AI-сервіси.

Тому на нормативному рівні постає необхідність у:

- створенні окремих складів злочинів, пов'язаних із генеративним ШІ;
- регламентації збирання цифрових доказів;
- визначенні меж використання ШІ правоохоронцями;
- запровадженні стандартів відповідальності для розробників моделей.

Отже, сучасні злочини, пов'язані з використанням штучного інтелекту, створюють новий рівень загроз, оскільки deepfake-технології, голосові підробки та інші генеративні інструменти ускладнюють виявлення правопорушень традиційними методами. Оперативно-розшукові підрозділи стикаються з нестачею технічних засобів і нормативних механізмів, що вимагає впровадження алгоритмічних методів детекції, розвитку цифрової криміналістики та оновлення законодавства. Комплексне поєднання технологічних рішень і чітких правових рамок є ключем до ефективної протидії AI-злочинності та забезпечення безпеки в умовах швидкої цифрової еволюції.

Список використаних джерел

1. Черваньова Д. А., Курман О. В. Застосування штучного інтелекту в криміналістиці: перспективи та ризики // *Аналітично-порівняльне правознавство*. – 2025. URL: http://journal-app.uzhnu.edu.ua/article/view/334719

2. Шкелебей В. А., Галаган В. І. Проблеми законодавчого врегулювання використання штучного інтелекту під час досудового розслідування в умовах

воєнного стану // *Науковий вісник Ужгородського національного університету. Серія: Право*. – 2025. URL: http://visnyk-pravo.uzhnu.edu.ua/article/view/340195

3. Threat of Deepfakes to the Criminal Justice System: A Systematic Review // *Crime Science*. – 2024. URL: https://link.springer.com/article/10.1186/s40163-024-00239-1?utm_source

4. Xu Y., Ni Y., Zheng Y., Lee H., Ngo C.-W. Analyzing Fairness in Deepfake Detection With Massively Annotated Databases // *arXiv preprint*. – 2022. URL: https://arxiv.org/abs/2208.05845?utm_source

СИНИЦІНА Юлія
доцент кафедри інформаційних технологій Дніпровський державний університет внутрішніх справ
кандидат технічних наук, доцент

ІНТЕГРАЦІЯ НАЦІОНАЛЬНИХ І МІЖНАРОДНИХ ІНФОРМАЦІЙНИХ СИСТЕМ У ПРОТИДІЇ ВОЄННИМ ЗЛОЧИНАМ ТА ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ

Сучасна діяльність правоохоронних та міжнародних органів у сфері збору та аналізу цифрових доказів стикається з низкою серйозних проблем. По-перше, наявна фрагментарність і несумісність систем ускладнює інтеграцію національних та міжнародних баз даних, адже вони часто використовують різні стандарти й протоколи. По-друге, зростає загроза кібербезпеці: інформаційні системи, які містять докази воєнних злочинів та дані про організовану злочинність, стають об’єктом кібератак. Третім фактором є правові бар’єри: відсутність уніфікованих міжнародних механізмів для взаємного визнання цифрових доказів і регламентування доступу до персональних даних обмежує ефективність співпраці. Критичною залишається оперативність обміну даними, оскільки у воєнних умовах

швидкий обмін інформацією є надзвичайно важливим, проте наявні механізми часто бюрократизовані та повільні. Крім того, недостатнє використання технологій штучного інтелекту та аналізу великих даних (big data) знижує ефективність збору та обробки інформації. Проблемою також є брак кваліфікованих кадрів: недостатньо спеціалістів у сфері цифрових доказів, кібербезпеки та міжнародного інформаційного співробітництва. Сучасні виклики, пов'язані з веденням воєнних дій, суттєво ускладнюють роботу правоохоронних органів у сфері виявлення, документування та розслідування воєнних злочинів і проявів організованої злочинності. В умовах воєнного стану зростає потреба у швидкому доступі до достовірних даних, оперативному обміні інформацією між національними органами та міжнародними інституціями, а також у використанні єдиних стандартів збирання й аналізу доказів.

Інтеграція національних і міжнародних інформаційних систем дозволяє забезпечити: ефективний моніторинг та ідентифікацію підозрюваних осіб і злочинних угруповань; своєчасний обмін доказовою інформацією між правоохоронними органами різних країн; координацію дій у протидії транснаціональним загрозам; підвищення прозорості та довіри до результатів розслідувань на міжнародному рівні. Водночас використання інтегрованих інформаційних систем є ключовим чинником формування сучасної доказової бази для міжнародних судових інституцій, сприяє захисту прав потерпілих та забезпечує притягнення винних осіб до відповідальності. Тому дослідження питань інтеграції національних і міжнародних систем у сфері протидії воєнним злочинам та організованій злочинності має не лише теоретичне, а й важливе практичне значення для національної безпеки та міжнародної правової співпраці [1-3]. До основних методів інтеграції національних і міжнародних інформаційних систем у протидії воєнним злочинам та організованій злочинності потрібно віднести наступні: стандартизація даних та протоколів обміну; єдині захищені канали комунікації; API-інтеграція та міжсистемна інтероперабельність; використання блокчейн-технологій;

системи ідентифікації та автентифікації користувачів; машинне навчання та штучний інтелект; міжнародні центри даних і хмарні платформи; правові та процедурні механізми (таблиця 1).

Таблиця 1 Методи інтеграції

№	Назва методу інтеграції	Зміст методу інтеграції
1	Стандартизація даних та протоколів обміну	використання міжнародних форматів (XML, JSON, NIEM, Interpol Data Standards); уніфікація класифікаторів і термінології для забезпечення сумісності баз даних.
2	Єдині захищені канали комунікації	застосування криптографічних протоколів (TLS, VPN, IPsec); створення захищених шлюзів для обміну даними між національними та міжнародними системами.
3	API-інтеграція та міжсистемна інтероперабельність	впровадження відкритих програмних інтерфейсів (REST, SOAP) для автоматичного обміну інформацією; інтеграція через middleware-рішення (ESB, message brokers).
4	Використання блокчейн-технологій	забезпечення незмінності даних і ланцюга збереження доказів (chain of custody); підвищення довіри до інформації, що передається між юрисдикціями.

5	Системи ідентифікації та автентифікації користувачів	багатофакторна автентифікація (MFA), електронні підписи, біометрія; управління доступом на основі ролей (RBAC).
6	Машинне навчання та штучний інтелект	автоматизована класифікація доказів; аналіз великих масивів транскордонних даних для виявлення кореляцій і підозрілих зв'язків.
7	Міжнародні центри даних і хмарні платформи	використання хмарних рішень (EUROPOL, INTERPOL Cloud Services, NATO Federated Mission Networking); створення резервних репозиторіїв з доступом для авторизованих структур.
8	Правові та процедурні механізми	угоди про взаємне визнання електронних доказів; регламентування доступу до персональних даних відповідно до GDPR, Конвенції Ради Європи № 108 та Будапештської конвенції.

До основних практичних прикладів інтеграції національних і міжнародних інформаційних систем можемо віднести: Інформаційна система Європолу (Europol Information System, EIS). Національні правоохоронні органи країн ЄС мають прямий доступ до баз даних Європолу. Використовується для ідентифікації учасників організованих злочинних угруповань, простеження фінансових потоків та відстеження підозрюваних у воєнних злочинах. Приклад: співпраця України та Європолу для виявлення міжнародних каналів торгівлі зброєю. Інтегрована система Міжнародної організації кримінальної поліції (Interpol I-24/7). Глобальна платформа, що об'єднує понад 190 країн. Дозволяє правоохоронцям у режимі реального часу перевіряти дані про осіб, транспорт, зброю, документи. Приклад: внесення воєнних злочинців до червоних повідомлень (Red Notices) для міжнародного розшуку. ICC Evidence Platform (Міжнародний кримінальний суд). Використовується для збору, структурування й аналізу цифрових доказів воєнних злочинів. Українські органи слідства передають до ICC інформацію про воєнні злочини РФ, що інтегрується з іншими міжнародними джерелами. Приклад: використання супутникових даних та свідчень очевидців для

підтвердження обстрілів цивільних об’єктів. Система PRÜM (ЄС) Автоматичний обмін даними ДНК, відбитків пальців та реєстраційних даних транспортних засобів. Приклад: розслідування злочинів проти цивільного населення за участю підозрюваних, що перетинають кордони кількох країн. Інтеграція OSINT-платформ (Bellingcat, Mnemonic, InformNapalm). Використання відкритих джерел даних для документування воєнних злочинів. Приклад: розслідування катастрофи рейсу MH17 - інтеграція національних та міжнародних OSINT-розслідувань у доказову базу для суду в Нідерландах. Співпраця з міжнародними фінансовими системами (Egmont Group, FATF). Інтеграція банківських та фінансових даних для виявлення фінансування терористичних і злочинних угруповань. Приклад: блокування рахунків і транзакцій, що пов’язані з незаконним обігом зброї у зоні конфлікту. Національні кейси інтеграції. Український проект «Єдиний реєстр досудових розслідувань (ЄРДР)» інтегрується з міжнародними базами для передачі доказів у справах воєнних злочинів. Система «Трембіта» — інтероперабельність державних реєстрів, яка може бути використана для швидкого обміну інформацією з міжнародними структурами.

На основі вище викладеного до перспективних напрямів інтеграції національних і міжнародних інформаційних систем можливо віднести:

Уніфікація стандартів даних та протоколів обміну: розробка спільних міжнародних стандартів метаданих, структур баз даних, форматів доказів; забезпечення сумісності національних систем із глобальними платформами (Europol, Interpol, ICC).

Інтеграція систем штучного інтелекту та машинного навчання: автоматизований аналіз великих масивів доказів (супутникові знімки, перехоплення комунікацій, OSINT); прогнозування діяльності злочинних угруповань та ідентифікація їхніх цифрових слідів.

Створення єдиного хмарного середовища доказів: використання захищених міжнародних дата-центрів для зберігання цифрових доказів воєнних злочинів; спільний доступ слідчих, прокурорів та міжнародних

трибуналів.

Розвиток механізмів кібербезпеки та захисту інформації: впровадження багаторівневої криптографії, блокчейн-рішень для збереження автентичності даних; захист від кібератак на критичні бази даних із доказами.

Інтероперабельність між військовими та правоохоронними інформаційними системами: об'єднання даних розвідки, військових структур та слідчих органів; інтеграція з міжнародними військовими місіями та силами безпеки.

Розвиток спільних OSINT та GEOINT платформ: залучення громадських організацій, волонтерських ініціатив до міжнародних баз даних; використання супутникових технологій та штучного інтелекту для моніторингу порушень міжнародного гуманітарного права.

Формування правових і договірних механізмів обміну даними: укладення міжнародних угод щодо спрощення процедур передачі даних; визначення правових підстав використання цифрових доказів у судах різних юрисдикцій.

Розбудова навчальних програм і тренінгів для фахівців: підготовка слідчих, прокурорів та експертів у сфері цифрових доказів і міжнародного інформаційного співробітництва; створення навчальних симуляторів та віртуальних полігонів.

Виходячи з цього, ключовими висновками є необхідність стандартизації даних і протоколів обміну для забезпечення ефективної інтеграції інформаційних систем. Посилення міжнародної співпраці, зокрема інтеграція національних баз із системами Europol, Interpol, Міжнародного кримінального суду (ICC) та OSINT-платформами, створює умови для спільної протидії транснаціональним загрозам. Технологічний розвиток має стати пріоритетом: застосування штучного інтелекту, машинного навчання, блокчейн-рішень та хмарних дата-центрів дозволяє підвищити ефективність збору, обробки та збереження доказів. Інтегровані системи також сприяють зміцненню довіри та прозорості, підвищують легітимність результатів розслідувань та формують

сучасну доказову базу для міжнародних судових інституцій. Захист прав людини та дотримання принципів справедливого судочинства залишаються пріоритетними завдяки використанню інтегрованих платформ, що забезпечують належний захист прав потерпілих і сприяють покаранню винних. Стратегічне значення ефективної інтеграції інформаційних систем для національної безпеки проявляється у зміцненні обороноздатності країни, підвищенні ефективності боротьби з воєнними злочинами та організованою злочинністю, а також у поглибленні міжнародної правової співпраці.

Список використаних джерел:

1. Synytsina, Y. The impact of martial law on the organization's information security. *In Economic Security in the Context of Systemic Transformations*. International Conference, December 07-08, 2023, Chișinău, Moldova. / Academy of Economic Studies of Moldova, ISBN978-9975-167-43-7 (PDF). 2024. P. 169-172. URL: https://doi.org/10.53486/escst2023.20. (date of access: 11.09.2025).

2. SYNYTSINA , Y., ABRAMOV, S., MANOLE A. Improving the information system of the enterprise through the use of neural networks. *Philosophy, economics and law review Dnipropetrovsk State University of Internal Affairs.* [online] 2022. Vol. 2, no. 1. P. 127 – 138. DOI: 10.31733/2786-491X-2022-1-127-138 (date of access: 11.09.2025).

3. MILOV, O. et al. Development of the space-time structure of the methodology for modeling the behavior of antagonistic agents of the security system. *EasternEuropean Journal of Enterprise Technologies*. [online] 2020. Vol. 6, no.2. P. 30-32. URL: https://doi.org/10.15587/1729-4061.2020.218660 (date of access: 10.09.2025).

СНІЖКО Софія
курсантка 3-го курсу факультету підготовки фахівців для органів досудового розслідування Національної поліції України *Донецького державного університету*

внутрішніх справ

Науковий керівник:
ПЕКАРСЬКИЙ Сергій
доцент кафедри оперативно-розшукової діяльності та інформаційної безпеки Навчально-наукового інституту підготовки фахівців для підрозділів кримінальної поліції *імені Е. О. Дідоренка Донецького державного університету внутрішніх справ, кандидат юридичних наук, доцент*

OSINT ЯК ІНФОРМАЦІЙНИЙ ІНСТРУМЕНТ ПРИ ПРОВЕДЕННІ ОПЕРАТИВНО-РОЗШУКОВИХ ЗАХОДІВ

У сучасних умовах ведення воєнних дій та поширення гібридних загроз від країни-окупанта роль оперативно-розшукової діяльності правоохоронних органів значно зростає. Традиційні методи збору фактичних даних щодо протиправних дій особи чи групи осіб, що ґрунтуються на гласних та негласних заходах, залишаються важливими, однак їх ефективність істотно посилюється завдяки використанню новітніх інформаційних інструментів. Одним із таких інструментів є OSINT (Open Source Intelligence) – розвідка на основі відкритих джерел [1]. При цьому забезпечення верховенства права та законності, які визначені Конституцією України [2] є правовою дефініцією для суб’єктів оперативно-розшукової діяльності [3, ст. 3, ст. 5].

Сутність OSINT полягає у систематичному зборі, аналізі та використанні відомостей, отриманих із загальнодоступних інформаційних ресурсів. Йдеться про соціальні мережі, онлайн-ЗМІ, форуми, блоги, офіційні сайти державних і комерційних структур, бази даних відкритого доступу, картографічні сервіси, супутникові знімки, а також цифрові сліди користувачів у віртуальній мережі. Усі ці джерела можуть, на перший погляд, здаватися другорядними, однак у сукупності вони дають змогу створити цілісну картину діяльності окремої особи чи злочинної групи. Результатом є

інформація про особу чи групу осіб, тобто будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [4].

Практика доводить, що OSINT є надзвичайно корисним у розкритті незаконного обігу вогнепальної зброї, боєприпасів та вибухівки, що особливо актуально в умовах правового режиму воєнного стану. Моніторинг спеціалізованих інтернет-майданчиків, закритих груп у соціальних мережах або навіть публічних оголошень дозволяє правоохоронцям виявляти факти пропозицій продажу вогнепальної зброї, боєприпасів чи вибухівки. Актуальним також є і документування незаконного обігу наркотиків, вчинення корупційних дій тощо. Важливим напрямом є ідентифікація осіб, причетних до організації злочинних схем: навіть фрагментарні дані про місце проживання, коло контактів чи поведінкові особливості у віртуальному середовищі можуть стати підставою для заведення оперативно-розшукової справи [3, ст. 9].

Окремо варто відзначити можливості OSINT у виявленні фінансових потоків злочинних угруповань. Застосування інструментів відстеження криптовалютних транзакцій і аналіз публічних електронних гаманців допомагають встановлювати канали фінансування незаконної діяльності. Крім того, за допомогою відкритих джерел можна здійснювати моніторинг переміщення транспортних засобів, військової техніки країни-агресора, окремих осіб – військовослужбовців країни агресора, завдяки геолокаційним даним, знімкам із відкритих супутникових платформ і навіть фотографіям у соціальних мережах.

Отже особливе значення OSINT має у документуванні воєнних злочинів. Фото- та відеоматеріали очевидців, поширені у відкритому доступі, публікації в медіа, супутникові знімки чи записи камер спостереження можуть бути використані як доказова база у кримінальному провадженні [5]. У цьому контексті актуальним завданням є забезпечення їхнього ототожнення та ідентифікації, правильного процесуального закріплення в доказах та

подальшого використання при досудовому розслідуванні чи судовому розгляді кримінального провадження.

Однак, на нашу думку, застосування OSINT пов'язане і з низкою викликів. Найбільша проблема полягає у великій кількості неперевіреної або свідомо викривленої інформації, поширеної у відкритих джерелах. Це вимагає використання спеціальних методів перевірки достовірності даних, зокрема перехресного аналізу, геолокаційної верифікації чи зіставлення інформації з іншими оперативними джерелами. Не менш важливим є і правовий аспект: збирання та використання інформації має відбуватися у суворій відповідності до законодавства України [1; 3; 5; 6], а також міжнародних зобов'язань у сфері захисту прав людини.

При цьому перспективи розвитку OSINT в Україні безпосередньо пов'язані з інтеграцією цього інструмента з іншими видами аналітичної діяльності. Зокрема, поєднання OSINT із системами штучного інтелекту, технологіями аналізу великих даних (Big Data), автоматизованими платформами ідентифікації зображень чи голосів, а також геоінформаційними системами дозволить значно розширити можливості правоохоронних органів. На нашу думку важливим завданням залишається створення ефективних механізмів міжвідомчого обміну OSINT-даними між Національною поліцією, Службою безпеки України, Державною прикордонною службою та іншими органами, які уповноважені здійснювати оперативно-розшукову діяльність [3, ст. 5].

Таким чином, OSINT у сучасних реаліях виступає не лише допоміжним, а й одним із ключових інформаційних інструментів оперативно-розшукової діяльності. Його використання сприяє швидкому реагуванню на загрози, ефективному документуванню злочинів, розробці аналітичних прогнозів та формуванню доказової бази. Разом із розвитком правового регулювання, технічного забезпечення і професійної підготовки правоохоронців OSINT здатен стати потужним чинником у забезпеченні національної безпеки та боротьбі з організованими формами злочинності в умовах правового режиму

воєнного стану.

Список використаних джерел:

1. Дикий О. В., Сидорчук В. В. Поняття OSINT та суміжні категорії. *Юридичний науковий електронний журнал*. 2024. № 9. С. 332-335.

2. Конституція України від 28 червня 1996 року *Вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/254k/96-вр#Text (дата звернення: 26.09.2025).

3. Про оперативно-розшукову діяльність: Закон України від 18 лютого 1992 року № 2135-XII. *Вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/2135-12#Text (дата звернення: 26.09.2025).

4. Про інформацію: Закон України від 2 жовтня 1992 року № 2657-XII. *Вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 26.09.2025).

5. Кримінальний процесуальний кодекс України від 13 квітня 2012 року. *Вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 26.09.2025).

6. Про доступ до публічної інформації: Закон України від 13 січня 2011 року № 2939-VI. *Вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text (дата звернення: 26.09.2025).

7. Про Національну поліцію: Закон України від 2 липня 2015 року № 580-VIII. *Вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/580-19#Text (дата звернення: 26.09.2025).

8. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII. *Вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 26.09.2025).

СУПРОНЮК Віктор
курсант 3 курсу факультету підготовки фахівців для органів

досудового розслідування Національної поліції України Дніпровського державного університету внутрішніх справ

Науковий керівник:
КОПИЛОВ Едуард
старший викладач кафедри оперативно-розшукової діяльності, Дніпровський державний університет внутрішніх справ

НЕСПРАВ'ЖНІ ІМІТАЦІЙНІ ЗАСОБИ: ПОНЯТТЯ, ЗНАЧЕННЯ, НАПРЯМИ ВИКОРИСТАННЯ

У сучасних умовах розвитку організованих форм злочинності та використання злочинцями новітніх технологій для приховування слідів своєї діяльності особливого значення набувають спеціальні методи та засоби проведення оперативно-розшукових заходів та негласних слідчих (розшукових) дій. Одним із таких засобів є несправжні (імітаційні) засоби, використання яких регламентовано чинним законодавством України та має важливе значення для ефективності протидії злочинності. Актуальність дослідження поняття, значення та напрямів використання несправжніх імітаційних засобів зумовлена необхідністю розуміння правових меж їх застосування, забезпечення дотримання прав людини та підвищення ефективності правоохоронної діяльності.

Законодавче регулювання використання несправжніх імітаційних засобів здійснюється відповідно до положень Кримінального процесуального кодексу України та Закону України «Про оперативно-розшукову діяльність». Основним нормативним актом, що визначає правові засади використання таких засобів, є стаття 273 КПК України «Засоби, що використовуються під час проведення негласних слідчих (розшукових) дій» [1], [2].

Відповідно до частини 1 статті 273 КПК України, за погодженням з прокурором під час проведення негласних слідчих (розшукових) дій можуть бути використані заздалегідь ідентифіковані (помічені) або несправжні (імітаційні) засоби [1]. Це положення встановлює правову основу для застосування імітаційних засобів у кримінальному провадженні та визначає необхідність отримання погодження прокурора для їх використання.

Додатково, Закон України «Про оперативно-розшукову діяльність» у пункті 16 частини 1 статті 8 надає підрозділам, які здійснюють оперативно-розшукову діяльність, право використовувати несправжні (імітаційні) засоби згідно з положеннями статті 273 Кримінального процесуального кодексу України [2]. Таким чином, використання імітаційних засобів можливе як у межах кримінального провадження, так і під час здійснення оперативно-розшукової діяльності.

Поняття несправжніх імітаційних засобів не має чіткого законодавчого визначення, однак у науковій літературі та практичній діяльності під ними розуміють предмети, документи, речовини та інші об'єкти, які зовнішньо схожі на справжні, але насправді є підробками, створеними спеціально для проведення оперативно-розшукових заходів або негласних слідчих (розшукових) дій. Такі засоби можуть включати імітації грошових коштів, наркотичних речовин, документів, зброї та інших предметів, які можуть становити інтерес для злочинців.

Сутність використання несправжніх імітаційних засобів полягає у створенні контрольованих умов для документування злочинної діяльності без заподіяння реальної шкоди суспільству. Це дозволяє правоохоронним органам виявляти злочинців, встановлювати обставини підготовки та вчинення злочинів, а також збирати докази їх винуватості без ризику поширення справжніх небезпечних предметів або речовин.

Значення несправжніх імітаційних засобів у правоохоронній діяльності важко переоцінити. По-перше, вони забезпечують можливість проведення контролю за вчиненням злочину без створення реальної суспільної небезпеки.

По-друге, використання таких засобів дозволяє документувати умисел злочинця та його готовність до вчинення протиправних дій. По-третє, імітаційні засоби сприяють виявленню злочинних угруповань та встановленню ролі кожного учасника у протиправній діяльності.

Важливою гарантією законності використання несправжніх імітаційних засобів є положення частини 2 статті 273 КПК України, згідно з якою заборонено використовувати заздалегідь помічені матеріальні об'єкти або несправжні (імітаційні) засоби з іншою метою, ніж для проведення негласних слідчих (розшукових) дій [1]. Це положення унеможливлює зловживання правоохоронними органами наданими їм повноваженнями та забезпечує дотримання принципу цільового використання спеціальних засобів.

Стаття 272 КПК України встановлює загальні правила проведення негласних слідчих (розшукових) дій, зокрема визначає, що такі дії проводяться у випадках, коли відомості про злочин та особу, яка його вчинила, неможливо отримати в інший спосіб . Це означає, що використання імітаційних засобів має бути виправданим конкретними обставинами справи та відповідати принципу пропорційності. Процедурні аспекти використання несправжніх імітаційних засобів регламентуються положеннями глави 21 КПК України. Зокрема, стаття 246 КПК України визначає підстави для проведення негласних слідчих (розшукових) дій, стаття 248 встановлює порядок розгляду клопотань про їх проведення, а стаття 252 регламентує порядок оформлення результатів [1].

Контроль за використанням несправжніх імітаційних засобів здійснюється на кількох рівнях. На відомчому рівні такий контроль забезпечується керівниками оперативних підрозділів та слідчих органів. Прокурорський нагляд здійснюється через систему погоджень та санкціонування використання таких засобів. Судовий контроль реалізується через перевірку допустимості доказів, отриманих з використанням імітаційних засобів.

Міжнародний досвід використання імітаційних засобів свідчить про їх

ефективність у боротьбі з організованою злочинністю. У багатьох країнах світу такі засоби широко застосовуються правоохоронними органами для боротьби з наркозлочинністю, корупцією та іншими видами тяжких злочинів. При цьому особлива увага приділяється забезпеченню дотримання прав людини та принципів правової держави.

Таким чином, несправжні імітаційні засоби є важливим інструментом сучасної правоохоронної діяльності, який дозволяє ефективно протидіяти злочинності за умови дотримання законодавчих вимог та принципів правової держави. Їх поняття охоплює широкий спектр предметів та речовин, які імітують справжні об'єкти злочинних посягань. Значення таких засобів полягає у забезпеченні можливості документування злочинної діяльності без створення реальної суспільної небезпеки. Напрями використання визначаються специфікою конкретних видів злочинів та включають боротьбу з наркозлочинністю, корупцією, незаконним обігом зброї та іншими тяжкими злочинами. Подальший розвиток правового регулювання використання імітаційних засобів має бути спрямований на забезпечення балансу між ефективністю правоохоронної діяльності та дотриманням основних прав і свобод людини.

Список використаних джерел:

1. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 р. № 4651-VI. Дата оновлення : 28.09.2025. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 28.09.2025)

2. Про оперативно-розшукову діяльність : Закон України від 18.02.1992 р. № 2135-XII. Дата оновлення : 09.08.2024. URL: https://zakon.rada.gov.ua/laws/show/2135-12#Text (дата звернення: 28.09.2025).

ТКАЧУК Вікторія
курсант 3 курсу ННІПФПКП ім. Е.О Дідоренка
Донецький державний університет внутрішніх справ

Науковий керівник:
ПОТОЦЬКИЙ Мирослав
доцент кафедри кримінального процесу та криміналістики факультету підготовки фахівців для органів досудового розслідування НПУ
Донецький державний університет внутрішніх справ
доктор філософії за спеціальністю 081 «Право»

ЩОДО ЕЛЕКТРОННИХ ДОКАЗІВ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

Інформаційно-цифрові технології в наш час широко використовуються у сфері людського життя. Сучасний світ неможливо уявити без мобільного зв'язку, електронної пошти, месенджерів, мережі інтернет та інших корисних ресурсів які щодня застосовуються як у побуті, так і в професійній діяльності. Не оминув цифровий прогрес і сферу кримінального процесу. У кіберпросторі вчиняється велика кількість кримінальних правопорушень, та, як наслідок, окрема доказова інформація має зберігатись у електронному вигляді. Вказана тенденція дає поштовх до розвитку такої категорії як «електронні докази».

Стаття 84 Кримінального процесуального кодексу України (далі – КПК України) регламентує перелік процесуальних джерел доказів. Процесуальними джерелами доказів є показання, речові докази, документи, висновки експертів [1]. В положеннях даної статті окремо не виокремлюється поняття «електронні докази».

Більш детально зупинимось на таких процесуальних джерелах доказів як речові докази та документи. Так, речовими доказами відповідно до ст. 98 КПК України є матеріальні об'єкти, які були знаряддям вчинення кримінального правопорушення, зберегли на собі його сліди або містять інші

відомості, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження, в тому числі предмети, що були об'єктом кримінально протиправних дій, гроші, цінності та інші речі, набуті кримінально протиправним шляхом або отримані юридичною особою внаслідок вчинення кримінального правопорушення. Документом, відповідно до ст. 99 КПК України, є спеціально створений з метою збереження інформації матеріальний об'єкт, який містить зафіксовані за допомогою письмових знаків, звуку, зображення тощо відомості, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження [1].

Таким чином, до документів відносяться, в тому числі, матеріали фотозйомки, звуко-, відеозапису, комп'ютерні дані та інші носії інформації. Оригіналом електронного документа вважається його відображення (копія у відповідній формі), якому закон надає таке ж значення, як і паперовому документу [1].

Поняття «електронний доказ» визначається в Цивільному процесуальному кодексі України (далі – ЦПК України). Так, відповідно до положень ст. 100 ЦПК України електронними доказами є інформація в електронній (цифровій) формі, що містить дані про обставини, що мають значення для справи, зокрема, електронні документи (в тому числі текстові документи, графічні зображення, плани, фотографії, відео- та звукозаписи тощо), веб-сайти (сторінки), текстові, мультимедійні та голосові повідомлення, метадані, бази даних та інші дані в електронній формі. Такі дані можуть зберігатися, зокрема, на портативних пристроях (картах пам'яті, мобільних телефонах тощо), серверах, системах резервного копіювання, інших місцях збереження даних в електронній формі (в тому числі в мережі Інтернет) [2].

Науковці у своїх дослідження висловлюють різні точки зору щодо сутності поняття «електронні докази». На переконання Н.М. Ахтирської у кримінальному провадженні «електронними доказами» є дані, які

підтверджують факти, інформацію або концепцію у формі, придатній для обробки за допомогою комп'ютерних систем, у тому числі програми виконання комп'ютерною системою або інших дій. На думку авторки джерелами електронних доказів доцільно визнавати електронні пристрої: комп'ютери, периферійні пристрої, комп'ютерні мережі, мобільні телефони, цифрові камери та інші портативні пристрої, в тому числі мережу Інтернет. Інформація з цих джерел не має фізичної форми [3, с. 125].

Д.М. Цехан під категорією «електронні докази» розуміє фактичні дані, представлені у цифровій (дискретній) формі та зафіксовані на будь-якому типі носія, що стають доступними для сприйняття людиною після обробки електронно-обчислювальною машиною та на підставі яких слідчий, прокурор, слідчий суддя і суд встановлюють наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження та підлягають доказуванню [4, с. 259].

І.О. Крицька у своїх працях використовує категорію «цифрові джерела доказової інформації», які на її переконання об’єднує програми (програмне забезпечення), файли баз даних, аудіо-, відеозаписи тощо. Отже, і формою існування, виступають засоби цифрової техніки – машинні носії, до яких належать оперативні запам’ятовуючі пристрої, постійні запам’ятовуючі пристрої, накопичувачі на жорстких магнітних дисках, переносні машинні носії (оптичні носії, флеш-карти), NAS-системи тощо [5, с. 302].

Аналізуючи вищевказане можна відзначити, що електронні докази є особливим різновидом доказової інформації, що відображається в цифровій формі та висвітлює певні факти, події. Їхніми джерелами можуть бути електронні пристрої, носії інформації та інші дані, що знаходять в електронному вигляді. На підставі аналізу наукових праць Н.М. Ахтирської, Д.М. Цехана, І.О. Крицької можемо виокремити кілька ключових ознак електронних доказів: нематеріальний характер; отримання з технічних пристроїв; різні джерела отримання (комп'ютери, смартфони, інтернет, хмарні сховища , цифрові носії тощо).

Слід підсумувати, що пряма невизначеність електронних доказів у кримінальному процесуальному законодавстві, може створювати проблематику під час доказування. Електронним доказом слід вважати відомості, що містяться в електронному документі та на електронному носії інформації, на підставі яких встановлюється наявність чи відсутність обставин, що підлягають доказуванню у кримінальному провадженні, а також інші обставини, що мають значення для суті справи.

Список використаних джерел:

1. Кримінальний процесуальний кодекс України. Закон від 13.04.2012. № 4651-VI. URL : https://zakon.rada.gov.ua/laws/show/4651-17 (дата звернення: 28.09.2025).
2. Цивільний процесуальний кодекс України. Закон від 18.03.2004. № 1618-IV. URL : https://zakon.rada.gov.ua/laws/show/1618-15#Text (дата звернення: 28.09.2025).
3. Ахтирська Н.М. До питання доказової сили кіберінформації в аспекті міжнародного співробітництва під час кримінального провадження. *Науковий вісник Ужгородського національного університету.* Серія: Право. 2016. Вип. 36 (2). С. 123-125.
4. Цехан Д.М. Цифрові докази: поняття, особливості та місце у системі доказування. *Науковий вісник Міжнародного гуманітарного університету. Юриспруденція*. 2013. Вип. 5. С. 256-260.
5. Крицька І.О. Речові докази та цифрова інформація: поняття та співвідношення. *Часопис Київського університету права*. 2016. № 1. С. 301-305.

ТОКОЛОВ Олександр
курсант 4 курсу факультету підготовки фахівців
для органів досудового розслідування НПУ
Одеського державного університету внутрішніх справ

Науковий керівник:
ЛІСНІЧЕНКО Дмитро
кандидат юридичних наук
доцент кафедри кримінального процесу
та криміналістики,
Одеського державного університету внутрішніх справ

ВИКОРИСТАННЯ ЕЛЕКТРОННИХ ДОКАЗІВ У ПРОЦЕСІ ДОСУДОВОГО РОЗСЛІДУВАННЯ

Сучасний розвиток інформаційних технологій зумовлює істотні трансформації у сфері кримінального судочинства, зокрема на етапі досудового розслідування. Одним із найбільш актуальних питань у цьому контексті є використання електронних доказів, які поступово стають невід'ємною складовою кримінального процесу в Україні. З огляду на широке проникнення цифрових технологій у суспільні відносини, саме електронні дані часто містять ключову інформацію, що дозволяє підтвердити або спростувати факти, які мають значення для кримінального провадження. Їхня роль особливо зростає у справах, пов'язаних із кіберзлочинністю, шахрайством, корупційними правопорушеннями, злочинами проти безпеки держави та іншими злочинами, де цифрові сліди є головним або навіть єдиним джерелом доказової інформації.

Правове регулювання електронних доказів в Україні здійснюється у межах Кримінального процесуального кодексу України. Так, стаття 84 визначає докази як будь-які фактичні дані, на підставі яких уповноважені органи встановлюють обставини, що мають значення для кримінального провадження, а стаття 99 відносить до джерел доказів документи, включаючи електронні [1]. Таким чином, цифрові дані можуть використовуватися на рівні з традиційними документами та речовими доказами. У цьому контексті слід зазначити, що на відміну від матеріальних об'єктів, електронні докази існують

у вигляді інформаційного коду, що зумовлює специфіку їх виявлення, фіксації, вилучення та зберігання. Важливою гарантією достовірності таких доказів є забезпечення їх автентичності, оскільки навіть мінімальні зміни у цифровому файлі можуть призвести до сумнівів у його допустимості в суді.

У науковій літературі електронні докази визначаються як будь-яка інформація, що створена, зберігається чи передається у цифровій формі й може бути використана в кримінальному провадженні. Це поняття охоплює широкий спектр об'єктів: електронні документи, електронну пошту, текстові повідомлення, аудіо- та відеозаписи, інформацію з соціальних мереж, дані про геолокацію, записи з камер спостереження, інформацію з комп'ютерних систем чи мобільних пристроїв [2, с. 419]. Водночас ключовою рисою електронних доказів є необхідність застосування спеціальних технічних засобів і методів для їх вилучення та обробки, що робить процес доказування ускладненим та вимагає від слідчих і прокурорів належної підготовки.

Нормативна база використання електронних доказів охоплює не лише національне законодавство, але й міжнародні акти. Зокрема, Україна є учасницею Будапештської конвенції про кіберзлочинність 2001 року, яка встановлює стандарти збору, збереження та міжнародної передачі електронних доказів [3]. Це має особливе значення у випадках, коли інформація зберігається на серверах за кордоном і доступ до неї можливий лише у порядку міжнародного співробітництва. Водночас Закон України «Про електронні довірчі послуги» визначає правові засади використання електронних підписів і печаток, надаючи електронним документам юридичної сили та підвищуючи їх доказове значення [4].

Практика досудового розслідування свідчить про низку проблем, пов'язаних із використанням електронних доказів. По-перше, органи досудового розслідування досі відчувають брак технічних засобів для роботи з цифровими даними, особливо коли йдеться про зашифровану або видалену інформацію. По-друге, залишається складним питання підтвердження автентичності цифрових доказів, адже будь-яка зміна у структурі файлу може

поставити під сумнів його достовірність. По-третє, значна частина електронних доказів має транскордонний характер, а отже їх отримання вимагає активної взаємодії з компетентними органами інших держав, що часто затягує процес. Усе це впливає на якість та своєчасність досудового розслідування.

Особливу увагу слід приділити питанню допустимості електронних доказів. Відповідно до статті 86 КПК України, доказ визнається допустимим, якщо він отриманий у порядку, встановленому законом.

Для підвищення ефективності використання електронних доказів у досудовому розслідуванні в Україні доцільним видається кілька напрямів вдосконалення. По-перше, потребує оновлення технічне забезпечення органів досудового розслідування, а також запровадження сучасних методик цифрової криміналістики. По-друге, необхідно внести зміни до КПК України, передбачивши окремий розділ, присвячений електронним доказам, де буде детально врегульовано процедури їх збирання, перевірки та збереження. По-третє, важливим є розширення міжнародної співпраці у сфері боротьби з кіберзлочинністю.

Таким чином, електронні докази є важливим елементом доказової бази у кримінальних провадженнях, а їх значення з кожним роком зростає. Вони відображають тенденції цифровізації суспільних відносин і водночас ставлять перед правозастосувачами нові виклики, пов’язані із забезпеченням їх допустимості, автентичності та надійності. Для України, яка перебуває у процесі реформування кримінальної юстиції та адаптації до європейських стандартів, належне правове та практичне забезпечення використання електронних доказів є одним із ключових чинників ефективності досудового розслідування.

Список використаних джерел:

1. Кримінальний процесуальний кодекс України : Кодекс України від 13.04.2012 р. № 4651-VI : станом на 1 січ. 2025 року, URL:

https://zakon.rada.gov.ua/laws/show/4651-17/conv#n1713 (дата звернення 08.09.2025)
2. Козицька О.Г. Щодо поняття електронних доказів у кримінальному провадженні С. 418-421 URL: http://lsej.org.ua/8_2020/105.pdf
3. Конвенція про кіберзлочинність. Рада Європи; Конвенція, Міжнародний документ від 23.11.2001 URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення 08.09.2025)
4. Про електронну ідентифікацію та електронні довірчі послуги. Закон України від 05.10.2017 № 2155-VIII URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text (дата звернення 08.09.2025).

ЦИПА Сергій
аспірант
Донецького державного університету внутрішніх справ

Науковий керівник:
КОВАЛЬОВА Ольга
доктор юридичних наук, доцент
Донецький державний університет внутрішніх справ

ІНФОРМАЦІЙНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ПРАВ ПОТЕРПІЛОГО: ОСОБЛИВОСТІ ДОСТУПУ ДО ІНФОРМАЦІЇ НА СТАДІЇ ДОСУДОВОГО РОЗСЛІДУВАННЯ В УМОВАХ ВОЄННОГО СТАНУ

Повномасштабна збройна агресія та воєнний стан докорінно трансформували функціонування правової системи України. В умовах безпрецедентної кількості воєнних злочинів першочерговим завданням є захист прав потерпілих, для яких, власне, і здійснюється кримінальне провадження. Ключовим елементом процесуального статусу потерпілого є право на інформацію, оскільки своєчасне отримання відомостей про хід

розслідування забезпечує реалізацію інших його прав та ефективний захист інтересів. Проте, режим воєнного стану створює унікальну проблему: виникає конфлікт між правом потерпілого бути поінформованим та вимогами національної безпеки. Це протиріччя й визначає особливу актуальність цього дослідження.

Кримінальний процесуальний кодекс (КПК) України закріплює розгалужену систему прав потерпілого, центральне місце в якій посідає право на інформаційну обізнаність. Зокрема, стаття 56 КПК України гарантує потерпілому право знати суть підозри, отримувати копії матеріалів, що безпосередньо його стосуються, знайомитися з матеріалами досудового розслідування та отримувати інформацію про ключові процесуальні рішення [1]. Це право не є декларативним, а виступає інструментом, що дозволяє потерпілому активно брати участь у провадженні. Його головним обмежувачем є таємниця досудового розслідування, закріплена у статті 222 КПК України, що спрямована на захист процесу від зовнішнього впливу та перешкоджання встановленню істини [1].

Режим воєнного стану, введений відповідним Законом України [2], та зміни, внесені до Розділу IX-1 КПК України, створили нові реалії для кримінального провадження. Як зазначають І. В. Гловюк та ін, тривала збройна агресія та масштабні надзвичайні ситуації зумовлюють введення особливих правових режимів, де обмеження прав і законних інтересів осіб стає вимушеною необхідністю [3, с. 5]. Стосовно доступу потерпілого до інформації можна виділити такі ключові особливості.

По-перше, пріоритет безпекових інтересів. Розслідування воєнних злочинів та злочинів проти національної безпеки за своєю природою містить інформацію, що може становити державну таємницю. Її розголошення може завдати непоправної шкоди обороноздатності держави, що змушує слідчих застосовувати значно суворіший підхід до розкриття будь-яких матеріалів.

По-друге, об'єктивні перешкоди в роботі правоохоронних органів. Велика кількість роботи, небезпека та труднощі з пересуванням під час війни

не дозволяють швидко та регулярно підтримувати зв'язок із тисячами постраждалих людей.

По-третє, ризик зловживання таємницею слідства. Умови воєнного стану дають слідчим підстави для необґрунтованого обмеження права потерпілого на інформацію. Виникає серйозна проблема через відсутність ясного механізму розрізнення: що саме має бути засекреченим, а що можна оприлюднити без шкоди для національної безпеки. Навіть при реалізації права на отримання інформації через адвокатський запит розпорядники можуть обмежувати доступ, якщо розкриття інформації може зашкодити національній безпеці [4, с.1].

Для ефективного подолання викликів, пов'язаних із забезпеченням прав потерпілих під час воєнного стану, доцільно реалізувати такі шляхи вдосконалення, які стосуються інформаційно-правового забезпечення прав потерпілого:

1) необхідно розробити спеціалізовані методичні рекомендації

для слідчих та прокурорів. Ці рекомендації мають містити чіткі критерії та алгоритми для надання інформації потерпілим у справах про воєнні злочини, усуваючи прогалини у розмежуванні публічної та засекреченої інформації;

2) критично важливим є впровадження цифрових інструментів, зокрема захищеного «електронного кабінету потерпілого», який дозволить постраждалим особам оперативно відстежувати ключові етапи кримінального провадження та отримувати необхідні відомості;

3) необхідно посилити роль слідчого судді у процесі забезпечення прав

потерпілих. Це передбачає швидкий та ефективний розгляд скарг на будь-які процесуальні рішення чи дії, які перешкоджають потерпілому отримати інформацію або знайомство з матеріалами провадження, спираючись при цьому на актуальну судову практику Верховного Суду [5].

Підсумовуючи, варто наголосити, що інформаційно-правове

забезпечення прав потерпілого на досудовому розслідуванні в умовах воєнного стану є надзвичайно складним завданням, яке вимагає виваженого підходу. Обмеження, продиктовані національною безпекою, є об'єктивною необхідністю і неминучі, проте вони не повинні нівелювати фундаментальне право потерпілого на інформацію — ключовий елемент доступу до правосуддя. Таким чином, вдосконалення законодавчої бази та правозастосовної практики у цій сфері є пріоритетним завданням для правової системи України.

Список використаних джерел:

1. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012
р. № 4651-VI. Дата оновлення: 01.08.2025. URL: https://zakon.rada.gov.ua/laws/show/4651-17 (дата звернення: 05.10.2025).
2. Про правовий режим воєнного стану : Закон України від 12.05.2015 р. № 389-
VIII. Дата оновлення: 14.05.2025. URL: https://zakon.rada.gov.ua/laws/show/389-19 (дата звернення: 05.10.2025).
3. Особливий режим досудового розслідування, судового розгляду в умовах
воєнного стану: науково-практичний коментар Розділу IX-1 Кримінального процесуального кодексу України (станом на 25 серпня 2022 року) / І. В. Гловюк, О. М. та ін. 3-є вид., допов. і перероб. Дніпро : Дніпропетровський державний університет внутрішніх справ, 2022. 100 с.
4. Особливості розгляду адвокатських запитів на доступ до інформації в умовах воєнного стану: роз’яснення Уповноваженого ВРУ з прав людини. Офіційний сайт Омбудсмана України. URL: https://ombudsman.gov.ua/storage/app/media/%D0%92%D0%BE%D1%94%D0%BD%D0%BD%D0%B8%D0%B9%20%D1%81%D1%82%D0%B0%D0%BD/%D0%9F%D1%80%D0%B0%D0%B2%D0%BE%20%D0%BD%D0%B0%20%D0

%B7%D0%B2%D0%B5%D1%80%D0%BD%D0%B5%D0%BD%D0%BD%D1%8F%20%D1%82%D0%B0%20%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%8E/%D0%9F%D1%80%D0%B0%D0%B2%D0%BE%20%D0%BD%D0%B0%20%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%8E/%D0%A0%D0%BE%D0%B7%D0%B3%D0%BB%D1%8F%D0%B4%20%D0%B0%D0%B4%D0%B2%D0%BE%D0%BA%D0%B0%D1%82%D1%81%D1%8C%D0%BA%D0%B8%D1%85%20%D0%B7%D0%B0%D0%BF%D0%B8%D1%82%D1%96%D0%B2%20%D0%BD%D0%B0%20%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF%20%D0%B4%D0%BE%20%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%97.pdf (дата звернення: 05.10.2025).

5. Огляд судової практики Касаційного кримінального суду у складі Верховного Суду (актуальна практика). Рішення внесені до ЄДРСР, за серпень 2025 року. Офіційний сайт Судова влада України. URL: https://court.gov.ua/storage/portal/supreme/ogliady/Oglyad_KKS_08_2025_1.pdf (дата звернення: 05.10.2025).

