МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Ю.В. Пирожкова, М.О. Ларкін

ПРАВОВЕ РЕГУЛЮВАННЯ ВИКОРИСТАННЯ ТА ЗАХИСТУ ІНФОРМАЦІЇ

Навчальний посібник

для здобувачів ступеня вищої освіти бакалавра спеціальності «Правоохоронна діяльність» освітньо-професійної програми «Правоохоронна діяльність»

Затверджено
вченою радою ЗНУ
Протокол № 9 від 24.02.2026 р.

Запоріжжя
2026

УДК: 342.9:[007+004](075.8)
П335

Пирожкова Ю.В., Ларкін М.О. «Правове регулювання використання та захисту інформації» : навчальний посібник для здобувачів ступеня вищої освіти бакалавра спеціальності «Правоохоронна діяльність» освітньо-професійної програми «Правоохоронна діяльність». Запоріжжя : Запорізький національний університет, 2026. 108 с.

У навчальному посібнику «Правове регулювання використання та захисту інформації» висвітлено теоретичні та прикладні засади правового регулювання інформаційних відносин, розкрито правові механізми доступу до інформації та захисту інформації з обмеженим доступом, охарактеризовано систему забезпечення інформаційної безпеки України, проаналізовано особливості міжнародного обміну інформацією та інформаційно-аналітичного забезпечення правоохоронної діяльності, розглянуто питання інформаційно-аналітичного забезпечення протидії молодіжній злочинності в діяльності правоохоронних органів. Запропоновано питання для самоконтролю, практичні завдання та рекомендовану літературу.

Призначений для підготовки здобувачів ступеня вищої освіти бакалавра спеціальності «Правоохоронна діяльність» освітньо-професійної програми «Правоохоронна діяльність».

Рецензент
Мельковський О.В. кандидат юридичних наук, доцент, доцент кафедри кримінального права та правоохоронної діяльності Запорізького національного університету..

Відповідальний за випуск
Р.В. Бараннік, кандидат юридичних наук, доцент, в.о. завідувача кафедри кримінального права та правоохоронної діяльності Запорізького національного університету.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АІДС	Автоматизовані інформаційно-довідкові системи
АІС	Автоматизовані інформаційні системи
АІПС	Автоматизовані інформаційно-пошукові системи
АРМ	Автоматизовані робочі місця
АСОД	Автоматизовані системи обробки даних
АСУ	Автоматизовані системи управління
ГУНП	Головне управління Національної поліції
ДІАЗ	Департамент інформаційно-аналітичного забезпечення
ЄІС МВС	Єдина інформаційна система Міністерства внутрішніх справ України
ІАЗ ОРД	Інформаційно-аналітичне забезпечення оперативно-розшукової діяльності
ІР	Інформаційні ресурси
ІКС	Інформаційно-комунікаційна система
ЄС	Європейський Союз
ЄКПЛ	Європейська конвенція з прав людини
Мінцифри	Міністерство цифрової трансформації
НКЦК	Національний координаційний центр кібербезпеки України
ООН	Організація Об’єднаних Націй
OSINT	Open Source Intelligence
РЄ	Рада Європи
РНБО	Рада національної безпеки і оборони України
СБУ	Служба безпеки України
Стратегія	Стратегія інформаційної безпеки

ВСТУП

Навчальний посібник «Правове регулювання використання та захисту інформації» присвячений комплексному дослідженню правових, організаційних та інформаційно-аналітичних засад функціонування інформаційної сфери в умовах формування інформаційного суспільства, цифрової трансформації державного управління та зростання безпекових викликів. У сучасних умовах інформація перетворюється на стратегічний ресурс, що визначає ефективність державної політики, рівень національної безпеки, стан публічної безпеки і правопорядку, а також можливості захисту прав і свобод людини і громадянина.

Посібник спрямований на формування у здобувачів вищої освіти цілісного уявлення про інформацію як соціально-правове явище, систему інформаційних відносин, інформаційні права людини та механізми їх реалізації і захисту. Значна увага приділяється філософському осмисленню інформації, доктринальним підходам до її поняття, ознак та видів, а також законодавчому визначенню інформації відповідно до Закону України «Про інформацію». Розкрито сутність інформаційного суспільства, напрями його розвитку та місце інформаційних відносин у сучасній правовій системі.

У навчальному посібнику висвітлено поняття та структуру інформаційних правовідносин, принципи їх функціонування, інформаційну правосуб’єктність як невід’ємну характеристику учасників інформаційних відносин. Окреслено особливості реалізації інформаційної правосуб’єктності фізичними та юридичними особами, об’єднаннями громадян, органами публічної влади. Розглянуто інформаційне право як комплексну галузь права, його предмет, методи, принципи та джерела.

Окремий розділ присвячено аналізу загроз інформаційній безпеці держави, суспільства та особи, зокрема поширенню пропаганди, дезінформації, фейкових повідомлень, інформаційно-психологічному впливу, що використовуються як інструменти гібридної війни та спрямовані на дестабілізацію суспільно-політичної ситуації, підрив довіри до органів державної влади та правоохоронних інституцій.

Приділено увагу правовому регулюванню доступу до інформації як одній із ключових гарантій реалізації інформаційних прав людини. Розкрито правову природу відкритої інформації, безумовно відкритої інформації, а також інформації з обмеженим доступом. Проаналізовано правові режими конфіденційної, службової та таємної інформації, підстави та межі обмеження права на доступ до інформації, механізми захисту державної таємниці та особливості режиму секретності в умовах правового режиму воєнного стану. Окремо розглянуто міжнародні стандарти у сфері захисту даних та інформаційної безпеки.

У навчальному посібнику комплексно висвітлено поняття та зміст інформаційної безпеки України, її об’єкти та складові, принципи державної інформаційної політики, основні напрями її реалізації, а також повноваження Президента України, Кабінету Міністрів України, Ради національної безпеки і оборони України, Національної поліції, Служби безпеки України, Державної служби спеціального зв’язку та захисту інформації України у сфері забезпечення інформаційної та кібербезпеки. Розкрито основні загрози інформаційній безпеці України та засоби їх нейтралізації, у тому числі в умовах збройної агресії та воєнного стану.

Особливу увагу приділено міжнародно-правовим засадам інформаційної безпеки та міжнародному обміну інформацією як важливому інструменту протидії транснаціональній злочинності, кіберзлочинності, тероризму та іншим сучасним загрозам. Розкрито значення англомовної підготовки кадрів правоохоронних органів у контексті реалізації Закону України «Про застосування англійської мови в Україні» як необхідної умови ефективної міжнародної комунікації та співпраці з Інтерполом, Європолом та іншими міжнародними правоохоронними структурами.

Окремий розділ присвячено питанням інформаційно-правового та інформаційно-аналітичного забезпечення правоохоронної діяльності. Розкрито поняття, завдання, систему та принципи інформаційного забезпечення правоохоронних органів, охарактеризовано джерела інформаційно-аналітичної діяльності, сучасні автоматизовані інформаційні системи та аналітичні технології, а також функціонування Єдиної інформаційної системи Міністерства внутрішніх справ України як ключового елементу сучасної моделі інформаційно-аналітичного забезпечення.

Акцентовано увагу на інформаційно-аналітичних, організаційно-технологічних та правових засадах протидії молодіжній злочинності. Розглянуто особливості оперативно-розшукової діяльності у сфері протидії злочинам, учиненим членами неформальних молодіжних угруповань, методи збору, класифікації та систематизації інформації, аналізу цифрових слідів, виявлення стійких зв’язків, формування аналітичних профілів злочинних груп. Окремо проаналізовано тактичні аспекти отримання достовірної інформації, зокрема під час проведення допитів представників молодіжних неформальних об’єднань, з урахуванням психологічних особливостей цієї категорії осіб.

У посібнику окреслено етичні та правові межі використання інформації у правоохоронній діяльності, приділено увагу забезпеченню законності, недопущенню порушень прав людини, дотриманню вимог конфіденційності, допустимості та достовірності інформації, отриманої під час слідчих та оперативно-розшукових дій.

Посібник поєднує фундаментальні теоретичні положення з практично орієнтованими завданнями, питаннями для самоконтролю, кейсами та

рекомендованою літературою, що сприяє формуванню у здобувачів вищої освіти професійних компетентностей, аналітичного мислення та навичок застосування норм інформаційного законодавства у практичній діяльності.

Навчальний посібник спрямований на формування у здобувачів першого (бакалаврського) рівня вищої освіти системного уявлення про правові засади використання, обігу та захисту інформації у професійній діяльності, а також на розвиток здатності застосовувати норми інформаційного законодавства з урахуванням вимог законності, прав людини та інформаційної безпеки.

Метою вивчення курсу «Правове регулювання використання та захисту інформації» є формування у здобувачів вищої освіти системи знань, умінь і навичок щодо правового регулювання інформаційних відносин, захисту інформації з обмеженим доступом, забезпечення інформаційної безпеки в діяльності правоохоронних органів, а також розвиток здатності забезпечувати інформаційну безпеку у правоохоронній діяльності, дотримуючись норм чинного законодавства та етичних стандартів обігу інформації.

Досягнення мети вивчення курсу забезпечує формування у здобувачів вищої освіти таких ***компетентностей і результатів навчання:***

- використовувати інформаційні та комунікаційні технології;
- організовувати нагляд (контроль) за додержанням вимог законодавства у сфері правоохоронної діяльності;
- професійно оперувати категоріально-понятійним апаратом інформаційного права і правоохоронної діяльності;
- критично та системно аналізувати правові явища і застосовувати набуті знання та навички у професійній діяльності;
- самостійно збирати та критично опрацьовувати, аналізувати та узагальнювати правову інформацію з різних джерел; аналізувати та систематизувати одержані результати, формулювати аргументовані висновки та рекомендації;
- забезпечувати законність та правопорядок, безпеку особистості та суспільства, протидіяти нелегальній (незаконній) міграції, тероризму та торгівлі людьми;
- ефективно застосовувати сучасні техніку і технології захисту людини, матеріальних цінностей і суспільних відносин від проявів криміногенної обстановки та обґрунтовувати вибір засобів та систем захисту людини і суспільних відносин;
- визначати належні та придатні для юридичного аналізу факти;
- використовувати технічні прилади та спеціальні засоби, інформаційно-пошукові системи та бази даних;
- забезпечувати кібербезпеку, економічну та інформаційну безпеку держави, об’єктів критичної інфраструктури;

- забезпечувати охорону державної таємниці та працювати з носіями інформації з обмеженим доступом;
- збирати необхідну інформацію з різних джерел, аналізувати і оцінювати;
- здійснювати пошук інформації у доступних джерелах для повного та всебічного встановлення необхідних обставин;
- користуватись державною системою урядового зв'язку, Національною системою конфіденційного зв'язку, формування та реалізації державної політики у сферах кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, криптографічного та технічного захисту інформації, телекомунікацій, користування радіочастотним ресурсом України, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку;
- здійснювати пошук та аналіз новітньої інформації у сфері правоохоронної діяльності, мати навички саморозвитку та самоосвіти протягом життя, підвищення професійної майстерності, вивчення та використання передового досвіду у сфері правоохоронної діяльності;
- застосовувати інформаційні системи, інформаційні технології, технології захисту даних, методи обробки, накопичення та оцінювання інформації, інформаційно-аналітичної роботи, бази даних (в тому числі міжвідомчі та міжнародні), оперативні та оперативно-технічні засоби, здійснення оперативно-розшукової діяльності;
- організовувати та здійснювати заходи щодо дотримання режиму секретності та захисту інформації.

Курс «Правове регулювання використання та захисту інформації» належить до обов'язкових дисциплін циклу професійної підготовки. Він тісно пов'язаний з такими дисциплінами як: Етика та професійна поведінка правоохоронця, Вступ до спеціальності, Права і свободи людини і громадянина в Україні, Кібербезпека і управління інформаційними ресурсами, Кримінологія, Криміналістика, Оперативно-розшукова діяльність, Виробничою практикою.

ТЕМА 1.
ТЕОРЕТИЧНІ ОСНОВИ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНИХ ВІДНОСИН ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Хто володіє інформацією, той володіє світом
Уїнстон Черчилль

План

1. Інформація та інформаційні відносини: основні поняття та категорії сучасної інформаційної парадигми.
2. Поняття та види інформації.
3. Інформаційне право: поняття, предмет, методи, система.
4. Інформаційна безпека: загрози та виклики. Правове забезпечення інформаційної безпеки в Україні.

Мета: набути цілісного уявлення про інформацію як базову категорію сучасної правової науки, зміст і структуру інформаційних відносин, місце та роль інформаційного права в системі права України, а також про сутність інформаційної безпеки, основні загрози інформаційній сфері та правові механізми її забезпечення в умовах цифровізації та сучасних безпекових викликів.

Перелік ключових термінів і понять з теми: інформація, відомості, знання, дані, інформаційні відносини, інформаційний підхід, інформаційна сфера, інформаційне середовище, інформаційна система, інформаційні технології, інформаційна модель, інформаційна безпека, інформаційне право.

1. Інформація та інформаційні відносини: основні поняття та категорії сучасної інформаційної парадигми.