ШОПІНА Ірина
професор кафедри адміністративно-правових дисциплін
Львівського державного університету внутрішніх справ,
доктор юридичних наук, професор
ORCID: 0000-0003-3334-7548

ІНФОРМАЦІЙНІ МЕХАНІЗМИ ВПЛИВУ ДЕРЖАВИ-АГРЕСОРА НА ДІТЕЙ ТА МОЛОДЬ В УМОВАХ ЗБРОЙНОГО КОНФЛІКТУ

В Україні фіксується небезпечна тенденція: російські спецслужби активно вербують неповнолітніх українців для диверсійної діяльності. Йдеться не лише

про поширення фейків чи онлайн-агітацію — дітей буквально використовують як гарматне м’ясо, змушуючи їх за гроші виконувати бойові завдання на мирній території. Останні судові справи свідчать: підлітки спалюють автомобілі військових, готують вибухи біля адмінбудівель [1]

Як справедливо відзначає В. Ярмоленко, з ідеологічної точки зору, діти досить швидко демонструють лояльність і їх легко індоктринувати, оскільки вони мають менше попередньо сформованих концепцій і переконань, які вербувальникам потрібно було б спростувати або змінити [2]. Слід також погодитися із думкою В. Потапової і А. Воробйової, що діти, метафорично висловлюючись, уявляють собою вразливі «чисті дошки» і є дуже пластичними суб’єктами. Більше того, на відміну від дорослих, які можуть мати протилежні світогляди та можуть спиратися на досвід свого «попереднього життя» для опору індоктринації, індоктриновані або навіть народжені в екстремістському середовищі діти є «чистим» втіленням і носіями ідеології групи, які будуть лояльними охоронцями цієї ідеології для майбутніх поколінь. В контексті російської окупації індоктринація проявляється в різних аспектах: знищення української ідентичності та формування «російської ідентичності»; виховання з українських дітей «ідейних російських громадян», готових «свідомо» і «добровільно» боронити російську землю зі зброєю в руках; а також нав’язування ідеї штучності української нації і асоціювання сучасної України з нацистською Німеччиною; легітимації російської агресії проти України [3].

Слід також згадати активне використання противником засобів проведення інформаційно-психологічних операцій, метою яких є залучення українських дітей до російського культурного простору. На жаль, деякі українські батьки з раннього дитинства нав’язують своїм дітям культурний код «руського міру»: Уявляє інтерес, що у серпні 2025 року україномовний YouTube-канал «Маша та Ведмідь» посів перше місце серед дитячих каналів в Україні. Лише за 2025 рік канал отримав понад 800 мільйонів переглядів, а підписано на нього 18 мільйонів людей. Цей канал створений саме для української авдиторії – усі серії озвучені українською мовою. Описи до відео також додано українською. В описі до відео

вказується посилання на російський сайт. Фахівці зазначають, що на перегляді одного відео в Україні творці «Маші та Ведмедя» можуть заробляти по 3 долари. Лише за 2025 рік росіяни могли заробити на українських глядачах 2,4 мільйона доларів, тобто залучення до цінностей «руського міру» фактично фінансується україномовними громадянами нашої держави [4].

Російська блогерка Інстасамка залишається у лідерах серед українських слухачів не один місяць. У січні 2023 року вона посіла перше місце у «Топ-50 Україна» на Spotify. У російських соцмережах була поширена інформація, що ця особа перечислила армії держави-агресора 900 тисяч рублів, які вона заробила від рекордних прослуховувань своєї пісні «За деньги да» – тієї самої, що стала лідером серед українських слухачів [5].

У 2023 році першу сходинку в рейтингу «Топ-100 в Україні» на платформі для прослуховування музики Apple Music зайняла композиція під назвою «Пияла» російського гурту «Аигел». Це означає, що саме її найчастіше обирають і найбільше слухають українські користувачі. Ця композиція – саундтрек до російськоїкінострічки «Слово пацана. Кров на асфальті», що знімали за підтримки громадської організації «Інститут розвитку інтернету», яку фінансує російська влада з метою вироблення пропагандистського продукту. Сама кінострічка потрапила у тренди українського сегменту Google. Герою фільму 14 років, і найбільше фільм приваблює дитячу та юнацьку авдиторію. Особливістю кінострічки є поєднання радянських наративів (один із героїв пишається, що народився в один день з Леніним, виправдання війни в Афганістані, ненависть до США тощо) з культом сили та жорстокості [6].

Протидія спробам держави-агресора вплинути на свідомість і світогляд українських дітей та молоді потребує комплексної системної роботи, спрямованої на формування їх стійкості до загроз, притаманних збройним конфліктам і гібридним війнам. У цьому контексті особливої актуальності набуває розроблення державної стратегії інформаційної безпеки дітей, яка б передбачала механізми моніторингу, реагування та нейтралізації шкідливого контенту. Не менш важливим є створення конкурентоспроможного національного медіапродукту для

дитячої аудиторії, який би, з використанням сучасних методів впливу на аудиторію (зокрема, інфотейнменту як поєднання інформації та розваг, що дозволяє подати складні теми у доступній формі, викликаючи емоційний відгук, і геймифікації - застосування ігрових елементів у неігрових контекстах), дозволив би не лише перевершити російський медіа продукт, а й виступив би діючим засобом формування національної ідентичності через культурні архетипи. Варто також передбачити інституційне посилення співпраці у сферах освіти, культури, оборони та цифрової трансформації з метою координації заходів протидії російській інформаційній експансії. У сфері правового регулювання необхідно закріпити поняття «інформаційної індоктринації» як форми психологічного насильства, що має особливо небезпечні наслідки для неповнолітніх. Водночас слід розробити механізми захисту дітей, які перебували на окупованих територіях, з урахуванням їхнього можливого впливу з боку ворожої пропаганди. Усі ці заходи мають бути інтегровані в ширший контекст гуманітарної політики держави, спрямованої на збереження національної ідентичності та правосвідомості молодого покоління. Врешті-решт, питання захисту дітей від ідеологічного впливу держави-агресора слід розглядати як складову національної безпеки України.

Список використаних джерел:

1. Окупанти масово вербують підлітків у Telegram для диверсій. https://nenka.info/okupanty-masovo-verbuyut-pidlitkiv-u-telegram-dlya-dyversij/?utm_source=rss&utm_medium=rss&utm_campaign=okupanty-masovo-verbuyut-pidlitkiv-u-telegram-dlya-dyversij (дата звернення 3.10.2025)

2. Ярмоленко В. Спроби систематизації державної ідеології в Росії та розбудова системи індоктринації. URL: https://niss. gov. ua/doslidzhennya/mizhnarodni-vidnosyny/sproby-systematyzatsiyi-derzhavnoyi-ideolohiyi-v-rosiyi-ta (дата звернення 3.10.2025)

3. Потапова В., Воробйова А. Індоктринація молоді на тимчасово окупованої території Криму:проблеми та виклики майбутньої реінтеграції.

Крим - це Україна: стратегія деокупації та реінтеграції : зб. матеріалів Міжнар. наук.-практ. круглого столу з нагоди Дня спротиву окупації Автономної Республіки Крим та м. Севастополя. (м. Одеса, 24 лютого 2023 р.). Одеса, 2023. С.202-208.

4. російський YouTube-канал «Маша та Ведмідь» посів перше місце серед дитячих каналів в Україні. URL: https://wz.lviv.ua/news/538301-rosiiskyi-youtube-kanal-masha-ta-vedmid-posiv-pershe-mistse-sered-dytiachykh-kanaliv-v-ukraini (дата звернення 3.10.2025)

5. Інстасамка пожертвувала на війну 900 тисяч рублів, які заробила на прослуховуванні її пісні в Україні. URL: https://life.kyiv24.news/news/instasamka-pozhertvuvala-na-vijnu-900-tysyach-rubliv-yaki-zarobyla-na-prosluhovuvanni-yiyi-pisni-v-ukrayini (дата звернення 3.10.2025)

6. Мисловський І. Пропаганда криміналу: як російський серіал штовхає нас до насильства й авторитаризму. URL: https://detector.media/infospace/article/221387/2024-01-05-propaganda-kryminalu-yak-rosiyskyy-serial-shtovkhaie-nas-do-nasylstva-y-avtorytaryzmu/ (дата звернення 3.10.2025)

СЕКЦІЯ 4.
ІННОВАЦІЙНІ МЕТОДИ, КРИМІНАЛІСТИЧНІ МЕТОДИКИ ТА ЕКСПЕРТНІ ДОСЛІДЖЕННЯ, ЗОКРЕМА ІЗ ЗАСТОСУВАННЯМ ПОЛІГРАФА, У ПРОТИДІЇ ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ.

АФТАНАСІВ Валерія
здобувачка вищої освіти 4 курсу Навчально-наукового інституту права та правоохоронної діяльності Львівського державного

КРИМІНАЛІСТИЧНЕ ЗАБЕЗПЕЧЕННЯ ЕКСГУМАЦІЇ ТА ІДЕНТИФІКАЦІЇ ТІЛ ДЛЯ РЕПАТРІАЦІЇ

Ексгумація та ідентифікація тіл у контексті репатріації становлять за своєю природою процесуально значущі слідчі (розшукові) дії, що потребують цілісного криміналістичного забезпечення на всіх етапах їх реалізації – від місцезнаходження поховання до передачі ідентифікованих останків. Так, у межах кримінального провадження наведені дії виконують функцію вилучення, фіксації, трасологічної, біологічної та антропологічної ідентифікації об'єктів, які мають доказове значення для встановлення особи загиблого, реконструкції механізму смерті та правової кваліфікації події.

Своєю чергою, репатріація тіл осіб, загиблих внаслідок збройного конфлікту, передбачає не лише реалізацію гуманітарного імперативу, але й виконання міжнародно-правового обов'язку держави щодо належного поводження з останками. Окреслене охоплює їх ідентифікацію, судово-експертне документування, транспортування та передачу відповідно до криміналістичних стандартів доказової валідності.

З науково-доктринальних позицій, криміналістичне забезпечення ексгумації має передбачати: а) просторово-трасологічну реконструкцію поховання, з фіксацією положення тіла, супровідних об'єктів, слідів переміщення, ознак насильницької смерті чи вторинного захоронення [1]; б) біологічну та генетичну ідентифікацію, із застосуванням методики ДНК-профілювання, порівняльного аналізу з референтними зразками родичів, а також ідентифікації за стоматологічними, краніометричними та імплантологічними ознаками [2]; в) судово-медичну експертизу трупа, з оцінкою давності смерті, характеру ушкоджень, наявності слідів катування, бойових травм, термічного чи хімічного впливу [3]; г) документування та збереження доказового матеріалу, з урахуванням принципів континуальності

ланцюга збереження («chain of custody»), цифрової фіксації, фотограмметрії та 3D-моделювання [4].

В даному аспекті ексгумація набуває статусу не лише технічної процедури, але й криміналістично релевантного інструменту, що забезпечує доказову безперервність та дає можливість поєднати морфологічні, танатогенетичні, біохімічні та ситуаційні ознаки в єдину доказову систему. Зокрема, ексгумація виконує функцію вилучення об'єкта трасологічного аналізу з локалізованого середовища (місця поховання) з подальшим здійсненням судово-медичної стратиграфії, біологічної ідентифікації (генотипування, стоматологічної експертизи, остеологічної реконструкції), а також ідентифікації ознак можливої насильницької смерті [3; 5].

В межах обраної тематики окремої уваги заслуговує аспект організованої злочинності, яка в умовах російсько-української війни може виступати не тільки суб'єктом насильницьких дій, але й фактором системного приховування злочинів проти людяності. Практика виявлення масових поховань військовослужбовців і цивільних осіб, виявлені на деокупованих територіях України, свідчить про цілеспрямовану практику рф щодо приховування ознак жорстокого поводження, катування, позасудових страт та інших форм насильства, що мають ознаки міжнародних злочинів. Подібні дії часто супроводжуються спробами знищення тіл, фальсифікації обставин смерті, використання спільних могил без маркування, що також суттєво ускладнює процес ідентифікації та порушує норми міжнародного гуманітарного права.

Разом з тим, ідентифікація тіл у межах репатріаційного процесу передбачає застосування високоточних методів криміналістичної біометрії, дактилоскопії, судово-медичної антропології, краніометрії, одонтоскопії та цифрової трасології, які в сукупності формують модель персоніфікованої належності об'єкта, котра, своєю чергою, дає можливість не лише встановити особу загиблого з високим ступенем достовірності, але й здійснити порівняльний аналіз з реєстрами – генетичними, дактилоскопічними,

стоматологічними, імплантологічними – що зберігаються в національних та міжнародних базах даних. Слід звернути увагу, що в даному аспекті особливу роль відіграє цифрова трасологія, оскільки вона забезпечує реконструкцію унікальних слідових ознак (напр., шрамів, імплантів, особливостей остеологічної структури) з використанням 3D-моделювання, фотограмметрії та алгоритмів машинного зіставлення.

Принагідно зауважимо, що ексгумація як елемент криміналістичної тактики не може розглядатися ізольовано від загальної системи слідчих (розшукових) дій. У працях науковців ексгумація трактується як різновид огляду трупа, що здійснюється з метою встановлення причин смерті [6]. Проте, видається, в умовах масових поховань, характерних для збройних конфліктів, така дефініція є недостатньою. Доцільно розглядати ексгумацію як комплексну криміналістичну операцію, яка охоплює елементи трасології, судової медицини, біологічної ідентифікації, а також криміналістичної реєстрації та фіксації доказів. Більше того, в даному контексті ексгумацію слід визначити як процесуально регламентовану криміналістичну дію, що полягає у вилученні тіла або його фрагментів із локалізованого середовища з метою реконструкції обставин смерті, ідентифікації особи загиблого, виявлення ознак насильницького впливу та забезпечення доказової валідності матеріалів, отриманих в межах кримінального провадження.

У даному аспекті варто звернутися до положень міжнародного гуманітарного права, зокрема до Протоколу I до Женевських конвенцій 1949 року [7], який передбачає обов’язок держав забезпечити гідне поводження з останками загиблих. Ідентифікація тіл, що підлягають репатріації, є окремим етапом криміналістичного забезпечення, який в тому числі охоплює застосування методів біометричної верифікації, генотипування (ДНК-аналіз), дактилоскопії, стоматологічної експертизи, а також порівняльного аналізу особистих речей, одягу, імплантологічних конструкцій та інших індивідуалізуючих ознак.

Водночас, у випадках обмеженого доступу до реєстрів, відсутності

референтних зразків чи порушення ланцюга збереження доказів, окремої уваги заслуговує криміналістичний аналіз контексту поховання. Йдеться, насамперед, про реконструкцію місця виявлення, археологічну стратиграфію, аналіз супровідних матеріалів (одягу, особистих речей, маркерів належності до військових формувань), які дозволяють підтвердити чи спростувати гіпотезу щодо особи загиблого та обставин його смерті.

Окремого аналізу потребують процесуальні аспекти ексгумації як слідчої (розшукової) дії, яка має особливу доказову значущість у контексті збройного конфлікту. Будь-яка слідча дія повинна відповідати критеріям законності, обґрунтованості та доцільності, що випливає із загальних засад кримінального процесуального закону [8]. Тим не менш, в умовах війни та масового виявлення поховань цивільних і військовослужбовців, ексгумація доволі часто здійснюється поза межами кримінального провадження – за участі міжнародних місій, гуманітарних організацій, незалежних судово-експертних груп або мобільних слідчих підрозділів. Відповідно, з'являються проблеми, пов'язані з процесуальною легітимністю отриманих доказів та їх допустимістю в судовому провадженні. З даного приводу слід наголосити на доцільності розроблення спеціальних криміналістичних протоколів ексгумації, повною мірою адаптованих до умов репатріації тіл загиблих.

Список використаних джерел:

1. Management of Dead Bodies after Disasters: A Field Manual for First Responders. *International Federation of Red Cross and Red Crescent Societies*. 2006. URL:https://www.icrc.org/sites/default/files/external/doc/en/assets/files/other/icrc_002_0880.pdf (дата звернення: 25.09.2025 р.).

2. Missing People, DNA Analysis and Identification of Human Remains. A guide to best practice in armed conflicts and other situations of armed violence. 2nd edition. *International Committee of Red Cross*. 2009. URL: https://www.icrc.org/sites/default/files/external/doc/en/assets/files/other/icrc_002_

4010.pdf (дата звернення: 25.09.2025 р.).

3. Навчальний посібник з аудиторних занять з судової медицини для студентів та викладачів. Упор./ Б. Михайличенко, А. Біляков, Н. Ергард. Національний медичний університет ім. О.О. Богомольця. 237 с. URL: https://bit.ly/3IznLOO

4. Пашковський М. Ланцюг зберігання доказів (chain of custody): процесуальна форма. *Матеріали конференцій МЦНД*, (06.12.2024; Могилів-Подільський, Україна). 2024. С. 157-161.

5. Istanbul Protocol: Manual on the Effective Investigation and Documentation of Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment of 29.06.2022. URL: https://www.ohchr.org/en/publications/policy-and-methodological-publications/istanbul-protocol-manual-effective-0 (дата звернення: 25.09.2025 р.).

6. Криміналістика: *Підручник* / Кол. авт.: В. Ю. Шепітько, В. О. Коновалова, В. А. Журавель та ін. / За ред. проф. В. Ю. Шепітька. - 4-е вид., перероб. і доп. Х.: Право, 2008. 464 с.

7. Protocols Additional to the Geneva Conventions of 12 august 1949. *International Committee of Red Cross*. 2010. URL: https://www.icrc.org/sites/default/files/external/doc/en/assets/files/other/icrc_002_0321.pdf (дата звернення: 25.09.2025 р.).

8. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 №4651-IV. URL: https://zakon.rada.gov.ua/laws/show/4651-17 (дата звернення: 25.09.2025 р.).

БОНДАРЕНКО Артем
курсант 3-го курсу
Донецького державного
університету внутрішніх справ

Науковий керівник:
БОНДАРЧУК Руслан
суддя Кропивницького

апеляційного суду

СУДОВА ПРАКТИКА З ПИТАННЯ ДОПУСТИМОСТІ РЕЗУЛЬТАТІВ ЕКПЕРТНИХ ДОСЛІДЖЕНЬ ІЗ ЗАСТОСУВАННЯМ ПОЛІГРАФА

На сучасному етапі розвитку криміналістики та судової експертизи пошук нових засобів встановлення обставин кримінального правопорушення під час розслідування злочинів набуває особливого значення. Одним із дискусійних інструментів є використання поліграфа (так званого «детектора брехні»), що ґрунтується на реєстрації психофізіологічних реакцій людини у відповідь на певні стимули. Попри тривале використання поліграфних досліджень у багатьох країнах, питання їх судової прийнятності в Україні залишається складним і неоднозначним.

Правовий статус досліджень із використанням поліграфа визначений у Законі України «Про судову експертизу» та в Інструкції про призначення та проведення судових експертиз і експертних досліджень. Доказова сила результатів упровадження методики з’являється саме в межах призначеної судової експертизи. Технічні й методичні вимоги проведення досліджень визначають нацстандарти: ДСТУ 8692:2016 («Поліграфи. Технічні умови») і ДСТУ 9266:2023 («Судова психологічна експертиза. Використання поліграфа»). Вони встановлюють, на якому обладнанні допустимо працювати і як саме організовувати методику (перелік дозволених методик, порядок питань, регламенти реєстрації реакцій) [1, 2].

Результати застосування експертних досліджень із застосуванням поліграфа використовуються у практиці досудового розслідування для перевірки достовірності показань і опрацювання версій, для підтвердження або спростування причетності особи до вчинення кримінальних правопорушень.

Із урахуванням специфіки методики досліджень за допомогою

поліграфа, проведення такої перевірки лише на основі добровільної згоди відповідної особи. Результати подає суду сторона, що замовляла дослідження, або їх долучають у межах проведення вже призначеної експертизи.

Прийнятність отриманої інформації може розглядатися як доказ лише за наявності сукупності загальних та спеціальних умов допустимості й достовірності експертних висновків.

Так, дослідження за добровільною письмовою згодою респондента має проводити лише кваліфікований експерт, що має вищу психологічну освіту і профільну підготовку поліграфолога. Під час мають бути застосовані допустимі методики (за ДСТУ 9266:2023) з дотриманням етичних і процесуальних норм. Використане обладнання має відповідати ДСТУ 8692:2016, із чинною повіркою, а підсумковий висновок - обґрунтованим: описано методику, питання, параметри реєстрації, подано поліграми та їхній аналіз.

Міжнародна практика з цього питання є багатоманітною. У понад 70 країнах світу поліграф використовується як допоміжний інструмент, проте лідером є США. Там застосування регулюється як на федеральному, так і на штатному рівнях, наприклад, законом Каліфорнії №351.1 від 1983 року. У деяких штатах поліграф прямо передбачений у процесуальному законі при розслідуванні різних «сенситивних» категорій кримінальних правопорушень, наприклад, статевих злочинів [3].

Судова практика в Україні засвідчує, що питання прийнятності судом результатів проведених досліджень вирішується неоднозначно – від повного заперечення до визнання за деяких умов.

Прикладом кейсу прийнятності результатів застосування поліграфу є справа № 301/943/19, у якій вироком суду обвинуваченого було визнано винним у скоєнні умисного тяжкого тілесного ушкодження (ст. 121 КК України) за результатами оцінки, зокрема, висновку судової психологічної експертизи із застосуванням поліграфа як допустимого доказу [4].

Переглядаючи у касаційному порядку цивільну справу № 457/906/17,

Верховний Суд перевірив законність та обґрунтованість рішень судів першої та апеляційної інстанцій, які послалися на результати судової психологічної експертизи із застосування поліграфа як на підставу для своїх висновків. Визнавши неправильність висновків судів, які випливають із поданого стороною висновку експертизи із використанням поліграфа, Верховний Суд фактично у цілому констатував законність поданого стороною доказу [5].

Практичним прикладом заперечення можливості використання поліграфа у її у доказуванні є справа № 621/1308/18: вирішуючи клопотання сторони захисту про призначення судової експертизи із застосуванням поліграфу на предмет правдивості показань підозрюваного та потерпілого щодо способу заволодіння транспортним засобом, суд першої інстанції відмовив у його задоволенні, пославшись на те, що чинним кримінальним процесуальним законодавством не передбачено перевірку показань із застосуванням спеціального технічного засобу - поліграфу (детектора брехні) та використання отриманих даних як доказу. З висновками суду погодилася колегія суддів Другої палати Касаційного кримінального суду у складі Верховного Суду, переглядаючи справу у касаційному порядку [6].

У Постанові від 18 серпня 2020 року у справі № 628/2370/17 Верховний Суд визнав обґрунтованими висновки судів попередніх інстанцій про те, що висновок щодо проведення психофізіологічного дослідження обвинуваченого з використанням поліграфа, проведеного спеціалістом – поліграфологом, не є доказом у розумінні ст. 84 КПК України, а є додатковим аргументом на підтвердження правильності виправдання обвинуваченого [7]. Аналогічну позицію зайняв Верховний Суд у справі № 234/4850/17.

У справі №757/13635/17-к Вищий антикорупційний суд навів розгорнуту аргументацію про ймовірний та орієнтувальний характер використання поліграфа. В ухвалі від 22 червня 2022 року апеляційна палата ВАКС зауважила, що при аналізі чинних нормативно-правових актів, якими регламентується опитування із застосуванням поліграфа відповідних суб`єктів (співробітників), які мають відношення до конкретного виду професійної

діяльності, вбачається, що результати такого опитування не тягнуть правових наслідків, не можуть бути підставою для прийняття будь-яких адміністративно-управлінських рішень стосовно суб`єкта опитування та використовуються виключно як відомості ймовірного та орієнтувального характеру; результати опитування не мають будь-якої доказової сили, а лише орієнтують на здобуття доказової інформації в порядку, передбаченому законодавством. Оскільки законодавче закріплення доцільності використання поліграфа у кримінальних провадженнях наразі відсутнє, а показники поліграфа є лише фізіологічними даними про людину на певний момент, які виникають внаслідок психологічних реакцій, при інтерпретації результатів яких можна з легкістю помилитися, висновки такого дослідження мають виключно вірогідний характер і розцінюються як припущення [8].

Таким чином, аналіз судової практики в Україні дозволяє виснувати, що позиції судів стосовно висновків досліджень із застосування поліграфа загалом не є однозначними, натомість у кримінальних провадженнях вони оцінюються як такі, що не можуть бути покладені в основу висновків суду про винуватість особи.

Для усунення неоднозначності стосовно умов визнання допустимості результатів використання поліграфа це питання має бути врегульоване на законодавчому рівні.

Список використаних джерел:

1. ДСТУ 8692:2016 Поліграфи. Технічні умови. Київ, 2016.
2. ДСТУ 9266:2023 Судова психологічна експертиза. Використання поліграфа. Загальні вимоги. Державне підприємство «УкрНДНЦ». Київ, 2023.
3. К. Кольчинська. Поліграф у кримінальному процесі: ефективний засіб доказування чи сумнівний інструмент? URL: https://advokatpost.com/polihraf-u-kryminalnomu-protsesi-efektyvnyj-zasib-dokazuvannia-chy-sumnivnyj-instrument-advokat-kolchynska/.
4. Вирок Іршавського районного суду Закарпатської області від 13

лютого 2023 року. Справа №301/943/19. URL: https://reyestr.court.gov.ua/Review/108950519.

5. Постанова Верховного Суду від лютого 2020 року. Справа № 457/906/17 URL: http://www.reyestr.court.gov.ua/Review/87602624.

6. Постанова Касаційного кримінального суду від 11 червня 2020 року Справа № 621/1308/18.URL: http://www.reyestr.court.gov.ua/Review/89825037.

7. Постанова Касаційного кримінального суду Верховного Суду від 18 серпня 2020 року у справі № 628/2370/17. URL: http://www.reyestr.court.gov.ua/Review/91089402.

8. Ухвала колегії суддів апеляційної палати Вищого антикорупційного суду від 8 червня 2022 року у справі № 757/13635/17-к. URL: https://reyestr.court.gov.ua/Review/104751345.

ВОЙЧИШЕНА Марина
старший викладач кафедри кримінального процесу та криміналістики
факультету підготовки фахівців для органів досудового розслідування
Донецького державного університету внутрішніх справ
ORCID:https://orcid.org/0000-0002-1854-3631

КРИМІНАЛІСТИЧНІ АСПЕКТИ ПРОТИДІЇ ЗЛОЧИННОСТІ В УМОВАХ ЗБРОЙНОГО КОНФЛІКТУ

Протидія злочинності полягає у комплексному забезпеченні та гарантуванні безпеки і надійного захисту охоронюваних цінностей і благ від злочинних посягань на конституційні права і свободи громадян, політичні, економічні та соціальні інститути громадянського суспільства, матеріальні і духовні надбання Українського народу, територіальну цілісність, незалежність і суверенітет країни [1, с. 443]. На сьогодні, достатньо високими

є показники вчинення майнових злочинів (крадіжки, мародерство) та корисливо-насильницьких злочинів (грабежі, розбої), а також спостерігається зростання незаконного обігу наркотиків та зброї. Стабільно високими показниками (191763 злочинів) [3] характеризуються злочини, вчинені за період повномасштабного вторгнення рф, а саме: воєнні злочини, злочини агресії, пропаганда війни, злочини проти людяності та інші.

В сучасних умовах протидія злочинності вимагає поєднання зусиль правоохоронних органів та здійснення ними заходів щодо виявлення, розкриття, розслідування та профілактики вчинення кримінальних правопорушень. В даному напрямку науковцями удосконалюються та розробляються засоби, прийоми та методи протидії злочинності, а тому суттєве значення має вивчення та узагальнення практики розслідування, розроблення сучасних і дієвих механізмів протидії злочинності та впровадження наукових досягнень у практичну діяльність. Вагомим, на сьогодні, є розроблення шляхів протидії організованій злочинності, яка становить значну загрозу як для громадян, так і держави. Під організованою злочинністю розуміється сукупність кримінальних правопорушень, що вчиняються у зв'язку зі створенням та діяльністю організованих злочинних угруповань. Метою боротьби з організованою злочинністю є: встановлення контролю над організованою злочинністю, її локалізація, нейтралізація, ліквідація та усунення причин і умов існування організованої злочинності [4].

Основним завданням в боротьбі з організованою злочинністю є своєчасне виявлення, припинення, повне й об'єктивне розслідування злочинів і запобігання їм. Важливу роль у вирішенні вказаних завдань відіграє криміналістика, яка розробляє раціональні методи, прийоми й засоби дослідження та розкриття кримінальних правопорушень у процесі їх розслідування й судового розгляду [2, с. 12]. В даному напрямку науковцями в галузі криміналістики розробляються сучасні криміналістичні методи та засоби розслідування, до яких можна віднести особливості роботи із цифровими доказами, використання можливостей штучного інтелекту та

розвідки з відкритих джерел, криміналістичний ДНК-аналіз та використання спеціальних знань з метою дослідження доказів. Крім того, протидія організованій злочинності, зокрема транснаціональній потребує міжнародної співпраці та взаємодії з правоохоронними органами інших країн, що полягає у наданні взаємної правової допомоги та обміні інформацією відповідно до положень міжнародних договорів та нормативно-правових актів.

Успішне протистояння злочинності в сучасних умовах вимагає постійного розвитку технологій виявлення та дослідження матеріальних, ідеальних і цифрових слідів злочинів, тактичних прийомів і методичних рекомендацій із проведення окремих процесуальних дій, розслідування різних видів і груп кримінальних правопорушень. У цьому контексті криміналістична наука постійно розвивається за напрямами вдосконалення відповідних теоретичних положень, упровадження новітніх технічних засобів і тактичних прийомів, що дозволяють якісніше виконувати відповідні завдання [5, с. 7]. Криміналістичною наукою на основі узагальнення практики розслідування та тенденцій вчинення окремих видів кримінальних правопорушень розробляються видові та міжвидові методики розслідування, які спрямовані на забезпечення слідчих сучасними розробками щодо організації досудового розслідування та криміналістичного забезпечення досудового розслідування. Зокрема, виявлення причин та умов, які сприяють вчиненню кримінальних правопорушень та функціонування організованих злочинних груп, викриття діяльності організованих злочинних груп, документування злочинів та притягнення до відповідальності осіб, причетних до організованої злочинності.

Крім того, перед працівниками поліції постають завдання щодо здійснення досудового розслідування та документування кримінально-протиправної діяльності в умовах збройного конфлікту, зокрема, ускладнені умови збирання доказів на територіях, наближених до зони бойових дій, складнощі у проведенні слідчих (розшукових) дій на деокупованих територіях. Саме тому, наукові розробки мають бути орієнтованими на подолання

сучасних викликів, що пов’язані із забезпеченням розслідування та здійсненням протидії організованій злочинності в умовах збройного конфлікту.

Список використаних джерел:

1. Ковальов І.В., Сокуренко В.В. Тактикии і стратегії протидії злочинності як перспективний напрям наукових досліджень О.М. Бандурки та О.М. Литвинова: духовно-ціннісні аспекти проблеми. Юридичний науковий електронний журнал. 2022. № 12. С. 442-446. URL: http://lsej.org.ua/12_2022/104.pdf

2. Криміналістика: підруч. / за ред. В.В. Тіщенка. Одеса : Видавничий дім «Гельветика», 2019. 556 с.

3. Офіс Генерального прокурора України. URL: https://gp.gov.ua/

4. Про організаційно-правові основи боротьби з організованою злочинністю : закон України від 30.06.1993 № 3341-XII. URL: https://zakon.rada.gov.ua/laws/show/3341-12#Text

5. Степанюк Р. Л. Сучасні криміналістичні засоби та методи протидії злочинності : навч. посіб. / Р. Л. Степанюк, В. О. Гусєва. Харків : ХНУВС, 2024. 232 с.URL: https://files.znu.edu.ua/files/Bibliobooks/Inshi78/0058151.pdf

ГРУЗДЬ Олександр
завідувач кафедри кримінального процесу та криміналістики факультету підготовки фахівців для органів досудового розслідування Національної поліції України Донецького державного університету внутрішніх справ

ЦИФРОВА ТРАНСФОРМАЦІЯ КРИМІНАЛІСТИКИ: СУЧАСНІ ПІДХОДИ ДО ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ СЛІДЧОЇ

ДІЯЛЬНОСТІ

У сучасних умовах цифровізації суспільства відбувається докорінна трансформація криміналістики як науки та практичної діяльності. Розвиток інформаційних технологій сприяє формуванню нових підходів до організації, фіксації, аналізу й використання доказової інформації, що суттєво впливає на ефективність слідчої роботи.

На думку С. В. Власової «цифрові технології дозволять перейти від слідчого типу кримінального процесу до змагального. Повинен бути створений новий правовий механізм застосування кримінального закону, якщо завгодно – новий порядок притягнення до кримінальної відповідальності. Інший, ніж той, що склався в умовах слідчого процесу, централізованої слідчо-обвинувальної влади і її монополії на формування підстав правозастосовних актів» [1].

Одним із ключових аспектів цифрової трансформації є створення та впровадження єдиних інформаційно-аналітичних систем у діяльність правоохоронних органів. Такі системи забезпечують обмін даними між підрозділами, доступ до криміналістичних обліків, баз ДНК-профілів, дактилоскопічних, фото- та відеоархівів. Вони формують цифровий простір доказів, що дозволяє швидко ідентифікувати осіб, транспортні засоби, зброю чи інші об’єкти.

Про цифрову криміналістику веде мову К. Латиш, зазначаючи, що сьогодні не лише в Україні, а й в багатьох країнах світу спостерігається тенденція формування та застосування нового наукового напряму – цифрової криміналістики (Digital Forensics, Digital Forensic Science or Digital Criminalistics) [2, с. 31–37]. Щоправда, в цій її публікації не вказано на те, йдеться тут про окремий і самостійний науковий напрям чи новий напрям в межах розвитку всіх розділів традиційної для нас науки криміналістики. Адже питання розслідування комп’ютерних злочинів, збирання й використання в доказуванні цифрових доказів, експертного дослідження цифрових технічних

засобів та інших комп'ютерних об'єктів стосуються у повній мірі і теоретичних основ криміналістики як науки, і криміналістичної техніки, і тактики, і методики розслідування окремих видів злочинів. Вітчизняними дослідниками зазначених питань використовуються й інші терміни: «комп'ютерна криміналістика» [3, с. 29–30], «електронна криміналістика» [4, с. 79] та ін.

Важливим напрямом є використання штучного інтелекту, машинного навчання та аналітики великих даних (Big Data) у криміналістиці. Ці технології дають змогу автоматизувати процеси обробки доказової інформації, встановлювати закономірності злочинної поведінки, прогнозувати можливі дії злочинців, а також виявляти зв'язки між подіями, які раніше залишалися поза увагою слідства.

Суттєвого значення набуває цифрова криміналістика (digital forensics), що охоплює виявлення, фіксацію, аналіз і збереження цифрових слідів злочину. Вона включає дослідження комп'ютерних систем, мобільних пристроїв, електронної пошти, мережевих журналів, криптографічних даних тощо. Саме цифрові сліди стають дедалі частіше ключовими доказами у справах про кіберзлочини, шахрайство, незаконне втручання в інформаційні ресурси чи фінансові махінації.

Цифрова криміналістика є «однією з галузей криміналістики, яка зосереджена на кримінально-процесуальному праві і доказах стосовно комп'ютерів і пов'язаних з ними пристроїв» [5, с. 29]

Окремої уваги потребує забезпечення кібербезпеки та захисту інформації, отриманої в ході слідчої діяльності. Використання електронних баз даних і віддалених доступів створює нові ризики несанкціонованого втручання, витоку персональних даних або підроблення цифрових доказів. Тому цифрова трансформація криміналістики має супроводжуватися розробкою ефективних механізмів контролю та верифікації цифрової інформації.

Перспективним є впровадження інтегрованих платформ електронного

кримінального провадження, що об’єднують інструменти збору, зберігання й аналізу доказів, дозволяючи здійснювати досудове розслідування у цифровому середовищі. Це сприяє зменшенню бюрократичних процедур, підвищенню прозорості та підзвітності дій слідчого.

Таким чином, цифрова трансформація криміналістики є закономірним етапом розвитку правозастосовної діяльності в інформаційну епоху. Вона потребує не лише технічного переоснащення, а й переосмислення методологічних підходів до розслідування злочинів, підготовки кадрів, формування нової цифрової культури в органах правопорядку.

Цифрова криміналістика включає в себе процеси ідентифікації, отримання, збереження, аналізу та подання цифрових доказів. Цифрові докази повинні бути автентифіковані, щоб забезпечити їх допустимість в суді. В кінцевому рахунку артефакти для судово-експертного аналізу та використовувані криміналістичні методи (наприклад, збір даних в статичному режимі або в режимі реального часу) залежать від пристрою, його операційної системи та його засобів захисту. Запатентовані операційні системи (з якими слідчі можуть бути незнайомі) і засоби захисту (наприклад, шифрування) служать перешкодами для проведення цифрової судової експертизи. Наприклад, шифрування, яке блокує доступ третіх осіб до інформації про користувачів і їх повідомленнями, може завадити правоохоронним органам отримати доступ до даних, що містяться в цифрових пристроях, таких як смартфони. Втім, цифрова криміналістика в розвинутих країнах розвивається стрімкими темпами і гідно протистоїть поширенню кіберзлочинності. Не є винятком і наша країна. Зокрема, в складі національної поліції ще декілька років тому було створено спеціальний підрозділ з боротьби з кіберзлочинністю. Проте для того, щоб вітчизняні правоохоронні органи дійсно могли використовувати весь спектр можливостей, які надають сучасні технології, необхідно якомога швидше завершити процес інтеграції вітчизняних правоохоронних структур в європейський простір.

Список використаних джерел:

1. Власова С. В. К вопросу о приспосабливании уголовно-процессуального механизма к цифровой реальности. Библиотека криминалиста. Научный журнал. 2018. № 1. С. 9–18. URL: https://www.iuaj.net/node/2433 (дата звернення 15.09.2025)

2. Латиш К. Цифрова криміналістика у період війни в Україні: можливості використання спеціальних знань у сфері інформаційних технологій. Kriminalistika ir teismo ekspertologija : mokslas, studijos, praktika: XVIII, 2022. Т. 18. С. 31–37.

3. Полотаї О.І. Комп'ютерна криміналістика: основні завдання та проблеми. Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення: матеріали міжн. наук. конф. Тернопіль. Вип. 68. 2022. С. 29–30.

4. Заєць І.С. Перспективи криміналістики в умовах інформатизації суспільства. Актуальні питання виявлення та розкриття злочинів Національною поліцією: вітчизняний та зарубіжний досвід : матеріали Міжнар. наук.-практ. круглого столу (Київ, 19 лют. 2020 р.). Київ : НАВС, 2020. С. 77–81.

5. ISO/IEC 27037:2012 Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence. URL: https://www.iso.org/standard/44381.html (дата звернення 25.09.2025)

ГРУЗДЬ Олександр
завідувач кафедри кримінального процесу та криміналістики факультету підготовки фахівців для органів досудового розслідування Національної поліції України
Донецького державного університету внутрішніх справ

БЕРЕЗА Юлія
курсант 401/22КР-(П)-Б навчального взводу факультету підготовки фахівців для органів досудового розслідування Національної поліції України Донецького державного університету внутрішніх справ, рядовий поліції

ЦИФРОВІ ДОКАЗИ : ПОНЯТТЯ ТА ЗНАЧЕННЯ . ВАЖЛИВІСТЬ ЇХ ВИВЧЕННЯ ДЛЯ КРИМІНАСЛІСТИКИ В УМОВАХ ВОЄННОГО СТАНУ.

В умовах стрімкої комп'ютеризації суспільства та значного збільшення кількості правовідносин в інформаційному просторі з'явився якісно новий вид кримінальних доказів — цифрова (електронна) інформація, яка має в своїй основі дані, представлені в дискретному вигляді [7, с. 178]. Ця тенденція, за словами Метелева О.П., ставить перед кримінально-процесуальною наукою нагальне завдання законодавчого врегулювання способів та процедури отримання цифрових відомостей, з урахуванням дотримання вимог належності, допустимості, достовірності та достатності [7, с. 178].

У криміналістичній теорії для позначення цього явища активно використовується термін «цифрові сліди». Демидова Є.Є. визначає їх як специфічний вид даних, що виникають внаслідок використання інформаційних технологій під час вчинення кримінальних правопорушень [5, с. 72]. Вона акцентує увагу на відсутності єдиної термінології, що обумовлено швидким розвитком технологій [5, с. 72]. У свою чергу , Яна Найдьон наголошує на важливості вміти правильно виявляти, закріплювати та вилучати нові маловивчені «віртуальні сліди» на початковому етапі розслідування, поряд із традиційними [4, с. 306].

Унікальність цифрових слідів визначає їхнє особливе значення у доказуванні , яке полягає в декількох аспектах . А саме в тому , що по-перше

вони не мають звичної матеріальної форми і існують у цифровому просторі, виявляючись лише за допомогою спеціального обладнання [5, с. 73]. По-друге ці сліди схильні до віддаленої зміни чи знищення, що вимагає, як зауважує Демидова Є.Є., особливих правил виявлення для гарантування їхньої цілісності та автентичності [5, с. 74]. Волокітенко О.М. підтверджує, що електронні дані набагато легше змінити чи підробити, ніж традиційні форми доказів [6, с. 18].

Зважаючи на цю вразливість, процедура вилучення (фізичне відділення об'єкта чи виготовлення з нього копій) набуває вирішального значення. Метелев О.П. обґрунтовує необхідність виділення в окремі слідчі дії таких, як «цифровий (електронний) огляд інформаційного середовища» і «цифрове (електронне) копіювання» [7, с. 179]. Климчук М.П. та Кунтій А.І. розглядають електронне копіювання інформації як ключовий пізнавальний прийом під час огляду, зокрема, засобів стільникового зв'язку, що вимагає залучення фахівця та спеціалізованих технічних засобів [3, с. 115]. Для забезпечення допустимості доказів обов'язковим є дотримання стандартів, зокрема ДСТУ ISO/IEC 27037:2017 [6, с. 17], та фіксація способу вилучення та пакування в протоколі слідчої дії .

В умовах військової агресії та введеного правового режиму воєнного стану в Україні (відповідно до Закону України «Про правовий режим воєнного стану» [1]), критична роль цифрових доказів зростає багаторазово, оскільки вони стають основним джерелом фіксації подій, що мають ознаки воєнних злочинів.

Цифрові сліди у вигляді метаданих, листування, фото- та відеофіксації, отримані з засобів стільникового зв'язку та інших електронних носіїв [3, с. 114], є незамінними для встановлення хронології, місцезнаходження, командних ланцюгів та намірів. Нікішев О.В. зазначає, що в умовах надзвичайних правових режимів цифрові докази можуть компенсувати відсутність традиційних форм доказів [2, с. 369]. Деревягін О.О. підкреслює, що досвід використання електронних (цифрових) доказів є

важливим напрямом для зростання позитивного тренду у протидії кримінальним протиправностям в умовах воєнного стану [8, с. 50].

Особливої ваги набуває верифікація та процесуалізація цифрової інформації, отриманої з відкритих джерел (OSINT) [2, с. 368]. Нікішев О.В. вказує, що OSINT-розслідування стали інституціоналізованим підходом, який вимагає нормативного закріплення, а OSINT має бути визнаний повноцінним доказовим інструментом [2, с. 370].

Для забезпечення допустимості доказів як на досудовому розслідуванні , судовому провадженні та міжнародних судових інстанціях, де цілісність даних ставиться під особливий сумнів через легкість їх підробки [6, с. 18], необхідно суворо дотримуватись принципів Chain of Custody (ланцюг зберігання) та міжнародних стандартів [2, с. 370].

Таким чином, в умовах воєнного стану, коли доказова база воєнних злочинів значною мірою спирається на «доріжку цифрових слідів», для криміналістики вивчення та впровадження уніфікованих, науково обґрунтованих, міжнародно визнаних процедур збору, верифікації та процесуалізації цифрових доказів є стратегічно необхідним завданням.

Список використаних джерел:

1. Про правовий режим воєнного стану : Закон України від 12.05.2015 № 389-VIII : станом на 14 трав. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/389-19#Text (дата звернення: 12.10.2025).

2. Нікішев О. В. Цифрові (електронні) докази у кримінальному провадженні в умовах надзвичайних правових режимів. Право.UA. 2025. № 1. С. 365–371.

3. Климчук М. П., Кунтій А. І. Виявлення та вилучення слідів кримінальних правопорушень, учинених із використанням засобів стільникового зв’язку. Соціально-правові студії. 2020. Вип. 3 (9). С. 111–118.

4. Найдьон Я. Поняття та класифікація віртуальних слідів кіберзлочинів. Підприємництво, господарство і право. 2019. № 5. С. 303–307.

5. Демидова Є. Є. Цифрові сліди кримінального правопорушення: поняття та особливості. Науковий вісник Ужгородського Національного Університету. 2024. Вип. 85. Ч. 4. С. 71–75.

6. Виганяйло, С. М. Електронні цифрові докази в умовах воєнного стану / Виганяйло Світлана Миколаївна // Наука в умовах воєнного стану: пошуки, проблеми, перспективи розвитку: матер. Всеукр. наук.-практ. конф. молодих вчених (м. Дніпро, 3 трав. 2023 р.) / МВС України, Дніпропетров. держ. ун-т внутр. справ. – Дніпро : ДДУВС, 2023. – С. 17-19.

7. Метелев О. П. Збирання цифрової інформації як окремий спосіб отримання доказів під час кримінального провадження. Науковий вісник Ужгородського національного університету. 2020. Вип. 60. С. 177–180.

8. Деревягін О. О. Досвід використання електронних (цифрових) доказів за результатами оперативно-розшукової діяльності. 2024. С. 48–51.

Дерев'янко Крістіна
старший викладач кафедри адміністративного права і процесу
Навчально-наукового інституту підготовки фахівців для підрозділів превентивної діяльності Національної поліції України
Дніпровського державного університету внутрішніх справ,капітан поліції

ВИКОРИСТАННЯ БПЛА ЯК ІНОВАЦІЙНОГО МЕТОДУ РОЗСЛІДУВАННЯ ВОЄННИХ ЗЛОЧИНІВ ТА РЕАГУВАННЯ НА НАДЗВИЧАЙНІ ПОДІЇ

Сучасні умови повномасштабного вторгнення російської федерації на територію нашої держави дали потужний поштовх до перегляду ходу огляду місця події посадовими особами органів виконавчої влади, на яких покладено повноваження не лише несення служби в місцях, умовно

віддалених від бойових дій, а й у невідкладних ситуаціях, коли зволікання може нести тяжкі наслідки як для майна, так і для життя та здоров'я людей. Систематичні ракетні обстріли, в особливості цивільних об'єктів, відкрили нові грані огляду місця події, акцентуючи увагу на заходи в перші хвилини після прильотів ракет, коли постраждалі потребують екстреної допомоги, а ризик повторного ракетного удару в моменту повітряної небезпеки для рятувальників ще не минув. Саме в такий час приходять в нагоду сучасні технологічні здобутки: безпілотні літальні апарати та системи, а також їх оснащення додатковими девайсами для більш детальної оцінки масштабів завданої шкоди та характеру наслідків без якісних втрат.

В цілому, огляд місця події є одним із найважливіших етапів у розслідуванні воєнних злочинів. Від того, наскільки точно і швидко буде зібрана інформація, залежить якість подальших дій - від ухвалення негайних оперативних рішень до проведення криміналістичних експертиз. Завдяки своїм технічним можливостям дрони дозволяють проводити повітряну зйомку місця події з високою точністю та деталізацією, що є особливо корисним на великій або складнодоступній території, де традиційні методи огляду займають багато часу або становлять загрозу для людей. Відповідно до офіційної інформації Міністерства внутрішніх справ України, безпілотні літальні апарати є одним із найбільш перспективних напрямків у фіксації злочинів, які вчиняє країна-агресор, тож, на сьогоднішній день, вони активно використовуються для огляду місць подій та об'єктів, що зазнали руйнувань в результаті ракетних ударів, артилерійських обстрілів та бомбардувань [1].

Як підкреслили у своєму грунтовному дослідженні українські науковці Т. М. Івасишин та М. М. Ленський - інтеграція новітніх цифрових технологій у криміналістику відкриває принципово нові можливості у зборі, фіксації та аналізі доказової інформації. Безпілотники, оснащені високоякісними оптико-електронними засобами, здатні забезпечити оперативну та безконтактну фіксацію великих територій, важкодоступних ділянок і об'єктів із потенційно високим ризиком для життя учасників слідчих дій [2]. Дана думка спонукає

до дослідження не лише самого БПЛА, як окремого об’єкту, а й додаткових пристроїв та гаджетів, які можуть бути закріплені на корпусі апаратів і собою не тільки значно спрощують процедуру огляду місця події, а й роблять його якіснішим та незалежним від людського фактору.

Першим приладом, який є іноваційним проривом та сучасним допоміжним засобом у поліцейській діяльності варто згадати 3-D сканер, який може бути стаціонарним, встановлюватись в якості окремого пристрою безпосередньо на тіло безпілотного літального апарату або бути завантаженим як софт до програмного забезпечення для багатокадрової зйомки під час зльоту дрону з метою подальшої обробки відзнятого на дрон матеріалу задля створення якісної 3-D моделі місця події. Ця технологія дала поштовх у розвитку судової антропології, яка в умовах правового режиму воєнного стану набула нового контексту, вирішуючи проблемні питання у розслідуванні фактів виявлення масових поховань на деокупованих територіях, випадків геноциду та інших наслідків військових злочинів. Не можна не зауважити, що оснащення безпілотників GPS-модулями надали можливість з максимальною точністю визначати координати досліджуваних об’єктів та їх просторові характеристики без втручання людини, що є особливо важливим для збереження слідів злочину з метою якісного збору доказової бази.

Окремо варто згадати оптичні камери з інфрачервоними датчиками NIR, які працюють за принципом кількісного виявлення збільшеної концентрації хімічних речовин, притаманних для розкладання трупів (оксид азоту, формальдегід, фосфор та сірка). Дані прилади, встановлені на БПЛА допомагають встановити місцезнаходження захованого тіла за змінами в ґрунті та рослинах без фізичного втручання людини в місце події і значно економить часові ресурси на пошуки.

Ще одним важливим здобутком у розвитку криміналістики в розрізі цифровізації є мультиспектральна візуалізація. Як зауважують в своїй роботі науковці Тичина Д. М, Антощук А. О. та Перцев Р. В. спектральні дані, зібрані дроном, можна порівняти з існуючою базою даних, що допомагає

встановлювати зниклих безвісти і виявляти людські останки. Приклади каталогізованих спектральних даних включають зразки одягу у вологому та сухому стані, дані про колір шкіри та крові (як свіжої, так і витриманої) [3]. Досліджуючи цей феномен у криміналістиці варто звернути увагу на можливості сучасних камер, об'єктиви яких пропонують багатократне оптичне збільшення, а наявні функції штучного інтелекту допомагають працювати з температурними показниками виявлених об'єктів, виявляти задимлення, рух інших тіл поблизу, класифікувати людей, транспортні засоби, номерні знаки.

Окремою технологією, яку неодмінно варто згадати у розрізі надання першої допомоги постраждалим є тепловізійні прилади, які приєднуються на БпЛА і функціонально відіграють важливу роль у розслідуванні воєнних злочинів, особливо на місцях прильоту боєприпасів. Їх застосування дозволяє оперативно, точно й безпечно документувати наслідки атак, навіть у складних умовах. Як зауважує науковець Прокопенко Н.М. встановлення різних датчиків і пристроїв, таких як тепловізори, на БПЛА дозволяє виявити те, що неможливо побачити неозброєним оком [4]. Оскільки відповідно до Закону України «Про Національну поліцію» на поліцейських покладено завдання щодо вживання заходів, спрямованих на усунення загроз життю та здоров'ю фізичних осіб і публічній безпеці, що виникли внаслідок учинення кримінального, адміністративного правопорушення, безпілотник із тепловізором дозволяє провести первинне обстеження території без ризику для людей та вести моніторинг ситуації з безпечної відстані, не наражаючи поліцейських та рятувальників, які першими прибули на місце вибуху, на небезпеку [5]. Встановлення місцезнаходження постраждалих та поранених осіб, коли ризик повторного удару є високим, підвищує рівень швидкості та якості порятунку поранених, що є надзвичайно важливим в умовах підвищеного ризику.

З огляду на вищевикладене, можна кваліфікувати безпілотники як незамінний інструмент в умовах розслідування воєнних злочинів. В час, коли

інформація може бути сфальсифікована та прихована ворогом в результаті просування хибних наративів інформаційно-психологічні операції, БПЛА дають змогу зберегти незаперечні факти у боротьбі держави за справедливість та досягнути найвищого рівня якісно зібраних доказів та зберегти життя особового складу, уповноваженого на первинне прибуття на місце події.

Список використаних джерел:

1. Офіційна інформація Міністерства внутрішніх справ, 2024, URL: https://mvs.gov.ua/news/nacionalna-policiia-otrimala-vid-ssa-novii-paket-dopomogi-dlia-dokumentuvannia-zlociniv-rf.

2. «Застосування безпілотних літальних в криміналістиці», Івасишин Т. М., Ленський М.М // Прикарпатський юридичний вісник, № 3, 2025, С.114-119.

3. «Криміналістичне забезпечення використання безпілотного літального апарату (дрону) у досудовому розслідуванні», Тичина Д. М, Антощук А. О. та Перцев Р. В // Науковий вісник Ужгородського Національного Університету, 2023, С. 291-297.

4. «Аналіз методів дослідження місць злочинів: порівняння традиційних і сучасних підходів до огляду та обробки місць злочинів», Прокопенко Н.М // Юридичний науковий електронний журнал, № 8, 2024, С. 423-426.

5. «Про Національну поліцію»: Закон України, (Відомості Верховної Ради (ВВР), 2015, № 40-41), від 02.07.2015 р. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text.

ДРОБЕНКО Діна
старший викладач кафедри кримінального процесу та криміналістики факультету підготовки фахівців для рганів досудового розслідування Національної поліції України Донецького державного

ІННОВАЦІЙНІ МЕТОДИ ТА КРИМІНАЛІСТИЧНІ ОСОБЛИВОСТІ РОЗСЛІДУВАННЯ НЕЗАКОННОЇ ПОРУБКИ, ПЕРЕВЕЗЕННЯ, ЗБЕРІГАННЯ ЧИ ЗБУТУ ЛІСУ, ВЧИНЕНИХ В УМОВАХ НАДЗВИЧАЙНИХ ПРАВОВИХ РЕЖИМІВ

Стримування збройної агресії російської федерації вносить певні корективи у роботу лісової галузі України. Через необхідність у забезпеченні військової галузі деревиною для облаштування оборонних укріплень, використанні у забезпеченні побутових умов. Також хочемо зазначити, що масова вирубка лісів, включаючи і незаконну, призводить до досить серйозних негативних змін клімату ,що у свою чергу суттєво впливає на забезпечення життєдіяльності. Таким чином можемо впевнено сказати, що охорона лісового фонду від вчинення правопорушень у сфері використання лісових ресурсів, особливо в умовах надзвичайних правових режимів, - є один із важливих завдань нашої держави.

Наведені обставини визначають нагальну потребу в активізації наукових досліджень проблематики розслідування кримінальних правопорушень щодо незаконної порубки або незаконного перевезення, зберігання, збуту лісу, у зв’язку з тим, що судово-слідча практика відчуває потребу в сучасній криміналістичній методиці спрямованій на підвищення ефективності досудового розслідування таких кримінальних правопорушень [1, с. 88].

Серед вітчизняних науковців значну увагу розслідуванню злочинів щодо незаконної порубки або незаконного перевезення зберігання, збуту лісу розглядаються у наукових працях таких вчених, як В.О.Одерій, Б.М, Марець, О.І. Агаркова, С.В. Головкін, Є. О. Письменський, І.А. Федчак та ін. Беручи ждо уваги погіршення криміногенної обстановки, змін кримінального процесуального законодавства, правозастосовної практики, а найголовніше – ведення активних бойових дій на значній території України, що у свою чергу ускладнюють проведення огляду місця події та інших слідчих (розшукових)

дій під час проведення розслідування щодо незаконної порубки лісу або незаконного перевезення, зберігання, збуту лісу.

Відповідно до ч. 1 ст. 237 КПК України слідчий, прокурор з метою виявлення та фіксації відомостей щодо обставин вчинення кримінального правопорушення проводять огляд місцевості, приміщення, речей, документів та комп'ютерних даних [2].

Хочемо зазначити, що під час огляду місця події слідчий має бути налаштований на уточнення досить широкого кола питань, які визначатимуть не лише об`єм та сукупність зібрані докази, але і визначатимуть напрямок проведення досудового розслідування, висунення слідчих версій, послідовність проведення першопочаткових та подальших слідчих (розшукових) дій. Зокрема, під час дослідження практики розслідування злочинів щодо незаконної порубки лісу або незаконного перевезення, зберігання, збуту лісу О.В. Одерій виділяє той факт, що місце події та конкретно його огляд слідчим мають виняткове значення для розслідування конкретного злочину, оскільки саме місце події містить значну інформацію про подію злочину й осіб, що його вчинили. Воно являє собою фрагмент об'єктивно існуючої події, де відбито її окремі сторони, моменти. Більшою або меншою мірою воно містить об'єктивну інформацію про подію злочину, виражену в зміні обстановки, слідах перебування злочинця, слідах його дій, їхніх наслідках, намірах злочинця та інших даних, що дозволяють побудувати уявну або частково матеріальну модель злочину, його обставин. Кожний злочин призводить до певних змін матеріальної обстановки, відображається у свідомості людей. Зміни в обстановці місця події можуть бути виявлені, зафіксовані, досліджені й використані як докази [3, с. 324-325]. Таким чином, на нашу думку огляд місця події на початку проведення досудового розслідування злочину, передбаченого ст. 246 КК України, є достатньо важливою та місткою слідчою (розшуковою) дією, особливо його проведення в умовах правового режиму воєнного стану.

Особливе значення має те, що на даний час, близько 1 млн. га лісів

знаходяться в окупації чи перебувають під впливом активних бойових дій, що у свою чергу значно ускладнює документування та фіксацію незаконної порубки лісу або незаконного перевезення, зберігання, збуту лісу. Саме тому розслідування незаконної порубки лісу в умовах надзвичайних правових режимів потребує інноваційних підходів, таких як використання GPS - трекерів, супутникових знімків та дронів для фіксації фактів, а також криміналістичних методів для встановлення походження деревини, її марки та часу заготівлі. Також необхідно враховувати особливості, спричинені надзвичайним станом, зокрема, обмежені можливості доступу до місць подій та ускладнений збір доказів, що вимагає застосування мобільних криміналістичних лабораторій та цифрових технологій.

Можемо зупинитися більш детально на деяких з інноваційних методів щодо збору доказів та проведення розслідування незаконної порубки, перевезення, зберігання чи збуту лісу, вчинених в умовах надзвичайних правових режимів.

На нашу думку можемо виділити використання супутникових знімків та використання геоінформаційних систем, їх доцільно застосувати для проведення моніторингу незаконних порубок та виявлення осередків, особливо у віддалених районах чи районах ведення бойових дій, чи так званих «сірих зонах». Застосування геоінформаційних систем дасть змогу для проведення аналізу даних про лісові масиви.

Використання безпілотних літальних апаратів (БПЛА) дасть змогу на дистанційне виявлення осередків незаконної вирубки лісів, що полегшить фіксацію цих фактів у важкодоступних місцях. Також на нашу думку БПЛА зможуть забезпечити збір цифрових зображень та відеоматеріалів, що можуть бути використані як докази. Це має важливе значення для проведення оцінки нанесеної шкоди.

Також варто зазначити основні сфери та задачі, які застосовують інформацію, отриману із використанням БПЛА: 1) моніторинг повітряного простору, земної й водної поверхонь; 2) розвідка; 3) екологічний контроль

(контроль стану лісів, запобігання екологічним катастрофам, тощо); 4) контроль морського судноплавства та керування повітряним рухом; 5) контроль переміщення людей, техніки; 6) ідентифікація тварин; 7) створення географічних інформаційних систем (ГІС) [4, с. 28].

На підставі вищевикладеного ми можемо зробити наступні висновки, що в умовах надзвичайних правових режимів інноваційні технології та адаптована криміналістична методика стають ключовими інструментами для виявлення та доказування злочинів, пов`язаних з незаконною порубкою, перевезенням, зберіганням чи збутом лісу [5, с.].

Список використаних джерел:

1. Агаркова О. І. Особливості проведення огляду під час розслідування незаконної порубки або незаконного перевезення, зберігання, збуту лісу в Україні / О. І. Агаркова // Knowledge, Education, Law, Management. - 2023. - № 2 (54). - С. 87-93.

2. Закон України від 13 квіт. 2012 р. № 4651-VI [Електронний ресурс]. — Режим доступу: https://zakon.rada.gov.ua/laws/show/4651-17 (дата звернення 01.10.2925).

3. Одерій О. В. Теорія і практика розслідування злочинів проти довкілля: монографія. Харків: Діса плюс, 2015. 528 с.

4. Альперт С. І. Використання безпілотних літальних апаратів для вирішення задач підсупутникового моніторингу в аерокосмічному комплексі [Електронний ресурс] / С. І. Альперт // Український журнал дистанційного зондування Землі. — 2020. — Т. 27. — С. 26–30. — Режим доступу: https://ujrs.org.ua/ujrs/article/download/184/203— DOI: 10.36023/ujrs.2020.27.184. (дата зверення 01.10.2025).

5. Письменський Є. О., Коваленко А. В., Пилипенко О. М. та ін. Досудове розслідування незаконної порубки або незаконного перевезення, зберігання, збуту лісу : практ. порадник / за ред. проф. В. В. Коваленка та проф. Є. О. Письменського. — Івано-Франківськ : Супрун В. П., 2023. — 204 с. —

[Електронний ресурс]. — Режим доступу: https://rep.dnuvs.ukr.education/items/cead84c0-b5a1-4000-88c6-daf267e34a81 (дата звернення 01.101.2025).

ДРОБЕНКО Діна
викладач кафедри кримінального процесу та криміналістики факультету підготовки фахівців для органів досудового розслідування Національної поліції України Донецького державного університету внутрішніх справ

МУКОСІЙ Єва
курсант 3 курсу факультету підготовки фахівців для органів досудового розслідування Національної поліції України Донецького державного університету внутрішніх справ

ЕФЕКТИВНІСТЬ ЗАСТОСУВАННЯ ПОЛІГРАФА У РОЗСЛІДУВАННЯХ ОРГАНІЗОВАНОЇ ЗЛОЧИННОСТІ: МЕТОДОЛОГІЯ, ОБМЕЖЕННЯ ТА ПРАКТИЧНІ РЕЗУЛЬТАТИ

Організована злочинність – найбільш суспільно небезпечна форма протиправної діяльності. Наявність організованої злочинності у суспільстві вкрай негативно впливає на його розвиток, деформуючи суспільні відносини. На сьогодні вже ні у кого не викликає сумнівів факт існування організованої злочинності в нашому суспільстві. Юристи, кримінологи, соціологи, психологи намагаються знайти оптимальні шляхи подолання цього явища чи принаймні досягти звуження його впливу. Фактором існування організованої злочинності є її те, що вона здатна до самодетермінації, тобто справляє зворотній негативний вплив на обставини, що її обумовлюють, у тому числі економіку, соціальну ситуацію, політику, духовну сферу тощо [1].

Сучасний поліграф – це комплекс точних медичних приладів, які безперервно та синхронно фіксують таку динаміку опитуваної особи, як тиск крові, частоту пульсу, глибину і частоту дихання, гальванічні реакції шкіри, ступінь м'язового напруження, біотоки мозку – разом близько 20 показників. Кількість різних показників, які реєструє і записує поліграф, називається кількістю його каналів [2]. Методологія проведення поліграфних досліджень включає кілька етапів:

1. підготовчий етап: ознайомлення з матеріалами, складання та конструювання запитань; з'ясування психічного та фізичного стану опитуваної особи; установлення з опитуваною особою психологічного контакту; отримання від особи письмової добровільної згоди на участь в опитуванні із застосуванням поліграфа; перевірка та налагодження датчиків і каналів знімання (фіксації) інформації поліграфа; установлення фонового рівня та типу реагування опитуваної особи;

2. етап безпосереднього проведення опитування: проведення опитування шляхом запитань, побудованих відповідно до мети завдання; поточний контроль психічного та фізичного стану опитуваного; виявлення можливої протидії та вжиття заходів щодо її нейтралізації; фіксація реагувань особи на запитання; попередній аналіз результатів інтерв'ю;

3. завершальний етап: аналіз результатів опитування; проведення післятестової бесіди з опитуваною особою; отримання від опитуваної особи письмової заяви про відсутність скарг після проведення опитування з використанням поліграфа; підготовка спеціалістом довідки про результати опитування з використанням поліграфа [3, с.22].

Для підвищення об'єктивності результати поліграфного тестування мають оцінюватися кваліфікованими фахівцями, які пройшли відповідну сертифікацію. У практиці правоохоронних органів України поліграф найчастіше застосовується при кадровому доборі, службових розслідуваннях, а також при перевірці свідчень учасників кримінальних проваджень.

У справах, пов'язаних із організованими злочинними угрупованнями,

поліграф може бути надзвичайно корисним інструментом. По-перше, він дозволяє виявити рівень поінформованості учасників про діяльність групи, структуру, ролі та злочинні наміри. По-друге, сприяє перевірці правдивості свідчень у ситуаціях, коли докази мають суперечливий характер. По-третє, допомагає встановити психологічний портрет учасника злочинного угруповання, його мотивацію, рівень причетності та психологічну готовність до співпраці зі слідством.

Використання поліграфа особливо ефективне на початкових етапах розслідування, коли необхідно швидко окреслити коло осіб, причетних до організованої діяльності, та виявити потенційні джерела оперативної інформації. Практика показує, що в поєднанні з криміналістичними методами аналізу поліграф підвищує результативність слідчих дій на 20–30%.

Чинний Кримінальний процесуальний кодекс України не містить законодавчого визначення поняття доказування. Натомість, у науковій літературі існують власні підходи до розуміння сутності доказування та надаються визначення цьому поняттю. кримінально-процесуальне доказування розглядають як практичну діяльність уповноважених законом суб'єктів, яка відбувається в особливій процесуальній формі, шляхом збирання, перевірки й оцінювання доказів; діяльність відповідних державних органів щодо збирання, перевірки й оцінки доказів, достовірне встановлення яких необхідне для правильного вирішення кримінального провадження, прийнято називати доказуванням [4].

Ефективність поліграфа у розслідуваннях організованої злочинності визначається не лише технічними характеристиками приладу, а й професіоналізмом поліграфолога, правильністю постановки запитань і комплексним поєднанням результатів із іншими криміналістичними методами.

Його основна перевага полягає у можливості швидко отримати психофізіологічні реакції, що свідчать про можливу неправдивість або приховування інформації, що особливо цінно у справах, де мовчання або

неправда є поширеним засобом самооборони злочинців.

Таким чином, можемо сказати, що - поліграф є ефективним допоміжним інструментом у розслідуваннях організованої злочинності, який, при належному нормативному регулюванні та професійному застосуванні, здатен істотно підвищити результативність розкриття злочинів і забезпечити новий рівень довіри до криміналістичних методик у правоохоронній діяльності.

Список використаних джерел:

1. Конопельський В. Я., «Поняття організованної злочинності та її запобігання», 2023р., URL: https://doi.org/10.32850/sulj.2023.3.9 (дата звернення 30.09.2025).

2. Ромців О. І., Зубач І. М., «Використання поліграфа в процесі подолання протидії розслідуванню злочинів у сфері службової діяльності: реалії сьогодення», 2015р., URL: https://science.lpnu.ua/sites/default/files/journal-paper/2017/jun/4926/romtsivzubach.pdf (дата звернення 30.09.2025).

3. Куценко Д.В., «Ініціювання проведення психофізіологічних досліджень із застосуванням поліграфа: метод. рек.», Нац. акад. внутр. справ, 2019 р., 52 с., URL: https://elar.navs.edu.ua/server/api/core/bitstreams/6b5e4e89-f3ab-4938-b110-fee6f92f3786/content (дата звернення 30.09.2025).

4. Кабанець О., «Використання комп'ютерного поліграфа (детектора брехні) у кримінальному провадженні через призму судової практики», 2023 р., URL: https://www.hsa.org.ua/blog/vikoristannia-kompiuternogo-poligrafa-detektora-brexni-u-kriminalnomu-provadzenni-cerez-prizmu-sudovoyi-praktiki (дата звернення 30.09.2025).

ЗАВГОРОДНІЙ Євген
суддя Фортечного районного суду міста Кропивницького

СЕНИЧАК Ольга

курсантка 3-го курсу
Донецького державного університету внутрішніх справ

ЕТИЧНІ ТА ПРАВОВІ МЕЖІ ЗАСТОСУВАННЯ ПОЛІГРАФА ПІД ЧАС ДОПИТІВ : ГАРАНТІЇ ПРАВ ЛЮДИНИ

Використання поліграфа у кримінальному процесі України є складним і суперечливим питанням, яке поєднує правові, етичні та психологічні аспекти. З одного боку, поліграфічне опитування може сприяти отриманню додаткової інформації у ході розслідування, з іншого — воно може створювати ризики порушення основоположних прав людини, зокрема права на справедливий судовий розгляд і недоторканність приватного життя.

Поліграф (детектор брехні) — це технічний засіб, який фіксує психофізіологічні реакції людини під час відповідей на запитання. Його метою є виявлення можливих ознак неправдивості або приховування інформації. У правозастосовній практиці поліграф використовується під час службових перевірок, добору персоналу [1, с. 142]. В Україні відсутнє законодавче врегулювання порядку застосування поліграфа у кримінальному провадженні, що породжує неоднозначність у тлумаченні його результатів.

Згідно зі ст. 84 Кримінального процесуального кодексу України (далі – КПК) доказами в кримінальному провадженні є фактичні дані, отримані у передбаченому цим Кодексом порядку, на підставі яких слідчий, прокурор, слідчий суддя і суд встановлюють наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження та підлягають доказуванню. Процесуальними джерелами доказів є показання, речові докази, документи, висновки експертів [2].

Відсутність урегульованості на законодавчому рівні створює проблеми практичного застосування зазначеного технічного засобу та результатів,

отриманих за його допомогою, як доказів у кримінальному судочинстві [3, с.689].

Попри це, судова практика свідчить, що деякі органи досудового розслідування використовують поліграф як допоміжний засіб орієнтації під час перевірки показань чи версій. Такий підхід не суперечить закону лише за умов проведення дослідження фаховим поліграфологом та наявності добровільної згоди особи на участь у ньому.

Використання поліграфа під час допитів зачіпає основоположні права та свободи людини. Стаття 28 Конституції України гарантує кожному право на повагу до гідності та забороняє піддавати особу катуванню чи іншому жорстокому, нелюдському або принизливому поводженню. Стаття 63 передбачає право особи не свідчити проти себе чи своїх близьких родичів. Отже, будь-яке примушення до проходження поліграфа без згоди може розцінюватися як порушення цих гарантій.

Положення Конвенції про захист прав людини і основоположних свобод (ст. 6, 8) також підкреслюють право кожного на справедливий суд і повагу до приватного життя. Європейський суд з прав людини (далі — ЄСПЛ) у своїй практиці неодноразово наголошував, що використання примусових психофізіологічних методів суперечить принципу справедливого судового розгляду. У рішенні у справі «Яллох проти Німеччини» Суд підкреслив, що навіть непрямий примус до самообвинувачення суперечить ст. 6 Конвенції [4].

Таким чином, поліграф може застосовуватися лише на добровільних засадах, без примусу чи обману, із забезпеченням права особи на юридичну допомогу та конфіденційність результатів дослідження. В іншому випадку його використання порушує засади кримінального процесу та принцип поваги до прав людини.

Питання етичності застосування поліграфа тісно пов’язане з морально-правовими межами втручання у внутрішній світ людини. Під час поліграфічного тестування фіксуються показники фізіологічного стану, що стосуються не лише поведінки, а й емоційної сфери особи. Таке втручання

може впливати на психічний стан допитуваного, створювати відчуття контролю та тиску, що є несумісним із принципом поваги до людської гідності.

Поліграф не може вважатися об'єктивним інструментом встановлення істини, адже фізіологічні реакції не завжди свідчать про неправдивість висловлювань. Наприклад, хвилювання, страх або стрес можуть спотворити результати обстеження. Таким чином, некритичне сприйняття поліграфа як «машини істини» створює ризики технологічного редукціонізму, коли складні психологічні процеси зводяться до фізичних показників організму.

Етична проблематика полягає й у тому, що поліграф може бути використаний не для пошуку істини, а для психологічного тиску на підозрюваного. Така практика суперечить основним засадам кримінального судочинства — зокрема, принципам презумпції невинуватості, змагальності сторін і недопустимості примусу до свідчення проти себе (ст. 17, 22 КПК України).

Законодавчі ініціативи щодо регламентації використання поліграфа в Україні, зокрема, під час кримінального провадження, наразі не були реалізовані [5, 6]. Це створює колізії у правозастосуванні, коли результати поліграфічних досліджень можуть бути сприйняті судами по-різному — від повного заперечення до врахування як додаткової інформації.

Судова практика засвідчує неоднозначність у ставленні до поліграфа. Частина суддів відмовляється приймати такі дані через сумнівну достовірність і можливість маніпуляцій результатами, інші ж розглядають їх як допоміжний доказ, який може підтвердити або спростувати певну версію. Проте жоден судовий акт не визнає поліграф як самостійний доказ вини.

Таким чином, застосування поліграфа під час допитів вимагає дотримання чітких правових та етичних меж. Умовами проведення досліджень є добровільна згода особи, поінформованість про мету та наслідки процедури, а також участь професійного фахівця, що відповідає встановленим вимогам [7, с. 121]. Необхідно уникати будь-яких форм примусу чи тиску, що

можуть порушити права, гарантовані Конституцією України та міжнародними договорами. Водночас держава має розробити чітке нормативне регулювання порядку використання поліграфа в кримінальному процесі, визначити статус його результатів і вимоги до здійснення відповідної діяльності. Такий підхід сприятиме балансу між інтересами правосуддя та гарантіями прав людини, забезпечуючи принципи законності, справедливості та гуманізму.\

Список використаних джерел:

1. Мінка Т.П. Використання поліграфа у світі: генеза становлення та тенденції розвитку. Держава та регіони. Серія: ПРАВО 2024 р., № 1(83), с. 141-144. URL: http://law.stateandregions.zp.ua/archive/1_2024/1_2024.pdf#page=141 (дата звернення: 06.10.2025).
2. Кримінальний процесуальний кодекс України : Закон України від 13 квітня 2012 р. № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 06.10.2025).
3. Курман О. В., Балибіна А. Р. Використання поліграфа при розслідуванні кримінальних правопорушень: проблеми тактики та правового регулювання. Аналітичне-порівняльне правознавство. 2024. № 2. С. 686–691.URL: http://journal-app.uzhnu.edu.ua/article/view/303746/295786 (дата звернення: 06.10.2025).
4. Комюніке Секретаря Європейського суду з прав людини стосовно рішення у справі Jalloh проти Німеччини [ВП] - 54810/00; рішення від 11.7.2006. URL: https://ips.ligazakon.net/document/SO2742 (дата звернення: 07.10.2025).
5. Проект Закону про доповнення Кримінального процесуального кодексу України положеннями щодо використання поліграфа (детектора брехні) від 3611 від 10.12.2015 URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=57349 (дата звернення: 07.10.2025).
6. Проект Закону України «Про поліграфологічну діяльність» // URL:

https://ips.ligazakon.net/document/JH35Q1AA (дата звернення 07.10.2025).

7. Шульженко А. В. Проблеми використання поліграфа під час кримінального провадження //Приватне та публічне право. – 2018. – №. 2. – С. 119-122. URL: http://www.pp-law.in.ua/archive/2_2018/27.pdf.

КВАШУК Олександр
старший викладач кафедри кримінального процесу та криміналістики факультету підготовки фахівців для органів досудового розслідування Донецького державного університету внутрішніх справ, кандидат юридичних наук

ПРОБЛЕМНІ ПИТАННЯ ДІЯЛЬНОСТІ ЛІТ ІЗ РОЗСЛІДУВАННЯ ЗЛОЧИНІВ ОРГАНІЗОВАНИХ ГРУП В УМОВАХ ЗБРОЙНОГО КОНФЛІКТУ

Розслідування злочинів, скоєних організованими групами (ОЗГ) в умовах збройного конфлікту (воєнні злочини, кіберзлочинність, шахрайство з гуманітарною допомогою, торгівля людьми, контрабанда зброї та культурних цінностей, які використовують міграційні потоки та кіберпростір тощо), вимагає транскордонного збору доказів та координації дій правоохоронних органів різних держав.

Спільні слідчі групи (Joint Investigation Teams, JIT) є важливим інструментом міжнародного співробітництва у галузі кримінального провадження, що дозволяє об'єднувати зусилля кількох держав для ефективного розслідування складних та багатоепізодних злочинів, які часто діють через кордони та використовують хаос збройних конфліктів у своїх цілях.

Збройний конфлікт ускладнює діяльність JIT через неможливість проведення слідчих дій на окупованих територіях та систему інших викликів логістичного та безпекового характеру, які безпосередньо впливають на ефективність розслідування злочинів організованих груп та транснаціональних кримінальних мереж, що діють в умовах агресії.

JIT є ключовим інструментом міжнародного співробітництва в кримінальному процесі для ефективного розслідування складних, багатоепізодних і транскордонних злочинів. Міжнародна співпраця у формі JIT нейтралізує часові та територіальні бар'єри, усуває багатотижневі бюрократичні затримки, характерні для традиційної міжнародної правової допомоги, та виконує функції оперативного обміну інформацією, координації доказової бази, узгодження інформаційних потоків і юрисдикцій. Це дозволяє уникнути паралельних розслідувань, знизити витрати ресурсів і прискорити кримінальне переслідування [1, с. 3].

Необхідність удосконалення законодавства щодо створення та діяльності JIT є одним із пріоритетних завдань правового забезпечення міжнародного співробітництва в кримінальному процесі.

На міжнародно-правовому рівні створення спільних слідчих груп передбачено Конвенцією ООН проти транснаціональної організованої злочинності (ст. 19), Конвенцією ООН проти корупції (ст. 49), Конвенцією ООН про боротьбу проти незаконного обігу наркотичних засобів і психотропних речовин (ст. 9) та іншими актами. Стандарти діяльності JIT викладено у ст. 13 Конвенції про взаємодопомогу в кримінальних справах

між державами-членами Європейського Союзу 2000 року та ст. 20 Другого додаткового протоколу до Європейської конвенції про взаємну допомогу у кримінальних справах (ратифікований Україною у 2011 році та набрав чинності 1 січня 2012 року) [2, 3]. Розвиток національного законодавства пов'язаний з імплементацією ратифікованих міжнародних актів та врахуванням нових інструментів, зокрема Любляно-Гаазької конвенції про міжнародне співробітництво в розслідуванні та притягненні до

відповідальності за геноцид, злочини проти людяності, воєнні злочини та інші міжнародні злочини [4, с. 71–72].

Зазвичай за потреби здійснити спільне розслідування сторони керуються типовою (модельною) угодою, яку в 2003 році було затверджено Радою Європейського союзу (2003/C 121/01). Ця модель є комплексною та гнучкою, що дозволяє її адаптувати до конкретних обставин кожної справи. Фахівці експертно-консультативної групи Ради Європи з підтримки Офісу Генерального прокурора України наголошують, що питання укладання угоди з компетентними органами заінтересованих іноземних держав про створення слідчої групи, а також визначення в такій угоді повноважень групи та строку, на який вона створюється, не передбачено чинним КПК [5].

Правове регулювання діяльності спільних слідчих груп в Кримінальному процесуальному кодексі України (далі - КПК) обмежене ст. 571, яка доволі лаконічно визначає процедурні аспекти створення та діяльності, що перешкоджає ефективному розслідуванню [6].

У КПК відсутні вказівки на службову особу, що уповноважена ухвалювати рішення про створення JIT, невизначеною залишається процедура визначення складу групи, включаючи її керівника [7, с. 246–248].

Повноваження відряджених членів JIT є нечіткими та обмеженими, що продукує невизначеність їхнього процесуального статусу. Можливість членів спільної слідчої групи за письмовим погодженням зі старшим такої групи проводити слідчі (розшукові) та інші процесуальні дії на території держави, де вчинено кримінальне правопорушення, або на території однієї з держав, компетентні органи якої є членами групи, якщо цього вимагають потреби досудового розслідування та судового провадження, КПК не передбачає [8, с. 150-151]. Згідно зі ст. 563 КПК вони можуть лише спостерігати за процесуальними діями, а не проводити їх самостійно, що ускладнює обмін інформацією, може уповільнювати оперативність спільної роботи, зумовлює непропорційне навантаження у спільному розслідуванні транснаціональних злочинів. Як зазначено у тіньовому звіті для Єврокомісії, основний тягар

розслідування міжнародних злочинів лежить на українській системі, а залучення JIT гальмується через брак регламентації в КПК [9].

Розслідування на межі юрисдикцій містить потенціал порушень гарантій прав учасників провадження, які передбачені КПК, включаючи неконтрольований обіг персональних даних у JIT, що потребує уваги законодавця. Окремою проблемою є відсутність регламентації процедур, пов'язаних із використанням під час діяльності JIT інформації, що містить державну таємницю.

Однією з перешкод для використання результатів JIT у національних судах є колізія між стандартами прийнятності доказів у різних юрисдикціях, що створює ризик визнання їх недопустимими [8]. Критично важливим є узгодження норм КПК з міжнародними стандартами та практичними потребами ефективного досудового розслідування JIT. Усунення прогалин вимагає законодавчих змін, зокрема розгляду зареєстрованого ще 29.04.2022 проекту Закону України «Про внесення змін до КПК щодо удосконалення діяльності спільних слідчих груп», реєстр. номер 7330 [10].

03.09.2025 законопроект включено до порядку денного парламенту, що дає підстави сподіватися на швидке приведення КПК у відповідність до міжнародних вимог з метою забезпечення дієвості розслідувань JIT із урахуванням висловлених стосовно нього фахових зауважень [1, 9, 10].

Таким чином, діяльність JIT є ключовим інструментом, що перетворює міжнародний обмін інформацією з бюрократичного процесу на динамічний і дієвий організаційно-правовий механізм розслідування злочинів ОЗГ в умовах збройного конфлікту. Ефективність спільних розслідувань зумовлена подоланням комплексу об'єктивних та суб'єктивних факторів, у тому числі недостатньої регламентації на законодавчому рівні. Потреба забезпечення надійної правової основи діяльності спільних слідчих вимагає гармонізації із міжнародними стандартами, у тому числі, використання правового досвіду ЄС, нормативного удосконалення процесуального статусу та повноважень іноземних слідчих, вирішення питань про колізію стандартів допустимості

доказів, використання інформації, що містить державну таємницю, та забезпечення процесуальних гарантій прав та свобод учасників провадження.

Список використаних джерел:

1. Експертний висновок експертно-консультативної групи Ради Європи з підтримки Офісу Генерального прокурора України щодо проєкту Закону України «Про внесення змін до Кримінального процесуального кодексу України щодо удосконалення діяльності спільних слідчих груп». URL: https://rm.coe.int/coe-expert-opinion-ua-joint-investigative-teams-draft-law-7330-ukr/1680a71abd.

2. Конвенція про взаємну правову допомогу у кримінальних справах між державами-членами Європейського Союзу від 29 травня 2000 року. URL: https://zakon.rada.gov.ua/laws/show/994_415.

3. Другий додатковий протокол до Європейської конвенції про взаємну допомогу у кримінальних справах від 20 квітня 1959 року. URL: https://zakon.rada.gov.ua/laws/show/994_518#Text .

4. Гловюк І. В. Спільні слідчі групи за Любляно-Гаазькою конвенцією та КПК України. Збірник тез Міжнародної науково-практичної конференції (3 листопада 2023 року). Львів, 2023. с. 68–72. URL: file:///C:/Users/krlaw/Downloads/Hlovjuk_2%20(2).pdf.

5. Робота спільної слідчої групи в процесі документування злочинів рф: воєнний досвід України. JustTalk. 2024. URL: https://justtalk.com.ua/post/robota-spilnoi-slidchoi-grupi-v-protsesi-dokumentuvannya-zlochiniv-rf-voennij-dosvid-ukraini.

6. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 № 4651-VI. Офіційний вісник України. 2012. № 34. URL: https://zakon.rada.gov.ua/laws/show/4651-17 .

7. Красноборова А. А. Спільні слідчі групи: актуальні питання правового регулювання. Юридичний науковий електронний журнал. 2020. № 3. с. 58–63. URL: http://lsej.org.ua/3_2020/61.pdf.

8. Тіньовий звіт до розділу 23 «Правосуддя та фундаментальні

права» Звіту Європейської комісії щодо України у 2023 році. с. 149-151. URL: https://zmina.ua/wp-content/uploads/sites/2/2024/09/tinovyj-zvit-rozdil-23-yes-ukrayina.pdf.

9. Недоліки КПК щодо роботи іноземних слідчих груп заважають ефективному розслідуванню міжнародних злочинів в Україні – тіньовий звіт для Єврокомісії. ZMINA.info. 2024. URL: https://zmina.info/news/nedoliky-kpk-pro-robotu-inozemnyh-slidchyh-grup-zavazhayut-efektyvnomu-rozsliduvannyu-mizhnarodnyh-zlochyniv-v-ukrayini-tinovyj-zvit-dlya-yevrokomisiyi/.

10. Про внесення зміни до Кримінального процесуального кодексу України щодо удосконалення діяльності спільних слідчих груп: проєкт Закону України, реєстраційний № 7330 від 29.04.2022. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/39520.

КОМІСАРЧУК Руслан
кандидат юридичних наук, доцент, доцент кафедри кримінально-правових дисциплін Інституту права та безпеки Одеського державного університету внутрішніх справ (м, Одеса, Україна).

ОСОБЛИВОСТІ СТАНОВЛЕННЯ ЦИФРОВОЇ КРИМІНАЛІСТИКИ В УКРАЇНІ

Сучасні технології радикально змінюють природу злочинності. З поширенням Інтернету, цифрових пристроїв та онлайн-сервісів з’являються нові загрози: кіберзлочини, інформаційні атаки та злочини воєнного характеру. Це вимагає від системи протидії злочинності швидкої адаптації та інтеграції сучасних технологій у криміналістичну практику [1-4], оскільки, цифрова криміналістика забезпечує ефективне виявлення, фіксацію та дослідження електронних доказів, що стають ключовими у розслідуванні

таких злочинів. В умовах війни та євроінтеграційних процесів в Україні її роль особливо актуальна.

Мета дослідження – означити особливості становлення цифрової криміналістики в Україні. Тому, завдання дослідження: визначити концептуальні та методологічні основи цифрової криміналістики; проаналізувати законодавче та нормативне забезпечення роботи з цифровими доказами; дослідити практику застосування цифрових криміналістичних методик в Україні; оцінити перспективи розвитку освітніх та тренінгових програм для фахівців.

Цифрова криміналістика формується в Україні, як окрема галузь, що інтегрує класичні методи дослідження доказів із сучасними інформаційними та комп'ютерними технологіями. Її об'єкти – цифрові дані та інформаційні системи, включно з комп'ютерами, серверами, мобільними пристроями, мережевими ресурсами, електронними комунікаціями та хмарними сервісами, що використовуються у злочинній діяльності [5-8].

На наш погляд, основні завдання цифрової криміналістики можна визначити наступним чином: 1) виявлення та збереження цифрових доказів – забезпечення їх достовірності, цілісності та відповідності законодавству для використання в суді; 2) аналіз закономірностей електронної злочинної діяльності – встановлення методів, технологій та взаємозв'язків між діями учасників злочинних схем; 3) забезпечення доказової сили цифрових слідів – формування методично коректного результату, що може бути використаний як допустимий і переконливий доказ у суді.

На даний час цифрова криміналістика поєднує криміналістичні, інформаційно-технічні та правові знання, формуючи спеціалізовану методологічну базу для роботи з новими об'єктами та доказами. Серед основних методів: аналіз журналів доступу, атрибуція дій у мережевому середовищі, відновлення видалених файлів, ідентифікація цифрових підписів для підтвердження автентичності документів та транзакцій.

У практичній діяльності фахівці застосовують програмні комплекси

цифрової криміналістики, криптографічні засоби та інструменти аналізу мережевих слідів. Значну роль відіграють алгоритми штучного інтелекту [9-12], що автоматизують виявлення закономірностей і аномалій у великих даних.

Правове регулювання цифрової криміналістики в Україні базується на: Кримінальному процесуальному кодексі України [13], Законі України «Про електронні документи та електронний документообіг» [14], нормативних актах МВС, ДБР, СБУ та міжнародних стандартах ISO/IEC 27037 [15], 27041[16], 27042 [17].

На початковому етапі розвитку відбувалося відкриття перших лабораторій комп'ютерної експертизи, розробка методичних рекомендацій і поява перших наукових публікацій. У 2010–2020 рр. спостерігалося впровадження міжнародних стандартів підготовки фахівців, розширення сфер застосування цифрової криміналістики та формування тренінгових центрів.

У воєнний період (з 2022 р.) пріоритети змінилися: зросла кіберзлочинність, цифрова криміналістика інтегрується з військовою та інформаційною безпекою, розвиваються спеціалізовані полігони у Дніпрі, Києві та Харкові.

Тому, професіографічна підготовка фахівців, на даний час, передбачає знання ІТ-технологій, навички аналізу цифрових слідів і атрибуції дій користувачів. Для формування компетентностей застосовуються тренінги, криміналістичні полігони, лабораторні роботи, проектна діяльність та стажування. Також сучасна освіта використовує дистанційне та змішане навчання, інтерактивні моделі, цифрові платформи та симуляційні середовища.

Відповідно, розвиток цифрової криміналістики стикається з низкою викликів: кадровими та організаційними – нестача експертів, обмежені лабораторні ресурси та ПЗ; технічними та методологічними – складність відновлення та захисту цифрових доказів, відсутність єдиної національної методології; правовими та етичними – забезпечення законності збору доказів, баланс між правами людини та ефективністю розслідування, використання

цифрових доказів у судовій практиці та міжнародних справах.

Враховуючи вищезазначене, вважаємо, що перспективи розвитку пов’язані з розширенням сфер застосування: кіберзахисту державних і стратегічно важливих об’єктів, інтеграція штучного інтелекту, блокчейн-рішень та автоматизованих систем аналізу даних для підвищення ефективності збору та аналізу цифрових доказів. Розвиваються національні та міжвідомчі цифрові платформи для обміну доказами та координації дій. Щодо останнього аспекту, то, особливої уваги заслуговує Міжнародна координація, що передбачає гармонізацію стандартів із практиками ЄС та інших країн [18], спільні науково-освітні проєкти та обмін методиками і кращими практиками.

Висновки. Таким чином, цифрова криміналістика в Україні формується як самостійна галузь, що поєднує класичні криміналістичні знання з сучасними технологіями. Її розвиток визначають виклики кібербезпеки, військові загрози та євроінтеграційні процеси, що потребують удосконалення методології, підготовки фахівців та законодавчого регулювання. Перспективи пов’язані з розширенням сфер застосування, інтеграцією штучного інтелекту та автоматизованих систем аналізу даних, а також розвитком національних і міжвідомчих цифрових платформ. Міжнародна координація та спільні науково-освітні проєкти забезпечать, в даному напрямку, відповідну гармонізацію стандартів, підвищення якості цифрових доказів і їхню прийнятність у міжнародних кримінальних провадженнях.

Список використаних джерел:

1. Використання цифрових технологій у криміналістиці та судовій експертизі : матеріали міжнар. наук.-практ. круглого столу, м. Харків, 11 груд. 2023 р. : електрон. наук. вид. / редкол.: В. Ю. Шепітько, Г. К. Авдєєва; Нац. акад. прав. наук України; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса НАПрН України. Харків : Право,2024. 144 с.

2. Дуфенюк О.М. Майбутнє 3D криміналістики: інновації, які змінюють практику досудового розслідування. Юридичний електронний

журнал. 2024. № 3. С. 457–460.

3. Комісарчук Р.В. Аналітична парадигма криміналістичної технології /Р.В. Комісарчук // Visegrad Journal on Human Rights. - № 2 . – 2018. – С. 81-85.

4. Комісарчук Р.В. Інформаційно-технологічна парадигма криміналістики /Р.В. Комісарчук. // Матеріали VI Міжнародного круглого столу «Інформаційне забезпечення розслідування злочинів» (м. Одеса, 25 травня 2018 року.). - Одеса. 2018. С. 57-61.

5. Інноваційні методи та цифрові технології в криміналістиці й судо вій експертизі : монографія / [В. Ю. Шепітько, Г. К. Авдєєва, В. М. Шев чук та ін.] ; за заг. ред. В. Ю. Шепітька ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса Нац. акад. прав. наук України. – Харків : Право, 2024. – 208 с.

6. Латиш К. Цифрова криміналістика у період війни в Україні: можливості використання спеціальних знань у сфері інформаційних технологій. Criminalistics and Forensic Expertology: Science, Studies, Practice. XVIII International Congress. Vil nius, 2022. P. 31–37

7. Полотай О. І. Використання комп’ютерної криміналістики для забезпе чення ефективного розслідування інцидентів інформаційної та кібербезпеки. Вісник ЛДУБЖД. Bulletin of Lviv State University of Life Safety. 2023. № 28. С. 73–80

8. Степанюк Р. Л. Цифрова криміналістика й удосконалення системи криміналістичної техніки в Україні. Вісник ЛДУВС ім. Е. О. Дідоренка. 2022. Вип. 3 (99). С. 283–294.