Термін «інформація» у повсякденному вжитку нерідко сприймається інтуїтивно, без належного усвідомлення глибини та багатовимірності його змісту, і часто ототожнюється з такими суміжними поняттями, як «дані», «відомості» та «знання». Водночас, як слушно зауважує К. Бєляков у монографічному дослідженні «Інформація в праві: теорія і практика» (2006 р.), плутанина у визначеннях, що має місце в науковому обігу, нерідко призводить до непорозумінь і помилкових висновків, зокрема під час їх застосування у законодавстві. За цих умов інформація постає як одна з ключових категорій системи сучасних суспільних відносин, що зумовлює необхідність її чіткого доктринального та нормативного осмислення [1, с. 11 - 12].

У перекладі з латинської мови *informatio* означає «роз’яснення», «уявлення», що вказує на відомості або їх сукупність про предмети, явища та

процеси навколишнього світу. В енциклопедичних джерелах інформація визначається як відомості, що передаються людьми усним, письмовим або іншим способом, а також як загальнонаукове поняття, що охоплює обмін відомостями між людьми, між людиною й автоматизованими системами та обмін сигналами в живій природі. Для наведених визначень характерна спільна внутрішня сутність, що дозволяє застосовувати їх до різних систем і сфер людської діяльності. Наукове розуміння інформації зазнало суттєвої еволюції - від трактування її через категорії «уявлення», «поняття», «відомості» до концепції «передачі повідомлень». Аналізуючи сучасні підходи й теорії у сфері дослідження інформації та інформаційних процесів, К. Бєляков розглядає інформаційну парадигму крізь призму комплексного міждисциплінарного підходу та виокремлює основні напрями вивчення інформації [1, с. 12 - 42].

Зокрема, **теоретико-множинний підхід** передбачає аналіз множин інформаційних повідомлень і об'єктів з позицій їх кількісних характеристик без повного ігнорування якісних ознак.

Концепція різноманітності інформації ґрунтується на загальнонауковому понятті «різноманітність», пов'язаному з філософськими категоріями «відмінність» і «відображення». У правових дослідженнях цей підхід використовується, зокрема, під час трансформації інформації в інші форми, включаючи цифрові (наприклад, кодування папілярних візерунків у криміналістиці або формалізацію текстів нормативно-правових актів в інформаційно-пошукових системах).

Інформаційний підхід базується на принципі універсальності інформаційних процесів. Інформація розглядається як істотна сторона процесу відображення та його результат, пов'язаний із відтворенням структурно-функціональних властивостей однієї системи в іншій. Особливого значення в межах цього підходу набуває інформаційне моделювання - створення знакових, логіко-математичних моделей, що відображають ключові властивості системи-оригіналу. Сучасним різновидом таких моделей є інформаційні моделі, сформовані з використанням технологій штучного інтелекту.

Когнітивний підхід виходить із того, що рушійною силою соціального прогресу є розвиток інтелектуального потенціалу суспільства. Накопичення, обробка та використання інформації визначають інформаційну динаміку соціальних процесів, а когнітивний аспект інформації стає підґрунтям формування «ідеології знання».

Згідно із **системним підходом**, інформаційний обмін є необхідною умовою стабільності та розвитку соціальних систем. Економіка, освіта, наука, право, управління та інші підсистеми сучасного суспільства функціонують на основі активного використання інформаційних технологій і засобів масової інформації.

Праксіологічний підхід розмежовує поняття даних та інформації, розглядаючи дані як відображення подій і явищ, а інформацію — як результат їх аналітико-синтетичної обробки суб'єктом. Інформація формується в процесі усвідомлення даних людиною та може виникати як у професійній, так і в непрофесійній діяльності [1, с. 12 - 42].

У навчальному посібнику «Інформаційне право» (2022 р.) М. Ковалів, С. Єсімов, О. Ярема визначають інформацію як сукупність різних повідомлень про події, що відбуваються в будь-якій системі та навколишньому середовищі. Інформація є невіддільною від матеріального світу й може існувати у формі тексту, звуку, сигналів, радіохвиль тощо. При цьому повідомлення набуває інформативності лише за умови зміни його фізичних параметрів; статична, незмінна форма не створює інформаційного ефекту [2, с. 10 - 13].

Інформаційний потенціал суспільства охоплює інформаційні ресурси та інформаційну складову трудових ресурсів (інформаційних працівників). Сукупність показників розвитку інформаційного потенціалу суспільства умовно поділяється на кілька груп: показники розвитку інформації як базового ресурсу; показники розвитку технічної бази інформаційної сфери; рівень розвитку інформаційної техніки й технологій; показники розвитку трудових ресурсів інформаційної сфери; показники розвитку організаційної інфраструктури інформаційної діяльності. Науковці наголошують, що інформація як ресурс має низку унікальних властивостей: можливість необмеженого поширення без втрати змісту; здатність до зростання в процесі використання; відсутність фізичного зношування; високу мобільність, особливо з використанням інформаційних технологій; здатність підвищувати вартість матеріальних об'єктів, процесів і самої інформації.

Інформаційні ресурси є обов'язковим елементом здійснення будь-якого виду людської діяльності - виробничої, управлінської, науково-дослідної, освітньої, проектної, а також діяльності з підготовки та перепідготовки кадрів [2, с. 10 - 13].

Середовище функціонування інформаційних процесів визначається як **інформаційна сфера**, яка охоплює сукупність інформації, інформаційної інфраструктури та суб'єктів інформаційних відносин. Національна інформаційна сфера України формується як єдиний інформаційний простір і поступово інтегрується до європейського інформаційного простору з урахуванням вимог інформаційної безпеки. У навчальному посібнику «Актуальні питання інформаційного права» (2024 р.) В. Хахановський та О. Корнейко зазначають, що до основних об'єктів інформаційної сфери належать: інформація та інформаційні ресурси; інформаційна інфраструктура, яка включає організаційні, інформаційно-телекомунікаційні системи, інформаційні, комп'ютерні та телекомунікаційні технології, а також засоби масової інформації [3, с. 42 - 52].

У структурі інформаційної сфери традиційно виокремлюють процеси створення (виробництва) інформації, її поширення (безпосереднього й опосередкованого) та споживання. Ці процеси спрямовані на задоволення інформаційних потреб суб'єктів інформаційних відносин, до яких належать громадяни, їх об'єднання, підприємства, установи, органи державної влади та місцевого самоврядування. Право на інформацію в Україні гарантується законом, а держава забезпечує рівні можливості доступу до інформації, за винятком випадків, прямо передбачених чинним законодавством.

2. Поняття та види інформації

Згідно з ч. 1 ст. 1 Закону України «Про інформацію» від 02.10.1992 р. № 2657-XII (у редакції Закону України від 13.01.2011 р.), **інформація** - це будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді. Аналогічне визначення закріплено у ч. 1 ст. 200 Цивільного кодексу України.

У міжнародному стандарті ДСТУ ISO/IEC 2382:2022 **інформація** визначається як знання про факти, події, речі, ідеї або поняття, включаючи інструкції, які в певному контексті мають конкретне значення. Наведені дефініції свідчать про універсальний характер поняття інформації та його придатність для використання в різних сферах правового регулювання.

У доктрині інформаційного права сформовано розширений підхід до розуміння інформації як об'єкта правового регулювання. Так, у підручнику «Інформаційне право України» (2025 р.) за загальною редакцією О. Орлюк та О. Заярного виокремлюються основні ознаки інформації, до яких пропонується відносити:

– немайнова, неідеальна сутність інформації як об'єкта правового регулювання;

– трансформованість інформації, тобто можливість її передачі на різних матеріальних носіях із використанням різних способів обробки;

– універсальність інформації, що виявляється у її зв'язаності з будь-якими об'єктами, явищами та процесами реальної дійсності;

– субстанційна несамостійність інформації, тобто її нерозривний зв'язок із матеріальним носієм або технічним засобом передачі;

– нелінійний характер інформації, за якого кількісні та якісні характеристики не перебувають у прямій залежності;

– повнота змісту інформації як здатність вичерпно (для конкретного споживача) відображати об'єкт або процес;

– актуальність інформації, тобто її відповідність інформаційним потребам у визначений момент часу;

– релевантність інформації як відповідність інформаційного змісту запитам споживача;

– невичерпність інформації, що полягає у збереженні її обсягу незалежно від кількості користувачів;

– документальний характер інформації як первинного джерела;

– захищеність інформації, що передбачає заборону несанкціонованого доступу, використання, зміни чи знищення;

– наявність визначеного законом або договором правового режиму обігу інформації.

Багатозначність поняття «інформація», різноманітність форм її обробки та використання у різних сферах суспільної діяльності зумовили формування розгалуженої класифікації видів інформації.

Класифікація інформації за змістом

Відповідно до Закону України «Про інформацію», за змістом інформація поділяється на такі види:

- інформація про фізичну особу;
- інформація довідково-енциклопедичного характеру;
- інформація про стан довкілля (екологічна інформація);
- інформація про товар (роботу, послугу);
- науково-технічна інформація;
- податкова інформація;
- правова інформація;
- статистична інформація;
- соціологічна інформація;
- критична технологічна інформація;
- інші види інформації.

Інформація про фізичну особу

Інформація про фізичну особу (персональні дані) - відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована (ст. 11). Не допускаються збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та захисту прав людини. До конфіденційної інформації про фізичну особу належать, зокрема, дані про її національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, а також адреса, дата і місце народження.

Кожному забезпечується вільний доступ до інформації, яка стосується його особисто, крім випадків, передбачених законом.

Інформація довідково-енциклопедичного характеру

Інформація довідково-енциклопедичного характеру - систематизовані, документовані, публічно оголошені або іншим чином поширені відомості про суспільне, державне життя та навколишнє природне середовище (ст. 12).

Основними джерелами інформації довідково-енциклопедичного характеру є: енциклопедії, словники, довідники, рекламні повідомлення та оголошення,

путівники, картографічні матеріали, електронні бази та банки даних, архіви різноманітних довідкових інформаційних служб, мереж та систем, а також довідки, що видаються уповноваженими на те органами державної влади та органами місцевого самоврядування, об'єднаннями громадян, організаціями, їх працівниками та автоматизованими інформаційно-комунікаційними системами.

Правовий режим інформації довідково-енциклопедичного характеру визначається законодавством та міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України.

Інформація про стан довкілля (екологічна інформація)

Інформація про стан довкілля (екологічна інформація) - відомості та/або дані про:

- стан складових довкілля та його компоненти, включаючи генетично модифіковані організми, та взаємодію між цими складовими;
- фактори, що впливають або можуть впливати на складові довкілля (речовини, енергія, шум і випромінювання, а також діяльність або заходи, включаючи адміністративні, угоди в галузі навколишнього природного середовища, політику, законодавство, плани і програми);
- стан здоров'я та безпеки людей, умови життя людей, стан об'єктів культури і споруд тією мірою, якою на них впливає або може вплинути стан складових довкілля;
- інші відомості та/або дані (ст. 13).

Правовий режим інформації про стан довкілля (екологічної інформації) визначається законами України та міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України. Інформація про стан довкілля, крім інформації про місце розташування військових об'єктів, не може бути віднесена до інформації з обмеженим доступом.

Інформація про товар (роботу, послугу)

Інформація про товар (роботу, послугу) - відомості та/або дані, які розкривають кількісні, якісні та інші характеристики товару (роботи, послуги) (ст.14). Інформація про вплив товару (роботи, послуги) на життя та здоров'я людини не може бути віднесена до інформації з обмеженим доступом.

Науково-технічна інформація

Науково-технічна інформація - будь-які відомості та/або дані про вітчизняні та зарубіжні досягнення науки, техніки і виробництва, одержані в ході науково-дослідної, дослідно-конструкторської, проектно-технологічної, виробничої та громадської діяльності, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді (ст. 15). Правовий режим науково-технічної інформації визначається Законом України від 26.06.1993 р. № 3322-XII «Про науково-технічну інформацію», іншими законами та міжнародними договорами України, згода на обов'язковість яких надана

Верховною Радою України. Науково-технічна інформація є відкритою за режимом доступу, якщо інше не встановлено законами України.

Податкова інформація

Податкова інформація - сукупність відомостей і даних, що створені або отримані суб'єктами інформаційних відносин у процесі поточної діяльності і необхідні для реалізації покладених на контролюючі органи завдань і функцій у порядку, встановленому Податковим кодексом України (ст. 16). Правовий режим податкової інформації визначається Податковим кодексом України та іншими законами.

Правова інформація

Правова інформація - будь-які відомості про право, його систему, джерела, реалізацію, юридичні факти, правовідносини, правопорядок, правопорушення і боротьбу з ними та їх профілактику тощо (ст. 17). Джерелами правової інформації є Конституція України, інші законодавчі і підзаконні нормативно-правові акти, міжнародні договори та угоди, норми і принципи міжнародного права, а також ненормативні правові акти, повідомлення медіа, публічні виступи, інші джерела інформації з правових питань. З метою забезпечення доступу до законодавчих та інших нормативних актів фізичним та юридичним особам держава забезпечує офіційне видання цих актів масовими тиражами у найкоротші строки після їх прийняття.

Статистична інформація

Статистична інформація - документована інформація, що дає кількісну характеристику масових явищ та процесів, які відбуваються в економічній, соціальній, культурній та інших сферах життя суспільства (ст. 18). Офіційна державна статистична інформація підлягає систематичному оприлюдненню. Держава гарантує суб'єктам інформаційних відносин відкритий доступ до офіційної державної статистичної інформації, за винятком інформації, доступ до якої обмежений згідно із законом. Правовий режим офіційної державної статистичної інформації визначається Законом України від 16.08.2022 р. № 2524-IX «Про офіційну статистику», іншими законами України та міжнародними договорами України, згода на обов’язковість яких надана Верховною Радою України.

Соціологічна інформація

Соціологічна інформація - будь-які документовані відомості про ставлення до окремих осіб, подій, явищ, процесів, фактів тощо (ст. 19). Правовий режим соціологічної інформації визначається законами та міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України.

Критична технологічна інформація

Критична технологічна інформація - дані, що обробляються (приймаються, передаються, зберігаються) в системах управління технологічними процесами об’єктів критичної інфраструктури. Правовий режим критичної технологічної

інформації визначається законами України та міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України. Критична технологічна інформація за режимом доступу належить до інформації з обмеженим доступом та підлягає захисту згідно із законом.

Публічна інформація

Публічна інформація - це відображена та задокументована різними засобами та на будь-яких носіях інформація, що була отримана або створена в процесі виконання суб'єктами владних повноважень обов'язків, передбачених чинним законодавством, або яка знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених Законом України від 13.01.2011 р. № 2939-VI «Про доступ до публічної інформації». Публічна інформація є відкритою, крім випадків, установлених законом.

3. Інформаційне право: поняття, предмет, методи, система

В умовах розвитку інформаційного суспільства інформаційний вплив на державу, суспільство та окрему людину за своєю ефективністю нерідко перевищує політичний, економічний і навіть військовий вплив. Інформація перетворюється на реальну соціальну силу, здатну безпосередньо впливати на суспільні процеси, поведінку суб'єктів та механізми державного управління.

Інформаційне право як галузь права має власний предмет правового регулювання - **інформаційні відносини**, а також систему принципів і чітко окреслену сферу правового впливу - **інформаційну сферу**. Водночас інформаційне право функціонує як міжгалузева юридична наука, що досліджує інформаційну сутність права як складної соціальної системи, а також як навчальна дисципліна.

У доктрині інформаційного права воно розглядається у кількох взаємопов'язаних аспектах:

– як сукупність правових норм, що регулюють суспільні відносини у сфері інформації, зокрема в умовах інформатизації та цифровізації;

– як система норм, що визначають права та обов'язки суб'єктів інформаційних відносин;

– як міжгалузева юридична наука;

– як навчальна дисципліна.

Переважна більшість українських учених (Р. Калюжний, В. Хахановський, В. Цимбалюк та ін.) обґрунтовують позицію, згідно з якою інформаційне право є комплексною галуззю права, що має спеціальний предмет правового регулювання - суспільні інформаційні відносини. У цьому розумінні інформаційне право постає як система соціальних норм і відносин, що виникають в інформаційній сфері у зв'язку з виробництвом, перетворенням, поширенням і споживанням інформації.

Як галузева юридична наука інформаційне право досліджує сукупність правових норм, які регулюють інформаційні відносини, а також закономірності інформаційної діяльності та механізми її правового забезпечення. Узагальнюючи доктринальні підходи, М. Ковалів, С. Єсімов, О. Ярема визначають інформаційне право як комплексну галузь права, що складається з правових норм, які регулюють відносини, що виникають в інформаційній сфері - сфері виробництва, накопичення, обробки, перетворення і споживання інформації та перебувають під охороною держави. При цьому акцентується, що основним об'єктом таких відносин є інформація у формі відомостей, даних, знань, повідомлень тощо.

Предмет інформаційного права

Предметом інформаційного права є **інформація та суспільні відносини**, що виникають у процесі її створення (отримання), обробки, зберігання, поширення, використання й захисту, а також інформаційні права і свободи людини та громадянина. Особливості природи інформації зумовили формування галузі права, яка не може бути віднесена виключно ані до публічно-правових, ані до приватно-правових галузей.

Методи правового регулювання

Інформаційне право є комплексною галуззю і за методами правового регулювання. У цій сфері застосовується поєднання:

– імперативних методів (характерних для конституційного, адміністративного, кримінального права);

– диспозитивних методів (властивих цивільному та трудовому праву);

– приватно-правових засобів регулювання, зокрема правочинів, договорів, звичаїв, норм професійної етики, ділової практики та суспільної моралі.

Функції інформаційного права

Функції інформаційного права відображають основні напрями його впливу на інформаційні відносини та зумовлені його соціальним призначенням. До основних функцій належать:

– *регулятивна*, що полягає у визначенні прав, обов'язків і юридичних можливостей суб'єктів інформаційних відносин;

– *охоронна***,** спрямована на встановлення гарантій правомірної поведінки та профілактику правопорушень;

– *захисна*, яка забезпечує правові механізми відновлення порушених прав і притягнення до юридичної відповідальності;

– *інтегративна***,** що виявляється у поєднанні норм різних галузей права та використанні їх методів у сфері інформаційних відносин.

Система інформаційного права

Інформаційне право як галузь системи права становить сукупність правових норм, що регулюють діяльність суб'єктів у інформаційній сфері. Всередині галузі ці норми об'єднуються у підгалузі та правові інститути. Система інформаційного права є об'єктивною, оскільки відображає реальні суспільні відносини, та проявляється в інформаційному законодавстві, науці й навчальному процесі.

Структурно система інформаційного права поділяється на **загальну** та **особливу** частини. У загальній частині зосереджені норми, що визначають основні поняття, принципи, правові форми та методи регулювання інформаційної діяльності. Особлива частина охоплює правові інститути, які регулюють обіг відкритої та загальнодоступної інформації (інститут масової інформації, інститут інтелектуальної власності щодо інформаційних об'єктів, бібліотечна й архівна справа), а також інститути інформації з обмеженим доступом (інститути державної, комерційної таємниці, персональних даних тощо). Наведений поділ не є вичерпним, однак відображає основні групи правових норм, що різняться за особливостями правового режиму та соціальним значенням об'єкта регулювання. Більшість відповідних інститутів закріплені у чинних нормативно-правових актах України.

4. Інформаційна безпека: загрози та виклики. Правове забезпечення інформаційної безпеки в Україні.

Інформаційна безпека не є явищем, притаманним виключно сучасному етапу розвитку суспільства. Усвідомлення її значущості в історії людства змінювалося паралельно зі зростанням суспільної цінності інформації, проникненням інформаційної діяльності в усі сфери життєдіяльності та зростанням залежності особи, суспільства й держави від інформаційних процесів.

Поняття **«інформаційна безпека»** закріплене у низці нормативно-правових актів України, однак залежно від сфери правового регулювання воно наповнюється різним змістом. Так, у спеціальному фінансово-банківському законодавстві *інформаційна безпека* визначається як комплекс організаційних заходів, програмних і техніко-технологічних засобів, що функціонують на всіх організаційних рівнях відповідної установи та забезпечують захист інформації від випадкових та/або навмисних загроз, реалізація яких може призвести до порушення доступності, цілісності або конфіденційності інформації щодо діяльності установи чи її клієнтів (зокрема, Положення НБУ від 02.07.2019 р. № 88; Положення НБУ від 02.02.2024 р. № 15).

У низці актів Національного банку України інформаційна безпека розглядається крізь призму класичної тріади - конфіденційності, цілісності та доступності інформації (Положення про захист інформації та кіберзахист у

платіжних системах, затверджене постановою Правління НБУ від 19.05.2021 р. № 43).

Водночас у нормативних актах, що регулюють функціонування об'єктів критичної інфраструктури, інформаційна безпека трактується ширше - як стан захищеності, за якого забезпечуються функціональність, безперервність роботи, відновлюваність, цілісність і стійкість інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, конфіденційність, цілісність і доступність електронних інформаційних ресурсів, а також своєчасне виявлення, запобігання та нейтралізація реальних і потенційних загроз (Постанова Кабінету Міністрів України від 24.03.2023 р. № 257).

Системоутворюючим документом у сфері забезпечення інформаційної безпеки є **Стратегія інформаційної безпеки України**, затверджена Указом Президента України від 28.12.2021 р. № 685/2021. У Стратегії забезпечення інформаційної безпеки визначається як одна з найважливіших функцій держави, що спрямована на захист національних інтересів України в інформаційній сфері, прав і свобод людини, а також персональних даних.

У Стратегії інформаційна безпека України розглядається як складова частина національної безпеки та визначається як 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, а також існує ефективна система протидії шкоді, що може завдаватися через негативні інформаційні впливи.

Правовою основою Стратегії є Конституція України, закони України, Стратегія національної безпеки України, затверджена Указом Президента України від 14.09.2020 р. № 392, а також міжнародні договори, згода на обов'язковість яких надана Верховною Радою України. Питання кібербезпеки деталізуються у Стратегії кібербезпеки України, затвердженій Указом Президента України від 26.08.2021 р. № 447.

Стратегія класифікує загрози інформаційній безпеці України на глобальні та національні. До глобальних загроз віднесено зростання масштабів дезінформаційних кампаній, інформаційну політику держави-агресора, вплив соціальних мереж як суб'єктів формування інформаційного простору, а також недостатній рівень медіаграмотності населення в умовах стрімкого розвитку цифрових технологій. Серед національних викликів і загроз визначено інформаційний вплив держави-агресора на населення України, інформаційне домінування на тимчасово окупованих територіях, обмежені можливості реагування на дезінформаційні кампанії, несформованість системи стратегічних комунікацій, а також недосконалість правового регулювання інформаційної діяльності та захисту професійної діяльності журналістів.

Конституція України (ст. 17) прирівнює забезпечення інформаційної безпеки до найважливіших функцій держави поряд із захистом суверенітету та територіальної цілісності. Законодавство про інформаційну безпеку є складовою системи інформаційного законодавства України та регулює суспільні відносини у сфері захисту інформаційних ресурсів, інформаційної інфраструктури та інформаційних прав людини.

Розвиток національного законодавства у сфері інформаційної безпеки розпочався з прийняттям у 1994 році Закону України «Про захист інформації в інформаційно-телекомунікаційних системах». Водночас сам термін «інформаційна безпека» був нормативно закріплений пізніше - Указом Президента України від 23.04.2008 р. № 377/2008, яким введено в дію рішення Ради національної безпеки і оборони України щодо невідкладних заходів забезпечення інформаційної безпеки держави. Як зазначає І. Валюшко, з 2014 року законодавча база України у сфері інформаційної безпеки зазнала суттєвого розширення. Умовно її можна поділити на дві групи. Перша охоплює концептуальні документи - доктрини та стратегії, які визначають загальні напрями державної політики та основні загрози інформаційній безпеці. Друга група включає нормативно-правові акти, спрямовані на протидію інформаційній агресії, зокрема закони України, укази Президента та рішення РНБО, що обмежують або забороняють поширення контенту держави-агресора на радіо, телебаченні та в мережі Інтернет.

Важливу роль у забезпеченні інформаційної безпеки України відіграли нормативні акти, спрямовані на обмеження інформаційного впливу держави-агресора. Зокрема, Закон України від 29.03.2016 р. «Про внесення змін до статті 15 Закону України “Про кінематографію”» заборонив демонстрацію фільмів, знятих після 2013 року в державі-агресорі або таких, що популяризують її органи влади. Аналогічну спрямованість має Закон України від 06.10.2016 р. «Про внесення змін до Закону України “Про телебачення і радіомовлення”», яким уточнено умови розповсюдження програм телерадіоорганізацій у складі універсальної програмної послуги.

Список використаних джерел:

1. Бєляков К. І. Інформація в праві : теорія і практика : монографія. Київ : КВІЦ, 2006. 116 с.

2. Ковалів М. В., Єсімов С. С., Ярема О. Г. Інформаційне право : навч. посіб. Львів : ЛьвДУВС, 2016. 280 с.

3. Хахановський В., Корнейко О. Актуальні питання інформаційного права : навч. посіб. Київ : Право, 2024. 148 с.

4. Про інформацію : Закон України від 02.10.1992 № 2657-XII. Дата оновлення: 14.06.2025. URL: https://zakon.rada.gov.ua/laws/show/2657-12 (дата звернення: 19.12.2025).

5. Цивільний кодекс України : Закон України від 16.01.2003 № 435-IV. *Відомості Верховної Ради України*. 2003. № 40-44. Ст. 356.

6. ДСТУ ISO/IEC 2382:2022. Інформаційні технології. Словник термінів. Київ : Держстандарт України, 2022. 540 с.

7. Орлюк О., Заярний О. Інформаційне право України : підручник. Київ : КНЕУ, 2025. 312 с.

8. Конституція України : офіц. текст. Київ : КМ, 2013. 96 с.

9. Положення про організацію системи внутрішнього контролю в банках України та банківських групах : Постанова Правління Національного банку України від 02.07.2019 № 88. URL: https://zakon.rada.gov.ua/laws/show/v0088500-19 (дата звернення: 19.12.2025).

10. Положення про вимоги до системи управління кредитною спілкою : Постанова Правління Національного банку України від 02.02.2024 № 15. Дата оновлення: 01.09.2025. URL: https://zakon.rada.gov.ua/laws/show/v0015500-24 (дата звернення: 10.12.2025).