9. Демура М. І., Клепка Д. І. Перспективи застосування штучного інтелекту у галузі кримінального судочинства. Юридичний науковий юридичний журнал. 2022. № 5. С. 554–558. DOI: https://doi.org/10.32782/2524–0374/2022–5/133; URL: http://lsej.org.ua/5_2022/133.pdf

10. Колесніков А. П. Штучний інтелект в запобіганні та розслідуванні злочинів. Наукові записки. Серія: Право. 2023. Вип. 15. С. 292–295. DOI: 10.36550/2522-9230-2023-15-292-295 URL: https://pravo.cusu.edu.ua/index.php/

pravo/article/view/381/392

11. Чайковський Д. Штучний інтелект як новий інструмент для боротьби зі злочинами у сфері економіки. Юридичний вісник. 2023. № 6. С. 335 342. DOI: https://doi.org/10.32782/yuv.v6.2023.41

12. Ліхтанська А. П., Михайлов В. О. Практичне застосування штучного інтелекту у кримінальному провадженні. DICTUM FACTUM: Юридичний збірник. 2024. № 1(15). С. 120–125. URL: https:// df.duit.in.ua/index.php/dictum/article/view/32.

13. Кримінальний процесуальний кодекс України від 13.04.2012 р. № 4651-VI (зі змін. та допов.). URL : https://zakon.rada.gov.ua/laws/show/4651-17

14. Про електронні документи та електронний документообіг : Закон України від 22 травня 2003 № 851-IV. URL : https://zakon.rada.gov.ua/laws/show/851-15#Text

15. ДСТУ ISO/IEC 27037:2017 Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів (ISO/IEC 27037:2012, IDT). URL : https://online.budstandart.com/ua/catalog/doc-page?id_doc=74978

16. ДСТУ EN ISO/IEC 27041:2022 Інформаційні технології. Методи захисту. Настанова щодо забезпечення прийнятності та адекватності методів розслідування (EN ISO/IEC 27041:2016, IDT; ISO/IEC 27041:2015, IDT). URL :https://www.google.com/search?q=%D0%BC%D1%96%D0%B6%D0%BD%D0%B0%D1%80%D0%BE%D0%B4%D0%BD%D0%B8%D1%85+%D1%81%D1%82%D0%B0%D0%BD%D0%B4%D0%B0%D1%80%D1%82%D0%B0%D1%85+ISO%2FIEC+27041&sca_esv=9e604a3141a4b337&ei=LJPiaL2QDqCQxc8Pjqz0wQs&ved=0ahUKEwi91raRtI2QAxUgSPEDHQ4WPbgQ4dUDCBE&uact=5&oq=%D0%BC%D1%96%D0%B6%D0%BD%D0%B0%D1%80%D0%BE%D0%B4%D0%BD%D0%B8%D1%85+%D1%81%D1%82%D0%B0%D0%BD%D0%B4%D0%B0%D1%80%D1%82%D0%B0%D1%85+ISO%2FIEC+27041&gs_lp=Egxnd3Mtd2l6LXNlcnAiOdC80ZbQttC90LDRgNC-0LTQvdC40YUg0YHRgtCw0L3QtNCw0YDRgtCw0YUgSVNPL0lFQyAyNzA0

MTIIEAAYgAQYogQyBRAAGO8FMggQABiABBiiBDIFEAAY7wUyCBAAGI
AEGKIESJVPUP8GWPxHcAF4AJABAJgBkgWgAc0cqgELMC45LjIuMS4yLjG
4AQPIAQD4AQGYAgugAoEOwgIIEAAYsAMY7wXCAgsQABiABBiwAxiiBJ
gDAIgGAZAGBZIHBzEuNy4yLjGgB9lIsgcHMC43LjIuMbgH9A3CBwUwLjIu
OcgHMg&sclient=gws-wiz-serp

17. ДСТУ ISO/IEC 27042:2016 Інформаційні технології. Методи захисту. Настанови щодо аналізу та інтерпретації цифрового доказу (ISO/IEC 27042:2015, IDT). URL : https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=67149

18. Шевчук В. М. Цифрові технології та європейський вектор розвитку криміналістики під час війни. Використання цифрових технологій у криміналістиці та судовій експертизі : матеріали міжнар. наук.-практ. круглого столу, м. Харків, 11 груд. 2023 р.: електрон. наук. вид. / [редкол.: В. Ю. Шепітько, Г. К . Авдєєва] ; Нац. акад. прав. наук України ; НДІ вивч. проблем злочинності ім. акад. В. В. С ташиса НАПрН України. Харків: Право, 2024. С.133–136.

КРИВДЮК Сергій
Перший заступник керівника Криворізької центральної окружної прокуратури

ГЛУЩЕНКО Владислав
курсант 401/22КР-(П)-Б навчального взводу факультету підготовки фахівців для органів досудового розслідування Національної поліції України Донецького державного університету внутрішніх справ

ВИКОРИСТАННЯ ПОЛІГРАФА У БОРОТЬБІ З ОРГАНІЗОВАНОЮ ЗЛОЧИННІСТЮ

У боротьбі з організованою злочинністю одним із потенційно корисних інструментів виступає поліграф — спеціальний психофізіологічний технічний засіб, який здійснює реєстрацію динаміки протікання не менше п’яти незалежних психофізіологічних процесів людини у відповідь на пред’явлення за спеціальною методикою певних психологічних стимулів, не завдаючи шкоди життю, здоров’ю людини та навколишньому середовищу [1]. Проте, ефективність та правомірність його використання залежить від чіткого нормативного забезпечення, методологічних гарантій і дотримання прав людини. Згідно національного стандарту ДСТУ 8692:2016 «Поліграфи. Технічні умови» встановлено технічні вимоги та основні параметри до апаратури поліграфа, загальні вимоги, вимоги до безпеки, вимоги щодо охорони довкілля та інші аспекти [2]. Це дає нормативну основу для того, щоб прилад, що називається «поліграф», відповідав певним мінімальним стандартам. І саме з цього можна дійти висновку, що тільки поліграфи, які повністю відповідають ДСТУ 8692:2016, визнаються як допустимі для проведення експертизи, а ті, що не відповідають стандарту, легко можуть бути оскаржені як недопустимі у суді.

У законодавчій площині в Україні існують інструкції щодо застосування поліграфа у діяльності окремих органів. Наприклад, наказ Генерального прокурора від 17.09.2021 № 293 затверджує «Інструкцію про порядок проведення психофізіологічного дослідження із застосуванням поліграфа в органах прокуратури України», де визначено, що така перевірка проводиться з дотриманням загальнообов'язкових принципів добровільної згоди, правомірності, комплексності та всебічного забезпечення прав і свобод людини [3]. В діяльності Національної поліції також існує «Інструкція про порядок використання поліграфів у Національній поліції України», затверджена Наказом № 920 від 13.11.2017. [4]. Проте слід зауважити, що в Україні практика застосування поліграфа існує тільки щодо проведення внутрішніх службових перевірок та кадрової роботи. Тому в кримінально-

процесуальному кодексі України результати поліграфа не визначаються прямо як джерело доказів, тому їх використання у кримінальному провадженні часто реалізується тільки через включення в судово-психологічну експертизу або як допоміжний засіб [5].

У протидії організованій злочинності поліграф може виконувати ряд специфічних функцій: він може слугувати для попередньої оцінки осіб у злочинних мережах, допомагати в ідентифікації «слабких місць» у злочинних схемах правопорушників, або у відборі потрібних нам інформаторів. У таких випадках навіть орієнтовні результати можуть значно спрямувати слідство та заощадити ресурси. Однак наша та іноземна наукова критика вказує на фактори, котрі обмежують роботу поліграфа, а саме: неточності роботи, хибні позитивні або негативні спрацьовування поліграфу, вплив стресу досліджуваної особи, її хвилювання або її фізіологічний стан. Наприклад, оглядові дослідження вказують, що поліграф не є самодостатнім засобом детекції брехні, а лише інструментом, який може доповнювати інші методи. У дослідженні «How Reliable are Polygraph Examinations in Criminal …» підкреслюється, що в різних контекстах точність поліграфа є дискусійною, і його слід використовувати обережно [6].

Для того, щоб тестування на поліграфі давало максимально допустимі результати, необхідно суворо дотримуватися методологічних та процедурних вимог. Як зазначає Гезь А.І. у статті «Загальні вимоги до проведення тестування на поліграфі», навіть часткове недотримання умов може спотворити результат і зменшити достовірність тесту [7].

Ризики використання поліграфа в боротьбі з організованою злочинністю полягають у тому, що без нормативного підкріплення, та без визнання висновків поліграфа як допустимого доказу, результати можуть бути відхилені судами або викликати спори щодо допустимості доказів отримані за його допомогою.

Щоби максимально легітимізувати використання поліграфа в боротьбі з організованою злочинністю, доцільно запропонувати такі заходи: прийняти

спеціальний закон про діяльність поліграфологів, де були б врегульовані права та обов'язки сторін, механізми їх контролю, гарантії прав людини; також внести зміни до КПК та кримінального законодавства, щоб чітко визначити умови, за якими результати поліграфа можуть бути визнаними як допустимим доказом; створити офіційний державний реєстр атестованих поліграфологів із вимогами до їхньої освіти; стандартизувати протоколи тестування, шаблони запитань, режим інструктажу, забезпечити контроль якості та аудит висновків; впроваджувати поліграф спочатку в пілотних проєктах у підрозділах боротьби з корупцією чи організованою злочинністю, з ретельним моніторингом ефективності та помилок; обмежити застосування поліграфа лише до справ із високим ступенем ризику, де інші засоби не дали результату; забезпечити обов'язкову письмову згоду особи та право відмови без подальших негативних наслідків; навчати слідчих, прокурорів і суддів особливостям поліграфа та його обмеженням, щоб вони могли правильно оцінювати висновки.

Зрештою, застосування поліграфа у боротьбі з організованою злочинністю може дати значні бонуси у вигляді додаткової орієнтовної інформації, психологічного впливу, та внутрішнього контролю, але тільки за умови, що воно здійснюватиметься у суворій правовій, методичній та етичній рамці. Без цього існує ризик, що поліграф стане джерелом суперечностей, оскаржень і порушень процесуальних гарантій.

Список використаних джерел:

1. Про затвердження Інструкції про порядок використання поліграфів у Національній поліції України : Наказ М-ва внутр. справ України від 13.11.2017 № 920 : станом на 13 груд. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/z1472-17#Text (дата звернення: 08.10.2025).

2. ДСТУ 8692:2016 Поліграфи. Технічні умови URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=67992 (дата звернення: 08.10.2025).

3. Про затвердження Інструкції про порядок проведення психофізіологічного дослідження із застосуванням поліграфа в органах

прокуратури України : Наказ Офісу Ген. прокурора від 17.09.2021 № 293. URL: https://zakon.rada.gov.ua/laws/show/v0293905-21#Text (дата звернення: 08.10.2025).

4. Про затвердження Інструкції про порядок використання поліграфів у Національній поліції України : Наказ М-ва внутр. справ України від 13.11.2017 № 920 : станом на 13 груд. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/z1472-17#Text (дата звернення: 08.10.2025).

5. Чи дозволяє КПК України використовувати комп'ютерний поліграф як доказ: судова практика URL: https://yur-gazeta.com/publications/practice/kriminalne-pravo-ta-proces/chi-dozvolyae-kpk-ukrayini-vikoristovuvati-kompyuterniy-poligraf-yak-dokaz-sudova-praktika.html (дата звернення: 09.10.2025).

6. Dow, David R. and Jeu, Cassandra and Watkins, Scarlett, How Reliable are Polygraph Examinations in Criminal Investigations? An Empirical Assessment (August 30, 2024). URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5202561 (дата звернення: 09.10.2025).

7. Гезь А.І. Загальні вимоги до проведення тестування на поліграфі. Судово-психологічна експертиза. Застосування поліграфа та спеціальних знань в юридичній практиці: Електронний журнал / [редкол.: Назаров О. А. (голов. ред.) та ін.]. К., 2018. № 5 (17). Дата публікації: 30.02.2018.

КРІПАК Роман
курсант, здобувач першого (бакалаврського) рівня вищої освіти Військово-юридичного інституту Національного юридичного університету імені Ярослава Мудрого

Науковий керівник:
ГАШЕНКО Сергій

старший викладач кафедри загальновійськових дисциплін Військово-юридичного інституту Національного юридичного університету імені Ярослава Мудрого, підполковник

«ІННОВАЦІЙНІ ЗАСОБИ КОНТРОЛЮ ЕФЕКТИВНОСТІ СТРІЛЕЦЬКОЇ ТА ВОГНЕВОЇ ПІДГОТОВКИ: ПРАВОВІ Й КРИМІНАЛІСТИЧНІ АСПЕКТИ»

В умовах сучасних воєнних конфліктів, коли точність, швидкість та якість застосування вогневих засобів безпосередньо впливають на виживання військовослужбовців і результат виконання бойових завдань. Ефективність стрілецької та вогневої підготовки постає фундаментальною передумовою національної безпеки та правомірності застосування сили, проте якість її контролю критично страждає від низького рівня інноваційного забезпечення. Проблема не обмежується лише технологічним відставанням, вона має глибокі правові, криміналістичні та організаційні наслідки. Ключові прояви цієї кризи - брак сучасних, високоточних електронних тренажерів, їхня неповна відповідність реальним бойовим зразкам (зброя, боєприпаси, тактичне середовище) та системні проблеми із впровадженням вже існуючих інноваційних рішень у навчальний процес та стандарти оцінювання.

Система стрілецької підготовки традиційно базувалася на класичних підходах, що передбачали проведення занять на полігонах, стрільбищах і в умовах максимально наближених до бойових. Проте такий підхід вимагає значних матеріальних і часових ресурсів, пов'язаний з ризиком травмування, зношуванням зброї та боєприпасів, а головне - не завжди забезпечує належний рівень об'єктивного контролю за ефективністю навчання. Аналіз цієї проблематики вимагає впровадження інноваційних засобів контролю, зокрема електронних тренажерів, інтерактивних систем і цифрових комплексів оцінки

результативності стрільби, а також інтеграції юридичного, криміналістичного та військово-технічного підходів, оскільки лише належно підтверджені, впроваджені інноваційні засоби контролю, можуть гарантувати як високий рівень підготовки, так і доказову базу правомірності дій фахівців.

Недосконаліть нормативно-правової бази є основним бар'єром для впровадження інноваційних засобів контролю. Чинне законодавство часто концентрується на традиційних методах оцінювання, залишаючи поза увагою стандартизацію, сертифікацію електронних та віртуальних тренажерів. Це породжує прямі правові ризики. Неповна відповідність електронних тренажерів (особливо в імітації віддачі, звукового тиску, балістики та інтерфейсу) може сформувати некоректні рухові та психологічні стереотипи у того, хто навчається. В свою чергу, це може призвести до неправомірного або неефективного застосування зброї в реальній ситуації, що неминуче стає предметом кримінального розслідування за статтями про перевищення повноважень або необережне поводження зі зброєю. Відсутність чітких норм щодо юридичної сили результатів інноваційних засобів контролю робить їх недієздатними як належний доказ рівня підготовки. Результати, зафіксовані симулятором, потребують правової легітимізації через процедури повірки, калібрування та забезпечення цифрової цілісності (захисту від несанкціонованої модифікації чи фальсифікації). Проблема впровадження також тісно пов'язана з правовими механізмами державних закупівель, які часто орієнтовані на найнижчу ціну, а не на криміналістично та технічно обґрунтовану якість та інноваційність, що посилює проблему браку високоякісних електронних тренажерів. Крім того, неврегульованість питань інтелектуальної власності та трансферу технологій перешкоджає локалізації виробництва інновацій, що робить системи дорогими та неадаптованими до вітчизняних зразків зброї.

З криміналістичної точки зору, інноваційні засоби контролю є революційним джерелом інформації для аналізу та прогнозування поведінки особи, що застосовує зброю. Сучасні інноваційні комплекси (наприклад,

віртуальні полігони з аналізом біометрії) здатні фіксувати не лише кінцевий результат (влучання), але й процес прийняття рішень: час реакції на загрозу, послідовність тактичних дій, психофізіологічні показники (зміни серцевого ритму, тремор, окулографічні дані про фокусування погляду). Ці дані формують унікальний профіль стрільця, який є незамінним для судово-балістичної та психологічної експертизи після інциденту з бойовим застосуванням зброї. Криміналістичний аналіз результатів інноваційних засобів контролю може допомогти встановити, чи був рівень підготовки особи, її натренованість у стресових умовах та спроможність до усвідомлених дій достатнім, щоб виправдати застосування зброї. Інноваційні засоби контролю дозволяють перейти від суб'єктивної оцінки до об'єктивного доказу рівня професійної придатності.

Інноваційні засоби контролю ефективності стрілецької та вогневої підготовки є перспективним напрямом розвитку військової освіти та бойового навчання, але їхнє повноцінне впровадження вимагає рішення низки проблем. Для подолання кризи необхідно впровадити інтегровану стратегію, що поєднує правові та криміналістичні вимоги. Потрібно розробити технічні регламенти та державні стандарти для інноваційних засобів контролю, які будуть юридично зобов'язувати виробників забезпечувати повну відповідність тренажерів фізичним, балістичним та функціональним параметрам реальних зразків зброї. До розробки цих стандартів мають бути залучені криміналістичні експертні установи як основні валідатори, що підтверджують, що тренажер формує навички, адекватні реальності. Потрібно внести зміни до процесуального законодавства, які б чітко визначали процедуру збору, фіксації та зберігання результатів, отриманих за допомогою інноваційних засобів контролю. Це вимагає вбудованого у тренажери криптографічного захисту, часових міток та незалежних модулів верифікації, що унеможливлюють фальсифікацію та забезпечують доказову цінність даних. Необхідно реформувати систему державних закупівель, надаючи перевагу рішенням, які пройшли криміналістичну валідацію та мають підтверджену

високу точність і відповідність. Впровадження інноваційних засобів контролю, що використовують біометричні дані, вимагає суворого дотримання законодавства про захист персональних даних. Правова база має гарантувати, що інформація про психофізіологічний стан особи, зібрана під час тренувань, буде використана виключно для навчальних та доказових цілей і не стане інструментом дискримінації чи неправомірного тиску. Таким чином, інноваційні засоби контролю - це не просто технологія, а невід'ємна складова правової та криміналістичної інфраструктури підготовки. Лише через повну інтеграцію інновацій, підкріплену надійною правовою та криміналістичною базою, можливо гарантувати як високий професіоналізм стрільців, так і незаперечну законність кожного пострілу у сучасних умовах гібридної війни.

Список використаних джерел:

1. Конституція України: Документ 254к/96-ВР від 28.06.1996. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр

2. Про національну безпеку України: Документ 2469-VIII від 21.06.2018. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text

3. Про правовий режим воєнного стану: Документ 389-VIII від 12.05.2015. URL: https://zakon.rada.gov.ua/laws/show/389-19

4. Статут внутрішньої служби Збройних Сил України: Документ 548-XIV від 24.03.1999. URL: https://zakon.rada.gov.ua/laws/show/548-14#Text

5. Статут гарнізонної та вартової служб Збройних Сил України: Документ 550-XIV від 24.03.1999. URL: https://zakon.rada.gov.ua/laws/show/550-14#Text

РЯДІНСЬКА Валерія
доктор юридичних наук, професор
Департамент забезпечення діяльності
Голови Національної поліції України,
Національна поліція України
01024, вул. Богомольця, 9, Київ, Україна

ORCID: orcid.org/0000-0002-2210-5933
v.riadinska@gmail.com

ЗАСОБИ НЕЙРО-ПСИХОФІЗІОЛОГІЧНОГО ДОСЛІДЖЕННЯ ПОВЕДІНКИ ЛЮДИНИ ТА ПЕРСПЕКТИВИ ЇХ ЗАСТОСУВАННЯ В ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

На сучасному етапі в діяльності Національної поліції України у трудових відносинах, що виникають при професійному кадровому відборі персоналу, адміністративних відносинах, що виникають у зв'язку з реалізацією владно-управлінських функцій, кримінально-процесуальних відносинах, що виникають у межах кримінального провадження застосовується поліграф, більш відомий суспільству як «детектор брехні». Поліграф є засобом психофізіологічних досліджень, що забезпечує реєстрацію динаміки фізіологічних процесів організму людини (дихання, серцево-судинної активності, електропровідності шкіри тощо) у процесі опитування.

Застосування поліграфа в Україні пройшло тривалий шлях. Від наказу МВС України «Про проведення експерименту щодо використання комп'ютерних поліграфів у діяльності органів внутрішніх справ» № 743 від 28 серпня 2001 року, в якому поліграф впроваджувався у сферу правоохоронних органів України [1] та Інструкції про порядок використання в діяльності органів внутрішніх справ поліграфів (комп'ютеризованих приладів реєстрації психофізіологічних реакцій людини) від 28 липня 2004 року № 842 [2], яка встановила нормативні підстави застосування поліграфа в органах внутрішніх справ, зокрема, міліції, до прийняття Інструкції про порядок використання поліграфів у Національній поліції України, затвердженій наказом Міністерства внутрішніх справ України від 13 листопада 2017 року № 920 [3] пройшло вже більше 20 років.

З перших десяти поліграфів моделі «Аксітон», переданих в 1997 році українською діаспорою із США до міліції України, кількість поліграфів, які в 2025 році працюють в Національній поліції України, зросла до 214. З перших

п’яти англомовних офіцерів із Національної академії внутрішніх справ (м. Київ) та Львівського юридичного інституту МВС України, які в 1999 році пройшли навчання в Academy for Scientific Investigative Training у м. Ларго (штат Флорида, США), кількість сертифікованих поліцейських-поліграфологів в Національній поліції України на сьогодні становить 220 осіб.

Темпи впровадження та використання поліграфа в діяльності Національної поліції України не можна оцінити однозначно. З одного боку, за останні десятиліття спостерігається істотне зростання – кількість поліграфів і підготовлених поліграфологів збільшилася майже у двадцять разів. Водночас, з огляду на стрімкий розвиток технологій і загальну цифрову трансформацію суспільства, такі показники не можна вважати високими. Динаміка впровадження залишається відносно помірною, що свідчить про поступовий, еволюційний характер інтеграції поліграфа в систему діяльності Національної поліції України.

Така ситуація зумовлена як зовнішніми об’єктивними чинниками – відсутністю спеціального закону, який би комплексно врегульовував правові відносини, пов’язані із застосуванням поліграфа в Україні, тривалою дискусією щодо наукової валідності та доказової надійності поліграфа, неоднозначністю зарубіжного досвіду його використання, так і внутрішніми суб’єктивними факторами, серед яких варто відзначити нестачу чіткої управлінської волі та системного підходу до інтеграції поліграфа у практичну діяльність Національної поліції України.

Законодавчі ініціативи останніх років, а також поступове впровадження поліграфа як інструмента кадрового добору, проведення службових розслідувань та атестації персоналу в більшості органів сектору безпеки й оборони України свідчать про зростання рівня суспільного визнання його ефективності як засобу психофізіологічного оцінювання, поступову інституціоналізацію його застосування в системі державного управління персоналом. Крім цього, прийняття 31 липня 2025 року Закону України «Про внесення змін до деяких законодавчих актів України щодо посилення

повноважень Національного антикорупційного бюро України та Спеціалізованої антикорупційної прокуратури» № 4560-IX, у пункті 2 розділу II «Прикінцеві положення» якого закріплено, що *підрозділ внутрішнього контролю Національного антикорупційного бюро України, Спеціалізованої антикорупційної прокуратури, Бюро економічної безпеки України, Офісу Генерального прокурора, Державного бюро розслідувань, Національної поліції України за методологією, узгодженою із Службою безпеки України, не менше одного разу на два роки проводить поліграфологічні дослідження працівників Національного антикорупційного бюро України, Спеціалізованої антикорупційної прокуратури, Бюро економічної безпеки України, Офісу Генерального прокурора, Державного бюро розслідувань, Національної поліції України, які мають допуск до державної таємниці, на предмет вчинення дій на користь держави, визнаної Верховною Радою України державою-агресором* [4], свідчить про пряме законодавче визнання поліграфа як засобу контррозвідувальної діяльності, що інтегрує його використання як засобу забезпечення національної безпеки в діяльність окремих державних органів. Уперше на законодавчому рівні поліграф було визнано не лише як допоміжний засіб кадрового відбору та перевірки персоналу, але й як складову частину механізму виявлення внутрішніх загроз, оцінки лояльності, запобігання проникненню агентурного впливу у державні органи, виявлення прихованих зв'язків і т.ін.

Водночас, у контексті стрімкого науково-технічного прогресу, поліграф не залишається єдиним засобом психофізіологічного дослідження поведінки людини. Створюються новітні засоби, що поєднують досягнення психології, біометрії та штучного інтелекту.

Засоби психофізіологічного дослідження поведінки людини – це комплекс технічних, програмних та методичних інструментів, призначених для виявлення, вимірювання та аналізу фізіологічних реакцій організму людини, які відображають її психоемоційний стан, когнітивну активність або рівень стресу у відповідь на зовнішні стимули[3].

Крім поліграфа, до таких засобів відносяться:

електроенцефалограф (ЕЕГ) – пристрій для реєстрації біоелектричної активності головного мозку,

електрокардіограф (ЕКГ) – інструмент для фіксації електричної активності серця, що дозволяє аналізувати варіабельність серцевого ритму (HRV) як індикатора автономної нервової системи та рівня стресу;

електроміограф (EMG) – пристрій для реєстрації електричної активності м'язів, зокрема лицьових, для вивчення емоційних виразів та моторних реакцій;

функціональна ближньо-інфрачервона спектроскопія (fNIRS) – оптичний метод для вимірювання оксигенації крові в мозку, що дозволяє досліджувати когнітивну активність у реальних умовах;

пупілометрія – техніка фіксації змін діаметра зіниці як маркера когнітивного навантаження та уваги, а також трекери очей (eye-tracking) для аналізу рухів очей та фіксацій погляду, що відображають процеси уваги та сприйняття тощо.

---

[3] Макарчук, М. Ю., Куценко, Т. В., Кравченко В.І., Данилов С.А. Психофізіологія: навчальний посібник / М. Ю. Макарчук, Т. В. Куценко, В.І. Кравченко, С.А.Данилов – К. : ООО «Інтерсервіс» , 2011. – 329 с

Також протягом останнього десятиріччя психофізіологія розвивається у тісному взаємозвязку з нейронаукою, що сприяло появі нових напрямів досліджень – когнітивної нейропсихофізіології, нейрокогнітивної діагностики тощо. Така інтеграція дала змогу поєднати методи і засоби психофізіологічного та нейрофізіологічного аналізу, використовуючи їх для комплексного дослідження нейродинамічних процесів, когнітивних функцій, емоційних реакцій, адаптаційних механізмів людини і т. ін.

Засобами нейро-психофізіологічних досліджень поведінки людини є інструменти, що поєднують методи нейронауки та фізіології для вивчення психологічних станів людини, дозволяють візуалізувати мозкову активність у реальному часі, розкриваючи нейронні основи поведінки тощо. До них

відносяться:

функціональна магнітно-резонансна томографія (фМРТ) застосовується для аналізу активності мозкових зон;

позитронно-емісійна томографія (ПЕТ) застосовується для оцінки метаболічних процесів;

інфрачервона спектроскопія (NIRS) застосовується для моніторингу оксигенації мозку;

магнітоенцефалографія (MEG) – аналогічна EEG, але вимірює магнітні поля і т.ін.

Засоби нейро-психофізіологічних досліджень поведінки людини в діяльності поліції можуть застосовуватися у тих самих сферах, що й поліграф (кадровій, адміністративній та кримінально-процесуальній), проте вони здатні суттєво розширити можливості нейро-психофізіологічного аналізу завдяки комплексній оцінці когнітивних, емоційних і нейродинамічних процесів.

Виникає питання – чи є доцільним застосовувати інших, крім поліграфа, засобів нейро-психофізіологічного дослідження поведінки людини в діяльності Національної поліції України?

З одного боку, необхідність у цьому може здаватися сумнівною, бо запровадження нових технологій потребує значних фінансових, організаційних та кадрових ресурсів, наукова валідність окремих засобів (зокрема ЕЕГ, fNIRS, eye-tracking) ще не має однозначного підтвердження для правоохоронної практики, а в більшості зарубіжних країн такі засоби використовуються переважно у дослідницьких, а не у прикладних цілях.

З іншого боку, відмова від їх застосування може повторити ситуацію, що свого часу склалася з поліграфом, коли тривалий період скепсису та відсутності нормативного врегулювання відтермінували його інтеграцію у практичну діяльність правоохоронних органів, в той час як сьогодні поліграф є невід'ємною частиною кадрової політики не лише Національної поліції, а й органів сектору безпеки та оборони країни в цілому, та ефективно розвивається в інших сферах.

Вирішення питання щодо доцільності застосування в діяльності Національної поліції України інших, окрім поліграфа, засобів нейро-психофізіологічного дослідження поведінки людини потребує науково обґрунтованого, системного підходу. Для формування підґрунтя прийняття виваженого управлінського рішення з цього приводу необхідно здійснити комплексне вивчення низки взаємопов'язаних аспектів, зокрема:

науково-методологічного, що передбачає оцінку валідності, надійності та точності сучасних нейро-психофізіологічних засобів;

порівняльно-правового, спрямованого на аналіз зарубіжного досвіду використання таких засобів у діяльності правоохоронних органів (зокрема поліції) та визначення моделей їх нормативного регулювання;

етико-правового, що має забезпечити дотримання прав людини, принципів добровільності участі, конфіденційності та захисту персональних даних;

організаційно-технологічного, який охоплює оцінку матеріально-технічної спроможності, кадрової підготовки, наявних лабораторних потужностей і можливостей інтеграції сучасних технологій у структуру поліції;

соціально-психологічного, спрямованого на виявлення ставлення поліцейських і суспільства до використання таких технологій, рівня довіри до них і потенційного впливу на сфери застосування.

Дослідження зазначених напрямів дозволить сформувати наукове та нормативне підґрунтя для прийняття виваженого управлінського рішення щодо можливостей і меж застосування сучасних нейро-психофізіологічних засобів у діяльності Національної поліції України. У цьому контексті важливо об'єднати зусилля науковців, практиків і представників правоохоронних органів для спільного опрацювання визначених раніше аспектів впровадження таких засобів. Пропонуємо ініціювати діалог, спрямований на обговорення доцільності застосування нейро-психофізіологічних засобів як у діяльності Національної поліції України, так і в інших органах сил безпеки та оборони

України.

Література:

1. Про проведення експерименту щодо використання комп'ютерних поліграфів у діяльності органів внутрішніх справ України : наказ МВС України від 28.08.2001№ 743. URL: http://zakon4.rada.gov.ua/ laws/main.

2. Інструкції про порядок використання в діяльності органів внутрішніх справ поліграфів (комп'ютеризованих приладів реєстрації психофізіологічних реакцій людини) від 28 липня 2004 року № 842. https://zakon.rada.gov.ua/laws/show/z1373-04#Text

3. Інструкція про порядок використання поліграфів у Національній поліції України : наказ Міністерства внутрішніх справ України 13 листопада 2017 року № 920. URL. https://zakon.rada.gov.ua/laws/show/z1472-17#n14

4. Про внесення змін до деяких законодавчих актів України щодо посилення повноважень Національного антикорупційного бюро України та Спеціалізованої антикорупційної прокуратури : Закон України від 31 липня 2025 року був прийнятий № 4560-IX. URL. https://zakon.rada.gov.ua/laws/show/4560-20#Text

САЄНКО Владлен
аспірант Донецького державного університету
внутрішніх справ (м. Кривий Ріг)

Науковий керівник:
ГРУЗДЬ Олександр
завідувач кафедри кримінального процесу та криміналістики Донецького державного

університету
внутрішніх справ (м. Кривий Ріг),
кандидат юридичних наук

СЛІДОВА КАРТИНА ЯК ЕЛЕМЕНТ КРИМІНАЛІСТИЧНОЇ ХАРАКТЕРИСТИКИ ПРАВОПОРУШЕНЬ, ПОВ'ЯЗАНИХ З ВИКОРИСТАННЯМ ВІРТУАЛЬНИХ АКТИВІВ

Термін «слідова картина» у криміналістиці вперше запропонував знаний український криміналіст М. В. Салтевський який зазначав, що типова слідова картина вчинення злочину як елемент криміналістичної характеристики – поняття збірне, що включає опис матеріальних та ідеальних відображень ознак злочину на момент його виявлення. Тому поняття «слідова картина» містить матеріальні сліди, як наявні, так і ймовірні, їх розташування і види, особливості місця, часу вчинення злочину, розташування і видів схованок та деякі інші ознаки, що іноді називаються самостійними елементами криміналістичної характеристики. Слідова картина включає також джерело ідеальних відображень, тобто людини, яка виступає в події злочину підозрюваним, потерпілим, свідком-очевидцем [1, с. 269].

Слідова картина кримінальних правопорушень, пов'язаних з використанням віртуальних активів, є вкрай специфічною і відмінною від традиційних правопорушень. Така слідова картина безпосередньо корелює зі специфікою засобів вчинення кримінального правопорушення – сліди являють собою сукупність матеріально-фіксованих і віртуальних слідів, перші – це відбитки пальців на пристроях периферії, елементах системного блоку, другі – на жорстких дисках комп'ютерів, в історії браузерів, в історії «крапок поновлення системи», «кеші», файлах-cookie [2, с. 78-79]. Цифрові або віртуальні сліди є зафіксованими у вигляді цифрового образу формальної моделі зміни стану інформації в пам'яті абонентських електронних пристроїв (терміналів, білінгових систем тощо), викликані алгоритмом встановленого

програмного забезпечення і пов’язані з подією кримінального правопорушення.

Вище зазначені сліди, під час розслідування кримінальних правопорушень у цій сфері комп’ютерної інформації, мають вирішальне значення, оскільки найчастіше є єдиним джерелом криміналістично значущої інформації та відіграють важливу роль в ході аналізу події слідчим, адже дозволяє відновити механізм вчинення правопорушення [3, с. 5-9].

Більшість віртуальних активів, зокрема криптовалют, базуються на технології Blockchain. Ця новітня технологія є ланцюжком з блоків із записами транзакцій, які пов’язані між собою і захищені з використанням криптографії. Кожен блок містить власний унікальний криптографічний ідентифікатор, який вказує (пов’язує) його з попереднім блоком ланцюга. Після додавання в Blockchain, блоки вже неможливо змінити без втрати даних про весь наступний ланцюг, що негайно дає іншим користувачам знати, що було здійснено стороннє втручання в обхід правил. Це дає можливість просто відмовити у використанні модифікованої версії ланцюжка (бо без визнання модифікованого блоку з боку більшості учасників процесу він не є корисним) і продовжувати працювати з вихідною гілкою. Криптогаманці можуть бути прив’язані до Blockchain, щоб гарантувати, що їхній баланс відповідає дійсності, а нові транзакції перевіряються за допомогою даних у ланцюжку блоків для гарантії того, що кожна з них є справжньою і була зроблена криптовалютою, яка реально належить платнику (або його криптогаманцю) [4, с. 124-125].

З одного боку такий підхід забезпечує безпеку транзакцій (взаємних розрахунків). З іншого боку, ідентифікувати відправників та одержувачів зазначених активів стає проблемним завданням для правоохоронців. Саме за рахунок зазначених вище технологічних рішень цей актив став популярним серед осіб, які здійснюють злочинну діяльність.

При зберіганні віртуальних активів, зокрема криптовалюти, використовують різноманітні програмно-апаратні засоби: десктопні програми

(встановлюються на персональні комп’ютери користувачів); мобільні програми (аналогічні попереднім додаткам, за винятком того, що встановлюються на мобільні пристрої); онлайн-гаманці (працюють за принципом звичайного сайту, користувач може за допомогою логіну і пароля увійти в акаунт з будь-якого пристрою, що має вихід в мережу Інтернет); апаратні гаманці у форматі фізичних пристроїв (підключаються до комп’ютера через відповідні роз’єми, найчастіше пристрій має дисплей, на якому відображається основна інформація, при цьому забезпечується холодне зберігання ключів лише в автономному середовищі); текстовий вигляд (різновид холодного криптогаманця, його власник зберігає ключі криптогаманця у файлі на персональному комп’ютері або на паперовому носії інформації у вигляді рядка символів).

Усі ці способи зберігання криміналістично значущої інформації про віртуальні активи чи доступ до них піддаються виявленню шляхом проведення процесуальних дій (огляд, обшук, експертиза) .

Пошук відповідних файлів з криміналістично значущою інформацією про віртуальні активи (їх розміщення та доступ до них) може здійснюватися в ході огляду вмісту персонального комп’ютера з використанням вбудованого програмного функціоналу операційної системи (вбудований пошуку у файловій системі) або спеціалізованих програм. Зазвичай, щоб виявити файли, в яких містяться рядки, що містять ключі криптогаманців необхідно з метою пошуку ввести послідовність символів, що точно повторюють ключ криптогаманця.

Завдання слідчим значно ускладняються коли ключ криптогаманця (певна послідовність символів) зберігається у вигляді растрових зображень (скриншот екрану, цифрова фотографія). При такому способі зберігання ймовірність виявлення електронних файлів з ключами криптогаманців стає мінімальною, однак вже наявне програмне забезпечення, яке дає змогу здолати і цю перешкоду. У даному випадку програмно шукають записи схожі до послідовних символів ключів криптогаманця.

Специфічною є обстановка вчинення кримінальних правопорушень, пов'язаних з використанням віртуальних активів – це віртуальний кібернетичний простір. Його особливістю є те, що унаслідок використання інформаційних мереж (провідних та бездротових технологій) під час вчинення одного кримінального правопорушення одночасно може бути задіяно безліч комп'ютерів. Перебувати ці комп'ютери можуть у просторово віддалених один від одного місцях і навіть у різних державах. Місце кримінального правопорушення, пов'язаного з використанням віртуальних активів характеризується двома складовими: 1) місцезнаходженням у реальному просторі (роль індивідуалізуючої криміналістично значущої інформації відіграє адресу місцезнаходження фізичної особи, організації, використовуваних ними апаратно-програмних засобів); 2) місцезнаходженням, яке постійно ототожнюється в локальній та глобальній мережі з унікальним номером – IP-адресою.

До електронно-цифрових слідів при розслідуванні злочинів, пов'язаних із використанням віртуальних активів, зокрема криптовалют, слід відносити: 1) адресу криптогаманця (ідентифікатор, необхідний для здійснення операцій у розподілених реєстрах даних, який дозволяє відстежити рух віртуального активі (зокрема, криптовалюти) у межах здійснення транзакції та гаманця відправника / одержувача); 2) історія транзакцій (відкритий розподілений реєстр даних, то він містить відомості про кожну транзакцію, що була проведена); 3) відомості про баланс криптогаманця та їх зміни в межах терміну, що цікавлять слідство; 4) приватні та публічні ключі (для користування можливостями розподілених реєстрів даних необхідні ключі, приватний – для посвідчення транзакції, тобто її підпису, публічний – дозволяє приймати криптовалюту).

Крім матеріальних слідів, під час розслідування злочинної діяльності, пов'язаної з використанням віртуальних активів слідчому доцільно вести пошук й ідеальних слідів, шляхом проведення відповідних процесуальних дій з підозрюваними, свідками, потерпілими.

Список використаних джерел:

1. Салтевський М. В. Криміналістика: підручник: у 2-х ч. Харків: Консум, 2001. Ч. 2. 528 с.

2. Старушкевич А. Організація огляду місця події. Аналіз криміналістично значимої інформації при розслідуванні злочинів у сфері комп'ютерної інформації. Вісник прокуратури. 2003. № 12 (30). С. 77-87.

3. Одерій О. В., Корона С. О., Самойлов С.В. Тактика слідчого огляду комп'ютерних систем та їх елементів: наук.-практ. посібник. Донецьк: ТОВ «ВПП «ПРОМІНЬ», 2010. 88 с.

4. Динту В. А., Мітрофанов А. А. BITCOIN у системі легалізації доходів, одержаних злочинним шляхом. Наукові праці Національного університету «Одеська юридична академія». 2017. Т. XIX. С. 122- 129.

ТРЕТЯК Софія
курсантка 303/23-(П)-Б навчального взводу
факультету підготовки фахівців для органів досудового розслідування НПУ Донецького державного університету внутрішніх справ

Науковий керівник:
ДРОБЕНКО Діна
Підполковник поліції
викладач кафедри кримінального процесу та криміналістики факультету підготовки фахівців для органів досудового розслідування НПУ
Донецького державного університету внутрішніх справ

ПРАВОВЕ РЕГУЛЮВАННЯ ВИКОРИСТАННЯ ПОЛІГРАФА У КРИМІНАЛЬНОМУ СУДОЧИНСТВІ

Сучасний світ динамічно розвивається, і застосування нових науково-технічних досягнень у правові сфері є невід'ємною частиною ефективного розслідування кримінальних правопорушень. Одним із таких досягнень є використання поліграфу, так званого «детектору брехні», який дозволяє фіксувати психофізіологічні реакції людини. Незважаючи на його популярність та використання в деяких країнах, питання щодо правового регулювання його використання, правового статусу, допустимості доказів, отриманих за його допомогою є невирішеним.

Згідно з «Інструкцією про порядок використання поліграфів у Національної поліції України», затвердженою Наказом МВС України від 13 листопада 2017 року № 920, поліграф визначається як спеціальний психофізіологічний технічний засіб, призначений для фіксації динаміки щонайменше п'яти автономних психофізіологічних процесів людини у відповідь на пред'явлення певних психологічних стимулів за спеціальною методикою, без завдання шкоди життю, здоров'ю людини чи довкіллю [1].

Підставою широкого застосування поліграфів правоохоронними органами України є Закон України «Про оперативно-розшукову діяльність» від 18.02.1992 р. № 2135-XII. Стаття 8 цього Закону закріплює право органів, що здійснюють ОРД, опитувати осіб за їх згодою (п. 1 ч. 1 ст. 8). Використання поліграфа розглядається як особлива форма опитування. Водночас інформація, здобута таким способом, не визнається судами належними доказами у справі, а може застосовуватися лише як орієнтир для подальшого збирання офіційних доказів. Відповідно до ч. 16 ст. 9 цього Закону, з метою отримання відомостей забороняється застосування технічних засобів, а також психотропних, хімічних та інших речовин, що здатні пригнічувати волю особи або завдавати шкоди її здоров'ю та навколишньому середовищу [2].

В українській судовій практиці послідовно підтверджується, що результати поліграфічного дослідження не можуть визнаватися допустимим доказом. Верховний Суд у низці постанов підкреслював, що такі висновки

мають розглядатися виключно як допоміжна інформація, яка не наділена самостійною доказовою силою. Аналогічний підхід простежується і в міжнародній судовій практиці: Верховний Суд США у справі United States v. Scheffer прямо заборонив використовувати поліграф у кримінальних процесах, визнавши його суперечним стандартам допустимості [3, с. 5].

У законодавчій ініціативі існувало декілька варіантів, щодо впровадження поліграфу у слідчу діяльність. Так, наприклад, у Верховній Раді України розглядався проект Закону України «Про доповнення Кримінального процесуального кодексу України положеннями щодо використання поліграфа (детектора брехні)» № 2521. Також існує законопроект «Про поліграфологічну діяльність», який так і не був прийнятий.

Законодавство України передбачає використання результатів дослідження з використанням поліграфа лише за умови, якщо таке дослідження було проведено на підставі постанови про проведення судово-психофізіологічної експертизи з використанням поліграфа та результат експертизи викладено у висновку експерта, який є процесуальним джерелом доказу. Поліграф може мати юридичну доказову силу лише в рамках судової експертизи, яка регулюється законодавством України, зокрема, КПК України, Законом «Про судову експертизу», Інструкцією про призначення та проведення судових експертиз та експертних досліджень та Науково-методичними рекомендаціями з питань підготовки та призначення судових експертиз та експертних досліджень, затвердженими Наказом Міністерства юстиції України від 08.10.98 № 53/5 зі змінами та доповненнями і має назву «судова психофізіологічна експертиза з використанням поліграфа» [4, с. 687].

Це засвідчує, що результати використання поліграфа офіційно набули статусу значущих орієнтовних відомостей для кримінальних, цивільних, адміністративних, господарських та інших проваджень, а також для забезпечення запитів зацікавлених фізичних і юридичних осіб. У підпункті 6.8.1 цього розділу визначено предмет опитування із застосуванням комп'ютерного поліграфа, а підпункт 6.8.2 встановлює, що таке опитування

може проводитися виключно за умови отримання письмової згоди особи, яка підлягає опитуванню [5, с. 72].

Комп'ютерні поліграфи, використовувані для судових психологічних експертиз, повинні відповідати вимогам ДСТУ 8692:2016, що набув чинності з 15 листопада 2016 року. Цей стандарт чітко визначає технічні характеристики та критерії, які повинні відповідати такі поліграфи [4, с. 687].

Як висновок, зазначимо, що 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.

Список використаних джерел:

1. Наказ Міністерства внутрішніх справ Про затвердження Інструкції про порядок використання поліграфів у Національній поліції України від 13.11.2017 №920. URL: https://zakon.rada.gov.ua/laws/show/z1472-17#Text (дата звернення 19.09.2025)

2. Закон України «Про оперативно-розшукову діяльність». URL: https://zakon.rada.gov.ua/laws/show/2135-12#Text (дата звернення 19.09.2025)

3. Варенья Н. М., Бедратий Ю. В., Алекумов С. С. Правове регулювання використання поліграфа в кримінальному процесі: за та проти. Соціальний розвиток: економіко-правові проблеми. 2025. №9. С. 1-6. URL: https://www.eu-scientists.com/index.php/sdel/article/view/346/335 (дата звернення 19.09.2025)

4. Курман О. В., Балибіна А. Р. Використання поліграфа при розслідуванні кримінальних правопорушень: проблеми тактики та правового регулювання. Електронне наукове видання «Аналітично-порівняльне

правознавство». 2024. №2.С.686-691URL: https://dspace.uzhnu.edu.ua/server/api/core/bitstreams/3c85118e-b089-425b-9a6d-910da4e9a215/content (дата звернення 19.09.2025)

5. Градун С. А. Правова регламентація використання поліграфа в секторі безпеки і оборони України. Центральноукраїнський вісник права та публічного управління. 2024. Вип. 3(7). С. 67-80. URL: https://cuj.dnuvs.ukr.education/index.php/cuj/article/view/69/65 (дата звернення 19.09.2025)

ШЕВЧУК Віктор
доктор юридичних наук, професор, завідувач кафедри криміналістики Національного юридичного університету імені Ярослава Мудрого, головний науковий співробітник НДІ вивчення проблем злочинності імені академіка В. В. Сташиса НАПрН України, заслужений юрист України

ІННОВАЦІЙНІ КРИМІНАЛІСТИЧНІ ТЕХНОЛОГІЇ, ЗАСОБИ І МЕТОДИ ПРОТИДІЇ КОРУПЦІЇ В СУЧАСНИХ УМОВАХ ВІЙНИ

Корупція залишається одним з найгостріших викликів сучасного світу, що підриває ефективність державного управління, знижує довіру громадян до влади та створює перешкоди для сталого економічного розвитку. В епоху цифрової трансформації світового співтовариства традиційні методи боротьби з корупцією часто виявляються недостатніми для протидії складним та багатошаровим корупційним схемам, що використовують сучасні технологічні рішення для приховування злочинної діяльності [1, с. 59-77]. Стрімкий розвиток інформаційних технологій та їх інтеграція в усі сфери

суспільного життя створюють не лише нові можливості для підвищення ефективності антикорупційної діяльності, але й породжують серйозні виклики для правоохоронних органів, що вимагають переосмислення підходів до виявлення та розслідування корупційних правопорушень [2, с. 453].