11. Положення про захист інформації та кіберзахист у платіжних системах : Постанова Правління Національного банку України від 19.05.2021 № 43. Дата оновлення: 01.08.2022. URL: https://zakon.rada.gov.ua/laws/show/v0043500-21 (дата звернення: 19.12.2025).

12. Порядок проведення незалежного аудиту інформаційної безпеки на об’єктах критичної інфраструктури : Постанова Кабінету Міністрів України від 24.03.2023 № 257. URL: https://zakon.rada.gov.ua/laws/show/257-2023 (дата звернення: 19.12.2025).

13. Стратегія національної безпеки України : Указ Президента України від 14.09.2020 № 392/2020. URL: https://www.president.gov.ua/documents/3922020-35037 (дата звернення: 19.12.2025).

14. Стратегія кібербезпеки України : Указ Президента України від 26.08.2021 № 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013 (дата звернення: 19.12.2025).

15. Стратегія інформаційної безпеки України : Указ Президента України від 28.12.2021 № 685/2021. URL: https://www.president.gov.ua/documents/6852021-41069 (дата звернення: 19.12.2025).

16. Валюшко І. О. Правове забезпечення інформаційної безпеки України в умовах гібридної війни. *Юридичний науковий електронний журнал*. 2019. № 6. С. 133 - 135.

17. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI. URL: https://zakon.rada.gov.ua/laws/show/2939-17 (дата звернення: 19.12.2025).

Питання для обговорення:

1. Інформація як соціально-правова категорія: еволюція наукових підходів до її розуміння.
2. Співвідношення понять «дані», «відомості», «знання» та «інформація» у праві.
3. Інформаційні відносини: поняття, ознаки, суб'єкти та об'єкти.
4. Інформаційна сфера та інформаційне середовище: зміст і структура.
5. Інформаційні ресурси як стратегічний ресурс суспільства і держави.
6. Поняття, предмет і методи інформаційного права як комплексної галузі права.
7. Система інформаційного права України: загальна та особлива частини.
8. Класифікація інформації за законодавством України: значення для правового регулювання.
9. Інформаційна безпека як складова національної безпеки України.
10. Актуальні загрози інформаційній безпеці та правові механізми їх нейтралізації.

Тестові завдання:

1. *Інформація відповідно до Закону України «Про інформацію» - це:*

а) знання, отримані в результаті наукових досліджень;

б) будь-які відомості та/або дані, що можуть бути збережені на матеріальних носіях або відображені в електронному вигляді;

в) лише документована інформація;

г) повідомлення, що мають економічну цінність.

2. *Який підхід розглядає інформацію як результат аналітико-синтетичної обробки даних суб'єктом?*

а) системний;

б) когнітивний;

в) праксіологічний;

г) теоретико-множинний.

3. *Яка з наведених ознак НЕ є характерною для інформації як ресурсу?*

а) невичерпність;

б) зношуваність у процесі використання;

в) можливість багаторазового використання;

г) здатність до трансформації.

4. *Інформаційна безпека України відповідно до Стратегії інформаційної безпеки є*:

а) окремою галуззю права;

б) складовою національної безпеки України;

в) різновидом державної таємниці;

г) формою публічної інформації.

5. *До інформації з обмеженим доступом належить:*

а) екологічна інформація;

б) статистична інформація;

в) критична технологічна інформація;

г) інформація довідково-енциклопедичного характеру.

✍Практичні завдання:

1. Проаналізуйте норми Закону України «Про інформацію».

Визначте: хто є суб'єктами інформаційних відносин (хто створює, отримує, поширює або використовує інформацію); об'єкти інформаційних відносин (що є предметом правового регулювання); види інформаційної діяльності (створення, поширення, використання, захист інформації).

Результати оформіть у формі таблиці, наведіть конкретні практичні приклади.

Приклад заповненої таблиці

Параметр	Визначення за Законом України «Про інформацію»	Приклади в університеті
Суб'єкти інформаційних відносин	Фізичні особи, юридичні особи, органи державної влади та місцевого самоврядування, об'єднання громадян	Студенти, викладачі, адміністрація університету, Міністерство освіти України
Об'єкт інформаційних відносин	Будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або в електронному вигляді	Персональні дані студентів та викладачів, оцінки, наукові публікації, статистика відвідуваності, внутрішні накази та звіти
Види інформаційної діяльності	1. Створення інформації - формування нових відомостей 2. Поширення інформації - передача інформації іншим суб'єктам 3. Використання інформації - застосування інформації для досягнення цілей 4. Захист інформації - запобігання незаконному доступу, зміні або знищенню інформації	1. Створення електронних журналів оцінок студентів, наукових звітів 2. Публікація розкладу занять на веб-сайті, розсилка офіційних повідомлень студентам 3. Використання статистики для підготовки звітів університету та МОН

Параметр	Визначення за Законом України «Про інформацію»	Приклади в університеті
		4. Захист бази даних студентів паролями та шифруванням, обмеження доступу до внутрішніх документів

2. На прикладі будь-якої інформаційної системи (ЄДР, реєстр судових рішень, електронний кабінет платника податків) визначте суб’єктів, об’єкт та зміст інформаційних правовідносин.

3. Складіть порівняльну таблицю видів інформації за змістом відповідно до Закону України «Про інформацію» та визначте особливості їх правового режиму.

4. Проаналізуйте одну з сучасних загроз інформаційній безпеці (дезінформація, кібератаки, витік персональних даних) та визначте, які норми інформаційного законодавства України спрямовані на її нейтралізацію.

5. Визначте місце інформаційного права в системі права України та обґрунтуйте його комплексний характер із наведенням прикладів використання методів різних галузей права. *Результати оформлюються письмо у формі таблиц*і.

Рекомендована література:

1. Конституція України : офіц. текст. Київ : КМ, 2013. 96 с.
2. Про інформацію : Закон України від 02.10.1992 № 2657-XII. Дата оновлення : 14.06.2025. URL: https://zakon.rada.gov.ua/laws/show/2657-12.
3. Стратегія інформаційної безпеки України : Указ Президента України від 28.12.2021 № 685/2021. URL: https://www.president.gov.ua/documents/6852021-41069 (дата звернення: 19.12.2025).
4. ДСТУ ISO/IEC 2382:2022. Інформаційні технології. Словник термінів. Київ : Держстандарт України, 2022. 540 с.
5. Бєляков К. І. Інформація в праві: теорія і практика : монографія. Київ : КВІЦ, 2006. 116 с.
6. Ковалів М. В., Єсімов С. С., Ярема О. Г. Інформаційне право : навч. посіб. Львів : ЛьвДУВС, 2016. 280 с.
7. Хахановський В., Корнейко О. Актуальні питання інформаційного права : навч. посіб. Київ : Право, 2024. 148 с.

ТЕМА 2.
ПРАВОВЕ РЕГУЛЮВАННЯ ДОСТУПУ ДО ІНФОРМАЦІЇ. ЗАХИСТ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

План

1. Правове регулювання доступу до інформації.
2. Державні електронні інформаційні ресурси.
3. Офіційні веб-сайти органів державної влади та органів місцевого самоврядування: механізми доступу до публічної інформації.
4. Інформація з обмеженим доступом: види, правові засади захисту.
5. Особливості правового регулювання режиму секретності. Поняття та правовий режим державної таємниці.

Мета: систематизувати знання з питань змісту та структури інформаційних правовідносин, видів інформації та правових режимів доступу до неї; ознайомити з інституційними та законодавчими механізмами захисту публічної інформації, державної таємниці та службової інформації; охарактеризувати основні проблеми, що виникають у процесі забезпечення доступу до інформації та дотримання режиму секретності; ознайомити з міжнародними та національними стандартами у сфері обмеження доступу до інформації і захисту національної безпеки.

Перелік ключових термінів і понять з теми: баланс публічного та приватного інтересу; публічні електронні реєстри; доступ до інформації; державні інформаційні ресурси; інформаційні обмеження; інформаційна безпека; збирання, використання, поширення, обіг інформації; звернення, заява, скарга; публічна інформація; відкрита інформація, інформація з обмеженим доступом, конфіденційна, таємна, службова інформація.

1. Правове регулювання доступу до інформації.

Відповідно до статті 34 Конституції України кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб - на свій вибір [1]. Це положення є фундаментальною конституційною гарантією реалізації свободи інформації та визначає загальні межі інформаційної свободи особи в демократичному суспільстві. Конституційний зміст права на інформацію був предметом офіційного тлумачення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України. У пункті 4 мотивувальної частини Рішення Суд

зазначив, що зазначеним конституційним положенням відповідають приписи Цивільного кодексу України, якими встановлено, що фізична особа має право вільно збирати, зберігати, використовувати і поширювати інформацію (абзац перший частини першої статті 302 ЦК України) [2].

Конституційне та цивільно-правове регулювання права особи на інформацію узгоджується з міжнародно-правовими стандартами у сфері прав людини. Так, відповідно до пункту 2 статті 19 Міжнародного пакту про громадянські і політичні права 1966 року, кожна людина має право на вільне вираження свого погляду; це право включає свободу шукати, одержувати і поширювати будь-яку інформацію та ідеї незалежно від державних кордонів, усно, письмово чи за допомогою друку або художніх форм вираження чи іншими способами на свій вибір.

Однією з ключових гарантій реалізації конституційних прав на вільне збирання, зберігання, використання і поширення інформації є законодавче закріплення права кожного на доступ до інформації. Відповідно до статті 5 Закону України «Про доступ до публічної інформації», таке право забезпечується шляхом:

– систематичного та оперативного оприлюднення інформації в офіційних друкованих виданнях;

– розміщення інформації на офіційних веб-сайтах у мережі Інтернет;

– оприлюднення інформації на інформаційних стендах;

– надання інформації на запити;

– використання будь-яких інших способів, що не суперечать законодавству.

Разом з тим частина третя статті 34 Конституції України встановлює, що здійснення прав на вільне збирання, зберігання, використання і поширення інформації може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку, з метою запобігання заворушенням чи злочинам, для охорони здоров’я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя.

Таке конституційне обмеження узгоджується з пунктом 2 статті 29 Загальної декларації прав людини 1948 року, відповідно до якого при здійсненні своїх прав і свобод кожна людина повинна зазнавати лише таких обмежень, які встановлені законом виключно з метою забезпечення належного визнання і поваги прав і свобод інших осіб та забезпечення справедливих вимог моралі, громадського порядку і загального добробуту в демократичному суспільстві. Ст. 3 Конвенції Ради Європи про доступ до офіційних документів також визначає, що право доступу до офіційних документів все ж може обмежуватися державою.

Але такі обмеження повинні бути чітко встановлені у законі, та мають бути необхідними у демократичному суспільстві і бути пропорційними цілям захисту: національної безпеки, оборони та міжнародних відносин; громадської безпеки; попередження, розслідування та судового переслідування кримінальної діяльності; дисциплінарного розслідування; перевірки, контролю та нагляду з боку державних органів; приватного життя та інших законних приватних інтересів; комерційних та інших економічних інтересів; економічної, монетарної політики і політики обмінного курсу держави; рівності сторін у судовому провадженні та ефективного здійснення правосуддя; навколишнього середовища; обговорень всередині державного органу або між такими органами стосовно вивчення питання.

Таким чином, *Конституція України визначає вичерпний перелік підстав*, за наявності яких законами України може передбачатися обмеження прав особи на вільне збирання, зберігання, використання і поширення інформації. Це положення конкретизується в абзаці другому статті 5 Закону України «Про інформацію»**,** відповідно до якого реалізація права на інформацію не повинна порушувати громадські, політичні, економічні, соціальні, духовні, екологічні та інші права, свободи і законні інтереси інших громадян, а також права та інтереси юридичних осіб. Право на інформацію, закріплене Конституцією України, деталізується у спеціальному законодавстві, зокрема в Законах України «Про звернення громадян»**,** «Про інформацію»**,** «Про доступ до публічної інформації» та інших нормативно-правових актах.

Ст. 5 Закону України «Про інформацію» встановлює, що кожен має право на інформацію, яке передбачає можливість її вільного одержання, використання, поширення, зберігання та захисту, необхідних для реалізації своїх прав, свобод і законних інтересів [3]. Водночас Закон підкреслює, що реалізація цього права не повинна порушувати права інших осіб. Закон України «Про інформацію» також закріплює основні принципи інформаційних відносин **(**ст. 2**),** до яких належать: гарантованість права на інформацію; відкритість і доступність інформації; свобода обміну інформацією; достовірність і повнота інформації; свобода вираження поглядів і переконань; правомірність одержання, використання, поширення, зберігання та захисту інформації; захищеність особи від втручання в її особисте та сімейне життя. Відповідно до ст. 7 Закону право на інформацію охороняється законом, а держава гарантує всім суб’єктам інформаційних відносин рівні права і можливості доступу до інформації. Ніхто не може обмежувати права особи у виборі форм і джерел одержання інформації, за винятком випадків, прямо передбачених законом. Крім того, суб’єкт інформаційних відносин має право вимагати усунення будь-яких порушень свого права на інформацію.

Види інформації за порядком доступу (режимом доступу). Відповідно до ст. 20 Закону України «Про інформацію» за порядком доступу інформація

поділяється на *відкриту інформацію* та *інформацію з обмеженим доступом*. При цьому законодавець закріплює презумпцію відкритості інформації, відповідно до якої будь-яка інформація є відкритою, крім тієї, що віднесена законом до інформації з обмеженим доступом.