Особливої гостроти набуває проблема зростаючої складності корупційних схем, які все частіше використовують цифрові технології, криптовалюти, офшорні юрисдикції та розподілені мережі для приховування слідів злочинної діяльності. Транскордонний характер сучасної корупції створює особливі виклики для національних правоохоронних систем, оскільки корупційні операції можуть здійснюватися з території будь-якої держави, маскуючи своє справжнє походження через складні ланцюжки фінансових транзакцій та цифрових слідів. Це суттєво ускладнює процес виявлення корупційних схем та притягнення винних до відповідальності, вимагаючи розробки нових механізмів використання інноваційних криміналістичних засобів та технологій [3, с. 137].

Вбачається, що досить потужним інструментом у боротьбі з корупцією є аналіз великих даних (Big Data). Він передбачає використання статистичних методів та машинного навчання для обробки величезних обсягів структурованих та неструктурованих даних з метою виявлення трендів, шаблонів та зв'язків. Основні методи аналізу включають описову (що сталося), діагностичну (чому сталося), прогнозну (що буде) та прескриптивну (що робити) аналітику. Переваги використання Big Data полягають у можливості обробляти дані в реальному часі, виявляти приховані тенденції, знижувати витрати та ефективніше управляти ризиками (Big Data). Прикладами використання Big Data є інструмент Digiwhist (ЄС), створений для виявлення шахрайства в державних закупівлях на європейському рівні шляхом аналізу великих даних, та система швидкого оповіщення SALER (Валенсія, Іспанія), що відповідає за ідентифікацію ознак нерегулярності в адміністративних файлах на основі аналізу даних [4].

Певну зацікавленість з практичної точки зору також набувають використання технологій OSINT у антикорупційних розслідуваннях. Вони можуть включати: моніторинг соціальних мереж для виявлення стилю життя посадовців, що не відповідає їхнім доходам, аналіз декларацій та їх зіставлення з даними з відкритих реєстрів нерухомості, транспортних засобів, бізнесу; використання геолокаційних даних та супутникових знімків для виявлення незадекларованого майна; аналіз фото- та відеоматеріалів для ідентифікації осіб та подій; виявлення прихованих зв'язків між політично значущими особами (PEP), їх родичами та бізнес-структурами; аналіз державних закупівель та тендерної документації для виявлення конфліктів інтересів та ознак змови [5].

Крім цього, OSINT-технології досить ефективно застосовується для виявлення незадекларованих активів, прихованих конфліктів інтересів, фіктивних компаній, що використовуються у корупційних схемах, відстеження фінансових потоків через офшорні юрисдикції (у поєднанні з аналізом витоків даних, таких як Panama Papers (Dalby, 2019), та загалом для збору доказової бази у справах про корупцію.

Корупція залишається однією з найгостріших та найактуальніших соціальних проблем сучасної України, що становить реальну загрозу її національній безпеці, демократичному розвитку та конституційному ладу. При цьому характерною рисою корупції в Україні є її системність та високий рівень інституціоналізації. Спостерігається небезпечний симбіоз олігархічного бізнесу з корумпованими представниками державного апарату, що призводить до ухвалення управлінських рішень на користь вузьких груп осіб та перерозподілу суспільних благ Це створює ситуацію, коли корупція стає невід'ємною частиною функціонування певних секторів економіки та владних структур.

В Україні створено систему спеціалізованих антикорупційних органів, ключовими з яких є Національне антикорупційне бюро України (НАБУ), Спеціалізована антикорупційна прокуратура (САП) та Державне бюро

розслідувань (ДБР). Їхня ефективність значною мірою залежить від здатності використовувати сучасні інноваційні засоби та технології. НАБУ є головним органом, відповідальним за розслідування топ-корупції. У своїй діяльності НАБУ приділяє значну увагу впровадженню цифрових інструментів.

Аналіз наявної інформації свідчить про певну нерівномірність у впровадженні та використанні інноваційних технологій різними антикорупційними органами України. НАБУ та САП демонструють більш активне та системне впровадження цифрових інструментів, таких як система «іКейс» та аналітичні програмні комплекси, що підтверджується їхніми стратегічними документами, звітами та публічними заявами. Інформація про аналогічні системні зусилля з боку ДБР у сфері інноваційної криміналістики є значно менш деталізованою у наданих джерелах. Ця нерівномірність може бути зумовлена різними факторами, включаючи відмінності у мандатах та підслідності цих органів, рівні пріоритезації технологічного розвитку, обсягах фінансування та наявній технічній спроможності. Така ситуація може створювати певні проблеми у міжвідомчій взаємодії та координації зусиль, а також впливати на загальну ефективність антикорупційної системи країни [6]. Для забезпечення синергетичного ефекту та уникнення «технологічних розривів» важливо прагнути до більш збалансованого та скоординованого технологічного розвитку всіх ланок антикорупційної інфраструктури.

Аналіз міжнародного досвіду демонструє високу ефективність інноваційних технологій у боротьбі з корупцією. Систематизація практик використання штучного інтелекту та аналізу великих даних у провідних країнах світу показала суттєве підвищення точності виявлення підозрілих транзакцій, значне скорочення помилкових спрацьовувань та можливість обробки величезних масивів документів у стислі терміни. Водночас виявлено критичні виклики, серед яких залежність від якості даних, ризики алгоритмічної упередженості та високі вартості впровадження технологічних рішень.

Блокчейн-технології показують найбільшу ефективність у сферах з

чіткими процедурами та великою кількістю учасників, зокрема земельних реєстрах та державних закупівлях. Міжнародні кейси засвідчують значне зниження ризиків шахрайства та підвищення прозорості державних процесів. Успішні проекти характеризуються поетапним впровадженням, державною підтримкою та адаптацією до місцевих умов, проте стикаються з проблемами масштабованості, регуляторними обмеженнями та необхідністю кардинальних законодавчих змін.

OSINT-технології революціонізували підходи до антикорупційних розслідувань, демократизувавши розслідувальні можливості та надавши потужні інструменти не лише спеціалізованим державним органам, але й громадським організаціям та журналістам-розслідувачам. Це створило альтернативні канали виявлення корупції, незалежні від можливого політичного впливу чи ресурсних обмежень державних структур, та суттєво розширило коло суб'єктів, здатних ефективно викривати корупційні правопорушення.

В Україні спостерігається нерівномірність технологічного оснащення антикорупційних органів. НАБУ демонструє лідерство у впровадженні інноваційних технологій, активно використовуючи систему іКейс, штучний інтелект, аналіз великих даних та OSINT-методики, що підтверджується стратегічними документами та угодами про співпрацю з профільними міністерствами. САП ефективно координує з НАБУ через спільні цифрові платформи, тоді як ДБР потребує значного розвитку технологічних спроможностей та інвестицій у сучасні засоби розслідування.

Вбачається, що ефективність інноваційних технологій критично залежить від системної інтеграції різних цифрових рішень та якості підготовки персоналу. Найвищий економічний ефект демонструють інтегровані системи, що поєднують штучний інтелект, блокчейн, OSINT та цифрову форензіку в рамках єдиних аналітичних платформ [7]. Водночас виявлено прямий зв'язок між складністю корупційного правопорушення та доцільністю використання високотехнологічних рішень. Більше того, українські експертні установи,

громадські організації та журналісти-розслідувачі відіграють надзвичайно важливу роль у використанні інноваційних методів виявлення корупції. Їхня діяльність формує потужний недержавний сегмент антикорупційної системи, який часто компенсує обмеження офіційних інституцій та стимулює їх до більш активної роботи.

Одним із найбільш перспективних напрямів забезпечення протидії корупційних кримінальних правопорушень, на наш погляд, сьогодні набуває їх належне криміналістичне забезпечення, яке набуває комплексного характеру. Успішне забезпечення діяльності щодо розслідування корупційних кримінальних правопорушень передбачає врахування комплексного підходу до вирішення завдань протидії корупції. Серед видів та форм забезпечення діяльності в цьому контексті особливого значення набуває врахування: організаційного; інформаційно-аналітичного; психологічного; матеріально-технічного; фінансового; фінансового; соціального; науково-методичного; законодавчого; криміналістичного та інших форм забезпечення протидії корупції в умовах війни.

Таким чином, проведене дослідження засвідчує, що реалізація потенціалу інноваційних криміналістичних засобів та технологій у боротьбі з корупцією потребує комплексного системного підходу. Такий підхід має включати розвиток цифрових компетенцій персоналу, формування відповідної інституційної культури, забезпечення технологічної інтеграції, кардинальне удосконалення правового регулювання цифрових доказів та розробку стратегії цифрової трансформації антикорупційних органів. Лише за умови синхронізації всіх цих компонентів можлива ефективна модернізація національної системи боротьби з корупцією відповідно до сучасних технологічних можливостей та міжнародних стандартів.

Література:

1. Shevchuk, V., Zhuravel, V., Yevdokimenko, S., Yevdokimenko, S.,

Myshkov, Y. (2025). Forensic Examination and Criminalistics in Investigating War Crimes: European and Ukrainian Experiences. *Jurnal Media Hukum*, 32(1), 59-77. DOI: https://doi.org/10.18196/jmh.v32i1.25056

2. Шевчук В. М. Формування та реалізації криміналістичної методики розслідування корупційних кримінальних правопорушень. *Юридичний науковий електронний журнал.* № 6. 2022. С. 450 – 455.

3. Baltrūnienė J., Shevchuk V. Artificial Intelligence Technologies in Law Enforcement and Justice: Ukrainian and European experience. *Цифрова трансформація кримінального провадження в умовах воєнного стану* : мат-ли Всеукр. круглого столу (Харків, 16.12.2022). Харків, 2022. С.135-140.

4. Konovalova V. O., Shevchuk V. M. Application of digital technologies in criminalistics in the conditions of war. *Цифрова трансформація кримінального провадження в умовах воєнного стану*: матеріали круглого столу (м. Харків, 23 груд. 2022 р.).; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса НАПрН України. Х.: Право, 2022. С.141-146.

5. OSINT-інструменти 2025: Топ-10 рішень для збору та аналізу даних. (2025). https://softlist.com.ua/ua/news/osint-instrumenty-2025-top-10-resheniy-dlya-sbora-i-analiza-dannyh

6. Shevchuk, V., Morozova T., Chornyi, H., Nehrebetskyi V., and Slobodeniuk, I. (2025). Artificial Intelligence in Criminal Proceedings: Criminalistic and Criminal Procedural Problems. *International Annals of Criminology,* 2025. Pp. 1-19. DOI: https://doi.org/10.1017/cri.2025.10090

7. Shevchuk V., Bululukov O., Chornyi H., Tyshchenko O., Baranchuk V. Latest Criminalistic Tools and Technologies in the Investigation of Cybercrimes: International and Ukrainian Experience. *Revista de Direito, Estado e Telecomunicacoes*. 2025. Vol. 17, iss. 2. Pp. 207–235. DOI: https://doi.org/10.26512/lstr.v17i2.55927

ЯГОЛЬНИК Олег
старший викладач кафедри кримінального процесу та криміналістики Донецького державного університету внутрішніх справ, кандидат юридичних наук

ІННОВАЦІЙНІ КРИМІНАЛІСТИЧНІ ТЕХНОЛОГІЇ У ПРОТИДІЇ ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ: СУЧАСНИЙ СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ

Організована злочинність в Україні набула нової технологічної якості: організовані групи та злочинні організації використовують цифрові технології й віртуальні активи для приховування доходів шляхом виведення активів у криптовалюту, нелегального експорту капіталу через інтернет-платформи, підпорядкування собі криптовалютних бірж та обмінних пунктів [1, с. 2]. Це позначається на результатах викриття: з 1 січня по 1 травня 2023 р. у сфері господарської діяльності зареєстровано 1 629 кримінальних проваджень, з них лише 42 – з ознаками вчинення організованою групою чи злочинною організацією, і жодне на той момент не було скеровано до суду [1, с. 53].

Під інноваційними криміналістичними технологіями пропонуємо розуміти науково обґрунтовані системи технічних засобів, методів і алгоритмів їх застосування, що ґрунтуються на новітніх досягненнях природничих, технічних та інформаційних наук і пристосовані до збирання, дослідження та використання доказової й орієнтуючої інформації. Таке розуміння узгоджується з двоєдиним трактуванням криміналістичної техніки – як розділу науки і як сукупності засобів, прийомів і методів їх застосування [2, с. 11], а також із загальнотеоретичними положеннями криміналістики [4].

Сучасний стан криміналістичного забезпечення характеризується виокремленням інформаційної складової: до засобів криміналістичної техніки відносять засоби накопичення, обробки та систематизації інформації, зокрема автоматизовані інформаційно-пошукові системи [2, с. 15], формами

концентрації облікової інформації дедалі частіше є автоматизовані банки даних [2, с. 22], а система обліків охоплює облік генетичних ознак людини, записів голосів і мовлення осіб [2, с. 23]. Сучасні засоби розробляються на основі досягнень природничих наук, математики та кібернетики [3, с. 11]; до кібернетичних методів криміналістики відносять комп'ютерне моделювання, автоматизовані інформаційно-пошукові системи, бази даних і комп'ютерне розпізнавання образів [3, с. 43]. Окремим полем застосування цих технологій стала протидія злочинності у сфері високих інформаційних технологій, що потребує спеціального організаційно-правового і тактичного забезпечення [5].

Водночас інноваційність засобу не підміняє його допустимості. До криміналістичних засобів висувають вимоги безпечності, наукової спроможності та етичності [2, с. 19], а умови, порядок і результати їх застосування мають відображатися в процесуальних документах [3, с. 12]. Для цифрових технологій, результати яких суд має змогу перевірити, ці вимоги є визначальними.

Найбільш перспективним методичним напрямом є алгоритмізація розслідування. Як зазначає В. Ю. Шепітько, алгоритмізувати можна лише ті дії слідчого, для яких визначено вихідні дані – типові слідчі ситуації, сукупності слідів, способи та знаряддя кримінального правопорушення [6, с. 85], а окрема криміналістична методика по суті є системою типових програм дій слідчого [6, с. 86]. Типізація слідчих ситуацій є інформаційною основою для створення алгоритмів із використанням комп'ютерної техніки [3, с. 25], проте єдиного алгоритму для криміналістичних завдань будь-якого класу розробити неможливо [3, с. 28]. Отже, цифрові системи підтримки рішень слідчого мають бути видовими – під конкретні злочинні технології. Для угруповань у господарській сфері вихідною основою може слугувати специфічна слідча ситуація, коли їхні злочини пов'язані з кіберзлочинами та використанням віртуальних активів [1, с. 8].

Поруч з алгоритмізацією розвивається стандартизація: для

документування міжнародних злочинів запроваджено стандарти розслідування, зокрема Протокол Берклі щодо відкритих цифрових даних, які стосуються насамперед збирання окремих видів, зокрема цифрової, доказової інформації [6, с. 87]. Такий підхід доцільно поширити на роботу з цифровими слідами організованих угруповань. Серед найбільш дієвих негласних слідчих (розшукових) дій у цій категорії проваджень визначають зняття інформації з електронних інформаційних систем, зокрема контроль за криптовалютними біржами, а серед напрямів застосування спеціальних знань – дослідження закономірностей виникнення електронних слідів, їх фіксацію й вилучення, удосконалення комп'ютерно-технічної та телекомунікаційної експертиз [1, с. 10]. Головною перешкодою залишається кадровий чинник: більшість правоохоронців мало обізнані з можливостями віртуальних активів [1, с. 32].

Перспективи розвитку інноваційних криміналістичних технологій у протидії організованій злочинності вбачаємо в такому: 1) інтеграції криміналістичних обліків, баз даних і масивів електронних слідів, зокрема транзакцій з віртуальними активами, в єдине аналітичне середовище для виявлення стійких зв'язків між учасниками угруповань; 2) розробленні видових цифрових алгоритмів розслідування типових злочинних технологій; 3) стандартизації порядку фіксації, вилучення та збереження цифрових доказів; 4) удосконаленні експертних методик щодо віртуальних активів; 5) посиленні криміналістичної освіти як складової криміналістичного забезпечення [3, с. 8]; 6) нормативному врегулюванні обігу віртуальних активів, зокрема запровадженні окремої норми про їх незаконне використання [1, с. 6].

Отже, криміналістика має теоретичний фундамент для технологічної відповіді на цифровізацію організованої злочинності, однак наявні засоби переважно спрямовані на ідентифікацію окремих об'єктів і недостатньо пристосовані до аналізу злочинної діяльності угруповання як системи. Подолання цього розриву потребує поєднання інформаційно-аналітичних технологій, стандартизованих процедур роботи з цифровими слідами та

належної підготовки кадрів за умови дотримання вимог законності, наукової обґрунтованості й етичності.

Список використаних джерел:

1. Пашинська І. В. Теоретико-методологічні основи розслідування організованої злочинності у сфері господарської діяльності : дис. … д-ра філософії : 081 Право / Харків. нац. ун-т внутр. справ. Харків, 2023. 296 с. URL: https://dspace.univd.edu.ua/items/5de74ab8-9658-4796-8773-ccee5340353d (дата звернення: 29.09.2026).

2. Копча В. В., Копча Н. В. Криміналістична техніка, тактика і методика : навч. посіб. Одеса : Видавничий дім «Гельветика», 2022. 286 с. URL: https://fpk.in.ua/images/biblioteka/4bac_pravo/KRYMINALISTYCHNA-TEKHNIKA2022.pdf (дата звернення: 29.09.2026).

3. Пряхін Є. В. Криміналістичні засоби та методи розслідування кримінальних правопорушень : навч. посіб. Львів : Львів. держ. ун-т внутр. справ, 2022. 164 с. URL: https://dspace.lvduvs.edu.ua/handle/1234567890/4380 (дата звернення: 29.09.2026).

4. Криміналістика : підручник : у 2 т. / за ред. В. Ю. Шепітька. Харків : Право, 2019. Т. 1 / В. Ю. Шепітько, В. А. Журавель, В. О. Коновалова та ін. 456 с.

5. Організаційно-правові та тактичні основи протидії злочинності у сфері високих інформаційних технологій : навч. посіб. / В. М. Бутузов, В. Д. Гавловський, Л. П. Скалозуб та ін. ; за ред. Б. В. Романюка, Є. Д. Скулиша. Київ, 2011. 404 с.

6. Шепітько В. Ю. Проблеми алгоритмізації та стандартизації розслідування воєнних злочинів. Актуальні питання криміналістики та судової експертизи в умовах воєнного стану : матеріали наук.-практ. конф. (м. Київ, 3 лип. 2024 р.). Київ, 2024. С. 85–88. URL: https://elar.navs.edu.ua/handle/123456789/32892 (дата звернення: 29.09.2026).

СЕКЦІЯ 5.
НОВІ СТАНДАРТИ ПРОФЕСІЙНОЇ ПІДГОТОВКИ ФАХІВЦІВ ДЛЯ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ПРОТИДІЇ ЗЛОЧИННОСТІ В УМОВАХ КОНФЛІКТУ.

ВАЛЄЄВ Руслан
доцент кафедри адміністративного права і процесу ННІ ПФППД НПУ Дніпровського державного університету внутрішніх справ кандидат педагогічних наук

ІНТЕГРАЦІЯ INTELLIGENCE-LED POLICING ТА ПЕРЕДОВИХ ТЕХНОЛОГІЙ ЯК ОСНОВА СУЧАСНОЇ МОДЕЛІ ПРОТИДІЇ ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ

Масштабна військова агресія проти нашої країни змінила різні сфери життєдіяльності суспільства, зокрема, поліцейську діяльність. На сьогодні поліція здійснює багато нових завдань, пов’язаних з: дотриманням обмежень воєнного стану, контролем переміщення людей і транспорту, контролем за військово-мобілізаційним обліком, протидією диверсіям та мародерству, підтримкою і супроводом гуманітарної допомоги, забезпеченням евакуації населення, залученням територіальних громад до створення безпечного середовища, проведенням інформаційно-роз’яснювальної роботи щодо правил поведінки під час воєнного стану, тощо. Також поліція адаптувалась до виконання звичайних функцій в умовах воєнного часу, що передбачає, зокрема, підвищення мобільності, пильності поліцейських для реагування на загрози безпеці, посилення комунікації між поліцією та населенням через гарячі лінії, мобільні додатки та соціальні мережі. Разом з цим, ми спостерігаємо критичне зниження довіри населення до поліції, що створює додаткове психологічне навантаження на поліцейських

[1].

При цьому організована злочинність залишається однією з найбільш серйозних і стійких загроз для безпеки суспільства у західних демократіях та багатьох країнах перехідного типу. Її транснаціональний характер, фінансова спроможність і здатність проникати у національні економіки взагалі ставлять під сумнів ефективність традиційної поліцейської діяльності. У зв'язку з цим сучасна поліція дедалі більше спирається на інноваційні моделі поліцейської діяльності, новітні криміналістичні технології та експертні дослідження.

Протидія організованій злочинності в умовах воєнного стану набуває нових напрямів і характеристик. Якщо звернутися до закордонних досліджень, то ми побачимо широкий тренд на застосування так званої Intelligence-Led Policing (моделі поліцейської діяльності, що керується розвідкою) в контексті протидії організованій злочинності.

Як зазначають дослідники, підхід поліцейської діяльності, керованою розвідкою, і в кризових умовах воєнного стану залишається ефективною моделлю, хоч і потребує адаптації, зокрема, певної зміни пріоритетів (превалюють воєнні ризики), та внаслідок ускладнення процесів збору та захисту розвідданих, а також каналі міжвідомчої співпраці [2].

Концепція Intelligence-Led Policing ґрунтується на зборі, аналізі та стратегічному використанні кримінальної розвідки для нейтралізації організованих злочинних груп [3]. Комплексні наукові огляди доводять, що цей підхід дозволяє зосереджувати ресурси на ключових учасниках та інфраструктурах злочинності, замість розпорошення поліцейської уваги на одиничні події та прояви [4].

Поліцейська діяльність в контексті протидії організованій злочинності паралельно впроваджує криміналістичні інновації, які докорінно змінюють розкриття та розслідування злочинів. Особливе значення має цифрова криміналістика, що включає від вилучення даних зі смартфонів до аналізу зашифрованих хмарних сервісів. За висновком закордонних фахівців, такі методи дають можливість виявляти комунікаційні схеми, фінансові потоки та

внутрішню структуру злочинних мереж [5]. Не менш актуальними є фінансові розслідування, зокрема застосування блокчейн-аналізу та судово-бухгалтерської експертизи, які дозволяють завдавати удару по фінансовій основі організованої злочинності. Таким чином, інноваційні методи не лише викривають злочини, а й унеможливлюють подальше функціонування злочинних груп [6].

Серед сучасних технологій суперечливим залишається застосування поліграфа. У низці західних країн він використовується в розслідуваннях, однак його наукова валідність не є остаточно підтвердженою. Дослідники підкреслюють, що аналізи свідчать про середній рівень точності цієї технології, із суттєвими коливаннями залежно від контексту [7]. Тому загальним трендом на Заході є пропозиція розглядати поліграф не як самостійний метод, а як допоміжний інструмент, особливо у поєднанні з алгоритмами машинного навчання та психофізіологічним аналізом. При цьому критики наголошують на етичних ризиках, потенційних хибних результатах та обмеженій допустимості в суді [8].

Раніше ми відзначали перспективність створення додатку, який за допомогою технологій доповненої реальності (та, можливо, штучного інтелекту) допоможе поліцейським на блокпості ефективніше виконувати функції за рахунок автоматичної ідентифікації транспортних засобів, причетних раніше до порушень. А у разі використання технологій штучного інтелекту – цей додаток може бути здатний допомагати поліцейським визначати індикатори ризику [9].

Отже, інтеграція Intelligence-Led Policing, цифрових методів криміналістики та експертних досліджень формує основу сучасної західної моделі протидії організованій злочинності. Використання поліграфа ілюструє як перспективність інновацій, так і ризики їхнього некритичного впровадження. Ключовим завданням майбутнього є пошук балансу між технологічним прогресом, етичними стандартами та правовими гарантіями, щоб новітні засоби зміцнювали, а не підривали довіру до правоохоронних

органів.

Список використаних джерел:

1. Валєєв Р.Г., Герасимчук Ю.В. Стресори у роботі поліцейського: підходи західних науковців. Вісн. Луганського держ. ун-тету внутр. справ ім. Е.О. Дідоренка. 2019. № 3 (87). С. 220-234.

2. Khalfa R., Hardyns W. ‘Led by Intelligence': A Scoping Review on the Experimental Evaluation of Intelligence-Led Policing. Evaluation Review. 2024. T. 48. № 5. – С. 797-847.

3. Phythian R. Intelligence-led policing in the 21st century: a strategic review . Policing: A Journal of Policy and Practice. 2024. Vol. 18, № 1. – P. 55–70.

4. Calderoni F., Campedelli G.M., Marchesi M. Organised crime groups: systematic review protocols. Campbell Collaboration. 2022. (Research report). URL: https://www.campbellcollaboration.org. Дата звернення: 22.09.2025.

5. Inside Interpol’s innovation lab. Financial Times, 8 January 2025. URL: https://www.ft.com Дата звернення: 20.09.2025.

6. National Institute of Justice (U.S. Department of Justice). Law 101: legal guide for the forensic expert. Washington, D.C.: U.S. Dept. of Justice, National Institute of Justice, 2021. URL: https://nij.ojp.gov/library. Дата звернення: 20.09.2025.

7. Honts C.R., Amato S.L., Gordon A.K. A comprehensive meta-analysis of the comparison question test. International Journal of Psychophysiology. 2021. Vol. 165. P. 123 – 138.

8. Kotsoglou K.N., Winand J., Schreiber H. Polygraph-based deception detection and machine learning: a critical review. Journal of Investigative Psychology and Offender Profiling. 2024. Vol. 21, № 2. – P. 145 – 163.

9. Валєєв Р.Г. Впровадження технологій доповненої реальності (augmented reality) для виконання завдань блокпостів: постановка проблеми. Актуальні питання правового забезпечення сектору безпеки та оборони у сучасних умовах. ІІ всеукр. наук.-практ. конфер. Збірник тез доповідей, Харків: Друкарня Нац. академії Національної гвардії України, 2024. 149 с. С. 25 – 29.

ВОЛОБОЄВ Артур
доктор філософії в галузі права, начальник відділу організації освітнього процесу Донецького державного університету внутрішніх справ ORCID: https://orcid.org/0000-0002-7138-5847

ГАБОРЕЦЬ Ольга
доктор філософії, доцент, доцент кафедри оперативно-розшукової діяльності та інформаційної безпеки навчально-наукового інституту підготовки фахівців для підрозділів кримінальної поліції Донецького державного університету внутрішніх справ ORCID: https://orcid.org/0000-0001-7791-6795

РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ ТА СИСТЕМ ОБРОБКИ ВЕЛИКИХ ДАНИХ ПІД ЧАС ВІЙНИ

Трансформація сучасних збройних конфліктів під впливом цифрових технологій породжує нові виклики для міжнародного права та механізмів забезпечення правосуддя. Ця проблематика набуває актуальності з огляду використання штучного інтелекту та систем обробки великих даних для документування воєнних злочинів і протидії організованій злочинності в умовах активних бойових дій. Однак дослідження такого феномену вимагає комплексного підходу, що поєднує аналіз правових норм, технологічних можливостей та етичних обмежень.

Так, досвід російсько-української війни безпосередньо свідчить, як цифрові технології змінюють природу воєнного правосуддя. Вперше в історії збройних конфліктів спостерігається масштабне застосування алгоритмів розпізнавання обличчя для ідентифікації військових злочинців. Зокрема,

українські державні інститути через систему Clearview AI отримали доступ до бази даних обсягом понад 30 мільярдів зображень [1], що дозволяє ідентифікувати осіб з числа російських військових та державних службовців. Поряд з цим розвивається практика використання блокчейн-технологій для створення незмінних ланцюгів доказів. Наприклад, докази руйнувань освітніх закладів у Харкові були зафіксовані одночасно в семи різних блокчейн-протоколах, забезпечуючи їх автентичність для подальшого розгляду в Міжнародному кримінальному суді [2].

Однак технологічний прогрес випереджає розвиток правових механізмів регулювання. Аналіз чинної нормативної бази виявляє системні прогалини в регламентації використання алгоритмічних систем у воєнний час. Женевські конвенції, прийняті в середині XX століття, оперують категоріями фізичного світу й не передбачають регулювання цифрового простору. Навіть сучасні спроби адаптації міжнародного гуманітарного права до цифрових реалій залишаються фрагментарними [3]. Резолюція Генеральної Асамблеї ООН 79/239 хоча й проголошує принцип поширення норм міжнародного права на системи штучного інтелекту, але не містить конкретних механізмів імплементації цих норм. У зв’язку з цим, технічні характеристики сучасних систем аналізу даних створюють ілюзію об'єктивності та точності прийняття рішень. Так, дослідження Ніла Шаха, Нандіш Бхагата та Манан Шаха свідчить про те, що є можливість досягнення 94,25% точності в прогнозуванні злочинів за допомогою алгоритмів машинного навчання [4]. У військовій сфері згорткові нейронні мережі можуть забезпечувати розпізнавання об'єктів з великою точністю на найближчий відстані, проте саме висока ефективність цих систем породжує небезпечну тенденцію до автоматизації важливих рішень.

Практика застосування алгоритмічних систем у реальних бойових умовах розкриває суттєві протиріччя між технологічною ефективністю та гуманітарними принципами. Дослідження Міжнародного комітету Червоного Хреста фіксує феномен «упередженість автоматизації» – схильність

операторів некритично довіряти рекомендаціям машинних алгоритмів [5]. Коли система пропонує військовому командиру перелік потенційних цілей з розрахованими коефіцієнтами ймовірних втрат, виникає спроба делегувати моральну відповідальність алгоритму. Тобто людське життя прирівнюється до статистичної складової, а етичні дилеми підміняються математичними розрахунками.

Особливо гостро ця проблема проявляється в контексті ізраїльсько-палестинського конфлікту. Система «Lavender» [6], розроблена для ідентифікації потенційних бойовиків, присвоює числові рейтинги десяткам тисяч осіб на основі аналізу їхніх соціальних зв'язків, комунікацій та переміщень. При заявленій великій точності система вказує помилкові позитивні результати, що в умовах збройного конфлікту означає загибель цивільних осіб. До того ж, алгоритм «The Gospel» додатково генерує списки інфраструктурних об'єктів для ураження з метою «психологічного шоку», що є спробою легітимізації атаки на цивільні об'єкти через технократичну раціональність.

Водночас, розвиваються конструктивні форми міжнародної співпраці у сфері цифрового правосуддя. Створення Євроюстом централізованої бази даних доказів міжнародних злочинів вказує на перехід до нової концепції транснаціональної юстиції [7]. База включає інформацію про понад 107 тисяч проваджень, забезпечуючи безпрецедентні можливості для координації зусиль національних правоохоронних органів [8]. Інтеграція таких елементів машинного навчання дозволяє виявляти приховані зв'язки між окремими епізодами злочинної діяльності, формуючи цілісну картину системних порушень міжнародного права. Тут проблема збереження приватності в умовах тотальної цифровізації військових операцій виходить за межі безпосереднього конфлікту, формуючи нову соціальну реальність правоохоронного контролю та нагляду.

Крім того, квантові обчислення відкривають нові горизонти для аналізу великих даних, одночасно створюючи загрози для систем шифрування та

автономних бойових можливостей [9]. Здатність квантових комп'ютерів розв'язувати криптографічні задачі на порядок швидше за класичні системи означає потенційну вразливість усієї накопиченої зашифрованої інформації. Це породжує неоднозначну ситуацію – дані, зібрані сьогодні під захистом сучасних криптографічних протоколів, можуть стати повністю відкритими через декілька років з появою достатньо потужних квантових систем.

З огляду на це, пошук балансу між технологічною ефективністю та збереженням фундаментальних правових принципів вимагає переосмислення базових категорій міжнародного права. Зокрема, щодо збереження людського контролю та відповідальності, а також потенційного порушення міжнародних гуманітарних принципів, таких як розрізнення та пропорційність [10]. На нашу думку, еволюція правових механізмів повинна враховувати динамічну природу технологічного розвитку. Необхідні гнучкі регуляторні інструменти, здатні адаптуватися до нових викликів без тривалих процедур перегляду. Це може включати створення спеціалізованих міжнародних органів з повноваженнями на оперативне регулювання використання штучного інтелекту у військовій та правоохоронній сферах.

Отже, підсумовуючи слід зазначити, що досвід сучасних збройних конфліктів свідчить про невизначену природу цифрових технологій у контексті воєнного правосуддя. З одного боку, системи штучного інтелекту та обробки великих даних створюють нові можливості для документування злочинів і забезпечення невідворотності покарання. З іншого, – вони породжують нові форми дегуманізації конфлікту та розмивання моральної відповідальності.

Подальший розвиток цієї сфери залежатиме від здатності міжнародної спільноти виробити збалансовані підходи, що поєднують технологічну інновацію з непохитною прихильністю гуманітарним цінностям. Тут важливим є збереження людини як центрального суб'єкта прийняття рішень, попри випадки делегувати складні моральні вибори безстороннім алгоритмам. Оскільки лише через усвідомлене обмеження технологічних наслідків

можливе збереження етичності в цифрову епоху.

Список використаних джерел:

1. Clearview AI допомогла ідентифікувати 50 осіб, причетних до викрадення дітей з України. 2025. Вебпортал державного інформаційного агентства України «УКРІНФОРМ». URL: https://surl.li/pkziby.

2. Russian war crimes in Ukraine documented on blockchain. AI Business. 2022. URL: https://aibusiness.com/responsible-ai/russian-war-crimes-in-ukraine-documented-on-blockchain.

3. Seventy-ninth session (GA/DIS/3757). 2024. United Nations. URL: https://press.un.org/en/2024/gadis3757.doc.htm.

4. Shah N., Bhagat N., Shah M. Crime forecasting: a machine learning and computer vision approach to crime prediction and prevention. Visual Computing for Industry, Biomedicine, and Art. 4: 9 (2021). URL: https://vciba.springeropen.com/articles/10.1186/s42492-021-00075-z.

5. Transcending weapon systems: the ethical challenges of AI in military decision support systems. 2024. ICRC Law and Policy Blog. URL: https://blogs.icrc.org/law-and-policy/2024/09/24/transcending-weapon-systems-the-ethical-challenges-of-ai-in-military-decision-support-systems/.

6. Ізраїльські військові використовують ШІ для вибору цілей у Газі. Вебпортал «Українська правда». URL: https://mezha.media/2024/04/04/izrailski-viyskovi-shtuchnyy-intelekt/.

7. Core International Crimes Evidence Database. 2024. Eurojust. URL: https://www.eurojust.europa.eu/core-international-crimes-evidence-database.

8. Artificial Intelligence and War Crimes Investigations. Institute for War and Peace Reporting. URL: https://iwpr.net/global-voices/artificial-intelligence-and-war-crimes-investigations.

9. The Emerging Potential for Quantum Computing in Irregular Warfare. 2025. Irregular Warfare Center. URL: https://irregularwarfarecenter.org/publications/insights/the-emerging-potential-for-

quantum-computing-in-irregular-warfare/.
10. The Integration of AI in Modern Warfare: Ethical, Legal, and Practical Implications. 2024. CYIS. URL: https://www.cyis.org/post/the-integration-of-ai-in-modern-warfare-ethical-legal-and-practical-implications.

КАРПЕНКО Олександр
старший викладач кафедри вогневої підготовки Дніпровського державного університету внутрішніх справ

ВІРТУАЛЬНА РЕАЛЬНІСТЬ І ЛАЗЕРНІ СИМУЛЯТОРИ ЯК СУЧАСНІ ЗАСОБИ ПІДГОТОВКИ ПОЛІЦЕЙСЬКИХ ДО ВОГНЕВОЇ ПІДГОТОВКИ

Сучасні виклики у сфері забезпечення правопорядку вимагають від поліцейських не лише високого рівня фізичної підготовки, а й стійкої психологічної витривалості та здатності миттєво ухвалювати рішення в умовах ризику й невизначеності.

Традиційні методи вогневої підготовки, попри свою ефективність, не завжди здатні відтворити динаміку та непередбачуваність реальних подій. Також, як зазначає Карпенко Олександр Миколайович: «на жаль, на сьогодні, стан злочинності з використанням зброї, за даними кримінологів, значно зріс, а зумовлено тим, що за останніми статистичними даними, на руках українців зареєстровано близько мільйона одиниць зброї»[5, с. 115]. Саме тому впровадження технологій віртуальної реальності та лазерних симуляторів у систему вогневої підготовки поліцейських виступає сучасним інструментом запобігання ризикам і формування високого рівня професійної готовності.

У цьому контексті використання технологій віртуальної реальності (ВР) та лазерних симуляторів стає одним із ключових напрямів модернізації

професійної підготовки правоохоронців. Ці інструменти не лише розширюють спектр навчальних сценаріїв, а й дозволяють підвищити безпеку, оптимізувати ресурси та забезпечити системний розвиток професійних компетентностей поліцейських[3, с. 45].

Віртуальна реальність створює ефект повного занурення й дає змогу курсантам відпрацьовувати тактичні та стрілецькі навички в умовах, максимально наближених до реальних операцій, що суттєво підвищує якість підготовки. Завдяки ВР можна змоделювати широкий спектр сценаріїв - від рутинного патрулювання до складних тактичних операцій зі штурму приміщень і тим самим формувати вміння швидко та коректно оцінювати обстановку, ухвалювати правомірні рішення щодо застосування зброї та відрізняти реальну загрозу від поведінки цивільних осіб.

Тренування віртуальному середовищі забезпечують високий рівень безпеки для учасників і водночас дозволяють оптимізувати витрати на боєприпаси та утримання полігонів і стрільбищ, що особливо актуально в умовах воєнного стану та обмеженого фінансування. Окрім цього, ВР-моделювання створює контрольований стресовий контекст, у якому формуються стресостійкість і емоційний самоконтроль - критично важливі якості для службовця під час ризикованих ситуацій; реалістичні симуляції сприяють виробленню професійного реагування під тиском.

Лазерні симулятори в ролі технічного доповнення до ВР-систем дозволяють відшліфувати ключові елементи стрілецької майстерності - правильне прицілювання та утримання зброї, техніку натискання на спусковий гачок, швидкість і точність пострілів - і забезпечують миттєвий зворотний зв’язок для оперативної корекції помилок.

Також Зеленський Є.С. звертає увагу на те, що: «підготовка поліцейських до виконання завдань в умовах психологічних навантажень є надзвичайно важливою, оскільки виконання завдань під час виникнення надзвичайних ситуацій або під час дії воєнного стану супроводжується значними загрозами для життя та здоров’я»[4, с. 667].

Також штучний інтелект може використовуватися для аналізу інформації, прогнозування розвитку подій та прийняття рішень у складних ситуаціях, наприклад, під час бойових дій або масових заворушень[6, с. 299].

Правові аспекти підготовки правоохоронців є невід'ємною складовою цього процесу: ч. 1 ст. 36 Кримінального кодексу України закріплює право на необхідну оборону як засіб захисту від суспільно небезпечного посягання, а ст. 43 ККУ визначає правомірність дій працівників правоохоронних органів при застосуванні зброї за умови дотримання закону, що підкреслює необхідність професійної, юридично вивіреної підготовки для забезпечення пропорційності та законності застосування сили [1].

Крім того, положення ст. 223 Кримінального процесуального кодексу України зобов'язують проводити слідчі та процесуальні дії з повагою до прав і свобод людини; відповідно, інтеграція ВР і лазерних технологій у навчальний процес дозволяє відпрацьовувати сценарії затримання, обшуків і тактичних операцій у безпечних умовах, мінімізуючи ризики перевищення повноважень та порушень прав громадян у реальних операціях[2].

Інтеграція технологій віртуальної реальності та лазерних симуляторів у систему підготовки поліцейських є стратегічним напрямом інноваційного розвитку правоохоронної освіти. Ці інструменти не замінюють традиційні полігони, а формують комплексний підхід, який поєднує безпечність, ресурсну ефективність, розвиток психологічної стійкості та відточування техніки володіння зброєю.

Сучасна підготовка поліцейських має бути гнучкою, адаптивною та відповідати реаліям сьогодення, а симуляційні технології є найефективнішим засобом досягнення цієї мети. Також, варто враховувати, і як зазначає Карпенко О.М. :«ми повинні пам'ятати, що всі дії поліції суворо регламентуються національном законодавством України»[5, с. 115]. У свою чергу, Зеленський Є.С. підкреслює: «актуальні шляхи удосконалення вогневої підготовки поліцейських в умовах воєнного стану включають інтенсивне тренування з вогнепальної зброї, підготовку до роботи в умовах

психологічного стресу та спільну підготовку з іншими підрозділами сил сектору безпеки та оборони»[4, с. 668].

Таким чином, впровадження інноваційних технологій у навчальний процес має стати обов'язковою складовою освітніх програм для правоохоронців. Це дозволить забезпечити їхню готовність до дій у найскладніших умовах та суттєво підвищить ефективність діяльності поліції в Україні.

Список використаних джерел:

1. Кримінальний кодекс України : Закон України від 05.04.2001 № 2341-III (зі змінами та доповненнями). Відомості Верховної Ради України. 2001. № 25–26. Ст. 131. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата використання: 20.09.2025).

2. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 № 4651-VI (зі змінами та доповненнями). Відомості Верховної Ради України. 2013. № 9–10. Ст. 88. URL: https://zakon.rada.gov.ua/go/4651-17 (дата використання: 20.09.2025).

3. Захаров, А. П. Технології віртуальної реальності в силових структурах. Харків : Право, 2023. 245 с.

4. Зеленський Є.С., Глян Т. Актуальні шляхи удосконалення вогневої підготовки поліцейських в умовах воєнного стану. Матеріали VIII міжнародної науково-практичної конференції (ДДУВС, 15.03.2024). Частина II. Дніпро : ДДУВС, 2024. С.667-668.DOI:10.31733/15-03-2024/2/667-668.URL: https://er.dduvs.edu.ua/bitstream/123456789/13947/1/314.pdf (дата використання: 20.09.2025).

5. Карпенко О.М. Короткіх А.А. Завдання правоохоронних органів щодо запобігання правопорушенням у сфері обігу вогнепальної зброї. URL: https://er.dduvs.edu.ua/bitstream/123456789/5668/1/21.pdf (дата використання: 20.09.2025).

6. Бойко О.І., Мельник А.М. Перспективи використання сучасних інтерактивних технологій в процесі підготовки поліцейського до діяльності в

умовах воєнного стану. Аналітично-порівняльне правознавство. 2024. № 3 (50). С. 297-302. DOI: 10.24144/2788-6018.2024.03.50. URL: https://app-journal.in.ua/wp-content/uploads/2024/06/52.pdf (дата використання: 20.09.2025).

КОРОВКА Дар'я
курсантка 2-го курсу *факультету підготовки фахівців для органів досудового розслідування Національної поліції України Донецького державного університету внутрішніх справ*

Науковий керівник:
ХИТРОВСЬКИЙ Дмитро
старший викладач кафедри загальноправових дисциплін факультету підготовки фахівців для органів досудового розслідування Національної поліції України Донецького державного університету внутрішніх справ

МІЖНАРОДНІ СТАНДАРТИ ПРАВ ЛЮДИНИ ТА ЇХ ІМПЛЕМЕНТАЦІЯ У ПРОФЕСІЙНУ ПІДГОТОВКУ ПОЛІЦЕЙСЬКИХ

Повага до прав людини та їх захист становлять фундамент сучасної демократичної держави та є визначальними орієнтирами для діяльності всіх правоохоронних органів, зокрема поліції. У глобалізованому світі, де взаємодія держав та міжнародних інституцій стає все більш тісною, імплементація міжнародних стандартів прав людини у національну правову систему та практичну діяльність правоохоронців набуває особливої актуальності. Саме від рівня знань, правосвідомості та професійної підготовки поліцейських залежить ефективність реалізації цих стандартів на практиці та довіра суспільства до інститутів державної влади.

Міжнародні стандарти прав людини – це закріплені у міжнародних договорах, деклараціях та конвенціях норми, які визначають основні права та свободи особи, а також механізми їх забезпечення й захисту. Основоположними документами у цій сфері є Загальна декларація прав

людини 1948 року, Міжнародний пакт про громадянські та політичні права 1966 року, Європейська конвенція з прав людини 1950 року, Конвенція проти катувань та інших жорстоких, нелюдських або таких, що принижують гідність, видів поводження чи покарання 1984 року тощо. Ці акти встановлюють базові принципи, якими повинні керуватися правоохоронні органи: верховенство права, недискримінація, заборона катувань, право на справедливий суд, презумпція невинуватості, право на приватність та інші [1, 2].

Для поліції, як інституції, що здійснює примусові заходи від імені держави, дотримання міжнародних стандартів прав людини має подвійне значення. По-перше, вони виступають як нормативний орієнтир для розроблення внутрішніх законодавчих актів та підзаконних нормативів. По-друге, вони формують етичну основу професійної діяльності поліцейського, який повинен діяти не лише в межах закону, а й у дусі поваги до людської гідності [3].

Імплементація міжнародних стандартів у підготовку поліцейських передбачає інтеграцію відповідних знань, навичок та цінностей на всіх рівнях професійної освіти – від базового навчання до підвищення кваліфікації. Законодавство України, зокрема Закон «Про Національну поліцію», Кримінальний процесуальний кодекс та інші акти, містять посилання на міжнародні договори та принципи, які становлять основу навчальних програм поліцейських навчальних закладів. Це дозволяє забезпечити узгодженість національних стандартів з міжнародними вимогами. Навчальні плани поліцейських академій включають дисципліни, присвячені міжнародному праву, правам людини, етиці поліцейської діяльності та практиці Європейського суду з прав людини. Значна увага приділяється вивченню реальних кейсів, аналізу судових рішень, а також моделюванню ситуацій, у яких поліцейські мають приймати рішення відповідно до стандартів прав людини. Особливе місце займає тренінгова підготовка, яка включає відпрацювання алгоритмів дій у ситуаціях, пов’язаних із застосуванням сили,

затриманням осіб, проведенням обшуків, допитів тощо. Такий підхід дозволяє сформувати у поліцейських не лише теоретичні знання, а й практичні навички дотримання прав людини в реальних умовах. Професійна підготовка має включати компоненти, що сприяють розвитку емпатії, навичок ненасильницької комунікації, стресостійкості та толерантності. Це допомагає мінімізувати ризики порушення прав людини під час виконання службових обов'язків [4].