2. Державні електроні інформаційні ресурси.

Термін *«ресурси»* (від франц. *ressource* - «допоміжні засоби») традиційно розуміється як запаси, джерела або можливості, які можуть бути використані в разі потреби. Стратегія розвитку інформаційного суспільства в Україні, затверджена Розпорядженням Кабінету Міністрів України від 15.05.2013 р. № 386-р, визначає *інформаційний ресурс* як систематизовану інформацію або знання, що мають цінність у певній предметній області та можуть бути використані людиною у своїй діяльності для досягнення визначеної мети.

Уперше на законодавчому рівні поняття «інформаційні ресурси» було закріплено у ст. 1 Закону України від 04.02.1998 р. «Про Національну програму інформатизації», де вони розглядалися як сукупність документів в інформаційних системах (бібліотеках, архівах, банках даних тощо). Чинний Закон України від 01.12.2022 р. № 2807-IX «Про Національну програму інформатизації» істотно розширює та конкретизує це поняття, визначаючи *електронні інформаційні ресурси* як систематизовані відомості і дані, створені, оброблені та збережені в електронній формі за допомогою технічних засобів та/або програмних продуктів.

Аналіз нормативно-правових актів свідчить про поетапну еволюцію змісту поняття *«державні інформаційні ресурси»* та поступове ускладнення його правової конструкції. Так, у березні 2014 року до законодавства України було внесено визначення, відповідно до якого *державні інформаційні ресурси* це інформація, яка перебуває у володінні державних органів, військових формувань, а також інформація, створення якої передбачено законодавством та яка обробляється фізичними або юридичними особами відповідно до наданих їм повноважень суб'єктами владних повноважень [6].

Подальший розвиток цього підходу закріплено у новій редакції Закону України від 09.04.2014 р. № 1194-VII «Про Державну службу спеціального зв'язку та захисту інформації України», де *державні інформаційні ресурси* визначено як систематизовану інформацію, доступну за допомогою інформаційних технологій, право на володіння, використання або розпорядження якою належить державним органам, військовим формуванням, державним підприємствам, установам та організаціям, а також інформацію, створення якої передбачено законодавством і яка обробляється фізичними або юридичними особами в межах наданих їм повноважень.

Як зазначають А. Марущак, С. Петров у дослідженні «Зміст поняття «державні інформаційні ресурси» дослідники питань електронного урядування

виділяють чотири основні групи принципів організації національних електронних інформаційних ресурсів: принципи організації державних е-ІР (для державної служби), принципи організації громадянських е-ІР (для громадян), принципи організації підприємницьких (бізнесу) е-ІР (для юридичних осіб), принципи організації е-ІР для міжнародної спільноти (Інтернетресурси) [4, с. 130].

Перейдемо безпосередньо до розгляду змісту поняття «державні електронні інформаційні ресурси». У 2011 році у Положенні про Реєстр інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління, було внесено зміни, згідно з якими «державні електронні інформаційні ресурси» визначалися як «відображена та задокументована в електронному вигляді інформація, необхідність захисту якої визначено законодавством». Видову характеристику державних ресурсів у системі національних електронних інформаційних ресурсів було закріплено у Положенні про Національний реєстр електронних інформаційних ресурсів, аналізуючи яке виокремлюємо такі види державних електронних інформаційних ресурсів: кадастри, державні та інші обов'язкові класифікатори, а також інформаційні системи, які забезпечують їх функціонування та використовують інформацію з них. Зазначені нормативно-правові акти втратили чинність.

З метою запровадження електронної інформаційної взаємодії Постановою Кабінету Міністрів України від 08.09.2016 р. № 606 (у редакції Постанови КМУ від 10.05.2018 р. № 357) [5] визначено перелік *пріоритетних державних електронних інформаційних ресурсів*, до яких, зокрема, належать:

- Державний земельний кадастр
- Державний реєстр актів цивільного стану громадян
- Державний реєстр виборців
- Державний реєстр загальнообов'язкового державного соціального страхування
- Державний реєстр обтяжень рухомого майна
- Державний реєстр речових прав на нерухоме майно
- Державний реєстр фізичних осіб - платників податків
- Електронна система охорони здоров'я
- Єдина державна електронна база з питань освіти
- Єдина інформаційна система Міністерства внутрішніх справ
- Єдиний державний автоматизований реєстр осіб, які мають право на пільги
- Єдиний державний демографічний реєстр
- Єдиний державний реєстр Міністерства внутрішніх справ стосовно зареєстрованих транспортних засобів та їх власників
- Єдиний державний реєстр судових рішень

– Єдиний державний реєстр юридичних осіб, фізичних осіб - підприємців та громадських формувань

– Єдиний реєстр довіреностей

– Єдиний реєстр документів, що дають право на виконання підготовчих та будівельних робіт і засвідчують прийняття в експлуатацію закінчених будівництвом об’єктів, відомостей про повернення на доопрацювання, відмову у видачі, скасування та анулювання зазначених документів

– Єдиний реєстр об’єктів державної власності

– Реєстр платників податку на додану вартість.

Закон України від 18.11.2021 р. № 1907-IX «Про публічні електронні реєстри» [6] встановлює правові, організаційні та фінансові засади створення і функціонування публічних електронних реєстрів з метою захисту прав і законних інтересів фізичних та юридичних осіб.

Відповідно до ст. 5 цього Закону, об’єктами публічних електронних реєстрів є інформація про

1) фізичних осіб, юридичних осіб та об’єднання фізичних та/або юридичних осіб;

2) землі та земельні ділянки із розташованими на них об’єктами нерухомого майна;

3) окремі спеціальні статуси фізичних осіб та їх об’єднання, юридичних осіб, громадських формувань;

4) події;

5) сертифікати, ліцензії, декларації, повідомлення, дозволи, інші документи дозвільного характеру;

6) природні ресурси;

7) правові режими використання і забудови територій та окремих об’єктів;

8) рухоме майно, що відповідно до закону є об’єктом державного обліку;

9) майнові та немайнові права, їх обмеження та обтяження;

10) нормативно-правові акти, нормативні акти та документи технічного характеру, судові рішення, виконавчі документи, інші документи та їх реквізити, довіреності;

11) об’єкти будівництва та закінчені будівництвом об’єкти;

12) іншу інформацію, визначену цим Законом або іншим актом законодавства, згідно з якими створено відповідні реєстри.

Система реєстрів включає сукупність реєстрів, що функціонують та взаємодіють для створення, зберігання, оброблення та використання інформації під час провадження дозвільної діяльності, надання адміністративних, соціальних та інших публічних послуг, провадження іншої управлінської діяльності та здійснення державного регулювання.

До системи реєстрів належать:

1) базові реєстри;

2) інші реєстри;

3) визначені законом реєстри саморегулівних організацій.

До базових реєстрів належать реєстри, що забезпечують одноразовий збір інформації про об'єкт реєстру (його правовий статус) з метою багаторазового використання як юридично обов'язкової, достовірної та актуальної інформації про такий об'єкт реєстру (його правовий статус) в інших реєстрах та/або національних електронних інформаційних ресурсах під час провадження дозвільної діяльності, наданні адміністративних, соціальних та інших публічних послуг, провадження іншої управлінської діяльності та здійснення державного регулювання, вичерпний перелік яких встановлюється цим Законом.

До базових реєстрів належать:

1) Єдиний державний демографічний реєстр;

2) Єдиний державний реєстр юридичних осіб, фізичних осіб - підприємців та громадських формувань;

3) Державний земельний кадастр;

4) Єдиний державний реєстр транспортних засобів;

5) Реєстр будівель та споруд;

6) Єдиний державний реєстр адрес;

7) Державний реєстр речових прав на нерухоме майно.

До інших реєстрів належать реєстри, держателями яких є органи державної влади, органи місцевого самоврядування, юридичні особи публічного права, визначені законом, та які містять інформацію про окремі спеціальні статуси особи, про сертифікати, ліцензії, декларації, повідомлення, інші документи дозвільного характеру; про природні ресурси; про правові режими використання та забудови територій та окремих об'єктів; про рухоме майно, що відповідно до закону є об'єктом державного обліку; про майнові та немайнові права, їх обмеження та обтяження; про нормативно-правові акти, нормативні акти та документи технічного характеру, судові рішення, виконавчі документи, довіреності та про інші об'єкти, які відповідно до закону є об'єктами державного обліку, але не належать до об'єктів базових державних реєстрів, інші державні інформаційні ресурси.

Національний реєстр електронних інформаційних ресурсів (НРЕІР) – це державний репозитарій, створений для обліку всіх електронних інформаційних ресурсів держави: електронних реєстрів, кадастрів, класифікаторів, а також інформаційних систем, які забезпечують їх функціонування та використовують інформацію з них. Запровадження реєстру покликане нормалізувати перелік інформації у державних базах даних та не допустити створення джерел-дублів первинної інформації про об'єкти державної реєстрації. НРЕІР є невід'ємною складовою системи інтероперабельності країни й забезпечує організаційну

підтримку «Трембіти». Реєстр також має забезпечити електронний процес погодження та отримання доступу до держреєстрів шляхом укладання відповідної е-угоди між постачальником даних, їх отримувачем і тримачем НРЕІР. НРЕІР створений відповідно до Постанови Кабінету міністрів України від 10.05.2018 р. № 357 «Деякі питання організації електронної взаємодії державних електронних інформаційних ресурсів».

Постановою Кабінету Міністрів України від 01.09.2023р. № 969 «Про функціонування Реєстру публічних електронних реєстрів» затверджено порядок ведення Реєстру публічних електронних реєстрів, технічний опис (специфікацію) програмно-апаратних засобів Реєстру публічних електронних реєстрів, перелік класифікаторів, довідників, технічних специфікацій тощо, які є обов'язковими до використання в публічних електронних реєстрах [7], відповідно до якого:

Реєстр реєстрів - державна інформаційно-комунікаційна система, призначена для формування переліку шляхом реєстрації інформації про публічні електронні реєстри, державні та інші обов'язкові для використання класифікатори, довідники, технічні специфікації тощо (далі - класифікатори), а також інформаційно-комунікаційні системи, які забезпечують функціонування публічних електронних реєстрів та/або отримують інформацію з них в порядку електронної інформаційної взаємодії.

Держателем Реєстру реєстрів є Міністерство цифрової трансформації України (далі - Мінцифри). Власником Реєстру реєстрів та виключних майнових прав на його програмне забезпечення є держава в особі Мінцифри. Публічними реєстраторами Реєстру реєстрів є посадові особи або особи, які перебувають у трудових відносинах з держателем Реєстру реєстрів. Створювачами реєстрової інформації Реєстру реєстрів (далі - створювачі) є:

– щодо публічних електронних реєстрів - держателі публічних електронних реєстрів в особі їх керівників або уповноважених осіб, які перебувають у трудових відносинах з держателями публічних електронних реєстрів;

– щодо інформаційно-комунікаційних систем - власники відповідних систем в особі їх керівників або уповноважених ними осіб, які перебувають у трудових відносинах з власниками відповідних систем;

– щодо державних інформаційних ресурсів та електронних інформаційних ресурсів (далі - інформаційні ресурси) - власники інформаційних ресурсів в особі їх керівників або уповноважених ними осіб, які перебувають у трудових відносинах з власниками інформаційних ресурсів.

Об'єктами Реєстру реєстрів є інформація про:

1) публічні електронні реєстри;

2) публічні електронні реєстри, інформаційно-комунікаційні системи яких ще не створені;

3) інформаційно-комунікаційні системи, які забезпечують функціонування та/або отримують інформацію з публічних електронних реєстрів у порядку електронної інформаційної взаємодії;

4) інформаційні ресурси;

5) державні та інші обов'язкові для використання класифікатори.

На сучасному етапі в Україні нараховується близько 350 реєстрів. Обмін даними між ними здійснюється з 2019 року через систему «Трембіта».

3. Офіційні веб-сайти органів державної влади та органів місцевого самоврядування: механізми доступу до публічної інформації.

Призначенням офіційного веб-сайту органу державної влади або органу місцевого самоврядування є поширення публічної інформації. Веб-сайт є найбільш ефективним та оперативним способом надання інформації за допомогою мережі Інтернет. На сучасному етапі розвитку інформаційного суспільства уявити собі орган державної влади чи орган місцевого самоврядування, який не має власного офіційного веб-сайту, практично неможливо. Відповідно до міжнародних зобов'язань України, принципів демократичного врядування та положень Конституції України, держава зобов'язана забезпечити доведення до відома громадян інформації про діяльність органів публічної влади з метою гарантування їх участі в управлінні державними справами. Саме з цією метою прийнято низку нормативно-правових актів, які регулюють питання створення, функціонування та інформаційного наповнення офіційних веб-сайтів, насамперед органів виконавчої влади.

Своєчасна, оперативна, повна та достовірна інформація, що надається публічними органами через їхні офіційні веб-сайти, є запорукою ефективної взаємодії громадян з органами державної влади та органами місцевого самоврядування, а також важливим інструментом вирішення актуальних суспільно значущих питань.