Незважаючи на значні досягнення, існує низка проблем, що ускладнюють ефективну імплементацію міжнародних стандартів. Серед них: недостатній рівень практичної підготовки поліцейських у сфері прав людини, брак кваліфікованих викладачів та тренерів, обмежені ресурси для проведення тренінгів, а також відсутність системи постійного моніторингу та оцінки ефективності навчальних програм.

Для подолання цих викликів доцільно:

- розширити міжнародне співробітництво з поліцейськими академіями інших країн;
- запровадити обов'язкову сертифікацію викладачів із прав людини;
- створити національну систему стандартів професійної підготовки з акцентом на права людини;
- активно залучати представників громадянського суспільства до процесу навчання та оцінки діяльності поліції [5].

Отже, міжнародні стандарти прав людини є не лише юридичним орієнтиром, а й морально-етичною основою діяльності поліції. Їх ефективна імплементація у професійну підготовку працівників поліції дозволяє підвищити якість правоохоронної діяльності, зміцнити верховенство права, зменшити ризик порушень прав людини та підвищити рівень довіри громадян до державних інституцій. У сучасних умовах воєнного стану та трансформації суспільства цей процес набуває особливої важливості, оскільки саме поліція є одним із головних гарантів дотримання прав і свобод людини на практиці.

Перспективи подальшого дослідження міжнародних стандартів прав

людини та їх імплементації у професійну – підготовку поліцейських полягають у поглибленому аналізі ефективності існуючих освітніх програм, розробці нових тренінгових моделей з урахуванням сучасних викликів, таких як гібридні загрози, кіберзлочинність та діяльність правоохоронців в умовах воєнного стану. Важливим напрямом є вивчення практики застосування стандартів прав людини в реальних оперативних ситуаціях, порівняльний аналіз міжнародного досвіду, а також створення інтегрованих методик оцінки рівня правової культури поліцейських. Це дозволить не лише удосконалити систему підготовки кадрів, а й підвищити ефективність захисту прав людини в Україні відповідно до найкращих світових практик.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Загальна декларація прав людини: прийнята і проголошена Генеральна Асамблея ООН резолюцією 217 А (III) від 10.12.1948 р. – Режим доступу: https://www.un.org (дата звернення 01.10.2025).
2. Міжнародний пакт про громадянські і політичні права : прийнятий і відкритий для підписання, ратифікації і приєднання резолюцією 2200 А (XXI) Генеральної Асамблеї ООН від 16.12.1966 р. ратифікований : Указ Президії Верховної Ради УРСР № 2148-VIII від 19.10.1973 р. База даних «Законодавство України». – Режим доступу: https://zakon.rada.gov.ua/go/995_043 (дата звернення 01.10.2025).
3. Конвенція про захист прав людини і основоположних свобод: ратифікована Законом України від 17.07.1997 р. № 475/97-ВР. Відомості Верховної Ради України. 1997. № 40. С. 263. – Режим доступу: https://zakon.rada.gov.ua/laws/show/475/97-%D0%B2%D1%80.(дата звернення 01.10.2025).
4. Мащенко В. С. Теоретико-правові засади імплементації зарубіжних моделей поліцейського адміністративного нагляду як стратегічного превентивного механізму: компаративний дискурс та вектори адаптації в національну правову систему України. Український політико-правовий дискурс. 2025. С. 15-24. – Режим доступу:

https://ppdnz.com.ua/index.php/home/article/view/228/146.(дата звернення 01.10.2025).

5. Хоркавий С. В. Європейські стандарти діяльності поліції: досвід для України. Нове українське право. 2024. № 3. С. 186-192. – Режим доступу: http://newukrainianlaw.in.ua/index.php/journal/article/view/632/575 (дата звернення 01.10.2025).

КОРОЛЬ Михайло
доцент кафедри адміністративної діяльності, Національна академія Державної прикордонної служби імені Богдана Хмельницького, кандидат юридичних наук, доцент

ТАРАСЮК Оксана
здобувач вищої освіти факультету правоохоронної діяльності, Національна академія Державної прикордонної служби імені Богдана Хмельницького

ВИКОРИСТАННЯ БІОМЕТРИЧНИХ ДАНИХ У СИСТЕМІ ПРИКОРДОННОГО КОНТРОЛЮ ЯК ЗАСІБ БОРОТЬБИ З ОРГАНІЗОВАНОЮ ЗЛОЧИННІСТЮ СЕРЕД ІНОЗЕМЦІВ

У сучасних умовах активізації міграційних процесів забезпечення здійснення ефективного прикордонного контролю набуває особливої ваги. В цьому контексті використання біометричних даних розглядається як високотехнологічний інструмент, що дозволяє значно підвищити рівень ідентифікації осіб, запобігти використанню підроблених документів та протидіяти організованій злочинності в сфері охорони державного кордону.

Поєднання інформаційних технологій, криміналістики та вимог нормативно-правових актів забезпечує точність і оперативність процедур прикордонного контролю, що має вирішальне значення для безпеки держави.

Особливої актуальності це питання набуває в умовах воєнного стану, коли кордони стають не лише адміністративною межею, а й місцем де забезпечується національна безпека нашої держави. Використання біометричних даних дозволяє протидіяти диверсійно-розвідувальним групам, організованим нелегальним мігрантам та транснаціональним злочинним угрупованням, які прагнуть використати особливості функціонування правового режиму воєнного стану для реалізації кримінальних схем.

Слід зазначити, що необхідність впровадження біометричних технологій зумовлена кількома факторами: міжнародний досвід підтверджує їхню ефективність у боротьбі з нелегальною міграцією; інтеграція України до європейського безпекового простору вимагає уніфікації стандартів контролю; у воєнних умовах зростає потреба у швидкій та надійній ідентифікації потенційних загроз.

Таким чином, застосування біометрії на кордоні є не лише технічним нововведенням, а й стратегічною необхідністю, покликаною зміцнити обороноздатність держави та створити бар’єр на шляху зовнішніх і внутрішніх загроз.

Фіксація біометричних даних іноземців та осіб без громадянства у пунктах пропуску через державний кордон України виступає важливим складником сучасної системи прикордонного контролю, що визначається комплексом нормативно-правових актів, зокрема Законами України «Про прикордонний контроль» та «Про правовий статус іноземців та осіб без громадянства», а також низкою відомчих наказів Міністерства внутрішніх справ України та Державної прикордонної служби України. Під біометричною фіксацією розуміють процес збору, внесення та збереження індивідуальних ідентифікаційних параметрів іноземців у відомчих інформаційно-комунікаційних системах, зокрема у системі «Гарт-1». Такий підхід

передбачає довгострокове збереження даних (до 75 років), що забезпечує можливість їх подальшої верифікації та контролю [1, с. 78].

Сучасні виклики у сфері забезпечення національної безпеки та прикордонного контролю вимагають широкого впровадження цифрових технологій, зокрема біометричних даних. Державна прикордонна служба України, перебуваючи на передньому рубежі захисту державного суверенітету, потребує високоефективних інструментів ідентифікації осіб. Біометричні дані – відбитки пальців, відцифроване зображення обличчя чи інші унікальні фізіологічні параметри – слугують надійним засобом протидії використанню підроблених документів та приховуванню особистості, що є поширеною практикою організованих злочинних угруповань серед іноземців. У воєнний період роль таких технологій значно зростає. З одного боку, Україна стикається з посиленою активністю диверсійно-розвідувальних груп, які намагаються використовувати прогалини у прикордонному контролі, з іншого – збільшується масштаб незаконної міграції, що створює додатковий ризик проникнення кримінальних елементів. У цьому контексті впровадження інформаційно-комунікаційних систем у діяльність Державної прикордонної служби України має ключове значення для автоматизації процесів фіксації, перевірки та аналізу біометричних даних [2, с. 100].

Зміщення акцентів на необхідності цифровізації та впровадженні біометричних систем є цілком виправданим, адже саме ці технології формують новий рівень превентивного контролю. Інтеграція біометрії в єдині інформаційно-аналітичні комплекси забезпечує високий ступінь достовірності ідентифікації осіб та водночас створює надійний захисний бар’єр від проникнення організованої злочинності серед іноземців, що набуває особливої ваги в умовах воєнного стану.

За таких умов процедура фіксації біометричних даних здійснюється з урахуванням ризик-орієнтованого підходу та може відбуватися на різних рівнях контролю – від паспортної лінії до службових приміщень або місць адміністративного затримання. Верифікація передбачає сканування від одного

до п’яти відбитків пальців, що уможливлює підтвердження особи чи виявлення невідповідностей із наявними у базі даними. У разі відмови від надання біометричних параметрів питання пропуску вирішується на другій лінії контролю. Важливим є і те, що передбачено окремий порядок для категорій іноземців, визначених законодавством та міжнародними договорами, які звільняються від фіксації біометрії [1, с. 84].

Застосування біометричних даних у сфері прикордонного контролю є не лише технічною інновацією, а й важливим інструментом зміцнення національної безпеки та протидії організованій злочинності серед іноземців. Практика засвідчує, що біометричні технології істотно мінімізують ризики використання фальсифікованих документів, забезпечують оперативне виявлення правопорушників і запобігають повторному перетину кордону особами, пов’язаними зі злочинною діяльністю. Водночас залишаються невирішеними проблеми, пов’язані із обмеженою інтеграцією відомчих систем у міжнародний інформаційний простір, загрозами несанкціонованого доступу до персональних даних і потреба уніфікації правових норм відповідно до стандартів Європейського Союзу.

З метою подолання окреслених викликів доцільним убачається вжиття цілого комплексу взаємопов’язаних заходів стратегічного, нормативно-правового та організаційного характеру. Передусім необхідною є гармонізація національної законодавчої бази з міжнародними та європейськими стандартами у сфері використання біометричних даних, що дозволить забезпечити їх юридичну сумісність і взаємовизнання на транскордонному рівні. Водночас актуальним виступає створення багаторівневої системи технічного та правового захисту персональних даних, здатної мінімізувати ризики несанкціонованого доступу, кібератак і витоку конфіденційної інформації. Важливим завданням залишається поглиблення міжвідомчої координації та розширення міжнародної співпраці у сфері обміну біометричними даними, що сприятиме оперативному виявленню осіб, причетних до транснаціональної злочинної діяльності. Не менш значущим є

формування системи спеціалізованої професійної підготовки персоналу, орієнтованої на інтеграцію новітніх технологічних рішень у практику оперативно-службової діяльності Державної прикордонної служби України. Лише синергія правових, технологічних та інституційних інновацій здатна утворити дієвий захисний механізм, що гарантуватиме ефективне блокування каналів організованої злочинності та водночас слугуватиме важливим чинником зміцнення обороноздатності та безпекового потенціалу держави.

Список використаних джерел:

1. Сойко О. Прикордонний контроль: vademecum 2. Одеса: Видавництво «Айс Принт», 2024. 468 с.

2. Король М. Упровадження цифровізації процесів адміністративно-юрисдикційної діяльності у Державній прикордонній службі України. Migration & Law. 2025. № 5(2). С. 87-102.

КОРОЛЬОВ Андрій
старший викладач кафедри тактико-спеціальної підготовки та особистої безпеки поліцейського, Донецький державний університет внутрішніх справ

ЩОДО ОСОБЛИВОСТЕЙ ВИКОРИСТАННЯ БЕЗПІЛОТНИХ АВІАЦІЙНИХ СИСТЕМ ПОЛІЦІЄЮ: ЗАКОРДОННИЙ ДОСВІД

Аналізуючи питання щодо особливостей використання безпілотних авіаційних систем в зарубіжних країнах, варто наголосити на важливості вивчення та врахування міжнародного досвіду у сфері застосування безпілотних літальних апаратів, зокрема в діяльності поліцейських органів. Актуальність цього аспекту обумовлена тим, що поліція в багатьох країнах світу вже протягом тривалого часу успішно використовує БПЛА для виконання широкого спектра завдань — від моніторингу громадського

порядку та контролю дорожнього руху до участі в операціях з пошуку та рятування, боротьби з організованою злочинністю, а також забезпечення безпеки на масових заходах.

«Впровадження БПЛА в практику поліції, - твердить Є.І. Бакутін, - сьогодні є доцільним і бажаним, зважаючи на необхідність підвищення ефективності роботи поліції. Світовий досвід показує що БПЛА перестали бути прерогативою лише військових формувань, їх все більше застосовують поліція у профілактиці, документуванні протиправних дій підчас охорони публічного порядку і безпеки» [1, с. 314].

Варто зазначити, що застосуванням та використанням безпілотних авіаційних систем в державі опікуються на самому вищому рівні. Президент України Володимир Зеленський під час підсумкової прес-конференції висловився на підтримку «збільшення виробництва вітчизняних дронів, розвитку інфраструктури для підготовки операторів БпЛА та спеціальних підрозділів в українському війську» та заявив, що «наступного року в Україні заплановане нарощення виробництва БпЛА, зокрема виготовлення 1 мільйона FPV-дронів» [2].

У країнах Європейського Союзу поліція активно експериментує з можливостями безпілотних літальних апаратів (БПЛА), розширюючи спектр їх практичного застосування відповідно до сучасних викликів у сфері громадської безпеки. Зокрема, у деяких юрисдикціях дрони оснащуються спеціальними пристроями для розпилення сльозогінного газу, що дозволяє здійснювати контроль над масовими заворушеннями з мінімальним ризиком для особового складу. Також проводяться навчання, орієнтовані на виявлення та переслідування злочинців у складних урбанізованих умовах, зокрема в густонаселених міських районах, де оперативність і точність дій є критичними.

Іноземні правоохоронні органи дедалі частіше доходять висновку, що використання БПЛА є економічно вигіднішою та тактично доцільнішою альтернативою традиційним гелікоптерам, особливо в умовах переслідування

підозрюваних. У разі, якщо злочинці чинять збройний опір, застосування дронів дозволяє знизити ризики для життя та здоров'я поліцейських, оскільки дистанційне спостереження та супровід з повітря не потребує фізичної присутності правоохоронців у небезпечній зоні.

Крім того, важливою перевагою БПЛА є їхня малопомітність або повна невидимість для правопорушників, що забезпечує ефект раптовості та дозволяє патрульним силам здійснювати затримання без попередження злочинців. Подібний підхід активно використовується і для охорони об'єктів критичної інфраструктури: дрони регулярно патрулюють периметри важливих об'єктів — таких як електростанції, транспортні вузли, водозабірні споруди — з метою виявлення можливих порушень, спроб несанкціонованого проникнення або підготовки диверсій.

Особливий інтерес становлять нестандартні напрями використання поліцейських дронів у зарубіжній практиці. Наприклад, у Японії поліція протестувала спеціалізовані БПЛА, призначені для протидії несанкціонованому використанню дронів у заборонених зонах. Основним завданням таких безпілотників є нейтралізація ворожих або підозрілих дронів шляхом закидання на них спеціальних сіток у повітрі, що дозволяє блокувати їх подальший рух і примусово посадити. Така технологія є надзвичайно актуальною для захисту стратегічних об'єктів, державних установ, аеропортів, а також місць проведення масових заходів.

Крім того, в зарубіжних країнах поліція протягом тривалого часу використовує багато високотехнологічних досягнень, таких як оптичні датчики, які в контексті технології дронів являють собою пристрої, що можуть записувати відео високої чіткості, деякі приклади включають:

- Zenmuse Z30 – це камера від DJI з 30-кратним зумом, що може бути корисним в операціях, пов'язаних зі спостереженням та відстеженням;

- Zenmuse X5S – ще одна потужна камера від DJI, яка може легко знімати відео у форматі 4K.

Теплові датчики – пристрої, які можуть перетворювати інфрачервоне

випромінювання, невидиме для очей, на видимі кольори. Різні відтінки синього та червоного використовуються для позначення діапазону температур. Деякі з популярних корисних навантажень включають: DJI Zenmuse XT; FLIR Vue Pro; FLIR Duo Pro; FLIR Tau 2.

Гучномовці (Loudspeakers) – великі дрони здатні нести гучномовці, які можна використовувати для оголошень та контролю натовпу.

Прожектори (Spotlights) – важливі корисні навантаження для нічних операцій або операцій за умов низької видимості, особливо для пошуково-рятувальних місій.

Маяки (Beacons): допомагають дронам залишатися видимими в небі, особливо вночі, таким чином попереджаючи інших про свою присутність.

Зарубіжний досвід наочно демонструє, що належне технічне оснащення поліцейських підрозділів, зокрема використання сучасних гаджетів, планшетів та безпілотних літальних апаратів (БПЛА), здатне суттєво підвищити ефективність оперативного реагування та забезпечення публічної безпеки і порядку. Так, у Великій Британії та Нідерландах поліцейські активно використовують портативні сканери, за допомогою яких можливо миттєво встановити особу та перевірити її на предмет наявності в базах розшуку за підозрою у скоєнні злочинів. Такий підхід не лише підвищує мобільність працівників поліції, а й мінімізує час, необхідний для ухвалення рішень у ситуаціях, що потребують негайного втручання.

У Сполучених Штатах Америки з 2020 року спостерігається стрімке поширення практики регулярного використання дронів у діяльності поліції. Наприклад, у деяких містах передбачено можливість надсилання БПЛА на виклик служби екстреної допомоги — у разі, якщо громадянин телефонує до поліції, на місце події може бути направлений дрон для попередньої розвідки або спостереження. Проте ефективність таких операцій може залежати від конкретних обставин та технологічного рівня обладнання.

У Німеччині БПЛА активно застосовуються для медичних потреб, зокрема — для оперативної доставки дефібриляторів на місце інциденту.

Польща, у свою чергу, розробила спеціалізований безпілотник «AtraxM», призначений для медичних завдань, який оснащений змінними контейнерами для транспортування аптечок. Ці аптечки можуть включати перев'язувальні матеріали, рятувальні комплекси для стабілізації стану постраждалих, ліки, необхідні для невідкладного введення (наприклад, адреналін чи інсулін), а також пакети з кров'ю для осіб, які перебувають у зонах надзвичайних ситуацій або бойових дій. Зазначена практика свідчить про високий рівень адаптивності європейських країн до викликів, що супроводжують кризові чи надзвичайні ситуації.

Із міжнародного досвіду також можна стверджувати, що БпЛА зарекомендували себе корисними під час масових заходів, коли неможливо застосувати гелікоптер і людям на землі важко точно оцінити ситуацію. Наприклад, визнано, що на лондонські заворушення (кілька років тому) можна було б реагувати більш успішно, якби для оцінки ситуації, яка відбувалася в натовпі, у режимі реального часу були б задіяні дрони [3, с. 10].

Висновки. Узагальнюючи викладене, можна стверджувати, що інноваційне застосування БПЛА в поліцейській діяльності за кордоном демонструє високий потенціал для підвищення ефективності правоохоронних функцій. Це охоплює як традиційні напрями — спостереження, супровід, розвідка, охорона — так і новітні технології нейтралізації загроз. Досвід європейських та азійських країн у цьому контексті може бути цінним орієнтиром для формування сучасної стратегії використання БПЛА в національній системі безпеки, особливо в умовах збройного конфлікту чи надзвичайних ситуацій.

Міжнародна практика свідчить, що БПЛА використовуються не лише з метою оперативного реагування та затримання правопорушників, але й у гуманітарних цілях — для надання невідкладної медичної допомоги в районах, куди складно дістатися наземним транспортом. Швидкість, мобільність та функціональна гнучкість таких технологій роблять їх надзвичайно ефективним інструментом у діяльності правоохоронних структур як у мирний

час, так і в умовах надзвичайних ситуацій або збройного конфлікту.

Список використаних джерел:

1. Бакутін Є.І. Напрями вдосконалення законодавчого регулювання використання безпілотних літальних апаратів (БпЛА) в діяльності поліції України. Держава і право. № 77. С. 314-327.

2. Президент: Ми підтримуємо виробництво БпЛА для війська і наступного року виготовимо 1 млн FPV-дронів. Президент України. Офіційне Інтернет – представництво. URL: https://www.president.gov.ua/news/prezident-mi-pidtrimuyemo-virobnictvo-bpla-dlya-vijska-i-nas-87865.

3. Використання безпілотних літальних апаратів в діяльності Національної поліції: методичні рекомендації / С.О. Шатрава, Д.Є. Денищук, О.В. Джафарова, І. В. Кріцак, О.В. Погорілець. Харків: Харківський національний університет внутрішніх справ, 2022. 25 с.

ОДЕРІЙ Олексій
професор кафедри кримінального процесу та криміналістики Донецького державного університету внутрішніх справ, доктор юридичних наук, професор
ЛИТВИНЕНКО Ольга
доцент кафедри кримінального процесу та криміналістики Донецького державного університету внутрішніх справ, доктор філософії в галузі «Право», майор поліції

ПРОТИДІЯ ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ В УМОВАХ ВІЙНИ (КРИМІНАЛЬНО-ПРОЦЕСУАЛЬНИЙ АСПЕКТ)

Організована злочинність в України є одним із негативних соціальних явищ, яке інтегрувалося в наше життя після проголошення Україною своєї

незалежності. Повномасштабна війна в Україні суттєво загострила соціальні, економічні, гуманітарні та інші проблеми, чим організована злочинність скористалася значно активізувавшись [1]. Так, в умовах війни держава зіткнулася з явищами, які раніше не були такими масштабними. Прикладом цього, серед іншого, є *незаконне переправлення людей через державний кордон, торгівля трофейною зброєю чи боєприпасами*, зокрема криміналітету. Такі злочини становлять колосальну загрозу для національної безпеки, бо підривають обороноздатність і створюють ґрунт для діяльності організованих угруповань.

З іншого боку неабияким важливим є процес доказування кримінальних правопорушень, вчинених організованими групами. Такий процес має свої особливості, що зумовлено високим рівнем конспірації, складною структурою груп, наявністю чітко розподілених ролей між її учасниками, а також тиском на свідків та потерпілих. У зв'язку з цим органи досудового розслідування повинні володіти не лише ґрунтовними теоретичними знаннями у сфері кримінального процесуального права та криміналістики, а й практичними навичками щодо ефективного виявлення, фіксації та використання доказів.

З огляду на наведене розслідування кримінальних правопорушень вчинених організованими групами та злочинними організаціями потребує значно більше часу, ніж розслідування інших кримінальних правопорушень, але водночас затягування строків створює ризики, в першу чергу:

а) продовження злочинної діяльності;

б) впливу на свідків;

в) знищення доказів;

г) зловживання процесуальними правами однією зі сторін кримінального провадження.

Саме тому законодавцем передбачено певну процедуру продовження строків досудового розслідування відповідно до конкретного ступеню тяжкості вчиненого кримінального правопорушення. Так, відповідно до положень ч. 4 ст. 219 КПК України строк досудового розслідування може бути

продовжений у порядку, передбаченому параграфом 4 глави 24 КПК України [2]. При цьому граничним строком досудового розслідування тяжких та особливо тяжких злочинів - є строк в дванадцять місяців з дня повідомлення особі про підозру.

У свою чергу, за результатами аналізу опитування респондентів (співробітники Департаменту стратегічних розслідувань та регіональних Управлінь) щодо термінів завершення розслідування кримінальних проваджень (які вчинялися у складі організованої групи чи злочинної організації) встановлено, що строк розслідування тривав:

від 5-ти до 12 місяців – 57%;

від 3-х до 5-ти місяців – 30%;

від 2-х до 3-х місяців – 7%;

до 2-х місяців – 4%.

Наведені результати засвідчують, що переважно запропоновані законодавцем строки є достатніми (за наявності умов для продовження строку досудового розслідування) для здійснення ефективного розслідування злочинів вчинених у складі організованих груп та злочинних організацій. Разом з тим, практики відшукують шляхи оптимізації строку досудового розслідування конкретного кримінального провадження саме за рахунок криміналістичних рекомендацій. Серед причин цьому є той факт, що існують непоодинокі випадки, коли представники організованої злочинності *продовжують* злочинну діяльність навіть *після оголошення їм підозри*. З огляду на такі обставини та враховуючи що злочини, які вчиняються організованою групою чи злочинною організацією (за ступенем тяжкості) є тяжкі або особливо тяжкі, - в такій категорії кримінальних проваджень *має обиратись найбільш суворий запобіжний захід, який унеможливить продовження злочинної діяльності окремими членами вказаних злочинних формувань під час досудового розслідування.*

Що стосується питання стосовно оптимізації строків досудового

розслідування за рахунок криміналістичних рекомендацій, то такими (на наш погляд) можуть бути:

а) створення слідчих груп (груповий метод), що надає можливість здійснення розслідування злочинів одночасно в кількох напрямах, у різних місцях з усебічним і паралельним відпрацюванням усіх версій у провадженні, а також можливості зосереджувати зусилля на одному найбільш важливому його етапі;

б) залучення до проведення необхідних слідчих (розшукових) дій та негласних слідчих (розшукових) дій відповідних оперативних підрозділів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Одерій О.В. Проблеми протидії організованій злочинності в умовах війни (сучасні виклики) // Актуальні питання судової експертизи і криміналістики : зб. мат-лів Міжнар.наук.-практ. конф., присвяч. 150-річ. від дня народж. відом. вчен.-кримінал., д-ра наук, проф. Рудольфа Арчибальда Рейсса (Харків, 23.05.2025). — Харків : ННЦ «ІСЕ ім. Засл. проф. М. С. Бокаріуса», 2025. — С. 308-312. URL : https://drive.google.com/file/d/18Gx1C_EtcS0Oznhng0wfcopjriM0ESoo/view

2. Кримінальний процесуальний кодекс України. Закон від 13.04.2012. № 4651-VI. URL : https://zakon.rada.gov.ua/laws/show/4651-17

ТІТЕНКО Всеволод
курсант навчальної групи Нб – 251 інституту інформаційної безпеки та стратегічних комунікацій Національної академії Служби безпеки Україні

НОВІ СТАНДАРТИ ПРОФЕСІЙНОЇ ПІДГОТОВКИ ФАХІВЦІВ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ ДЛЯ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ПРОТИДІЇ ЗЛОЧИННОСТІ В УМОВАХ

КОНФЛІКТУ

Розвиток інформаційних технологій набувають значного поширення у абсолютно всіх сферах людської діяльності. Також достатньо стрімко розвивається систематизація та поширення інформації, через збільшення об`єму інформації відповідно зростає потреба у збільшенні кількості працівників у інформаційній сфері. Ми можемо сказати, що інформаційне забезпечення, зокрема у питанні протидії злочинності, - являється одним із затребуваних ресурсів держави.

Необхідність кримінально-правового стимулювання позитивних та мінімізації негативних наслідків інформатизації обумовила появу відносно самостійної групи суспільних відносин, що ми будемо називати інформаційна безпека та визначимо як систему суспільних відносин стосовно реалізації інформаційної потреби особи, суспільства, держави. Ця система складається з трьох елементів: відносини в сфері використання ІТ, відносини в сфері забезпечення доступу до інформації, відносини в сфері формування інформаційного поля [1, с. 5].

Щодо поняття «інформаційна безпека», то ми можемо спиратися на ст. 17 Конституції України, у якій зазначено: «Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу» [2].

Але також у свою чергу рішення Ради національної безпеки і оборони України від 15.10.2021 р. «Про Стратегію інформаційної безпеки», введене у дію Указом Президента України № 685/2021, визначає інформаційну безпеку значно ширше: «інформаційна безпека України – складова частина національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання,

зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом» [3].

Досить тривалий час поняття «інформаційна безпека» використовували у досить вузькому значенні, перш за все як збереження інформації, що містить державну таємницю, в контексті диспозиції ч.1 ст.111 Кримінального кодексу України. Це в значній мірі розглядали такі науковці, як - М. І. Хавронюк, Е. М. Кісілюк та В. І. Павліковський.

Звісно, що в умовах сьогодення така позиція не відповідає вимогам часу. Саме тому поняття «інформаційна безпека» сьогодні розглядається в набагато ширшому значенні.

Ми можемо розглядати поняття інформаційна безпека у таких контекстах. Перш за все, як систему суспільних відносин. Також можемо її розглядати, як нормативно-правовий вплив на відносини інформаційної безпеки здійснюється як у межах інформаційного права, так і за допомогою різноманітних інших конструктивних галузей права: конституційного, цивільного, банківського, комерційного тощо [1, с. 8]. Ще один аспект, як ми можемо розглядати «інформаційну безпеку» полягає у необхідності її захисту.

Таким чином, на нашу думку інформаційна безпека являє собою сукупність соціальних відносин, які забезпечують реалізацію інформаційних потреб, не лише суспільства, а й держави, доступу до інформаційних ресурсів, самі відносини, щодо доступу до інформаційних ресурсів.

Виходячи з викладеного вище, можемо сміливо зазначати, що безпосередня професійна підготовка фахівців для інформаційного забезпечення протидії злочинності в умовах конфлікту сьогодні вимагає не лише значного ресурсного потенціалу, а й нових стандартів, які мають йти в

ногу з науковим та технічним розвитком.

Оскільки, на основі розвитку інформаційних технологій не лише в правоохоронній системі впроваджуються нові інформаційно-пошукові, інформаційно-аналітичні системи, а й злочинці не зупиняються, а навпаки - удосконалюють нові методи збирання та аналізу інформації для вчинення протиправних діянь.

Створення комплексів для комп'ютерної та аналітичної розвідки й оснащення ними оперативних та інформаційно-аналітичних підрозділів Служби безпеки України потребує вдосконалення системи підготовки фахівців, які володіють як юридичними, так і спеціальними технічними знаннями у галузі інформаційних технологій. На нашу думку – здатність до інформаційно-аналітичної роботи потрібні не лише співробітникам інформаційно-аналітичних підрозділів, а й усім без винятку суб'єктам оперативно-розшукової діяльності, які виконують інформаційно-аналітичну роботу як спеціальну оперативно-розшукову функцію.

Щодо складності організації протидії сучасній злочинності, а особливо в умовах збройного конфлікту, зумовлена низкою причин, серед яких одна з найважливіших – нестача достатньої кількості досвідчених професіоналів і необхідного правового, технічного та методичного забезпечення державної безпеки України.

Оскільки, відповідно до ст. 1 «Про Службу безпеки України» - Служба безпеки України — це державний правоохоронний орган спеціального призначення, який забезпечує державну безпеку України [4], то задля вдосконалення підготовки фахівців Служби безпеки України для інформаційного забезпечення протидії злочинності в умовах конфлікту, можемо визначити наступні пріоритетні завдання – цільові, змістовні, навчально-технологічні, процесуальні та результативно-діагностичні.

Метою цільового завдання є підготовка фахівців у галузі інформаційної безпеки для Служби безпеки України, а також - готовність майбутніх фахівців до роботи в галузі інформаційних технологій.

Щодо змістовного завдання, то тут ми можемо зазначити, що воно полягає у створенні та затвердженні стандартами вищої освіти та відповідними освітньо – професійними програмами.

Навчально – технологічні завдання полягають у забезпеченні новітніх матеріально – технічних вимог, аналітичному та програмному забезпеченні. Також на нашу думку необхідно приділяти значну увагу мотивації у майбутніх фахівців у галузі інформаційної безпеки для Служби безпеки України, звертати увагу на цей аспект при проведенні відбору кандидатів, як для навчання у системі навчальних закладів СБУ, так і під час відбору кандидатів на проходження служби.

Процесуальне завдання полягає у забезпеченні на високому рівні спеціальних дисциплін під час навчання майбутніх фахівців інформаційної безпеки для Служби безпеки України. Слід також звертати увагу не лише на вивчення здобувачами теоретичних основ інформаційно-аналітичного забезпечення, але і надбання ними необхідних практичних умінь і навичок використання інформаційних технологій у забезпеченні державної безпеки.

Можемо зробити висновок, що в сучасних умовах стрімкого розвитку інформаційних технологій навчальний процес у закладах вищої освіти СБУ має та своєчасно реагувати не лише на зміни в правовому полі, а й відповідати сучасному розвитку інформаційних технологіях. Це вимагає удосконалення, як змісту, так і методики навчання відповідно до реальних умов і завдань щодо забезпечення державної безпеки та розвитку новітніх інформаційно-телекомунікаційних засобів. З метою оперативного реагування на потреби підрозділів щодо підготовки фахівців у галузі інформаційних технологій для СБУ, необхідно проводити підвищення кваліфікації та перепідготовки співробітників, проведення наукових досліджень з актуальних проблем застосування сучасних інформаційних технологій діяльності.

Список використаних джерел:

1. Міжнародні стандарти та національна кримінально-правова політика у сфері охорони інформаційної безпеки : монографія : електрон. наук. вид. / за

заг. ред. В. І. Борисова, М. В. Карчевського, М. В. Шепітька ; Нац. акад. прав. наук України ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса НАПрН України. – Харків : Право, 2023. – 152 с.

2. Конституція України: Закон України від 28 червня 1996 р. № 254к/96-ВР // Відомості Верховної Ради України. — 1996. — № 30. — Ст. 141. — Режим доступу: https://zakon.rada.gov.ua/laws/show/254к/96-вр (дата звернення: 27.09.2025).

3. Про Стратегію інформаційної безпеки: Рішення Ради національної безпеки і оборони України від 15 жовтня 2021 р., уведене в дію Указом Президента України від 28 грудня 2021 р. № 685/2021 // Офіційне інтернет-представництво Президента України. — Режим доступу: https://www.president.gov.ua/documents/6852021-41069 (дата звернення: 27.09.2025).

4. Про Службу безпеки України: Закон України від 25 березня 1992 р. № 2229-XII // Відомості Верховної Ради України. — 1992. — № 27. — Ст. 382. — Режим доступу: https://zakon.rada.gov.ua/laws/show/2229-12 (дата звернення: 27.09.2025).

ХИТРОВСЬКИЙ Дмитро
старший викладач кафедри загальноправових дисциплін факультету підготовки фахівців для органів досудового розслідування Національної поліції України Донецького державного університету внутрішніх справ

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ЕТИЧНІ СТАНДАРТИ В СИСТЕМІ ПРОФЕСІЙНОЇ ПІДГОТОВКИ ПРАЦІВНИКІВ ОРГАНІВ ВНУТРІШНІХ СПРАВ ПІД ЧАС ВОЄННОГО СТАНУ

Сучасні умови в Україні зумовлюють нові виклики для системи забезпечення національної безпеки, зокрема в інформаційній сфері. Інформаційна безпека набуває стратегічного значення як один із ключових

чинників протидії дезінформації, пропаганді, психологічному тиску та кіберзагрозам. Водночас діяльність працівників органів внутрішніх справ вимагає не лише високого рівня професійної підготовки, а й безумовного дотримання етичних стандартів, що забезпечують довіру суспільства до поліції та легітимності дій. У таких умовах особливого значення набуває поєднання принципів інформаційної культури, правової свідомості та поліцейської деонтології, які визначають відповідальну поведінку працівників поліції у сфері обігу інформації. Саме формування інформаційно-етичної компетентності стає необхідною складовою сучасної професійної підготовки майбутніх фахівців системи МВС України.

В умовах воєнного стану особливого значення набуває система професійної підготовки працівників органів внутрішніх справ, спрямована на формування в них високого рівня інформаційної культури, етичної стійкості та відповідальності за інформаційні дії. Сучасні стандарти підготовки фахівців системи МВС мають не лише забезпечувати знання з питань інформаційної безпеки, а й формувати здатність діяти в умовах інформаційних конфліктів, протидіяти дезінформації та кіберзагрозам, зберігаючи при цьому принципи законності, гуманізму та професійної етики. Саме інтеграція етичних і безпекових компонентів у навчальні програми є необхідною умовою підготовки компетентних фахівців, спроможних діяти професійно й виважено навіть у ситуаціях підвищеної складності та інформаційного тиску.

Як зауважують О.М. Мердова та І.О. Умрихіна, в системі професійної підготовки працівників органів внутрішніх справ особливе значення має дотримання морально-етичних засад, що визначають стандарти поведінки поліцейських під час виконання службових обов’язків. Від якості нормативно-правового врегулювання та чіткості визначення правил етичної поведінки безпосередньо залежить ефективність забезпечення прав і свобод людини та громадянина, а також правомірність застосування заходів дисциплінарної відповідальності та інших форм забезпечення службової дисципліни в Національній поліції України [1].

Таким чином, етичні стандарти формують професійну поведінку поліцейських і впливають на довіру суспільства, що особливо важливо в умовах воєнного стану.

В умовах сучасних викликів інформаційна безпека є важливою складовою національної безпеки України. Відповідно до проекту Доктрини інформаційної безпеки України, затвердженої Указом Президента України від 1 травня 2014 року № 449 [2], інформаційна безпека визначається як стан захищеності національних інтересів в інформаційній сфері від зовнішніх і внутрішніх загроз та є сукупністю інформаційно-психологічної й інформаційно-технологічної безпеки держави.

Для працівників органів внутрішніх справ це означає, що поряд із дотриманням етичних стандартів у професійній діяльності необхідно забезпечувати захист службової інформації, попереджати витоки та неправомірне використання даних, що особливо актуально в умовах воєнного стану. Таким чином, інформаційна безпека стає невід'ємною частиною професійної підготовки поліцейських та формує додаткові вимоги до їхньої компетентності.

У системі підготовки майбутніх працівників органів внутрішніх справ важливе місце відводиться формуванню етичних та правових компетенцій уже на першому та другому курсах навчання. Для цього студентам викладається навчальна дисципліна «Поліцейська деонтологія», яка забезпечує засвоєння правил етичної поведінки, формує внутрішній морально-етичний імператив поліцейського, а також підвищує усвідомлення відповідальності за свої дії під час виконання службових обов'язків.

Поряд із навчальними дисциплінами, які формують етичні норми, велике значення має викладання «Конституційного права», яке формує у здобувачів освіти правову свідомість та розуміння значення Конституції України як основного закону держави. Зокрема, Стаття 17 Конституції України гарантує кожному громадянину право на інформаційну безпеку: «Захист суверенітету і територіальної цілісності України, забезпечення її

економічної та інформаційної безпеки є найважливішими функціями держави, справою всього українського народу»[3].

Професійна підготовка майбутніх працівників Національної поліції України передбачає комплексний підхід, що поєднує формування морально-етичних стандартів та правової свідомості. Вивчення дисципліни «Поліцейська деонтологія» дозволяє здобувачам освіти засвоїти правила етичної поведінки, виробити внутрішній моральний імператив поліцейського та усвідомлювати відповідальність за свої дії під час виконання службових обов'язків. Поряд із цим, дисципліна «Конституційне право» забезпечує розуміння значення Конституції України як основного закону держави та гарантій прав громадян, зокрема права на інформаційну безпеку.

Такий інтегрований підхід сприяє формуванню у майбутніх поліцейських високого рівня професійної компетентності, що включає дотримання етичних стандартів, правомірну поведінку та здатність забезпечувати захист інформаційних ресурсів у сучасних умовах, включаючи воєнний стан. У результаті підготовка фахівців стає не лише формальним навчальним процесом, а й ефективним механізмом формування довіри суспільства до правоохоронної системи та забезпечення національної безпеки України.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Мердова О. М., Умрихіна І. О. Правила етичної поведінки поліцейських: формально-юридичні аспекти. Правовий часопис Донбасу. 2025. № 1. С. 115–121. Режим доступу: https://doi.org/10.32782/2523-4269-2025-90-115-121 (дата звернення 03.10.2025).

2. Доктрина інформаційної безпеки України: Указ Президента України від 01.05.2014 №449 «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України». Режим доступу: https://www.president.gov.ua/documents/4492014-17157 (дата звернення 03.10.2025).

3. Конституція України: Закон України від 28.06.1996 № 254к/96-ВР. Режим доступу: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-BP#Text (дата звернення 03.10.2025).

ШУЛЬГА Андрій
доцент кафедри державно-правових дисциплін Навчально-наукового інституту права та соціального менеджменту Донецького державного університету внутрішніх справ, кандидат юридичних наук, доцент

КІБЕРБЕЗПЕКА В КРИМІНАЛЬНИХ ПРОВАДЖЕННЯХ: ПРОТИДІЯ ДЕЗІНФОРМАЦІЇ ТА ГІБРИДНИМ ЗАГРОЗАМ

У сучасних умовах повномасштабної агресії проти України кібербезпека набуває критичного значення в кримінальних провадженнях, оскільки гібридні загрози, включаючи дезінформацію та кібератаки, безпосередньо впливають на розслідування злочинів, пов'язаних з національною безпекою. Дезінформаційні кампанії в соціальних мережах та кібероперації ворога ускладнюють збір та аналіз доказів, вимагаючи інтеграції аналітичних інструментів для оперативного виявлення фейкових наративів та протидії маніпуляціям. У воєнний час роль кримінальних проваджень у сфері кібербезпеки посилюється, оскільки вони стають інструментом нейтралізації терористичних актів та диверсій, забезпечуючи стійкість правосуддя. Актуальність теми зумовлена необхідністю адаптації законодавства та технологій для захисту цифрових доказів від втручання, що гарантує ефективність протидії гібридним викликам.

Інформаційно-аналітична діяльність у кримінальних провадженнях Національної поліції України (НПУ) є ключовим елементом протидії

гібридним загрозам, особливо в контексті дезінформації та кібератак. Згідно з ч. 2 ст. 25 Закону України «Про Національну поліцію», поліція формує реєстри та бази даних у єдиній інформаційній системі МВС, користується ресурсами інших органів влади та здійснює інформаційно-пошукову та аналітичну роботу, що включає взаємодію з Interpol для обміну даними про транскордонні загрози. Ця норма підкреслює роль поліції у створенні централізованих банків даних для ідентифікації підозрюваних та аналізу злочинів, що є основою для оперативних рішень у воєнних умовах. Наприклад, пункт 3 ч. 2 ст. 25 цього нормативно-правового акту прямо вказує на «інформаційно-пошукову та інформаційно-аналітичну роботу», яка забезпечує автоматизований доступ до реєстрів для пошуку розшукуваних осіб, транспортних засобів чи доказів, з обов'язковим логуванням дій для відповідності [1, с. 12]. У кримінальних провадженнях це дозволяє ефективно протидіяти дезінформаційним кампаніям, де фейкові акаунти в соцмережах використовуються для поширення паніки, шляхом аналізу метаданих та трафіків.

Еволюція інформаційно-аналітичної роботи в оперативно-розшуковій діяльності НПУ, застосовувана в кібербезпеці кримінальних проваджень, пройшла п'ять ключових етапів, що відображають перехід від ручних методів до автоматизованих систем для протидії гібридним загрозам. Як зазначає А. В. Мовчан, перший етап (початок XVIII ст. – жовтень 1917 р.) характеризувався витоками систематизованих знань про боротьбу зі злочинністю, з появою антропометричних методів (Бертільйон, 1882) та дактилоскопії (1887), а також створенням центрального реєстраційного бюро в Департаменті поліції. Другий етап (жовтень 1917 р. – середина 50-х рр. XX ст.) пов'язаний з радянським періодом, коли у 1919 р. створено Центральне реєстраційне бюро для дактилоскопічного та алфавітного обліку, а у 1938 р. – Перший спецвідділ НКВС як центральний інформаційний підрозділ. Третій етап (середина 50-х – початок 90-х рр.) ознаменувався комп'ютеризацією: впровадженням перших автоматизованих інформаційно-пошукових систем (АІПС) як «Облік», «Розшук», «Сигнал» та «Фільтр», що замінили 70 типів

карткових файлів і дозволили прогнозування злочинності. Четвертий етап (початок 90-х – 19 листопада 2012 р.) після незалежності України включав мережеві системи «Бінар», «Кронус», «Єрмак» та «Кондор», з інтеграцією до Interpol і Europol для міжвідомчого обліку [2, с. 54-55]. Нарешті, п'ятий етап (з 20 листопада 2012 р.) пов'язаний з новим КПК, запровадженням негласних слідчих розшукових дій (НСРД) та створенням Національної автоматизованої інформаційної системи (НАІС), що забезпечує систематизацію даних у єдиній мережі МВС для реформованої НПУ [2, с.8-23]. Ця еволюція дозволяє в кримінальних провадженнях ефективно протидіяти диверсіям та дезінформації, прогнозуючи тенденції на основі великих даних, включаючи моніторинг соцмереж для виявлення гібридних операцій.

У воєнний період акцент у кібербезпеці кримінальних проваджень робиться на контролі інформаційного простору та захисті від дезінформації, де законодавче забезпечення адаптується для протидії кібершахрайствам. На переконання С.В. Смика та Н.Є. Бурака GPS-навігація та хмарні технології слугують інструментами для оперативної діяльності, але вимагають посилення норм для протидії крадіжкам конфіденційної інформації через неякісне шифрування. Дослідники вважають, що хмарні технології вражають ефективністю завдяки масштабованості та гнучкості, що дозволяють швидко адаптуватися до змін у роботі та до сучасних користувацьких потреб [3, с. 152-154]. Вважаємо думку С.В. Смика та Н.Є. Бурака цілком слушною, адже в такому разі виникає можливість зменшувати витрати на інфраструктуру до таких пристроїв, а в умовах війни це може стати ефективним захистом від різних кіберзагроз у кримінальних провадженнях, де цифрові докази є ключовими. Сьогодні поліція вже адмініструє Єдину інформаційну систему МВС через Інформаційний портал НПУ, обробляючи дані про правопорушення та розшук для протидії гібридним загрозам у розслідуваннях. Серед підсистем виділяється «СЛІД» для реєстрації досудових розслідувань [4]. Інформаційно-телекомунікаційна система «Гарпун» створена для пошуку розшукуваних осіб і є досить ефективним засобом відшукання [5] та «Єдиний

облік» для інтеграції даних по всій системі МВС, що забезпечують централізоване адміністрування з автентифікацією користувачів та обробкою метаданих для координації розслідувань дезінформаційних злочинів [6].

Концепція інформаційної безпеки України чітко підкреслює роль МВС у нейтралізації кіберзлочинів та тероризму в умовах війни, особливо коли це напряму координується із ЗСУ [7, с. 12]. Вважаємо, що координація зусиль НПУ зі ЗСУ здатна створити щільну атмосферу превентивності порушень в галузі кіберзлочинності, а от так і суттєво посилити захист національного інформаційного простору від зовнішніх впливів у кримінальних провадженнях. Крім того, як слушно зазначає у своїй роботі А.А. Нікітін, роль НПУ в національній безпеці зокрема включає і моніторинг соціальних мереж для виявлення різних видів дезінформації. У воєнний час, зазначає дослідник, функції поліції розширені різними наказами МВС України де особливу увагу звернуто на кібербезпеку, контрдиверсійні дії, посилену перевірку документів, участь у забезпеченні воєнної комендантської години, протидії дезінформації [8, с. 394]. Здійснення правоохоронної діяльності на основі прогнозів штучного інтелекту (Predictive Policing) у сучасному виразі є поліцейською інновацією, що застосовується в кібербезпеці кримінальних проваджень. Ця модель передбачає застосування різних кількісних методів для того, щоб заздалегідь ідентифікувати приблизний час, місце або осіб, які матимуть стосунок до злочину. І хоча не можна сказати, що модель є повністю новою, проте адаптація до потреб правоохоронної діяльності математичних алгоритмів прогнозування, використання сучасних систем ШІ дають змогу на практиці побачити конкретний результат. Така робота включає моделювання корупційних сценаріїв та моніторинг бюджетних потоків для превентивних заходів проти гібридних загроз, включаючи дезінформацію [9, с. 123]. У кримінальних провадженнях це дозволяє використовувати ШІ для аналізу великих даних з соцмереж, виявляючи патерни фейкових кампаній та забезпечуючи збір цифрових доказів для обвинувачень.

Таким чином по-перше, кібербезпека в кримінальних провадженнях є

основою протидії гібридним загрозам через еволюцію від ручних бюро до НАІС, що інтегрує дані для розслідувань. По-друге, інтеграція GPS, хмарних технологій та підсистем як «Гарпун» підвищує ефективність протидії дезінформації у воєнний час. По-третє, законодавча база, включаючи ст. 25 Закону «Про НПУ», гарантує законність та захист даних від кібершахрайства в провадженнях. По-четверте, координація з МВС та ЗСУ посилює моніторинг соцмереж та транскордонних ризиків дезінформації. По-п’яте, прогнозування злочинності за допомогою Predictive Policing з ШІ забезпечить стійкість до інформаційних атак та гібридних операцій.

Список використаних джерел:

1. Закон України «Про Національну поліцію»: від 02.07.2015 № 580-VIII. – Київ: ВРУ, 2015. – 100 с. URL: https://zakon.rada.gov.ua/laws/show/580-19

2. Мовчан А. В. Інформаційно-аналітична робота в оперативно-розшуковій діяльності Національної поліції: навч. посіб. – Львів: ЛьвДУВС, 2017. – 244 с. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/318/1/%D0%BC%D0%BE%D0%B2%D1%87%D0%B0%D0%BD.pdf

3. Смик С. В. Інформаційно-аналітичне забезпечення діяльності органів сектору безпеки і оборони України: матер. Наук.-практ. конф. – Львів: ЛНУВС, 2023. – 192 с. URL: https://sci.ldubgd.edu.ua/jspui/bitstream/123456789/14197/1/Smyk.pdf

4. Інформаційно-аналітичне забезпечення правоохоронної діяльності: навч. прогр. – Харків: НЮУ ім. Я. Мудрого, 2023. – 30 с. URL: https://nlu.edu.ua/wp-content/uploads/2024/12/ok1.1.22.pnd_informaczijno-analitychne-zabezpechennya-pravoohoronnoyi-diyalnosti.pdf

5. Концепція інформаційної безпеки України. – Київ: РНБО, 2016. – 20 с. URL: https://www.osce.org/files/f/documents/0/2/175056.pdf

6. Нікітін А.А. Роль Національної поліції України в системі забезпечення національної безпеки // Проблеми підготовки та перепідготовки фахівців для Збройних Сил та інших військових формувань України: наук. журнал. – 2024.

– № 3. – С. 392-395. URL: http://www.pdu-journal.kpu.zp.ua/archive/3_2024/59.pdf

7. Федунь А.В., Поляк С.П. Роль штучного інтелекту у здійсненні правоохоронної діяльності на основі прогнозів (PREDICTIVE POLICING). Інформаційно-аналітичне забезпечення діяльності органів сектору безпеки і оборони України: матеріали Науково-практичної конференції (Львів, 22 грудня 2023) / упорядник: Т. В. Магеровська. – Львів : ЛьвДУВС, 2024. – 192 с. URL: file:///C:/Users/%D0%90%D0%BD%D0%B4%D1%80%D1%96%D0%B9/Downloads/20_12_2024.pdf

СЕКЦІЯ 6.
МІЖНАРОДНЕ СПІВРОБІТНИЦТВО ПІД ЧАС ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ПРОТИДІЇ ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ В УМОВАХ ЗБРОЙНОГО КОНФЛІКТУ.

БРЕДІХІНА Марія
магістр 2-го курсу факультету підготовки фахівців для органів досудового розслідування Донецького державного університету внутрішніх справ, старший лейтенант поліції

Науковий керівник:
ВОЛОБОЄВ Артур
начальник відділу організації освітнього процесу Донецького державного університету внутрішніх справ, доктор філософії в галузі права

МІЖНАРОДНО-ПРАВОВІ МЕХАНІЗМИ ПРОТИДІЇ ТРАНСНАЦІОНАЛЬНІЙ ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ

В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ СУСПІЛЬСТВА

Сучасний етап розвитку міжнародних відносин характеризується суттєвою трансформацією організованої злочинності під впливом глобалізації, стрімкого розвитку цифрових технологій та соціально- політичних потрясінь. Торгівля наркотичними засобами, контрабанда зброї, фінансові злочини та кіберзлочинність все частіше виходять за межі окремих держав, створюючи нові виклики для національних правоохоронних систем. Ця проблема особливо загострюється під час збройних конфліктів, коли можливості державних інституцій обмежені, а злочинні угруповання використовують прогалини у правовому регулюванні, впроваджуючи складні схеми незаконного обігу, зокрема через криптографічні платформи та мережі Darknet.

За таких умов міжнародне співробітництво та ефективний обмін інформацією стають вирішальними чинником у протидії з організованою злочинністю. Бо тільки координована взаємодія держав та міжнародних організацій дозволяє не лише виявляти й розкривати злочинні схеми, а й запобігати їхньому подальшому розвитку та поширенню на нові території. Як приклад, операція «Dark HunTor» проведена у 2021 році стала однією з успішних у міжнародному колі за участю дванадцяти країн, серед яких Сполучені Штати Америки, Великобританії, Німеччини, Франції, Італії та Нідерландів. Головна мета полягала у ліквідації транснаціональних мереж торгівлі опіоїдами через заборонені онлайн-платформи, які використовували криптовалюту та анонімні протоколи для приховування незаконних операцій.

Завдяки комплексному підходу до збору та аналізу даних, поєднанню цифрової аналітики зі спільними оперативними заходами вдалося затримати 151 особу, вилучити понад сто мільйонів євро, закрити декілька нелегальних ринків та ліквідувати численні канали незаконної торгівлі. Серед вилученого було 234 кілограми різних наркотичних засобів і понад 200 тисяч пігулок психоактивних речовин [1].

Тобто результати операції довели, що навіть у високоанонімізованому цифровому середовищі міжнародна співпраця може бути надзвичайно ефективною за умови швидкого обміну інформацією, взаємної довіри між державами та застосування сучасних методів аналізу великих масивів даних.

Логічним продовженням цієї тенденції стала операція «RapTor», сфокусована на протидії з незаконним обігом фентанілу та інших сильнодіючих препаратів. За участю понад п'ятнадцяти країн було вилучено активів на суму понад двісті мільйонів доларів США, заарештовано 270 осіб, конфісковано дві тони наркотичних засобів, 144 кілограми фентанілу та понад 180 одиниць вогнепальної зброї. Тут новизна операції полягала у застосуванні передових технологій: аналізу фінансових потоків, цифрової трасології та блокчейн-аналітики, що забезпечило ефективне відстеження маршрутів транспортування та ідентифікацію причетних осіб [2].

Однак поряд з очевидними успіхами існують системні проблеми, що об'єктивно знижують ефективність міжнародної взаємодії. Несумісність інформаційних систем, гетерогенність стандартів обліку та зберігання даних створюють значні темпоральні витрати при обміні інформацією. Правові обмеження конфіденційності та захисту персональних даних також нерідко перешкоджають оперативному обміну важливими відомостями, що особливо акцентується в контексті Загального регламенту ЄС про захист даних (GDPR, 2016), який встановлює імперативні вимоги до процесингу та трансферу персональних даних, включаючи транскордонні потоки [3].

З огляду на це, зауважимо, що до нормативно-правового фундаменту міжнародного співробітництва слід віднести Конвенцію ООН проти транснаціональної організованої злочинності (2000), що визначає механізми взаємодії держав, регламентує екстрадицію, обмін доказами та координацію спільних розслідувань [4]. Відповідною є й Конвенція ООН проти незаконного обігу наркотичних засобів і психотропних речовин (1988), яка встановлює стандарти контролю та сприяє обміну інформацією щодо наркоторгівлі [5]. Конвенція про психотропні речовини (1971) доповнює цю систему,

визначаючи категорії психотропних препаратів та механізми контролю за їх обігом.

Між тим, важливим інструментом регіонального рівня є Європейська конвенція про взаємну допомогу у кримінальних справах (1959) [6], що створює правові підстави для обміну доказами та проведення слідчих (розшукових) дій.

Поряд з правовими чинниками вагому роль відіграють політико-дипломатичні аспекти, оскільки міждержавна напруженість може суттєво впливати на обсяг і темпоральність обміну інформацією. Для недопущення цих викликів міжнародні організації – ООН, Інтерпол, Європол, забезпечують координацію, аналітичну підтримку та розвиток міждержавної довіри, створюють стандартизовані механізми інформаційного обміну, організовують спільні тренінги та сприяють консолідації законодавств.

Отже, вважаємо, що міжнародно-правові механізми протидії організованій злочинності через цифрові канали є важливим елементом глобальної безпеки. Операції «Dark HunTor» та «RapTor» показують ефективність скоординованих дій і застосування сучасних технологій. Водночас подальше підвищення результативності вимагає розв'язання проблем несумісності інформаційних систем, правових обмежень та політичних бар'єрів. Лише інтеграція міжнародних стандартів, високий рівень міждержавної взаємодії та активне використання інноваційних технологій дозволяють сформувати системну, стійку та ефективну відповідь на виклики транснаціональної злочинності в умовах цифрової трансформації та збройних конфліктів.

Список використаних джерел:

1. Операція проти Darknet: поліція США та Євросоюзу заарештувала 150 осіб. *УкрІнформ.* URL: https://www.ukrinform.ua/rubric-world/3339597-operacia-proti-darknet-policia-ssa-ta-evrosouzu-zaarestuvala-150-osib.html (дата звернення 07.10.2025).

2. Міжнародна операція RapTor завдала нищівного удару по злочинних

мережах Даркнету. *CyberSecureFox.* URL: https://cybersecurefox.com/uk/operatsiya-raptor-mizhnarodnyy-udar-po-darknet-torhivli/ (дата звернення 02.10.2025).

3. Про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних). Регламент Європейського Парламенту і Ради (ЄС) від 27.04.2016 № 2016/679. *Офіційний вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення 07.10.2025).

4. Конвенція Організації Об'єднаних Націй проти транснаціональної організованої злочинності. Конвенція, Міжнародний документ від 15.11.2000. *Офіційний вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/995_789#Text (дата звернення 10.10.2025).

5. Конвенція Організації Об'єднаних Націй про боротьбу проти незаконного обігу наркотичних засобів і психотропних речовин. Конвенція, Міжнародний документ від 25.04.1988. *Офіційний вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/995_096#Text (дата звернення 12.10.2025).

6. Європейська конвенція про взаємну допомогу у кримінальних справах. Конвенція, Міжнародний документ від 20.04.1959. *Офіційний вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/995_036#Text (дата звернення 11.10.2025).

ЗАВГОРОДНІЙ Євген
суддя Фортечного районного суду міста Кропивницького

СЕНИЧАК Ольга
курсантка 3-го курсу факультету підготовки фахівців для органів досудового розслідування Донецького державного

університету внутрішніх справ

ЕТИЧНІ ТА ПРАВОВІ МЕЖІ ЗАСТОСУВАННЯ ПОЛІГРАФА ПІД ЧАС ДОПИТІВ : ГАРАНТІЇ ПРАВ ЛЮДИНИ

Використання поліграфа у кримінальному процесі України є складним і суперечливим питанням, яке поєднує правові, етичні та психологічні аспекти. З одного боку, поліграфічне опитування може сприяти отриманню додаткової інформації у ході розслідування, з іншого - воно може створювати ризики порушення основоположних прав людини, зокрема права на справедливий судовий розгляд і недоторканність приватного життя.

Поліграф (детектор брехні) - це технічний засіб, який фіксує психофізіологічні реакції людини під час відповідей на запитання. Його метою є виявлення можливих ознак неправдивості або приховування інформації. У правозастосовній практиці поліграф використовується під час службових перевірок, добору персоналу [1, с. 142]. В Україні відсутнє законодавче врегулювання порядку застосування поліграфа у кримінальному провадженні, що породжує неоднозначність у тлумаченні його результатів.

Згідно зі ст. 84 Кримінального процесуального кодексу України (далі – КПК) доказами в кримінальному провадженні є фактичні дані, отримані у передбаченому цим Кодексом порядку, на підставі яких слідчий, прокурор, слідчий суддя і суд встановлюють наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження та підлягають доказуванню. Процесуальними джерелами доказів є показання, речові докази, документи, висновки експертів [2].

Відсутність урегульованості на законодавчому рівні створює проблеми практичного застосування зазначеного технічного засобу та результатів, отриманих за його допомогою, як доказів у кримінальному судочинстві [3, с.689].

Попри це, судова практика свідчить, що деякі органи досудового

розслідування використовують поліграф як допоміжний засіб орієнтації під час перевірки показань чи версій. Такий підхід не суперечить закону лише за умов проведення дослідження фаховим поліграфологом та наявності добровільної згоди особи на участь у ньому.

Використання поліграфа під час допитів зачіпає основоположні права та свободи людини. Стаття 28 Конституції України гарантує кожному право на повагу до гідності та забороняє піддавати особу катуванню чи іншому жорстокому, нелюдському або принизливому поводженню. Стаття 63 передбачає право особи не свідчити проти себе чи своїх близьких родичів. Отже, будь-яке примушення до проходження поліграфа без згоди може розцінюватися як порушення цих гарантій.

Положення Конвенції про захист прав людини і основоположних свобод (ст. 6, 8) також підкреслюють право кожного на справедливий суд і повагу до приватного життя. Європейський суд з прав людини (далі — ЄСПЛ) у своїй практиці неодноразово наголошував, що використання примусових психофізіологічних методів суперечить принципу справедливого судового розгляду. У рішенні у справі «Яллох проти Німеччини» Суд підкреслив, що навіть непрямий примус до самообвинувачення суперечить ст. 6 Конвенції [4].

Таким чином, поліграф може застосовуватися лише на добровільних засадах, без примусу чи обману, із забезпеченням права особи на юридичну допомогу та конфіденційність результатів дослідження. В іншому випадку його використання порушує засади кримінального процесу та принцип поваги до прав людини.

Питання етичності застосування поліграфа тісно пов’язане з морально-правовими межами втручання у внутрішній світ людини. Під час поліграфічного тестування фіксуються показники фізіологічного стану, що стосуються не лише поведінки, а й емоційної сфери особи. Таке втручання може впливати на психічний стан допитуваного, створювати відчуття контролю та тиску, що є несумісним із принципом поваги до людської гідності.

Поліграф не може вважатися об’єктивним інструментом встановлення

істини, адже фізіологічні реакції не завжди свідчать про неправдивість висловлювань. Наприклад, хвилювання, страх або стрес можуть спотворити результати обстеження. Таким чином, некритичне сприйняття поліграфа як «машини істини» створює ризики технологічного редукціонізму, коли складні психологічні процеси зводяться до фізичних показників організму.

Етична проблематика полягає й у тому, що поліграф може бути використаний не для пошуку істини, а для психологічного тиску на підозрюваного. Така практика суперечить основним засадам кримінального судочинства — зокрема, принципам презумпції невинуватості, змагальності сторін і недопустимості примусу до свідчення проти себе (ст. 17, 22 КПК України).

Законодавчі ініціативи щодо регламентації використання поліграфа в Україні, зокрема, під час кримінального провадження, наразі не були реалізовані [5, 6]. Це створює колізії у правозастосуванні, коли результати поліграфічних досліджень можуть бути сприйняті судами по-різному — від повного заперечення до врахування як додаткової інформації.

Судова практика засвідчує неоднозначність у ставленні до поліграфа. Частина суддів відмовляється приймати такі дані через сумнівну достовірність і можливість маніпуляцій результатами, інші ж розглядають їх як допоміжний доказ, який може підтвердити або спростувати певну версію. Проте жоден судовий акт не визнає поліграф як самостійний доказ вини.

Таким чином, застосування поліграфа під час допитів вимагає дотримання чітких правових та етичних меж. Умовами проведення досліджень є добровільна згода особи, поінформованість про мету та наслідки процедури, а також участь професійного фахівця, що відповідає встановленим вимогам [7, с. 121]. Необхідно уникати будь-яких форм примусу чи тиску, що можуть порушити права, гарантовані Конституцією України та міжнародними договорами. Водночас держава має розробити чітке нормативне регулювання порядку використання поліграфа в кримінальному процесі, визначити статус його результатів і вимоги до здійснення відповідної діяльності. Такий підхід

сприятиме балансу між інтересами правосуддя та гарантіями прав людини, забезпечуючи принципи законності, справедливості та гуманізму.

Список використаних джерел:

1. Мінка Т.П. Використання поліграфа у світі: ґенеза становлення та тенденції розвитку. Держава та регіони. Серія: ПРАВО 2024 р. № 1(83). С. 141-144. URL: http://law.stateandregions.zp.ua/archive/1_2024/1_2024.pdf#page=141 (дата звернення: 06.10.2025).

2. Кримінальний процесуальний кодекс України: Закон України від 13 квітня 2012 р. № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 06.10.2025).

3. Курман О.В., Балибіна А.Р. Використання поліграфа при розслідуванні кримінальних правопорушень: проблеми тактики та правового регулювання. Аналітичне-порівняльне правознавство. 2024. № 2. С. 686–691.URL: http://journal-app.uzhnu.edu.ua/article/view/303746/295786 (дата звернення: 06.10.2025).

4. Комюніке Секретаря Європейського суду з прав людини стосовно рішення у справі Jalloh проти Німеччини [ВП] - 54810/00; рішення від 11.7.2006. URL: https://ips.ligazakon.net/document/SO2742 (дата звернення: 07.10.2025).

5. Проект Закону про доповнення Кримінального процесуального кодексу України положеннями щодо використання поліграфа (детектора брехні) від 3611 від 10.12.2015. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=57349 (дата звернення: 07.10.2025).

6. Проект Закону України «Про поліграфологічну діяльність». URL: https://ips.ligazakon.net/document/JH35Q1AA (дата звернення 07.10.2025).

7. Шульженко А.В. Проблеми використання поліграфа під час кримінального провадження. Приватне та публічне право. 2018. №2. С. 119-122. URL: http://www.pp-law.in.ua/archive/2_2018/27.pdf (дата звернення

07.10.2025).

ЛИСЮК Артьом
курсант ННІ 1-24-203Пр
Харківський національний університет внутрішніх справ

Науковий керівник:
ЛОГВИНЕНКО Євгенія
професор кафедри конституційного і міжнародного права та прав людини, кандидат юридичних наук, доцент

ДОСВІД НАТО ТА ЄС У КООРДИНАЦІЇ ІНФОРМАЦІЙНОЇ ВЗАЄМОДІЇ ЩОДО ПРОТИДІЇ ОРГАНІЗОВАНИМ ЗЛОЧИННИМ УГРУПОВАННЯМ У КРИЗОВИХ СИТУАЦІЯХ

Організовані злочинні угруповання (далі – ОЗУ) становлять серйозну загрозу для глобальної безпеки та стабільності, особливо в кризових ситуаціях, коли державні інститути можуть бути ослаблені або перевантажені. За таких обставин швидкий обмін інформацією, аналіз розвідданих та координація дій міжнародних суб'єктів стають надзвичайно важливими. Організація Північноатлантичного договору (далі – НАТО) та Європейський Союз (далі – ЄС), як провідні політичні та безпекові об'єднання, мають значний досвід у координації обміну інформацією для боротьби з ОЗУ.

Згідно зі статтею 28 Кримінального кодексу України, злочинна організація – це стабільне ієрархічне об'єднання кількох осіб, члени або структурні елементи якого заздалегідь змовилися організувати спільну діяльність з метою вчинення тяжких або особливо тяжких злочинів [1].

НАТО та ЄС визнають, що сучасні виклики вимагають комплексного підходу, який поєднує військові та цивільні засоби впливу. Збройні групи

часто діють за межами кордонів і виступають каталізаторами нестабільності, створюючи додаткові виклики для кожної організації. У цьому контексті ефективний обмін інформацією відіграє важливу роль у забезпеченні спільного розуміння ситуації та оптимальному використанні ресурсів і можливостей кожної сторони. Термін «інформаційна взаємодія», що міститься у статті 2 Постанови Кабінету Міністрів України «Деякі питання електронної взаємодії електронних інформаційних ресурсів», означає обмін конкретним набором даних між двома електронними інформаційними ресурсами суб'єктів електронної взаємодії за допомогою програмних інтерфейсів [2].

ЄС має значний досвід у сферах цивільного кризового управління, реформування правової системи, забезпечення верховенства права та боротьби з фінансовою злочинністю та корупцією, які часто сприяють діяльності організованих злочинних угруповань. НАТО, зі свого боку, надає військові та оборонні можливості і відіграє ключову роль у стабілізації регіонів, де ситуація з безпекою вимагає військового втручання.

Правовою основою для обміну інформацією між сторонами є Угода між Європейським Союзом та Організацією Північноатлантичного договору про безпеку інформації, підписана 14 травня 2003 року [3]. Ця угода дозволяє НАТО та ЄС обмінюватися розвідданими та критичною інформацією в рамках спільних операцій та політичних консультацій, що є надзвичайно важливим для реагування на гібридні загрози та діяльність транснаціональної організованої злочинності в кризових регіонах.

Прикладом ефективної координації між НАТО та ЄС у сфері протидії ОЗУ є операція SFOR та її наступниця – місія EUFOR Althea в Боснії і Герцеговині (БіГ). Після закінчення війни в Боснії і Герцеговині в 1995 році (в результаті Дейтонської мирної угоди) НАТО проводило стабілізаційну місію SFOR, покликану підтримувати мир. 2 грудня 2004 року в рамках угод «Берлін плюс» ЄС перейняв естафету, розпочавши військову операцію EUFOR Althea. Мета місії полягала в забезпеченні дотримання положень Дейтонської угоди та створенні безпечного середовища. Хоча EUFOR Althea є військовою місією,

її діяльність безпосередньо пов’язана з боротьбою проти організованих злочинних угруповань, які продовжували дестабілізувати ситуацію в країні.

Ця координація базується на поєднанні військових заходів НАТО та цивільних інструментів ЄС: політичного діалогу, програм допомоги, поліцейських місій та обміну конфіденційною інформацією. Важливість такої співпраці була підтверджена в Салонікській декларації 2003 року про європейське майбутнє Західних Балкан [4].

Водночас ця співпраця не є безпроблемною. Серед основних проблем – політичні та бюрократичні обмеження, історичні суперечності та положення угод «Берлін плюс» [5], які можуть ускладнювати обмін критично важливою інформацією. Важливо також враховувати відмінності в характері обох організацій: НАТО є політико-військовим альянсом, тоді як ЄС – це насамперед цивільна та юридична структура.

Це вимагає постійної координації термінології, процедур та підходів. Щоб подолати ці виклики, НАТО та ЄС працюють над цифровою трансформацією та поліпшенням взаємодії своїх систем командування, контролю, зв’язку, інформаційних технологій, розвідки, спостереження та розвідки (C4ISR).

Таким чином, досвід НАТО та ЄС показує, що лише тісна співпраця в галузі обміну інформацією дозволяє ефективно боротися з організованими злочинними угрупованнями в кризових ситуаціях. Спільні дії дозволяють максимально використати унікальні можливості кожної організації: військову потужність НАТО та цивільний і юридичний досвід ЄС.

Список використаних джерел:

1. Кримінальний кодекс України: Закон України від 05.04.2001 № 2341-III. URL: https://zakon.rada.gov.ua/laws/card/2341-14 (дата звернення 12.10.2025).

2. Деякі питання електронної взаємодії електронних інформаційних ресурсів: Постанова Кабінету Міністрів України від 08.09.2016 № 606. URL:

https://zakon.rada.gov.ua/laws/card/606-2016-%D0%BF (дата звернення: 06.10.2025).

3. Угода між Європейським Союзом та Організацією Північноатлантичного договору про безпеку інформації від 14.05.2003 №22003A0327(01). URL: https://eur-lex.europa.eu/eli/agree_internation/2003/211/oj (дата звернення: 06.10.2025).

4. An official website of the European Union. EUFOR BOSNIA-HERZEGOVINA Military Operation ALTHEA. EEAS. 30.11.0220. URL: https://www.eeas.europa.eu/eufor-althea/eufor-bosnia-herzegovina-military-operation-althea_und_en (дата звернення: 04.10.2025).

5. Berlin Plus agreement. URL: https://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/berlinplus_/berlinplus_en.pdf (дата звернення: 01.10.2025).

ЛЕПІШ Наталія
кандидат юридичних наук, доцент
доцент кафедри адміністративно-правових дисциплін
Навчально-наукового інституту права та правоохоронної діяльності
Львівський державний університет внутрішніх справ

АДМІНІСТРАТИВНО-ПРАВОВІ ЗАСАДИ МІЖНАРОДНОГО ІНФОРМАЦІЙНОГО ОБМІНУ У СФЕРІ ПРОТИДІЇ ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ ПІД ЧАС ЗБРОЙНОГО КОНФЛІКТУ

У науковому дослідженні розглянуто адміністративно-правові засади міжнародного інформаційного обміну у сфері протидії організованій злочинності в умовах збройного конфлікту. Обґрунтовано значення адміністративного права як правової основи для взаємодії національних та

міжнародних інституцій, визначено особливості правового регулювання обміну даними в умовах війни, а також акцентовано увагу на необхідності вдосконалення механізмів кіберзахисту та гармонізації національного законодавства із міжнародними стандартами.

Сучасні умови глобальної безпеки зумовлюють необхідність переосмислення підходів до боротьби з організованою злочинністю, яка набуває транснаціональних ознак і дедалі частіше використовує інформаційні технології для розширення сфер свого впливу. Збройний конфлікт, що триває на території України, значно ускладнює діяльність державних органів, послаблює внутрішні механізми захисту, водночас підвищуючи потребу у міжнародному співробітництві. У цьому контексті ключове значення набуває адміністративно-правове забезпечення міжнародного інформаційного обміну [3, с. 48].

Адміністративне право виконує функцію нормативної та організаційної основи для взаємодії органів виконавчої влади у сфері протидії організованій злочинності. З одного боку, воно визначає компетенцію національних інституцій, які здійснюють інформаційне забезпечення у боротьбі зі злочинністю, з іншого – встановлює правові механізми взаємодії з іноземними та міжнародними структурами. В умовах збройного конфлікту така взаємодія стає не лише питанням правопорядку, а й елементом національної безпеки.

Міжнародний інформаційний обмін у сфері протидії організованій злочинності реалізується через Інтерпол, Європол, Спільні слідчі групи, угоди про правову допомогу та міжвідомчі меморандуми. Проте ефективність цього процесу безпосередньо залежить від адміністративно-правових умов: прозорих процедур обробки інформації, захисту персональних даних, узгодженості міжвідомчої взаємодії, а також від наявності механізмів контролю за правомірністю використання даних [2, с. 56].

Особливістю періоду збройного конфлікту є зростання потреби у швидкому, достовірному та захищеному обміні даними. Це стосується інформації про транснаціональні злочинні угруповання, канали незаконної

торгівлі зброєю, людьми, наркотиками, а також фінансові схеми відмивання коштів [1]. Водночас ризики витоку даних, кібератак та використання інформаційних ресурсів у гібридній війні потребують додаткового нормативного врегулювання.

Адміністративно-правові засади міжнародного інформаційного співробітництва під час війни мають включати:

– удосконалення національного законодавства у сфері захисту інформації та персональних даних;

– гармонізацію правових норм із міжнародними стандартами;

– створення спеціалізованих міжвідомчих координаційних центрів;

– розвиток електронних систем обміну, що відповідають вимогам кібербезпеки;

– посилення адміністративної відповідальності за порушення у сфері обробки та передачі даних.

Таким чином, адміністративне право відіграє системоутворюючу роль у формуванні правових засад міжнародного інформаційного обміну в умовах збройного конфлікту. Воно визначає механізми взаємодії державних органів та міжнародних партнерів, забезпечує баланс між потребою у відкритості та необхідністю захисту національних інтересів. Розвиток цього напряму має стати пріоритетним завданням державної політики, оскільки саме інформаційна взаємодія дозволяє ефективно протидіяти транснаціональній організованій злочинності навіть у складних умовах воєнного стану.

Список використаних джерел:

1. Про національну безпеку України: Закон України від 21.06.2018 р. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 30.09.2025).

2. Леган І. М. Міжнародне співробітництво у сфері запобігання та протидії транснаціональній злочинності: монографія. Чернігів: НУ «Чернігівська політехніка», 2021. 328 с.

3. Адміністративне право України. Повний курс: підручник / В. Галунько, П. Діхтієвський, О. Кузьменко та ін.; за ред. В. Галунька, О. Правоторової. Видання четверте. Херсон : ОЛДІ-ПЛЮС, 2021. 656 с.

МОВЧАН Анатолій
професор кафедри оперативно-розшукової діяльності Львівського державного університету внутрішніх справ доктор юридичних наук, професор

ГОРОШКО Олександр
здобувач ступеня доктора філософії у галузі права кафедри оперативно-розшукової діяльності Львівського державного університету внутрішніх справ

ПРОВЕДЕННЯ СПІЛЬНИХ МІЖДЕРЖАВНИХ ОПЕРАЦІЙ У ПРОТИДІЇ ТРАНСНАЦІОНАЛЬНІЙ ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ

Важливе значення у протидії транснаціональній організованій злочинності має проведення спільних міждержавних операцій, у яких беруть участь представники поліції країн-членів Інтерполу та Європолу. Зокрема, у рамках проєкту Millennium Інтерпол пропонує передовий досвід і підтримує зусилля країн-членів Інтерполу у протидії кримінальній мережі євразійської організованої злочинності, надаючи доступ у режимі реального часу до інформації про злочини, вчинені цією злочинною мережею, та глобальних баз даних. Проєкт Millennium сприяє країнам-членам Інтерполу обмінюватися процесуальною інформацією, яка допомагає ідентифікувати людей і компанії,

що стоять за транснаціональною євразійською організованою злочинністю. Крім того, файл аналізу проєкту Millennium надає країнам-учасницям дані про високопоставлених членів російськомовних ОЗГ, включаючи персональні та біометричні дані, відомих учасників, місця злочинної діяльності та впливу, особисті ідентифікаційні ознаки (татуювання, фізичні атрибути тощо). Завдяки активному обміну інформацією та внесення розвідувальних даних у файл аналізу проєкту Millennium, поліція отримує повноваження діяти локально за підтримки глобальних даних [1].

Відтак, Україна співпрацює із 42 державами-членами Інтерполу у боротьбі з транснаціональною євразійською організованою злочинністю з метою попередження поширення та нейтралізації впливових євразійських злочинних угруповань країн Східної Європи та кавказського регіону на території Євросоюзу, які займаються торгівлею наркотиками, людьми, автотранспортом та вогнепальною зброєю, злочинністю у сфері фінансів та легалізацією (відмиванням) злочинних доходів.

Натомість, одним із ключових напрямів Європолу є діяльність ESOCC (European Serious and Organised Crime Centre), який формує оцінки загроз, координує оперативні дії та веде аналітичне супроводження стратегічних операцій. У рамках платформи EMPACT (European Multidisciplinary Platform Against Criminal Threats) визначаються пріоритетні напрями боротьби зі злочинністю на періоди 4 роки з подальшим щорічним оновленням планів дій. Зокрема, у ході проведення великомасштабної операції «Троянський щит» затримано понад 800 підозрюваних, проведено понад 700 обшуків в Європі, Новій Зеландії, Австралії та США, у рамках яких конфісковано понад 30 тонн наркотиків, зброю та готівку. За інформацією ФБР, слідчим вдалося отримати доступ до зашифрованої платформи ANOM, що використовується злочинними організаціями, і увійти в їх чати. Більш ніж у 100 країнах були розповсюджені захищені від прослуховування телефони серед 300 злочинних угруповань. Упродовж 18 місяців з їх допомогою прослуховувалися телефонні розмови та відстежувалися інші види комунікації, було перевірено понад 27 млн

електронних повідомлень. За допомогою криптотелефонів було розкрито плани членів мафіозних угруповань, злочинних кланів та азіатських злочинних синдикатів у сферах наркоторгівлі та відмивання грошей, а також вбивства, що планувалися, більш ніж у 100 країнах [2].

26 жовтня 2021 р. Європол повідомив про успішно проведену операцію Dark Huntor проти організованої злочинності в даркнеті. У Німеччині було затримано 47 осіб, конфісковано готівку на загальну суму близько одного млн євро та криптовалюту, а також вогнепальну зброю, електрошокери та понад 260 кг наркотиків. У США було затримано 65 осіб, у Великій Британії – 24, а також по чотири – в Італії та Нідерландах. Загалом поліція конфіскувала 26,7 млн євро, 45 одиниць зброї, 152 кг амфетаміну та метамфетаміну, 22 кг кокаїну та 27 кг опіоїдів [3].

29 жовтня 2021 р. у ході міжнародної поліцейської операції під егідою Європолу, в якій брала участь Німеччина та сім інших країн, було розкрито мережу кібервимагачів, які, ймовірно, здійснили комп'ютерні атаки з метою отримання викупу від компаній у десятках країн. Після дворічного розслідування було заарештовано 12 підозрюваних в Україні та Швейцарії, при обшуках у них конфісковано близько 52 тис. доларів та п'ять автомобілів класу люкс. Жертвами злочинців стали близько 1800 компаній у 71 країні. Члени злочинного угруповання отримували доступ до ІТ-систем фірм за допомогою так званих фішингових електронних листів та іншими способами. Потім за допомогою вірусів-вимагачів (ransomware) блокували фірмам доступ до документації, шифруючи його, і вимагали викуп за надання ключа для розшифрування [4].

Одним із найбільш відомих прикладів глобальної скоординованої боротьби з транснаціональною організованою злочинністю є операція HAKA II, проведена під егідою Інтерполу у 2021 році. За результатами операції ідентифіковано понад 300 злочинних угруповань, що спеціалізуються на фальсифікації, переміщенні нелегальних мігрантів, схемах фінансового шахрайства; виявлено сотні викрадених або фальшивих паспортів, віз,

посвідчень особи, водійських прав; заморожено активи, пов'язані з незаконним переміщенням коштів через підставні рахунки або схеми «money mule»; проведено затримання посередників нелегальної міграції в транзитних країнах (зокрема на Балканах, Близькому Сході та Західній Африці) [5].

У рамках HAKA II через I-24/7 здійснювалася звірка підозрюваних осіб із базами даних Інтерполу, передача даних про підроблені документи, що дозволяло швидко виявляти серійні схеми фальсифікації, обмін біометричною інформацією, зображеннями, відбитками пальців, описами «модус операнді». Ключову роль у реалізації HAKA II відіграли Frontex, Інтерпол, Європол, національні спецслужби з імміграційного контролю, прикордонні служби, митниці. Відтак, операція «HAKA II» – це зразок ефективного міжнародного поліцейського співробітництва, що поєднує технології, швидку комунікацію та скоординовану дію у відповідь на зростання глобальних міграційних ризиків, індустрії фальшивих документів, міжнародного фінансового шахрайства.

Натомість, у ході проєкту TOPCOP в партнерстві з Європолом CEPOL прагне створити мережу аналітичних контактів і контактних пунктів для розбудови потенціалу, проведення аналізу оперативних потреб у підготовці правоохоронних органів, посилення оперативної співпраці між країнами-партнерами, а також між Східним партнерством, державами-членами ЄС та агентствами ЄС (CEPOL та Європол) [6].

Водночас в останні роки в Україні збільшується кількість державних органів, які можуть напряму обмінюватись оперативною інформацією з питань протидії організованій злочинності з іноземними колегами. Зокрема Департамент стратегічних розслідувань Національної поліції за Угодою між Україною та Європейським поліцейським офісом про оперативне та стратегічне співробітництво може безпосередньо здійснювати обмін інформацією з Європолом та правоохоронними органами іноземних держав.

Список використаних джерел:

1. Interpol. Project Millennium. Project Millennium helps countries identify the people and companies behind transnational Eurasian organized crime. URL: https://www.interpol.int/Crimes/Organized-crime/Project-Millennium (дата звернення: 06.10.2025).

2. У рамках операції Європолу затримано понад 800 осіб. DW. 08.06.2021. URL: https://www.dw.com/ru/evropol-i-fbr-soobshhili-ob-uspeshnom-provedenii-krupnomasshtabnoj-operacii-v-bolee-chem-100-stranah/a-57813672 (дата звернення: 10.10.2025).

3. Європол затримав 150 ймовірних злочинців із даркнету. DW. 08.06.2021. URL: https://www.dw.com/ru/evropol-zaderzhal-po-vsemu-miru-150-podozrevaemyh-v-prestuplenijah-v-darknete/a-59633465 4 (дата звернення: 06.10.2025).

4. Шаталін В. Європол розкрив мережу кіберздирників. DW. 29.10.2021. URL: https://www.dw.com/ru/evropol-raskryl-set-kibervymogatelej/a-59669666 (дата звернення: 29.09.2025).

5. Понад 1000 арештів та вилучено 27 мільйонів доларів США в рамках масштабної операції з боротьби з фінансовими злочинами. URL: https://www.interpol.int/News-and-Events/News/2021/More-than-1-000-arrests-and-USD-27-million-intercepted-in-massive-financial-crime-crackdown (дата звернення: 02.10.2025).

6. TOPCOP Strengthening strategic and operational cooperation in the Eastern Partnership countries to fight against organised crime. URL: https://www.cepol.europa.eu/international-cooperation/topcop (дата звернення: 06.10.2025).

НОВІКОВ Євгеній
курсант 2 курсу ННІ №4 Харківського національного університету внутрішніх справ

ІННОВАЦІЙНІ АДМІНІСТРАТИВНО-ПРАВОВІ ПІДХОДИ ДО ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ ПІД ЧАС СПІВПРАЦІ З МІЖНАРОДНИМИ ПРАВООХОРОННИМИ СТРУКТУРАМИ

Розвиток глобальних комунікаційних технологій та інтенсивне міжнародне співробітництво правоохоронних органів призводить до зростання обсягів персональних даних, що передаються, обробляються та зберігаються у транскордонному форматі. Україна, перебуваючи в умовах збройного конфлікту, змушена активно протидіяти організованій злочинності, яка дедалі більше набуває транснаціонального характеру.

Національна поліція України у своїй діяльності активно взаємодіє з міжнародними правоохоронними організаціями: Інтерпол, Європол, CEPOL тощо. Така співпраця потребує не лише технічного захисту інформації, а й чітко нормованих адміністративно-правових процедур.

Система захисту персональних даних в Україні базується на Конституції України, Законі України «Про захист персональних даних», Законі України «Про Національну поліцію» та інших нормативних актах.

Стаття 34 Конституції України закріплює право збирати, зберігати, використовувати і поширювати інформацію, проте частина 2 відповідної статті вказує на те, що: «Здійснення цих прав може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку...[1].».

Правові підстави обробки персональних даних у діяльності органів поліції визначені Законом України «Про захист персональних даних». Так, відповідно до статті 11 цього Закону, обробка персональних даних здійснюється лише за наявності визначених законом підстав. До таких підстав належать:

1) Згода суб'єкта персональних даних на їх обробку;
2) Дозвіл на обробку персональних даних,

3) Укладення та виконання правочину, стороною якого є суб'єкт персональних даних, або правочину, укладеного на користь цього суб'єкта чи для здійснення заходів, що передують укладенню правочину на його вимогу[2];

Стаття 4 Закону України Про Національну поліцію зазначає, що: «Взаємовідносини у сферах діяльності поліції з відповідними органами інших держав та міжнародними організаціями базуються на міжнародних договорах, а також на установчих актах та правилах міжнародних організацій, членом яких є Україна[3].».

Адміністративно-правова діяльність поліції у цій сфері охоплює реалізацію інформаційно-аналітичних повноважень. Так, відповідно до частині 2 статті 25 Закону України «Про Національну поліцію», поліція у межах інформаційно-аналітичної діяльності:

1) Формує реєстри та бази даних;

2) Здійснює інформаційно-пошукову та інформаційно-аналітичну роботу[3];

4)Здійснює інформаційну взаємодію з іншими органами державної влади України, органами правопорядку іноземних держав та міжнародними організаціями[3].

Національна поліція України є членом та партнером міжнародних правоохоронних організацій: Інтерпол з 1992 року, Європол та FRONTEX. У рамках такої взаємодії вона передає й отримує інформацію про осіб, причетних до транснаціональних злочинів, переміщення зброї, наркотичних засобів, фінансових потоків.

Серед основних проблем у сфері захисту персональних даних під час співробітництва з міжнародними партнерами можемо виокремити:

1) Фрагментарність правового регулювання, що проявляється у недостатній деталізації процедур обміну інформацією, невизначеності стандартів захисту даних та ризиках порушення прав людини;

2) Відсутність уніфікованих стандартів шифрування та контролю

доступу;

3) Низький рівень усвідомлення ризиків, пов’язаних із витоком даних.

Для ефективного забезпечення захисту персональних даних у діяльності поліції доцільно впровадити комплекс інноваційних адміністративно-правових рішень, серед яких:

1) Удосконалення нормативно-правової бази. Адаптації внутрішніх стандартів Національної поліції України до положень GDPR та Конвенції Ради Європи №108.

Конвенція Ради Європи №108 визначає міжнародні стандарти захисту персональних даних та встановлює принципи їх законної обробки. Основні положення конвенції включають: законність, справедливість, прозорість, точність, обмеження зберігання тощо. Стаття 7 визначає, що: «Для захисту персональних даних, що зберігаються у файлах даних для автоматизованої обробки, уживають відповідних заходів безпеки, спрямованих апобігання випадковому чи несанкціонованому знищенню або випадковій утраті, а також на запобігання несанкціонованим доступу, зміні або поширенню [4].»;

2) Запровадження інтегрованих електронних реєстрів із багаторівневою аутентифікацією, журналюванням доступу та автоматичним повідомленням про несанкціоновані операції, наприклад: SIEM, DLP, DAM системи. Ці системи успішно використовуються у компаніях Microsoft, NASA, Intel, Adobe та низці державних та силових структур США та ЄС;

3) Risk-based підхід передбачає проведення оцінки ризиків порушення конфіденційності;

4) Незалежний внутрішній контроль, який напряму залежить від поосилення існуючих підрозділів внутрішнього аудиту (Data Protection Officer), які здійснюють моніторинг, консультацію, оцінку ризиків, відповідають на запити громадян та контролюють безпеку даних.

В умовах реалізації державної політики України та євроінтеграційних процесів перспективним є впровадження сучасних стандартів захисту персональних даних у діяльності Національної поліції а саме:

1) Ратифікація міжнародних стандартів у сфері захисту інформації з інтеграцією національних цінностей і правових традицій;

2) Удосконалення національної сертифікації технологій захисту даних, що використовуються правоохоронними органами;

3) Ініціювання розвитку сучасних процедур захисту даних;

4) Залучення фахівців для створення та вдосконалення інформаційних систем, що зміцнює держсектор і цифрову сферу країни.

Захист персональних даних у процесі міжнародного інформаційного співробітництва є ключовим елементом адміністративної діяльності, особливо в умовах збройного конфлікту та зростання масштабів транснаціональної злочинності. Впровадження інноваційних адміністративно-правових підходів, адаптованих до міжнародних стандартів, дозволить не лише гарантувати права і свободи людини, а й підвищити ефективність боротьби з організованою злочинністю.

Список використаних джерел:

1. Конституція України від 28.06.1996 № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254к/96-ВР#Text (дата звернення: 05.10.2025).

2. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/go/2297-17 (дата звернення: 05.10.2025).

3. Про Національну поліцію: Закон України від 02.07.2015 № 580-VIII. URL: https://zakon.rada.gov.ua/laws/show/580-19#n17 (дата звернення: 05.10.2025).

4. Конвенція про захист осіб у зв’язку з автоматизованою обробкою персональних даних: Рада Європи, Конвенція, Міжнародний документ від 28.01.1981. URL: https://zakon.rada.gov.ua/go/994_326 (дата звернення: 05.10.2025).

ОЛІЙНИК Іван
студент-магістрант 1 курсу
Кам'янець-Подільського
національного
університету імені Івана Огієнка

ПЕРЕШКОДА ТА ПЕРСПЕКТИВИ У МІЖНАРОДНОМУ ІНФОРМАЦІЙНОМУ СПІВРОБІТНИЦТВІ ДЛЯ ПРОТИДІЇ ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ В УМОВАХ ЗБРОЙНОГО КОНФЛІКТУ

Міжнародна інформаційна співпраця у сфері протидії організованій злочинності – це комплексна та багатогранна проблема, що має як серйозні перешкоди, так і значні перспективи. Її ефективність залежить від подолання глибоких політичних, правових та психологічних бар'єрів. Передусім, варто розуміти, що збройний конфлікт створює ідеальні умови для розквіту організованої злочинності, яка часто інтегрується в економічні та соціальні структури, що ослабли через війну.

Стратегія боротьби з організованою злочинністю виходить за межі державних кордонів і потребує скоординованих глобальних зусиль, оскільки її масштаби не обмежуються лише національним рівнем [2, с. 78]. Дефіцит довіри та координації є однією з найглибших перешкод, що виникає з політичних реалій збройного конфлікту. Постійна напруженість та ворожість між країнами створюють атмосферу, де обмін інформацією, особливо тією, що стосується національної безпеки, розглядається як потенційний ризик. Наприклад, країна, що надає розвідувальні дані, може побоюватися, що вони будуть використані іншою стороною для досягнення власних політичних чи військових цілей, що можуть суперечити її інтересам. Цей «інформаційний параліч» дозволяє злочинним синдикатам вільно діяти, використовуючи

ситуацію хаосу та відсутності єдиного фронту. Вони створюють транснаціональні злочинні мережі, що займаються кримінальною діяльністю (контрабандою зброї та наркотиків), отримуючи величезні прибутки, які потім використовуються для фінансування подальших злочинних операцій або навіть підриву стабільності у регіоні [3, с. 63].

Ще однією критичною перешкодою є відсутність уніфікованої стратегії, правових та технічних стандартів [2, с. 83]. Кожна країна має власну законодавчу систему, що визначає як збирається, зберігається та передається інформація. Закони про захист персональних даних, такі як європейський GDPR, можуть значно ускладнити передачу інформації до країн з менш суворим законодавством, адже це може порушити права громадян. Такі розбіжності створюють юридичні «сірі зони», які злочинні угруповання активно експлуатують. Додатково, технічна несумісність є не менш важливою проблемою. Системи баз даних, що використовуються в одній країні, можуть бути нечитабельними для систем іншої країни. Це вимагає додаткових ресурсів та часу для конвертації даних, що може призвести до втрати їх актуальності й цінності. Злочинці ж, навпаки, використовують єдині цифрові інструменти та платформи для координації своїх дій, що дає їм значну перевагу у швидкості та ефективності.