Формування правових засад функціонування офіційних веб-сайтів органів державної влади розпочалося з прийняттям Указів Президента України: від 31 липня 2000 р. № 928 «Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні»; від 17 травня 2001 р. № 325 «Про підготовку пропозицій щодо забезпечення гласності та відкритості діяльності органів державної влади».

З метою реалізації зазначених указів, поліпшення умов для розвитку демократії, забезпечення гласності та відкритості діяльності органів виконавчої влади Постановою Кабінету Міністрів України від 4 січня 2002 р. № 31 (у редакції постанови КМУ від 13.09.2024 р. № 1066) затверджено Порядок оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади.

Зазначеним Порядком встановлено, що оприлюднення інформації у мережі Інтернет здійснюється з метою: підвищення ефективності та прозорості діяльності органів виконавчої влади; впровадження сучасних інформаційних технологій у діяльність органів публічної влади; надання інформаційних та інших послуг громадськості; забезпечення впливу громадськості на процеси, що відбуваються у державі. Оприлюднення інформації здійснюється шляхом розміщення та постійного оновлення інформації на офіційних веб-сайтах (веб-порталах) відповідно до вимог Закону України «Про доступ до публічної інформації» та зазначеного Порядку.

Відповідно до Порядку, на офіційному веб-сайті (веб-порталі) міністерства чи іншого центрального органу виконавчої влади розміщується, зокрема, така інформація:

– найменування органу;
– основні завдання та нормативно-правові засади діяльності;
– структура та керівництво органу;
– прізвища, імена та по батькові керівників;
– місцезнаходження апарату та територіальних органів;
– основні функції структурних підрозділів і контактні дані їх керівників;
– нормативно-правові акти з питань компетенції органу;
– плани підготовки проєктів регуляторних актів та звіти про їх результативність;
– відомості про регуляторну діяльність;
– перелік і порядок надання адміністративних послуг;
– інформація про взаємодію з громадськими радами;
– відомості про проведення консультацій з громадськістю;
– зразки документів для звернення громадян;
– розпорядок роботи та графік прийому керівництва;
– підприємства, установи та організації сфери управління;
– цільові програми;
– відомості про публічні закупівлі;
– державні інформаційні ресурси з питань компетенції органу;
– поточні та заплановані заходи;
– відомості про вакансії.

На офіційному веб-сайті обов’язково розміщується адреса електронної пошти структурного підрозділу, відповідального за приймання та реєстрацію вхідної кореспонденції. Не допускається розміщення інформації, поширення якої заборонено законодавством, а також реклами (крім соціальної), у тому числі політичної реклами.

Інформація на офіційних веб-сайтах органів виконавчої влади подається українською мовою, а за потреби - англійською мовою та мовами національних

меншин. Обсяг інформації, що підлягає перекладу, визначається відповідним органом виконавчої влади.

Офіційні веб-сайти повинні бути доступними для осіб з порушеннями зору, слуху, опорно-рухового апарату, мовлення та інтелектуального розвитку, а також для осіб з комбінованими порушеннями. Технічні завдання на створення або модернізацію веб-сайтів мають відповідати вимогам, установленим у додатку до Порядку та постанові Кабінету Міністрів України від 21.07.2023 р. № 757 «Деякі питання доступності інформаційно-комунікаційних систем та документів в електронній формі».

Функціонування офіційних веб-сайтів органів державної влади здійснюється відповідно до положень про них, що затверджуються керівниками відповідних публічних органів.

У 2025 році в межах проєкту «Цифрові, інклюзивні, доступні: підтримка цифровізації державних послуг в Україні» [8] проведено моніторинг базової веб-доступності 100 веб-сайтів органів державної влади, зокрема веб-ресурсів Кабінету Міністрів України, Президента України, Верховної Ради України, міністерств, центральних органів виконавчої влади, державних електронних сервісів та реєстрів, зокрема:

1. https://www.kmu.gov.ua/ Сайт Кабінету Міністрів
2. https://www.president. gov.ua/ Офіційне інтернет представництво Президента України
3. https://www.rada.gov.ua/ Офіційний веб портал Верховної ради України
4. https://ssu.gov.ua/ Сайт Служби безпеки України
5. https://bank.gov.ua/ Сайт Національного банку України
6. https://minagro.gov.ua Міністерство аграрної політики та продовольства
7. https://mev.gov.ua Міністерство енергетики України.
8. https://minre.gov.ua/ Міністерство з питань реінтеграції тимчасово окупованих територій
9. https://mms.gov.ua/ Міністерство молоді та спорту України
10. https://thedigital.gov.ua/ Міністерство цифрової трансформації України
11. https://www.me.gov.ua/ Міністерство економіки України
12. http://mvs.gov.ua/ Міністерство внутрішніх справ України
13. https://mepr.gov.ua/ Міністерство захисту довкілля та природних ресурсів України
14. https://mfa.gov.ua/ Міністерство закордонних справ України
15. https://mtu.gov.ua/ Міністерство розвитку громад, територій та інфраструктури України

16. https://mkip.gov.ua/ Міністерство культури та інформаційної політики України
17. https://www.mil.gov.ua/ Міністерство оборони України
18. https://mon.gov.ua/ua Міністерство освіти і науки України
19. https://moz.gov.ua/ Міністерство охорони здоров'я України
20. https://dsp.gov.ua/ Державна служба України з питань праці
21. https://www.msp.gov.ua/ Міністерство соціальної політики України
22. https://mva.gov.ua/ Міністерство у справах ветеранів України
23. https://mof.gov.ua/uk Міністерство фінансів України
24. https://minjust.gov.ua/ Міністерство юстиції України
25. https://mspu.gov.ua Міністерство з питань стратегічних галузей промисловості України
26. https://id.gov.ua/ Інтегрована система електронної ідентифікації
27. https://data.gov.ua/ Єдиний державний вебпортал відкритих даних
28. https://diia.gov.ua Загальнодержавний сервіс Дія.
29. https://osvita.diia.gov.ua Дія. Освіта
30. https://business.diia.gov. ua Дія.Бізнес
31. https://court.gov.ua/fair/ Пошук судових справ
32. https://guide.diia.gov.ua/ Гід з державних послуг
33. https://center.diia.gov.ua/ Дія.Центр
34. https://city.diia.gov.ua/ Дія.City
35. https://e.land.gov.ua/ services Вебресурс електронних послуг Держгеокадастру
36. https://cabinet.tax.gov.ua/ Електроний кабінет платника податків ДПС
37. https://asvpweb.minjust. gov.ua/#/search-debtors Пошук виконавчих проваджень
38. https://portal.pfu.gov.ua/ sidebar/Templates/Default Портал електронних послуг ПФУ
39. https://rezerv.gov.ua/ Державне агентство резерву України
40. https://policy.mtsbu.ua/ Перевірка чинності страхового полісу ОСАГО
41. https://corruptinfo.nazk. gov.ua/ Єдиний державний реєстр осіб, які вчинили корупційні або пов’язані з корупцією правопорушення
42. https://legalaid.gov.ua/ Безоплатна правнича допомога
43. https://fiu.gov.ua Державний фінмоніторинг
44. https://e-services.davr. gov.ua Портал електронних послуг, Державне агентство водних ресурсів України
45. https://e-services.msp. gov.ua/ Призначення допомоги при народженні дитини

46. https://wanted.mvs.gov. ua/passport/ Перевірка паспорта в базі викрадених або втрачених
47. https://dmsu.gov.ua/ services/online.html Запис до електронної черги онлайн
48. https://bf.diia.gov.ua/ Дія.Безбар'єрність
49. https://www.spfu.gov.ua/ Фонд державного майна України
50. https://dpsu.gov.ua/ua/ map Інтерактивна мапа пунктів пропуску/КПВВ
51. https://lms.e-school.net. ua/ Всеукраїнська школа онлайн
52. https://registry.edbo.gov. ua/ Реєстр суб'єктів освітньої діяльності
53. https://e-services.dsns. gov.ua/ Портал електронних послуг ДСНС
54. https://nszu.gov.ua/ Національна служба здоров'я України
55. https://spending.gov.ua/ login Єдиний вебпортал використання публічних коштів
56. https://acskidd.gov.ua/ manage-certificates Повторне (дистанційне) формування сертифікатів за електронним запитом
57. https://czo.gov.ua/verify Онлайн сервіс перевірки кваліфікованого електронного підпису чи печатки для електронних документів
58. https://nads.gov.ua/ Національне агентство України з питань державної служби
59. https://info.edbo.gov.ua/ edu-documents/ Реєстр документів про освіту
60. https://dsns.gov.ua/ ДСНС
61. https://id.court.gov.ua/ Електронний суд
62. https://online.minjust.gov. ua/dokumenty/choise Онлайн будинок юстиції
63. https://wanted.mvs.gov. ua/searchtransport/ Транспортні засоби у розшуку
64. https://petition.president. gov.ua/ Електронні петиції, представництво Президента України
65. https://itd.rada.gov.ua/ services/Account/LogOn? returnUrl=%2Fservices %2FPetition%2FCreate Електронні сервіси ВРУ
66. http://www.drlz.com.ua/ Реєстр лікарських засобів
67. https://nabu.gov.ua/ Національне антикорупційне бюро України
68. https://reyestr.court.gov. ua/ Єдиний державний реєстр судових рішень
69. https://ek-cbi.msp.gov.ua/ Електронний кабінет особи з інвалідністю
70. https://www.npu.gov.ua/ Національна поліція України
71. https://ern.minjust.gov. ua/pages/default.aspx Єдиний реєстр нотаріусів
72. https://apostille.minjust. gov.ua/ Єдиний реєстр апостилів
73. https://pasport.org.ua/ services Послуги Центрів «Паспортний сервіс»

74. https://e-construction. gov.ua/ Портал державної електронної системи у сфері будівництва

75. https://usr.minjust.gov.ua/ content/free-search Єдиний державний реєстр юридичних осіб, фізичних осіб-підприємців та громадських формувань (безкоштовний пошук).

76. https://grants.vzaemo. diia.gov.ua Простір електронних конкурсів.

Також було здійснено аналіз веб-доступності офіційних веб-сайтів обласних державних адміністрацій та підготовлено аналітичний звіт із визначенням основних недоліків, що потребують усунення.

Для прикладу зупинимося на аналізі веб-сайту Верховної Ради України. Так, Розпорядженням Голови Верховної Ради України від 31.01.2022 р. № 21 «Про деякі питання функціонування офіційного веб-сайту та інших веб-ресурсів Верховної Ради України» [9] затверджено:

1) Положення про офіційний веб-сайт та інші веб-ресурси Верховної Ради України;

2) Структуру інформації на головній сторінці офіційного веб-сайту Верховної Ради України ;

3) Технологічну схему інформаційного наповнення веб-ресурсів Верховної Ради України

Положення про офіційний сайт та інші веб-ресурси Верховної Ради України визначає статус офіційного веб-сайту та інших веб-ресурсів Верховної Ради України як інформаційного ресурсу, що забезпечує діяльність електронного парламенту.

Веб-ресурси Верховної Ради України - сукупність програмних, інформаційних та медійних засобів, логічно пов'язаних між собою, що розміщені на серверах Верховної Ради України. До веб-ресурсів Верховної Ради України належать офіційний веб-сайт Верховної Ради України, веб-сайти і веб-сторінки органів Верховної Ради України та структурних підрозділів Апарату Верховної Ради України, бази даних, пошукові системи та інші сервіси Верховної Ради України (які працюють окремо та як складові офіційного веб-сайту Верховної Ради України, у тому числі через прикладний програмний інтерфейс у форматі відкритих даних). Головна сторінка офіційного веб-сайту Верховної Ради України - сторінка офіційного веб-сайту Верховної Ради України, що першочергово відкривається за адресою www.rada.gov.ua.

Офіційний веб-сайт Верховної Ради України - головний веб-ресурс Верховної Ради України, призначений для інтеграції даних про роботу Верховної Ради України, що складається з головної сторінки офіційного веб-сайту Верховної Ради України, веб-сайтів і веб-сторінок органів Верховної Ради України, структурних підрозділів Апарату Верховної Ради України, сторінок баз даних, пошукових систем та інших сервісів Верховної Ради України і працює на спільних програмно-апаратних засобах для забезпечення функціонування

електронного парламенту. Публічна інформація, розміщена на офіційному веб-сайті та інших веб-ресурсах Верховної Ради України, є офіційним джерелом інформації.

4. Інформація з обмеженим доступом: види, правові засади захисту.

Згідно зі ст. 21 Закону України «Про інформацію», *до інформації з обмеженим доступом належать* конфіденційна, таємна та службова інформація**.**

Конфіденційною інформацією є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, а також інформація, визнана конфіденційною на підставі закону (ч.2 ст. 21 Закону України «Про інформацію»). Конфіденційна інформація може поширюватися лише за згодою відповідної особи або в інших випадках, передбачених законом. *Конфіденційна інформація була предметом офіційного тлумачення Конституційного Суду України, зокрема:*

Медична інформація, тобто свідчення про стан здоров'я людини, історію її хвороби, про мету запропонованих досліджень і лікувальних заходів, прогноз можливого розвитку захворювання, в тому числі і про наявність ризику для життя і здоров'я, за своїм правовим режимом належить до конфіденційної, тобто інформації з обмеженим доступом. Лікар зобов'язаний на вимогу пацієнта, членів його сім'ї або законних представників надати їм таку інформацію повністю і в доступній формі.