Нарешті, психологічна травматизація та вигорання фахівців, що працюють у зонах збройних конфліктів, мають прямий вплив на ефективність міжнародної співпраці. Постійне перебування в умовах високого стресу, пов’язаного з ризиком для життя та необхідністю приймати складні рішення, призводить до емоційного виснаження та зниження когнітивних функцій [5, с. 189]. Це може проявлятися у вигляді зниженої концентрації, помилок в аналізі інформації та нездатності до критичного мислення. Коли фахівці виснажені, вони менш схильні до співпраці, адже це вимагає додаткових зусиль. В результаті, якість обміну інформацією знижується, а злочинні організації, що не мають подібних психологічних обмежень, легко використовують цю «слабку ланку» для реалізації своїх планів.

Однак, давайте поглянемо на цю ситуацію з іншого боку. Однією з ключових перспектив є створення спільних платформ для обміну інформацією. Ці платформи можуть функціонувати як міжнародні аналітичні центри, де експерти з різних країн працюватимуть над єдиною метою – протидією злочинності. Замість окремого обміну інформацією між країнами, що часто є повільним і недовіреним процесом, такий центр може бути єдиним «вікном» для швидкої передачі та аналізу інформації. Це дасть змогу миттєво реагувати на оперативні повідомлення, як-от дані про переміщення злочинних угруповань, їхні фінансові операції або схеми торгівлі зброєю. У Великій Британії за боротьбу з організованою злочинністю відповідає Національне агентство по боротьбі зі злочинністю, відоме як NCA [4, с. 78]. Іншим прикладом може бути створення міжнародної бази даних, доступ до якої матимуть лише перевірені фахівці. У такій базі можна буде зберігати інформацію про відомих злочинців, їхні зв'язки, а також дані про вилучені предмети та засоби, що дозволить швидше ідентифікувати злочинні мережі.

Іншою важливоюперспективою є стандартизація та уніфікація процедур. Це включає розробку та впровадження єдиних міжнародних стандартів для збору, обробки та передачі інформації. Коли всі країни-партнери дотримуються одних і тих же протоколів, це значно спрощує співпрацю і мінімізує юридичні «вузькі місця». Можна створити єдиний формат для звітів про злочинні інциденти або уніфіковані процедури для запитів про правову допомогу. Як провідна міжнародна структура, Інтерпол володіє необхідною правовою базою, технічним обладнанням та організаційною будовою, що дозволить йому ефективно та злагоджено координувати співпрацю між поліцейськими службами різних країн [1, с. 103].

Нарешті, застосування психологічних підходів для підтримки фахівців є критичною, але часто недооціненою перспективою. В умовах збройного конфлікту, фахівці, що працюють у сфері безпеки, піддаються постійному стресу [5, с. 189]. Інвестування у психологічну стійкість цих людей є інвестицією у їхню ефективність. Запровадження обов'язкових програм

психологічної підтримки, регулярні сесії з психологами, а також тренінги з управління стресом та попередження емоційного вигорання допоможуть зберегти їхню професійну продуктивність. Коли робітники почуваються психологічно захищеними та підтриманими, вони більш здатні до прийняття зважених рішень, об'єктивного аналізу інформації та ефективної комунікації з іноземними колегами. Це створить надійний фундамент для довіри, яка є основою успішної міжнародної співпраці.

Підсумовуючи, варто зазначити, що ефективна протидія організованій злочинності в умовах збройного конфлікту потребує не лише технічних та правових рішень, а й глибокого психологічного та емоційного підходу. Розбудова довіри, гармонізація законодавства та турбота про психологічний стан фахівців є ключем до успішної та ефективної міжнародної співпраці.

Список використаних джерел:

1. Вітюк Д.Л. Міжнародна співпраця у сфері запобігання злочинності на сучасному етапі. *Юридична наука.* № 10 (112). 2020. С. 100 – 107. URL: https://journal-nam.com.ua/index.php/journal/article/view/532/505 (дата звернення: 21.09.2025)

2. Герасименко О.В., Орлов Ю.В. Проблеми протидії організованій злочинності в умовах війни: від актуальних викликів до стратегічного управління. *Вісник кримінологічної асоціації України.* 2023. №1 (28). С. 72 – 86.

3. Леган І.М. Міжнародне співробітництво у сфері запобігання та протидії транснаціональній злочинності: монографія. Чернігів: НУ «Чернігівська політехніка», 2021. 328 с.

4. Луценко Ю. В. Протидія організованій злочинності: національний та іноземний досвід. *Вчені записки Таврійського національного університету імені В. І. Вернадського. Юридичні науки*. 2024. № 2. С. 75 – 81. URL: https://juris.vernadskyjournals.in.ua/journals/2024/2_2024/14.pdf (дата звернення: 21.09.2025)

5. Удод А.М. Криміналізація кримінальних правопорушень в особливий період. *Злочинність і протидія їй в умовах війни та у повоєнній перспективі: міждисциплінарна панорама*: зб. тез доп. Міжнар. наук.-практ. конф. (м. Вінниця, 19 квіт. 2024 р.). Вінниця: ХНУВС, 2024. 662 с. URL: https://dspace.univd.edu.ua/server/api/core/bitstreams/68b74520-989d-4908-a5c5-542e7a95a6dc/content (дата звернення: 21.09.2025)

ОНДА Вікторія
студентка 2 курсу кафедри підготовки офіцерів запасу Військово- юридичного інституту Національного юридичного університету імені Ярослава Мудрого
Науковий керівник*:*
КУРТОВ Анатолій
кандидат технічних наук, доцент, професор кафедри, завідувач кафедри підготовки офіцерів запасу Військово- юридичного інституту Національного юридичного університету імені Ярослава Мудрого

МІЖНАРОДНИЙ ДОСВІД ІНФОРМАЦІЙНОЇ ПОЛІТИКИ ПРОТИДІЇ ОРГАНІЗОВАНЙ ЗЛОЧИННОСТІ ПІД ЧАС ЗБРОЙНОГО КОНФЛІКТУ АГРЕСІЇ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ ПРОТИ УКРАЇНИ

Відповідно до ст. 3 Конституції України - людина, її життя і здоров‘я, честь і гідність, недоторканність і безпека визнаються в Україні найвищою соціальною цінністю [1, с.7]. Повномасштабна агресія Російської Федерації проти України, що розпочалася у 2014 році та досягла апогею 24 лютого 2022 року, створила безпрецедентні виклики не лише у сфері оборони та безпеки,

але й у протидії організованій злочинності. Так, в умовах триваючого повномасштабного вторгнення агресора, першочерговим завданням органів правопорядку країни залишається фіксація та розслідування злочинів проти основ національної безпеки України, миру, безпеки людства та міжнародного правопорядку. Умови воєнного стану формують особливе середовище, у якому злочинні угруповання використовують слабкі місця державних інституцій, дестабілізацію суспільства, зростання незаконного обігу зброї та економічні потрясіння, як наслідок, починаючи з 2025 р. стрімкого зростання рівня окремих видів злочинності й зміна характеру динаміки тяжких і дуже суттєво - особливо тяжких злочинів. За вчинення окремих видів злочинів, пов'язаних зі збройним конфліктом, обліковано 14 027 кримінальний правопорушень.

Починаючи з 1 січня 2025 року до вересня 2025 року, особам повідомлено 5 390 підозр, кримінальне провадження на 3 237 зазначеної категорії злочинів направлено до суду, 575 кримінальних правопорушень у провадженнях, досудове розслідування у яких зупинене відповідно до ст. 280, 615 Кримінального процесуального кодексу України, кримінальних проваджень на 568 епізодів зупинене у зв’язку з розшуком обвинувачених (підозрюваних) [2, с.9].

Організована злочинність у таких умовах набуває нових форм та методів діяльності, що вимагає від кримінології розробки адекватних засобів протидії. Важливу роль у цьому відіграють системні наукові дослідження, спрямовані на виявлення і аналіз нових проявів злочинної діяльності, вивчення соціальних, політичних та економічних факторів, що сприяють її поширенню, а також розробку нових стратегій та підходів до протидії цим явищам [3, с.216]. Інформаційна політика у сфері безпеки та оборони розглядається як комплекс державних і міждержавних заходів, спрямованих на забезпечення ефективної комунікації, обмін даними між правоохоронними органами та суспільством, а також боротьбу з пропагандою і дезінформацією. Міжнародні підходи та досвід є дуже важливими аспектами у сучасній війні агресії

російської федерації проти України. Європейський Союз активно розвиває інформаційну політику у сфері протидії організованій злочинності через Європол, Євроюст та інші інституції. Основними напрямками Європейського Союзу є використання аналітичних центрів координації дії правоохоронцями з різних країн. Окремо звернути увагу на тему НАТО та її досвід в інформаційній політики під час агресії російської федерації проти України. Організація Північноатлантичного договору приділяє увагу інформаційній безпеці в умовах гібридної війни, НАТО виробило комплексну стратегію, що спрямована на захист інформаційного простору, протидію злочинним мережам і дезінформаційним кампаніям. НАТО щороку проводить багатонаціональні навчання Cyber Coalition**,** у яких відпрацьовуються сценарії кіберзагроз під час воєнних конфліктів [4, с.13].

Значна увага приділяється імітації гібридних операцій, де одночасно застосовуються кібератаки, дезінформація та дії організованих злочинних угруповань. НАТО співпрацює з Європолом та Інтерполом у сфері виявлення організованої злочинності, яка діє в інтересах держав-агресорів. Особлива увага приділяється структурам, що здійснюють контрабанду зброї та боєприпасів; беруть участь у кібератаках; поширюють дезінформацію або фінансують злочинні операції. Вивчення досвіду інших держав у сфері інформаційної політики є важливим чинником для вироблення ефективної стратегії протидії організованій злочинності в умовах воєнних конфліктів.

У різні періоди світ стикався з різними викликами. Саме тому аналіз конфліктів, як Балкани, Афганістан та Ірак, а також досвід Європейського Союзу дозволяє сформувати практичні уроки для України в умовах протидії агресії російської Федерації. Балкани (1990-ті роки) Під час воєн на території колишньої Югославії організована злочинність контролювала контрабандні канали зброї, наркотиків та людей. Європейський Союз та НАТО створили спільні програми інформаційного моніторингу, які дозволили локалізувати джерела фінансування воєнізованих угруповань. Досвід Балкан показав: ефективна інформаційна політика можлива лише у тісній співпраці

міжнародних структур із місцевими урядами. Афганістан та Ірак в умовах збройних конфліктів міжнародні коаліції застосовували інформаційні операції для обмеження впливу наркокартелів і терористичних структур. Ключовим елементом було інформаційне картографування (mapping) злочинних мереж, що дозволяло ідентифікувати зв'язки між криміналітетом і бойовиками. Європейський Союз, стикаючись із міграційними кризами та воєнними конфліктами на периферії, створив Європейський центр протидії організованій злочинності (ЕС3) при Європолі. Він застосовує інформаційні платформи для швидкого обміну даними між державами-членами, що є надзвичайно важливим і для України в умовах війни.

Аналіз міжнародного досвіду свідчить, що інформаційна політика виступає одним із найбільш дієвих інструментів протидії організованій злочинності в умовах воєнних конфліктів. Для України актуальним є не лише адаптація кращих практик НАТО, Європейського Союзу та інших держав, але й формування власної, цілісної моделі інформаційної стратегії, здатної врахувати специфіку триваючої агресії російської федерації. Вона має ґрунтуватися на розширенні міжнародної співпраці, створенні інтегрованих баз даних, застосуванні новітніх цифрових технологій та активному інформаційному впливі держави на суспільство. Лише такий комплексний підхід забезпечить ефективне блокування кримінальних та проросійських наративів, зміцнить національну безпеку й сприятиме посиленню стійкості України перед гібридними загрозами.

Список використаних джерел:

1. Конституція України: Закон від 28.06.1996 р. № 254к/96-ВР. URL: http://zakon.rada.gov.ua/laws/show/254к/96-вр (дата звернення: 30.09.2025)

2. Статистика. Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування. Офіс Генерального прокурора України. URL: https://gp.gov.ua/ua/posts/statistika (дата звернення: 30.09.2025)

3. Тітко І.А. Оцінні поняття в кримінально-процесуальному праві

України: монографія. Харків.: Право, 2010. 216 с.

4. АрміяInform, в Естонії відбуваються масштабні кібернавчання НАТО Cyber Coalition. 30 Листопада 2022, 11:52. URL: https://armyinform.com.ua/2022/11/30/v-estoniyi-vidbuvayutsya-masshtabni-kibernavchannya-nato-cyber-coalition/(дата звернення: 30.09.2025)

ПЕРЕДЕРІЙ Олександр
старший викладач кафедри підготовки офіцерів запасу Військово-юридичного інституту Національного юридичного університету імені Ярослава Мудрого,
кандидат юридичних наук, доцент

Дар'я ЯРЕМА
студентка 2 курсу 1 групи кафедри підготовки офіцерів запасу Військово-юридичного інституту Національного юридичного університету імені Ярослава Мудрого

ПРОБЛЕМАТИКА ФУНКЦІОНУВАННЯ МІЖНАРОДНОГО КРИМІНАЛЬНОГО СУДУ

Міжнародний кримінальний суд (далі – МКС) є центральним інститутом у сфері міжнародного кримінального правосуддя, створеним для притягнення до відповідальності осіб, винних у вчиненні найтяжчих злочинів: геноциду, злочинів проти людяності, військових злочинів та злочину агресії [1]. Його діяльність має особливе значення для України, яка протягом тривалого часу залишалася поза колом держав-учасниць Римського статуту, проте фактично

співпрацювала з МКС у зв'язку з агресією Російської Федерації та воєнними злочинами, скоєними на її території.

Протягом багатьох років питання ратифікації Римського статуту залишалося проблемним через низку політичних та правових причин, однак, з огляду на повномасштабну агресію росії, Ритання ратифікації стало невідкладним і вже 21 жовтня Україна офіційно ратифікувала Римський статут. Відтак, з 1 січня 2025 року він набрав чинності для України [1], що означає офіційне приєднання нашої держави до системи міжнародного кримінального правосуддя.

Попри цей історичний крок, функціонування МКС у контексті України має низку проблемних аспектів. Перш за все, йдеться про питання співвідношення юрисдикції МКС та національних судів. Згідно з принципом комплементарності, МКС втручається лише у випадку, коли держава не здатна або не бажає належним чином здійснювати розслідування і судовий розгляд. Україна має розвинену судову систему, однак війна, перевантаження правоохоронних органів і складність доведення воєнних злочинів ставлять під сумнів ефективність внутрішніх механізмів. У цьому контексті МКС виступає важливим додатковим механізмом, здатним забезпечити реальне притягнення до відповідальності винних у міжнародних злочинах.

Другою проблемою є обмеженість ресурсів самого МКС. Він розглядає справи з усього світу, і навіть попри історичний ордер на арешт президента РФ у 2023 році [2], кількість справ, які МКС реально може опрацювати, є невеликою. Станом на 31 січня 2025 року правоохоронці України відкрили 140 956 кримінальних проваджень за фактами злочинів, скоєних військовими рф та їх пособниками на території України [3]. Це викликає занепокоєння в українському суспільстві, оскільки масштаби воєнних злочинів в Україні величезні, і лише частина з них може бути предметом розгляду в Гаазі.

Третьою проблемною площиною виступає політичний аспект. Хоча МКС формально є незалежною інституцією, його діяльність часто перебуває під тиском з боку великих держав. Так, США, Росія та Китай не є сторонами

Римського статуту, що обмежує універсальність юрисдикції МКС. У випадку України це означає, що головний агресор відмовляється визнавати юрисдикцію МКС, а отже, постає проблема виконання рішень МКС, зокрема ордерів на арешт. 17 березня 2023 МКС, підозрюючи президента РФ і Уповноважену Президента з прав дітей РФ в незаконній депортації дітей з окупованих територій України на територію Росії, видав ордери на їх арешт і кваліфікував їхні дії відповідно до статуту МКС. 24 червня 2024 року Друга палата МКС видала ордери на арешт секретаря Ради безпеки РФ (екс-міністра оборони) Сергія Шойгу та начальника Генерального штабу РФ Валерія Герасимова. Їх підозрюють у вчиненні воєнних злочинів, як цілеспрямовані напади на цивільні об'єкти і заподіяння надмірної випадкової шкоди цивільним особам або пошкодження цивільних об'єктів, а також злочину проти людяності – інших нелюдських діянь [4].

Водночас, приєднання України до Римського статуту має й позитивні наслідки. По-перше, воно зміцнює міжнародний імідж нашої держави як країни, що поділяє принципи верховенства права та міжнародного правосуддя. По-друге, це відкриває шлях для більшої міжнародної підтримки у документуванні воєнних злочинів та співпраці з інституціями МКС. По-третє, ратифікація стимулює розвиток українського кримінального права і практики, оскільки вимагає гармонізації національного законодавства із міжнародними стандартами.

Проблематика функціонування МКС у контексті України полягає в пошуку балансу між національною юрисдикцією та міжнародними механізмами правосуддя, у вирішенні питань ресурсної спроможності та у подоланні політичних перепон, пов’язаних із небажанням деяких держав визнавати його авторитет. Водночас, приєднання України до Римського статуту є кроком історичного значення, що зміцнює позиції нашої держави у боротьбі за справедливість і створює додаткові можливості для притягнення до відповідальності осіб, винних у найтяжчих міжнародних злочинах.

Список використаних джерел:

1. Римський статут Міжнародного кримінального суду: Міжнародний документ від 17.07.1998, ратифікований Законом України від 20.01.2000 № 1401-XIV. URL: https://zakon.rada.gov.ua/laws/show/995_588 (дата звернення: 11.10.2025).

2. Прес-служба Апарату Верховної Ради України. 17 березня 2023 року Міжнародний кримінальний суд (МКС) в Гаазі видав ордери на арешт президента росії володимира путіна та уповноважену при президенті росії з прав дитини марії львової-бєлової. URL: https://www.rada.gov.ua/news/news_%20kom/259864.html (дата звернення: 21.09.2025)

3. Офіційна сторінка Міністерства внутрішніх справ. Російські воєнні злочини: оновлені дані станом на 31 січня 2025 року. URL:https://mvs.gov.ua/news/zlocini-vcineni-viiskovimi-rf-pid-cas-povnomasstabnogo-vtorgnennia-v-ukrayinu-stanom-na-31012025 (дата звернення: 21.09.2025)

4. International Criminal Court. Trying individuals for genocide, war crimes, crimes against humanity, and aggression. Ukraine. Situation in Ukraine. URL: https://www.icc-cpi.int/situations/ukraine (дата звернення: 21.09.2025)

ФІВКІН Петро
начальник кафедри права Національної безпеки та правової роботи Військово-юридичного інституту Національного юридичного університету імені Ярослава Мудрого, полковник поліції

ПАРХОМЕНКО Олександра
студентка 2 курсу 1 групи кафедри підготовки офіцерів запасу Військово-юридичного інституту Національного юридичного

університету імені Ярослава Мудрого

МІЖНАРОДНЕ СПІВРОБІТНИЦТВО ПІД ЧАС ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ПРОТИДІЇ ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ В УМОВАХ ЗБРОЙНОГО КОНФЛІКТУ

Міжнародне співробітництво в інформаційному забезпеченні протидії організованій злочинності в умовах збройного конфлікту являє собою складну, багаторівневу задачу, що вимагає водночас правової узгодженості, оперативної координації та захищених технологічних рішень, оскільки збройні конфлікти призводять до активізації злочинності, зокрема, у сфері незаконної торгівлі зброєю, наркотиками, людьми, фінансових махінацій, що використовуються як для збагачення транснаціональних злочинних угруповань, так і для фінансування терористичної діяльності.

Правову основу міжнародного співробітництва у цій сфері становить Конвенція Організації Об'єднаних Націй проти транснаціональної організованої злочинності, відома як Палермська конвенція, яка ратифікована Законом України від 4 лютого 2004 року № 1433-IV «Про ратифікацію Конвенції Організації Об'єднаних Націй проти транснаціональної організованої злочинності та протоколів, що її доповнюють (Протоколу про попередження і припинення торгівлі людьми, особливо жінками і дітьми, і покарання за неї і Протоколу проти незаконного ввозу мігрантів по суші, морю і повітрю)» з відповідними заявами та застереженнями і набула чинності для України 21 травня 2024 року. Дана конвенція у статтях 18, 26 та 27 визначає встановлені механізми взаємної правової допомоги, обміну інформацією та співробітництва правоохоронних органів і зобов'язує держави-учасниці забезпечувати максимально можливий обмін оперативною інформацією про транснаціональні злочинні групи, їхню структуру, методи діяльності та фінансові потоки [1].

Крім того, варто звернути увагу на Конвенцію Ради Європи про відмивання, пошук, арешт та конфіскацію доходів, одержаних злочинним шляхом, та про фінансування тероризму, яка ратифікована Законом України 17 листопада 2010 року № 2698-VI «Про ратифікацію Конвенції Ради Європи про відмивання, пошук, арешт та конфіскацію доходів, одержаних злочинним шляхом, та про фінансування тероризму» з відповідними заявами та застереженнями і набула чинності для України 01 червня 2011 року. Положення зазначеної конвенції є важливим міжнародно-правовим інструментом, що закріплює універсальні механізми боротьби з організованою злочинністю та тероризмом у фінансовій сфері. Головною її метою є уніфікація підходів держав до виявлення, блокування, арешту та конфіскації доходів злочинного походження, а також на створення ефективної системи міжнародного співробітництва у цій сфері. Конвенція зобов'язує держави-учасниці вживати законодавчих та організаційних заходів для оперативного заморожування й арешту активів, які можуть бути використані для фінансування терористичної діяльності або є результатом злочинної діяльності організованих угруповань. Вона також передбачає правову допомогу, обмін інформацією, взаємне визнання і виконання рішень щодо арешту та конфіскації майна, що значно посилює ефективність протидії транснаціональній злочинності та тероризму в умовах глобалізації та збройних конфліктів [2].

В умовах збройного конфлікту особливої ваги набуває діяльність міжнародних правоохоронних організацій, зокрема Європолу та Інтерполу. З Україною Європол уклав угоду про оперативне та стратегічне партнерство 14 грудня 2016 року, яка охоплює боротьбу з усіма видами злочинів, що належать до сфери компетенції Європолу, включно з пов'язаними правопорушеннями. Головне завдання такої співпраці - швидкий обмін даними про злочинців та злочинні мережі. Проте партнерство не обмежується лише цим. Воно також передбачає обмін експертними знаннями та досвідом, надання аналітичних звітів, інформування про методики розслідування та профілактики злочинів.

Крім того, українські правоохоронці можуть брати участь у спільних навчаннях, а Європол надає консультації та практичну допомогу у конкретних кримінальних справах. Завдяки цьому українські правоохоронці можуть оперативно отримувати дані про транснаціональні злочинні мережі, що особливо важливо для протидії контрабанді та організованій злочинності, які значно посилилися через російську агресію [3].

Інтерпол забезпечує глобальний обмін інформацією через систему I-24/7, де зберігаються дані про розшукуваних осіб, викрадені документи та транспортні засоби з усього світу, тощо. Це надзвичайно важливо в умовах, коли мільйони людей змушені залишати свої домівки. Крім того, Інтерпол видає спеціальні міжнародні сповіщення: червоні - для затримання та екстрадиції злочинців, помаранчеві - для попередження про небезпеку та загрозу життю, а тому завдяки карткам Інтерполу здійснюється координування та пошук ватажків злочинних угруповань, які намагаються скористатися хаосом війни та втекти в треті країни [4].

Крім того, навіть за умов збройного конфлікту інформаційний обмін має здійснюватися з дотриманням принципів верховенства права та прав людини, передусім у сфері захисту персональних даних і гарантій справедливого судочинства.

Отже, міжнародне співробітництво у сфері інформаційного забезпечення протидії організованій злочинності в умовах збройного конфлікту має багаторівневий характер і реалізується через поєднання правових механізмів, інституційних форматів та технологічних інновацій. Його ефективність залежить від гармонізації національного законодавства з міжнародними стандартами, підвищення інституційної спроможності органів державної влади, а також формування довіри між міжнародними партнерами шляхом прозорих процедур обміну інформацією. Лише комплексний підхід може забезпечити належний рівень стійкості держави до викликів організованої злочинності в умовах збройних конфліктів.

Список використаних джерел:

1. Конвенція Організації Об'єднаних Націй проти транснаціональної організованої злочинності: ратифікована Законом України від 04.02.2004 р. №433-IV. URL: https://zakon.rada.gov.ua/laws/show/995_789#Text (дата звернення: 03.10.2025).

2. Конвенція Ради Європи про відмивання, пошук, арешт та конфіскацію доходів, одержаних злочинним шляхом, та про фінансування тероризму: ратифікована Законом України 17.11.2010 р. № 2698-VI. URL: https://zakon.rada.gov.ua/laws/show/994_948?find=1&text=замор#Text (дата звернення: 03.10.2025).

3. Що потрібно знати про Європол та його співпрацю з Україною?. Юридична фірма GOLAW - комплексні юридичні послуги та консультації. URL: https://golaw.ua/ua/insights/publication/shho-potribno-znati-pro-yevropol-ta-jogo-spivpraczyu-z-ukrayinoyu/ (дата звернення: 04.10.2025).

4. Види «карток» Інтерполу. «Інтерпол у цифрах та фактах». Випуск 6. - VB Partners. VB Partners - Challenge accepted. URL: https://vbpartners.ua/publikacziyi/vidi-kartok-interpolu (дата звернення: 04.10.2025).

ФРОЛОВ Федір
прокурор відділу забезпечення обвинувачення в апеляційному суду Донецької обласної прокуратури

КРИМІНАЛЬНА ВІДПОВІДАЛЬНІСТЬ ЗА ЗЛОЧИНИ ОРГАНІЗОВАНИХ ГРУП, ЩО ВИКОРИСТОВУЮТЬ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ДЛЯ ПІДРИВУ ОБОРОНОЗДАТНОСТІ УКРАЇНИ: МІЖНАРОДНО-ПРАВОВИЙ ВИМІР

У сучасних умовах гібридних загроз та цифрової трансформації суспільства організовані злочинні угруповання дедалі частіше використовують інформаційні технології для здійснення злочинів проти

національної безпеки та обороноздатності держави. Особливої актуальності ця проблема набула для України в контексті протидії агресії та необхідності захисту критичної інфраструктури від кіберзагроз. Організовані групи, що діють у кіберпросторі, здатні завдавати значної шкоди обороноздатності країни через дезінформаційні кампанії, кібератаки на військові об'єкти, розголошення державної таємниці та координацію діяльності на користь противника.

Відповідно до статті 28 Кримінального кодексу України (далі – КК України), злочинною організацією визнається стійке ієрархічне об'єднання кількох осіб, члени або структурні елементи якого за попередньою змовою організувалися для спільної діяльності з метою безпосереднього вчинення тяжких або особливо тяжких злочинів [1]. У контексті використання інформаційних технологій такі групи можуть діяти як у межах однієї країни, так і транснаціонально, що ускладнює процес їх виявлення та притягнення до відповідальності.

КК України передбачає низку складів злочинів, які можуть вчинятися організованими групами з використанням інформаційних технологій для підриву обороноздатності України. Зокрема, стаття 111 передбачає відповідальність за державну зраду, в тому числі надання іноземній державі допомоги в проведенні інформаційної війни проти України. Стаття 114-1 встановлює покарання за перешкоджання законній діяльності Збройних Сил України та інших військових формувань, що може здійснюватися через кібератаки на системи управління військами. Стаття 328 криміналізує розголошення державної таємниці, яке може відбуватися через злам баз даних з використанням спеціального програмного забезпечення. Стаття 361 передбачає відповідальність за несанкціоноване втручання в роботу комп'ютерних систем, якщо це призвело до загрози національній безпеці [1].

Міжнародно-правову основу кримінальної відповідальності за такі злочини складають кілька ключових документів. Будапештська конвенція про кіберзлочинність 2001 року, ратифікована Україною у 2005 році, встановлює

стандарти криміналізації діянь у кіберпросторі та механізми міжнародної співпраці [2]. Конвенція зобов'язує держави-учасниці встановити кримінальну відповідальність за несанкціонований доступ до комп'ютерних систем, передбачити покарання за перехоплення даних, забезпечити процедури збереження та вилучення комп'ютерних даних, а також налагодити міжнародну співпрацю у розслідуванні кіберзлочинів.

Палермська конвенція ООН проти транснаціональної організованої злочинності 2000 року, ратифікована Україною у 2004 році, встановлює стандарти боротьби з організованою злочинністю транснаціонального характеру [3]. Конвенція вимагає від держав-учасниць криміналізувати участь в організованій злочинній групі, встановити відповідальність юридичних осіб, забезпечити конфіскацію доходів від злочинної діяльності та налагодити міжнародну правову допомогу. Римський статут Міжнародного кримінального суду 1998 року передбачає юрисдикцію МКС щодо злочинів проти людяності та воєнних злочинів, які можуть включати використання інформаційних технологій для координації злочинних дій [4].

Важливу роль у практичній реалізації міжнародного співробітництва відіграють спеціалізовані організації. Європейське поліцейське відомство (Європол) має спеціалізований Європейський центр боротьби з кіберзлочинністю (EC3), який координує розслідування транснаціональних злочинів у кіберпросторі. Україна з 2016 року має Угоду про операційну співпрацю з Європолом, що дозволяє обмінюватися інформацією та координувати спільні операції [5]. Євроюст забезпечує координацію судового переслідування у транснаціональних справах, і у 2021 році Україна підписала Угоду про співробітництво з цією організацією [6]. Міжнародна організація кримінальної поліції (Інтерпол) координує боротьбу з кіберзлочинністю через Global Complex for Innovation (IGCI) у Сингапурі.

Попри наявність розвиненої міжнародно-правової бази, існують суттєві перешкоди для ефективного притягнення до відповідальності організованих груп. Транснаціональний характер кіберзлочинів створює колізії між

національними правовими системами, адже злочинці можуть фізично знаходитися в одній країні, використовувати сервери в іншій, а завдавати шкоди третій державі. Цифрові докази є летючими та можуть бути легко знищені, а необхідність дотримання процесуальних норм при вилученні даних з серверів, розташованих за кордоном, сповільнює розслідування. Окремі держави можуть не співпрацювати у видачі осіб або наданні правової допомоги з політичних мотивів, особливо якщо злочинні групи діють в інтересах цих держав. Крім того, організовані групи використовують складні методи шифрування, анонімізації та приховування цифрових слідів, що вимагає від правоохоронних органів високого рівня технічної підготовки.

Для підвищення ефективності протидії таким загрозам доцільно гармонізувати національне законодавство з міжнародними стандартами, розвивати міжнародне співробітництво через укладення двосторонніх та багатосторонніх угод, створювати спеціалізовані підрозділи для розслідування кіберзлочинів проти національної безпеки, посилювати захист критичної інфраструктури та забезпечувати ефективну координацію між різними правоохоронними службами.

Таким чином, кримінальна відповідальність за злочини організованих груп, що використовують інформаційні технології для підриву обороноздатності України, є комплексною проблемою, яка вимагає застосування як національних, так і міжнародно-правових механізмів. Сучасне законодавство України загалом відповідає міжнародним стандартам, однак потребує постійного вдосконалення з огляду на динамічний розвиток технологій та еволюцію злочинних схем. Міжнародне співробітництво через механізми Ради Європи, ООН, Європолу, Євроюсту та інших організацій є критично важливим для ефективного розслідування та притягнення до відповідальності членів транснаціональних злочинних груп. Лише комплексний підхід, який поєднує правові, технічні та організаційні заходи, може забезпечити належний рівень захисту обороноздатності держави від загроз у кіберпросторі.

Список використаних джерел:

1. Кримінальний кодекс України від 05.04.2001. URL: https://zakon.rada.gov.ua/laws/show/2341-14 (дата звернення: 11.10.2025).

2. Конвенція про кіберзлочинність: Міжнародний документ від 23.11.2001, ратифікований Законом України від 07.09.2005 № 2824-IV. URL: https://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 09.10.2025).

3. Конвенція Організації Об'єднаних Націй проти транснаціональної організованої злочинності: Міжнародний документ від 15.11.2000, ратифікований Законом України від 04.02.2004 № 1433-IV. URL: https://zakon.rada.gov.ua/laws/show/995_789 (дата звернення: 11.10.2025).

4. Римський статут Міжнародного кримінального суду: Міжнародний документ від 17.07.1998, ратифікований Законом України від 20.01.2000 № 1401-XIV. URL: https://zakon.rada.gov.ua/laws/show/995_588 (дата звернення: 11.10.2025).

5. Угода про операційне та стратегічне співробітництво між Україною та Європейським поліцейським офісом: Міжнародний документ від 14.12.2016, ратифікований Законом України від 19.10.2017 № 2169-VIII. URL: https://zakon.rada.gov.ua/laws/show/984_001-16 (дата звернення: 28.09.2025).

6. Угода про співробітництво між Україною та Євроюстом: Міжнародний документ від 27.06.2016, ратифікований Законом України від 19.10.2017 № 2142-VIII. URL: https://zakon.rada.gov.ua/laws/show/984_007-16 (дата звернення: 11.10.2025).

ЧЕРНЕЦЬКА Ірина
Старший оперативноуповноважений
УСР в Кіровоградській області

ПРИРОДНИХ РЕСУРСІВ В УМОВАХ ЗБРОЙНОГО КОНФЛІКТУ: ОСОБЛИВОСТІ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ТА МІЖНАРОДНОГО СПІВРОБІТНИЦТВА

Сучасний етап розвитку українського суспільства характеризується складними безпековими умовами, пов'язаними із збройною агресією проти України та активізацією організованої злочинності у сфері незаконного використання природних ресурсів. В умовах збройного конфлікту незаконна вирубка лісів, видобуток бурштину, надр, браконьєрство та забруднення довкілля набувають системного та транснаціонального характеру. Ці злочини часто мають ознаки організованої діяльності, пов'язаної із корупцією, контрабандою та відмиванням доходів.

Кримінально-правова протидія таким проявам визначається низкою норм Кримінального кодексу України, зокрема статтями 240, 241, 246, 249, 255, 258-5, які передбачають відповідальність за порушення правил охорони надр, забруднення атмосферного повітря, незаконну порубку лісу, зайняття незаконним рибним промислом, створення злочинної організації та фінансування тероризму. В умовах збройного конфлікту ці діяння нерідко кваліфікуються у сукупності з тяжчими злочинами, такими як фінансування окупаційних адміністрацій чи підтримка незаконних збройних формувань.

Організовані злочинні угруповання, діючи в умовах воєнного стану, використовують слабкість державного контролю, складність доступу правоохоронних органів до окремих територій, а також підвищений попит на природні ресурси для військово-промислових і комерційних цілей. Це потребує комплексного інформаційно-аналітичного забезпечення діяльності правоохоронних органів.

Інформаційне забезпечення кримінально-правової протидії незаконному використанню природних ресурсів охоплює формування, інтеграцію та використання баз даних про екологічні правопорушення, фінансові потоки, рух техніки, вантажів, а також моніторинг публічних закупівель і державних

реєстрів. У цьому контексті важливим є розвиток взаємодії між Національною поліцією, Службою безпеки України, Держекоінспекцією, Держгеонадрами, Міністерством захисту довкілля та природних ресурсів і міжнародними структурами.

Міжнародне співробітництво у протидії організованій злочинності у сфері природокористування ґрунтується на положеннях Конвенції ООН проти транснаціональної організованої злочинності (2000 р.), Орхуської конвенції (1998 р.), Конвенції Ради Європи про захист довкілля через кримінальне право (1998 р.), а також угодах між правоохоронними органами держав — членів Інтерполу та Європолу. Зазначені міжнародні акти зобов'язують держави забезпечувати ефективний обмін інформацією, уніфікацію доказових стандартів та спільні розслідування у справах, що стосуються незаконного використання природних ресурсів.

В умовах війни особливого значення набуває кіберкомпонент - використання супутникових знімків, геоінформаційних систем, автоматизованих баз даних для відстеження незаконних рубок, розробок надр, транскордонного переміщення ресурсів. Інформаційна взаємодія між підрозділами Національної поліції, БЕБ, СБУ та міжнародними партнерами здійснюється через канали Інтерполу, Europol і SELEC, що дозволяє ідентифікувати організаторів злочинних схем і пов'язані з ними фінансові потоки.

Проблемними залишаються питання уніфікації форматів обміну інформацією, захисту персональних даних, своєчасного оновлення відомостей у базах даних та правового регулювання використання аналітичних систем. Не менш важливим є забезпечення кібербезпеки від несанкціонованого втручання з боку іноземних спецслужб та злочинних угруповань.

Для підвищення ефективності кримінально-правової протидії організованій злочинності у сфері незаконного використання природних ресурсів доцільно:

1) удосконалити інформаційно-аналітичну інфраструктуру

правоохоронних органів шляхом створення єдиної екологічної криміналістичної бази даних;

2) запровадити автоматизований моніторинг природокористування на базі штучного інтелекту та супутникових технологій;

3) розширити міжнародну співпрацю з Інтерполом, Європолом, UNODC у сфері протидії екологічним злочинам;

4) удосконалити кримінально-правові норми з урахуванням воєнних реалій, визначивши обтяжуючою ознакою вчинення злочину організованою групою в умовах збройного конфлікту.

Таким чином, ефективна протидія організованій злочинності у сфері незаконного використання природних ресурсів можлива лише за умови інтеграції кримінально-правових, інформаційно-аналітичних і міжнародно-правових механізмів. Сучасна модель має поєднувати інструменти цифрового моніторингу, аналітики та міжнародного партнерства для захисту національних природних багатств і екологічної безпеки України.

Список використаних джерел:

1. Кримінальний кодекс України: Закон України від 05.04.2001 № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 13.10.2025).

2. Конвенція ООН проти транснаціональної організованої злочинності: Міжнародний документ від 15.11.2000. URL: https://zakon.rada.gov.ua/laws/show/995_789#Text (дата звернення: 13.10.2025).

3. Орхуська конвенція про доступ до інформації, участь громадськості у процесі прийняття рішень та доступ до правосуддя з питань, що стосуються довкілля : Міжнародний документ від 25.06.1998. URL: https://zakon.rada.gov.ua/laws/show/994_015#Text (дата звернення: 13.10.2025).

4. Конвенція Ради Європи про захист довкілля через кримінальне право: Міжнародний документ від 04.11.1998.

URL: https://zakon.rada.gov.ua/laws/show/994_011#Text (дата звернення: 13.10.2025).

5. Про Національну поліцію : Закон України від 02.07.2015 № 580-VIII. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text (дата звернення: 13.10.2025).

ЧЕРНИХ Вадим
заступник начальника Головного управління Національної поліції в Кіровоградській області, підполковник поліції, аспірант Донецького державного університету внутрішніх справ

МІЖНАРОДНИЙ ДОСВІД ЗАТРИМАННЯ УПОВНОВАЖЕНОЮ ОСОБОЮ ОСОБИ, ПІДОЗРЮВАНОЇ У ВЧИНЕННІ ЗЛОЧИНУ

Проблематика затримання осіб, підозрюваних у вчиненні злочинів, традиційно привертає увагу дослідників кримінального процесу. І це цілком закономірно, адже саме в межах цього інституту найгостріше постає питання співвідношення публічних інтересів держави у сфері боротьби зі злочинністю та конституційних гарантій недоторканності особи. Вивчення того, як цю проблему вирішують у різних країнах, дає змогу не лише виявити загальні закономірності розвитку процесуального права, а й з'ясувати специфіку національних підходів до забезпечення балансу між ефективністю кримінального переслідування та захистом прав людини [1, с. 337].

Так, для англо-американської правової сім'ї характерним є практичний підхід до регламентації повноважень правоохоронних органів. Наприклад, конституційною основою інституту затримання у Сполучених Штатах Америки (далі – США) виступає Четверта поправка, яка проголошує захист

від безпідставних обшуків та арештів, проте концепція «probable cause» передбачає досить широку дискрецію правоохоронних органів – достатньо лише наявність обґрунтованих підстав вважати особу причетною до злочину. Такий критерій, порівняно з європейськими стандартами, є менш суворим, що, власне, й відображає американську кримінально-правову політику, орієнтовану на превентивні заходи.

Вагомим у цьому контексті стало рішення Верховного суду США у справі Terry v. Ohio [2], яким було введено в практику «stop and frisk» – короткочасну зупинку та поверхневий огляд особи навіть за відсутності достатніх підстав для арешту. Суд обґрунтував допустимість такого втручання необхідністю забезпечення безпеки поліцейських, встановивши стандарт «reasonable suspicion» (обґрунтованої підозри), який вимагає наявності конкретних фактів, що піддаються чіткому формулюванню. Процесуальними гарантіями прав затриманого слугує, зокрема, обов'язок правоохоронців негайно роз'яснити право не свідчити проти себе та право на адвоката, порушення яких тягне визнання отриманих доказів недопустимими.

Інший підхід демонструє англосаксонська модель запроваджена у Великій Британії. Police and Criminal Evidence Act 1984 року створив більш формалізовану систему процесуальних гарантій, яка, як зазначає М. Зандер, стала відповіддю на громадський запит щодо обмеження поліцейського свавілля [3, с. 47]. Підставою для затримання визначено наявність розумних підстав для підозри, при цьому законодавець диференціює повноваження залежно від категорії злочинів.

Принциповим підходом британського законодавця стало запровадження посади «custody officer» – інспектора з дотримання прав людини. Тобто, спеціально уповноваженого поліцейського, функціонально не пов'язаного з розслідуванням конкретного провадження, до компетенції якого належить перевірка правомірності кожного випадку доставлення особи до органу поліції. Така організаційна модель, як свідчать емпіричні дослідження, створює додатковий бар'єр для можливих зловживань з боку правоохоронних

органів[4, с. 350]. Часові межі затримання також структуровані за принципом пропорційності, де основний строк визначено у 24 години. Однак за наявності судового рішення ці часові межі можуть бути продовжено до 36 годин у провадженнях щодо тяжких злочинів, а в окремих категоріях проваджень, пов'язаних з тероризмом, – аж до 14 діб.

Суттєві відмінності в підходах до затримання демонструє континентальна система кримінального судочинства. Німецький «Strafprozessordnung» встановлює для органів поліції право на «vorläufige Festnahme» (попереднє затримання) лише за наявності двох умов: достатніх фактичних даних про причетність особи до злочину та підстав для застосування «Untersuchungshaft» (тримання під вартою як запобіжного заходу) [5, с. 298]. Водночас, процесуальною гарантією виступає норма параграфа 128 StPO [6], згідно з якою затриману особу необхідно без зволікання, але не пізніше наступного дня після затримання, доставити до судді для вирішення питання про застосування запобіжного заходу. У цьому виявляється фундаментальний для німецького права принцип «Rechtsstaat», де судовий контроль розглядається як найважливіша гарантія від правоохоронного свавілля.

Французька підхід «garde à vue» (поліцейське затримання) характеризується дещо іншою логікою побудови, яка тривалий час викликала критику з боку правозахисників та наукового кола. Система затримання у Франції зазнала кардинальних змін у 2011 році, причому ці зміни стали результатом не стільки внутрішньополітичного процесу, скільки зовнішнього тиску з боку наднаціональних інституцій, зокрема шляхом імплементації практики Європейського суду з прав людини (наприклад, рішення у справі Salduz v. Turkey) [7]. Як результат, встановлено право на присутність захисника з першої години затримання, причому перший допит не може відбутися раніше, ніж через дві години після звернення затриманого до адвоката. Але, французький законодавець, враховуючи специфіку та потреби оперативно-розшукової діяльності, передбачив і винятки, коли прокурор або

суддя може відтермінувати допуск адвоката до 12 годин у виняткових випадках. Тобто, основний строк «garde à vue» становить 24 години з можливістю продовження прокурором до 48 годин, а в провадженнях, пов'язаних з терористичними актами – до 96 годин. Характерною особливістю французької системи залишається чітке розмежування поліцейського затримання (garde à vue) та судового взяття під варту (détention provisoire), що відображає дуалістичну структуру французького кримінального процесу.

Отже, порівняльний аналіз наведених підходів дозволяє стверджувати, що процес поступової конвергенції національних систем відбувається під впливом стандартів міжнародного права, а саме щодо прав людини. Стаття 5 Конвенції про захист прав людини і основоположних свобод [8] у своїй конструкції передбачає необхідність негайного доставлення затриманого до судді, проте поняття «негайно» по-різному трактується державами-учасницями, що спричиняє певну неоднорідність правозастосовної практики. Водночас зберігається введена тенденція до розширення процесуальних прав затриманих осіб, передусім права на доступ до захисника з моменту фактичного обмеження свободи.

Вважаємо, що адаптація міжнародного досвіду до національної правової системи має відбуватися не через механічне копіювання окремих інститутів, а шляхом осмислення їхнього призначення з урахуванням особливостей кримінальних процесуальних традицій. Використання позитивних надбань іноземних правових систем за умови збереження національної ідентичності може сприяти досягненню оптимального співвідношення між інтересами ефективного кримінального переслідування та необхідністю гарантування основоположних прав особи.

Список використаних джерел:

1. Kusak M. Common EU Minimum Standards for Enhancing Mutual Admissibility of Evidence Gathered in Criminal Matters. *European Journal of Criminal Policy Research.* Vol. 23. 2017. P. 337–352.

2. Terry v. Ohio, 392 U.S. 1 (1968). Supreme Court of the United States. 1968. *JUSTIA.* URL: https://supreme.justia.com/cases/federal/us/392/1/ (дата звернення: 05.10.2025).

3. Zander M. PACE (The Police And Criminal Evidence) Act 1984: Past, Present And Future. *National Law School of India Review.* Vol. 23, No. 1. 2011. P. 47–62. URL: https://www.jstor.org/stable/44283738 (дата звернення: 05.10.2025).

4. Brown D., Ellis T., Larcombe K. The Detention of Suspects in Police Custody: The Impact of the Police and Criminal Evidence Act 1984. *British Journal of Criminology*. Vol. 31, No. 4. 1991. P. 347-364. URL: https://academic.oup.com/bjc/article-abstract/31/4/347/498642 (дата звернення: 05.10.2025).

5. Weigend T. Assuming the defendant is not guilty: The presumption of innocence in the German System of Criminal Justice. *Criminal Law, Philosophy.* Vol. 8. 2014. P. 285–299.

6. German Code of Criminal Procedure (Strafprozessordnung – StPO). *Federal Office of Justice.* URL: https://www.gesetze-im-internet.de/englisch_stpo/ (дата звернення: 05.10.2025).

7. Hodgson J. The French Garde À Vue Declared Unconstitutional. *Warwick School of Law Research Paper.* 2010. URL: https://papers.ssrn.com/sol3/papers.cfm? abstract_id=1669915 (дата звернення: 05.10.2025).

8. Конвенція з прав людини і основоположних свобод (з протоколами). Конвенція, Міжнародний документ від 04.11.1950. *Офіційний вебпортал Верховної ради України.* URL: https://zakon.rada.gov.ua/laws/show/995_004#Text (дата звернення: 05.10.2025).