В особливих випадках, як і передбачає частина третя статті 39 Основ законодавства України про охорону здоров'я, коли повна інформація може завдати шкоди здоров'ю пацієнта, лікар може її обмежити. У цьому разі він інформує членів сім'ї або законного представника пацієнта, враховуючи особисті інтереси хворого. Таким же чином лікар діє, коли пацієнт перебуває у непритомному стані.

У випадках відмови у наданні або навмисного приховування медичної інформації від пацієнта, членів його сім'ї або законного представника вони можуть оскаржити дії чи бездіяльність лікаря безпосередньо до суду або, за власним вибором, до медичного закладу чи органу охорони здоров'я.

Правила використання відомостей, що стосуються лікарської таємниці - інформації про пацієнта, на відміну від медичної інформації - інформації для пацієнта, встановлюються статтею 40 Основ законодавства України про охорону здоров'я та частиною третьою статті 46 Закону України "Про інформацію" *(пункт 2 резолютивної частини) Рішення Конституційного Суду України у справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України "Про інформацію" та статті 12 Закону України "Про прокуратуру" (справа К.Г. Устименка) від 30 жовтня 1997 року* № 5-зп/1997).

Вирішуючи питання ***щодо конфіденційності інформації про особу, яка займає посаду, пов'язану зі здійсненням функцій держави або органів місцевого самоврядування***, та членів її сім'ї, Конституційний Суд України виходить з такого, що належність інформації про фізичну особу до конфіденційної визначається в кожному конкретному випадку. Перебування особи на посаді, пов'язаній зі здійсненням функцій держави або органів місцевого самоврядування, передбачає не тільки гарантії захисту прав цієї особи, а й додаткові правові обтяження. Публічний характер як самих органів – суб'єктів владних повноважень, так і їх посадових осіб вимагає оприлюднення певної інформації для формування громадської думки про довіру до влади та підтримку її авторитету у суспільстві *(абзац перший підпункту 3.3 пункту 3 мотивувальної частини) Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України від 20 січня 2012 року* № 2-рп/2012**.**

Аналізуючи питання щодо ***поширення інформації про сімейне життя особи, яка займає посаду, пов'язану зі здійсненням функцій держави або органів місцевого самоврядування,*** Конституційний Суд України враховує, що така інформація зазвичай стосується не лише цієї особи, а й інших осіб, зокрема членів її сім'ї, яким Конституція України теж гарантує право на невтручання в їх особисте і сімейне життя, крім випадків, визначених законом. Тому поширення даних про таких фізичних осіб – членів сім'ї, що можуть стати відомими в результаті поширення інформації про саму посадову особу, крім випадків, визначених законом, може призвести до порушення їх конституційних прав, зашкодити гідності, честі, діловій репутації тощо. Застереження щодо недопущення порушення конституційних прав членів сімей посадових осіб Конституційний Суд України висловив у Рішенні від 6 жовтня 2010 року № 21-рп/2010.

Таким чином, Конституційний Суд України, даючи офіційне тлумачення частин першої, другої статті 32 Конституції України, вважає, що ***інформація про особисте та сімейне життя особи (персональні дані про неї)*** - це будь-які відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована, а саме: національність, освіта, сімейний стан, релігійні переконання, стан здоров'я, матеріальний стан, адреса, дата і місце народження, місце проживання та перебування тощо, дані про особисті майнові та немайнові відносини цієї особи з іншими особами, зокрема членами сім'ї, а також відомості про події та явища, що відбувалися або відбуваються у побутовому, інтимному, товариському, професійному, діловому та інших сферах життя особи, за винятком даних стосовно виконання повноважень особою, яка займає посаду, пов'язану зі здійсненням функцій держави або органів місцевого

самоврядування. Така інформація про фізичну особу та членів її сім'ї є конфіденційною і може бути поширена тільки за їх згодою, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини *(абзаци четвертий, п'ятий підпункту 3.3 пункту 3 мотивувальної частини) Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України від 20 січня 2012 року* № 2-рп/2012**.**

Положення частини другої статті 32 Основного Закону України передбачають ***вичерпні підстави можливого правомірного втручання в особисте та сімейне життя особи*** (в тому числі й тієї, яка займає посаду, пов'язану з функціями держави або органів місцевого самоврядування, та членів її сім'ї). Такими підставами є: згода особи на збирання, зберігання, використання та поширення конфіденційної інформації стосовно неї, а також, у разі відсутності такої згоди, випадки, визначені законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини. Даючи офіційне тлумачення положень частин першої, другої статті 32 Конституції України у системному зв'язку з частиною другою статті 34 цієї Конституції, Конституційний Суд України дійшов висновку, що збирання, зберігання, використання та поширення державою, органами місцевого самоврядування, юридичними або фізичними особами конфіденційної інформації про особу без її згоди є втручанням в її особисте та сімейне життя, яке допускається винятково у визначених законом випадках і лише в інтересах національної безпеки, економічного добробуту та прав людини *(абзаци третій, четвертий пункту 5 мотивувальної частини) Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України від 20 січня 2012 року № 2-рп/2012***.**

В Україні заборонена цензура (частина третя статті 15 Конституції України). Під цензурою слід розуміти контроль з боку інститутів публічної влади за змістом та розповсюдженням інформації з метою захисту інформаційного простору, тобто прямі або опосередковані дії держави, спрямовані на обмеження чи навіть заборону поширення інформації, яку вона вважає шкідливою чи не потрібною для суспільства *(абзац третій підпункту 2.1 пункту 2 мотивувальної частини) Рішення Конституційного Суду України (Перший сенат) у справі за конституційною скаргою Плескача В'ячеслава Юрійовича щодо відповідності Конституції України (конституційності) положень другого речення частини четвертої статті 42 Закону України „Про Конституційний Суд України" від 22 січня 2020 року № 1-р(I)/2020***.**

Таким чином, ***право особи на доступ до інформації, гарантоване статтею 34 Конституції України, не є абсолютним і може підлягати обмеженням***. Такі обмеження мають бути винятками, які передбачені законом, переслідувати одну або декілька законних цілей і бути необхідними у демократичному суспільстві. У разі обмеження права на доступ до інформації законодавець зобов'язаний запровадити таке правове регулювання, яке дасть можливість оптимально досягти легітимної мети з мінімальним втручанням у реалізацію вказаного права і не порушувати сутнісного змісту такого права *(абзац восьмий підпункту 2.2 пункту 2 мотивувальної частини).Рішення Конституційного Суду України (Перший сенат) у справі за конституційною скаргою Плескача В'ячеслава Юрійовича щодо відповідності Конституції України (конституційності) положень другого речення частини четвертої статті 42 Закону України „Про Конституційний Суд України" від 22 січня 2020 року* № 1-р(I)/2020**.**

Таємна інформація - це інформація, доступ до якої обмежується відповідно до ч. 2 ст.6 Закону, розголошення якої може завдати шкоди особі, суспільству і державі. Таємною визнається інформація, яка містить державну, професійну, банківську, розвідувальну таємницю, таємницю досудового розслідування та іншу передбачену законом таємницю (ст. 8 Закону України «Про доступ до публічної інформації»).

Закон України від 21.01.1994 р.№ 3855- XII «Про державну таємницю» регулює суспільні відносини, пов'язані з віднесенням інформації до державної таємниці, засекречуванням, розсекречуванням її матеріальних носіїв та охороною державної таємниці з метою захисту національної безпеки України. Цим законом визначено термін ***державна таємниця (секретна інформація)*** - вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому цим Законом, державною таємницею і підлягають охороні державою.

До таємниць, пов'язаних із професійною діяльністю належать:

– ***адвокатська таємниця*** - будь-яка інформація, що стала відома адвокату, помічнику адвоката, стажисту адвоката, особі, яка перебуває у трудових відносинах з адвокатом, про клієнта, а також питання, з яких клієнт (особа, якій відмовлено в укладенні договору про надання правової допомоги з передбачених Законом України «Про адвокатуру та адвокатську діяльність» підстав) звертався до адвоката, адвокатського бюро, адвокатського об'єднання, *зміст* порад, консультацій, роз'яснень адвоката, складені ним документи, інформація, що зберігається на електронних носіях, та інші документи і відомості, одержані адвокатом під час здійснення адвокатської діяльності (ст. 22 Закону України «Про адвокатуру та адвокатську діяльність»);

– ***банківська таємниця*** - інформація щодо діяльності та фінансового стану клієнта, яка стала відомою банку в процесі обслуговування клієнта та взаємовідносин з ним чи третім особам під час надання послуг банку (ст. 60 Закону України «Про банки і банківську діяльність»);

– ***військова таємниця*** - відомості військового характеру, предмети, документи або матеріали, що містять відомості військового характеру, які становлять державну таємницю (ст. 422 Кримінального кодексу України);

– ***журналістська таємниця*** - журналіст має право на збереження таємниці авторства та джерел інформації, за винятком випадків, коли ці таємниці обнародуються на вимогу суду (п. 11 ст. 26 Закону України «Про друковані засоби масової інформації (пресу) в Україні»);

– ***комерційна таємниця*** - інформація, яка є секретною в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить, у зв'язку з цим має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію. Комерційною таємницею можуть бути відомості технічного, організаційного, комерційного, виробничого та іншого характеру, за винятком тих, які відповідно до закону не можуть бути віднесені до комерційної таємниці (ст. 505 Цивільного кодексу України);

– ***лікарська таємниця*** - медичні працівники та інші особи, яким у зв'язку з виконанням професійних або службових обов'язків стало відомо про хворобу, медичне обстеження, огляд та їх результати, інтимну і сімейну сторони життя громадянина, не мають права розголошувати ці відомості, крім передбачених законодавчими актами випадків. Під час використання інформації, що становить лікарську таємницю, в навчальному процесі, науково-дослідній роботі, у тому числі у випадках її публікації у спеціальній літературі, повинна бути забезпечена анонімність пацієнта (ст. 40 Закону України «Основи законодавства України про охорону здоров'я»);

– ***нотаріальна таємниця*** - сукупність відомостей, отриманих під час вчинення нотаріальної дії або звернення до нотаріуса заінтересованої особи, в тому числі про особу, її майно, особисті майнові та немайнові права і обов'язки тощо (ст. 8 Закону України «Про нотаріат»).

- ***розвідувальна таємниця*** - вид таємної інформації, що охоплює відомості та дані, отримані або створені розвідувальними органами України під час виконання покладених на ці органи завдань та здійснення функцій, визначених Законом України «Про розвідку», розголошення яких може завдати шкоди функціонуванню розвідки і доступ до яких обмежено відповідно до Закону України «Про розвідку» в інтересах національної безпеки України (ст. 1 Закону України «Про розвідку»);

- ***завдання сертифікаційної роботи зовнішнього незалежного оцінювання*** належить до інформації з обмеженим доступом з моменту створення набору завдань сертифікаційної роботи зовнішнього незалежного оцінювання та до моменту його санкціонованого використання особами, що проходять зовнішнє незалежне оцінювання. У разі потреби спеціально уповноважена державою установа (організація) може відносити зміст завдань сертифікаційної роботи до інформації з обмеженим доступом на більш тривалий період часу (п. 8 ст. 45 Закону України «Про вищу освіту»);
- ***таємниця досудового розслідування*** – відомості досудового розслідування можна розголошувати лише з письмового дозволу слідчого або прокурора і в тому обсязі, в якому вони визнають можливим. Слідчий, прокурор попереджає осіб, яким стали відомі відомості досудового розслідування, у зв'язку з участю в ньому, про їх обов'язок не розголошувати такі відомості без його дозволу (ст. 222 Кримінального процесуального кодексу України (далі – КПК України);
- ***таємниця наради суддів*** - під час ухвалення вироку ніхто не має права перебувати в нарадчій кімнаті (нарадча кімната - приміщення, спеціально призначене для ухвалення судових рішень), крім складу суду, який здійснює судовий розгляд. Суд наділено правом перервати нараду лише для відпочинку з настанням нічного часу. Під час перерви судді не можуть спілкуватися з особами, які брали участь у кримінальному провадженні. Судді не мають права розголошувати хід обговорення та ухвалення вироку в нарадчій кімнаті (ст. 367 КПК України);
- ***таємниця нарадчої кімнати*** - під час ухвалення судового рішення ніхто не має права перебувати в нарадчій кімнаті, крім складу суду, який розглядає справу. Під час перебування в нарадчій кімнаті суддя не має права розглядати інші судові справи. Судді не мають права розголошувати хід обговорення та ухвалення рішення у нарадчій кімнаті (ст. 245 Цивільного процесуального кодексу України, ст. 228 Кодексу адміністративного судочинства України);
- ***таємниця сповіді*** – кожному громадянину в Україні гарантується право на свободу совісті, ніхто не має права вимагати від священнослужителів відомостей, одержаних ними під час сповіді віруючих (ст. 3 Закону України «Про свободу совісті та релігійні організації»);
- ***таємниця усиновлення*** - особа має право на таємницю перебування на обліку тих, хто бажає усиновити дитину, пошуку дитини для усиновлення, подання заяви про усиновлення та її розгляду, рішення суду про усиновлення. Дитина, яка усиновлена, має право на таємницю, в тому числі і від неї самої, факту її усиновлення (ст. 226 Сімейного кодексу України).

Службова інформація, згідно зі ст. 9 Закону України «Про доступ до публічної інформації»**,** включає інформацію, що міститься у внутрівідомчій

службовій кореспонденції суб’єктів владних повноважень, а також інформацію, зібрану в процесі оперативно-розшукової, контррозвідувальної діяльності та у сфері оборони держави, яка не віднесена до державної таємниці. Перелік відомостей, що становлять службову інформацію, який складається органами державної влади, органами місцевого самоврядування, іншими суб'єктами владних повноважень, у тому числі на виконання делегованих повноважень, не може бути обмеженим у доступі.

5. Особливості правового регулювання режиму секретності. Поняття та правовий режим державної таємниці.

Згідно зі ст. 1 Закону України «Про державну таємницю», *режим секретності* - це встановлений відповідно до вимог цього Закону та інших виданих на його виконання нормативно-правових актів єдиний порядок забезпечення охорони державної таємниці [10].

Під *віднесенням інформації до державної таємниці* слід розуміти визначену законом процедуру прийняття рішення державним експертом з питань таємниць щодо віднесення категорії відомостей або окремих відомостей до державної таємниці із встановленням відповідного ступеня їх секретності. Таке рішення ґрунтується на обґрунтуванні та визначенні можливої шкоди національній безпеці України у разі розголошення цих відомостей, передбачає включення відповідної інформації до *Зводу відомостей, що становлять державну таємницю*, та офіційне опублікування цього Зводу.

У зв’язку з цим *гриф секретності* є обов’язковим реквізитом матеріального носія секретної інформації, який засвідчує ступінь її секретності та визначає особливий порядок доступу, використання, зберігання і захисту такої інформації.

Охорона державної таємниці являє собою комплекс організаційно-правових, інженерно-технічних, криптографічних та оперативно-розшукових заходів, спрямованих на запобігання розголошенню секретної інформації, несанкціонованому доступу до неї, а також втратам її матеріальних носіїв.

Правове регулювання питань, пов’язаних із державною таємницею та дотриманням режиму таємності, здійснюється не лише Законом України «Про державну таємницю», а й низкою спеціальних нормативно-правових актів, зокрема: Законом України від 25.03.1992 р. № 2229-XII «Про Службу безпеки України», Законом України від 18.02.1992 р. № 2135-XII «Про оперативно-розшукову діяльність», Законом України від 02.07.2015 р. № 580-VIII «Про Національну поліцію», Законом України від 15.03.2018 р. № 2337-VIII «Про Дисциплінарний статут Національної поліції України» та іншими нормативно-правовими актами. Відповідно до ст. 8 Закону України «Про державну таємницю», *до державної таємниці у встановленому законом порядку може бути віднесена інформація* у таких сферах:

1. у сфері оборони;
2. у сфері економіки, науки і техніки;
3. у сфері зовнішніх відносин;
4. у сфері державної безпеки та охорони правопорядку.

Конкретні відомості можуть бути віднесені до державної таємниці за ступенями секретності «*особливої важливості», «цілком таємно» та «таємно»* лише за умови, що їх розголошення завдаватиме шкоди інтересам національної безпеки України. При цьому законодавством прямо забороняється віднесення до державної таємниці будь-яких відомостей, якщо це призводить до звуження змісту й обсягу конституційних прав і свобод людини і громадянина або створює загрозу життю, здоров'ю та безпеці населення.

Не належить до державної таємниці інформація:

- про стан довкілля, якість харчових продуктів і предметів побуту, а також про вплив товарів (робіт, послуг) на життя та здоров'я людини;
- про аварії, катастрофи, небезпечні природні явища та інші надзвичайні події, які сталися або можуть статися і загрожують безпеці громадян;
- про стан здоров'я населення, його життєвий рівень, включаючи харчування, одяг, житло, медичне обслуговування та соціальне забезпечення, а також соціально-демографічні показники, стан правопорядку, освіти і культури;
- про факти порушень прав і свобод людини і громадянина;
- про незаконні дії органів державної влади, органів місцевого самоврядування, їх посадових і службових осіб;
- інша інформація, доступ до якої відповідно до законів України та міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України, не може бути обмежений.

Строк дії рішення про віднесення інформації до державної таємниці встановлюється державним експертом з питань таємниць з урахуванням ступеня секретності інформації, критерії визначення якого встановлюються Службою безпеки України, а також інших обставин. При цьому такий строк не може перевищувати:

– для інформації зі ступенем секретності «особливої важливості» - 30 років;

– для інформації зі ступенем секретності «цілком таємно» - 10 років;

– для інформації зі ступенем секретності «таємно» - 5 років.

Після закінчення зазначеного строку державний експерт з питань таємниць приймає рішення про скасування рішення щодо віднесення інформації до державної таємниці або про продовження строку його дії в межах строків, установлених для відповідного ступеня секретності.

Отже, *ключовим критерієм належності інформації до державної таємниці є потенційна шкода, яка може бути завдана національній безпеці*

держави у разі її розголошення. Це свідчить не лише про особливу цінність такої інформації, а й про функціональне призначення інституту державної таємниці як складової системи забезпечення національної безпеки. У доктринальних дослідженнях домінує позиція, відповідно до якої предметом державної таємниці є інформація, засекречування якої зумовлене її винятковою значущістю для державних інтересів. Така інформація охоплює оборонну, економічну, науково-технічну, зовнішньополітичну, безпекову та правоохоронну сфери, а її правовий режим передбачає спеціальну процедуру засекречування, врегульований порядок допуску та доступу, облік, зберігання і використання, а також систему юридичних гарантій захисту, у тому числі засобами кримінально-правового впливу.

Використана література:

1. Конституція України : офіц. текст. Київ : КМ, 2013. 96 с.
2. Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України від 22.11.2006 № 12-рп/2006. URL: https://zakon.rada.gov.ua/laws/show/v012p606-06#Text (дата звернення: 26.12.2025).
3. Про інформацію : Закон України від 02.10.1992 № 2657-XII. Дата оновлення : 14.06.2025. URL: https://zakon.rada.gov.ua/laws/show/2657-12 (дата звернення: 26.12.2025).
4. Приймак Ю. Розвиток електронного урядування в Україні: організація національних електронних інформаційних ресурсів. URL: http://visnyk.academy.gov.ua/wp-content-/upload/2013/11/2011-4-18.pdf (дата звернення: 26.12.2025).
5. Про затвердження Порядку ведення та використання реєстрів : Постанова Кабінету Міністрів України від 08.09.2016 № 606. URL: https://zakon.rada.gov.ua/laws/show/606-2016-%D0%BF (дата звернення: 26.12.2025).
6. Про публічні електронні реєстри : Закон України від 18.11.2021 № 1907-IX. URL: https://zakon.rada.gov.ua/laws/show/1907-20 (дата звернення: 26.12.2025).
7. Про функціонування Реєстру публічних електронних реєстрів : Постанова Кабінету Міністрів України від 01.09.2023 № 969. URL: https://zakon.rada.gov.ua/laws/show/969-2023-%D0%BF (дата звернення: 26.12.2025).
8. Вебдоступність сайтів державних органів влади : Звіт за результатами моніторингу UNDP. URL:

https://www.undp.org/sites/g/files/zskgke326/files/2025-03/undp-ua-basic_web_accessibility_of_100_websites-2024.pdf (дата звернення: 26.12.2025).

9. Про деякі питання функціонування офіційного веб-сайту та інших веб-ресурсів Верховної Ради України : Розпорядження Голови Верховної Ради України від 31.01.2022 № 21. URL: https://zakon.rada.gov.ua/laws/show/21/22-%D1%80%D0%B3 (дата звернення: 26.12.2025).

10. Про державну таємницю : Закон України від 21.01.1994 № 3855-XII. URL: https://zakon.rada.gov.ua/laws/show/3855-12 (дата звернення: 26.12.2025).

Питання для обговорення:

1. Основи правового регулювання доступу до публічної інформації в Україні. Принципи прозорості та відкритості державних електронних інформаційних ресурсів: як забезпечується доступ громадян до даних.
2. Офіційні веб-сайти органів державної влади та місцевого самоврядування: механізми доступу, стандарти вебдоступності, цифрові сервіси.
3. Види інформації з обмеженим доступом.
4. Особливості правового режиму державної таємниці: порядок засекречування, класифікація ступенів секретності, строки дії рішень, правові наслідки порушень.
5. Практичні проблеми реалізації права на інформацію: обмеження доступу, конфлікт між публічністю та захистом державних інтересів.
6. Використання принципу пропорційності при обмеженні доступу до інформації: критерії оцінки законності та обґрунтованості обмежень.
7. Цифрові виклики та загрози інформаційній безпеці: кіберзлочини, несанкціонований доступ до державних електронних ресурсів, витоки даних.
8. Кейси з порушення доступу до публічної інформації та розголошення державної таємниці: аналіз реальних ситуацій і правові наслідки.
9. Перспективи розвитку законодавства про доступ до інформації та захист інформації з обмеженим доступом: роль міжнародних стандартів і цифровізації.

Тестові завдання:

1. *Який принцип є базовим для інформаційного законодавства України?*

а) принцип абсолютної секретності;

б) принцип вільного доступу до будь-якої інформації;

в) принцип відкритості інформації з можливістю її законного обмеження;

г) принцип пріоритету інтересів держави над правами людини.

2. *Який критерій є визначальним для віднесення інформації до інформації з обмеженим доступом?*

а) форма фіксації інформації;
б) суб’єкт, який володіє інформацією;
в) наявність законних підстав та шкоди від розголошення;
г) спосіб поширення інформації.

3. *До якого виду інформації з обмеженим доступом належить інформація, що міститься у внутрішніх документах органів влади, пов’язаних з процесом підготовки рішень*?
а) конфіденційної;
б) службової;
в) таємної;
г) персональних даних.

4. *Яка інформація відповідно до закону не може бути обмежена в доступі незалежно від сфери її походження?*
а) інформація про оборонні закупівлі;
б) інформація про стан довкілля;
в) інформація у сфері зовнішніх відносин;
г) інформація оперативно-розшукової діяльності.

5. *Ключовим критерієм віднесення інформації до державної таємниці є:*
а) рішення керівника органу влади;
б) рівень суспільного інтересу;
в) потенційна шкода національній безпеці у разі розголошення;
г) наявність грифа секретності.

✍Практичні завдання:

1. Проаналізуйте офіційний веб-сайт органу державної влади або органу місцевого самоврядування (за вибором). Визначте, які розділи веб-сайту містять публічну інформацію. З’ясуйте, чи передбачено механізм подання запиту на публічну інформацію. Оцініть повноту та доступність оприлюдненої інформації. *Форма виконання: аналітична таблиця з такими графами*: назва розділу веб-сайту - вид інформації - нормативне обґрунтування - висновок щодо доступності.

2. Керівник структурного підрозділу органу виконавчої влади присвоїв документу гриф «таємно», мотивуючи це тим, що документ містить внутрішню аналітичну інформацію щодо підготовки управлінського рішення. Визначте, чи може така інформація бути віднесена до державної таємниці. Відмежуйте державну таємницю від службової інформації. Оцініть правомірність дій посадової особи. *Форма виконання: письмовий правовий висновок (до 1 сторінки).*

3. Внутрішній ІТ-документ органу влади з описом архітектури кіберзахисту був позначений як службова інформація. Після кібератаки громадська організація вимагає його оприлюднення, посилаючись на суспільний інтерес. Відмежуйте службову інформацію від таємної. *Оцініть пропорційність обмеження доступу.*

4. Орган виконавчої влади відмовив у доступі до екологічного звіту, посилаючись на те, що документ містить відомості про об'єкти критичної інфраструктури і має гриф «таємно». Згодом з'ясувалося, що рішення про засекречування приймалося не державним експертом з питань таємниць. Оцініть юридичну чинність рішення про засекречування. Визначте правові наслідки для органу влади. Обґрунтуйте алгоритм відновлення доступу до інформації. *Форма виконання: письмовий правовий висновок із блок-схемою процедури*.

5. Журналіст онлайн-видання звернувся із запитом на публічну інформацію до державного органу щодо структури витрат бюджетних коштів на забезпечення функціонування захищених інформаційно-телекомунікаційних систем органу влади за попередній рік. У відповіді на запит орган влади відмовив у наданні інформації, зазначивши, що: запитувані відомості містяться у внутрішніх аналітичних звітах, які мають гриф «Для службового користування»; оприлюднення структури витрат може дозволити встановити архітектуру та вразливості інформаційних систем; частина відповідної інформації використовується у документах, віднесених до державної таємниці у сфері державної безпеки. Водночас на офіційному веб-сайті органу влади у розділі «Використання бюджетних коштів» оприлюднені загальні суми фінансування без деталізації, а рішення державного експерта з питань таємниць щодо віднесення запитуваної інформації до державної таємниці не оприлюднювалося і до відповіді на запит додано не було. Журналіст оскаржує відмову, посилаючись на принцип відкритості бюджетної інформації, суспільний інтерес та право на доступ до інформації. *Визначте правову природу запитуваної інформації та віднесіть її до відповідного виду інформації. Проаналізуйте правомірність застосування грифу «Для службового користування» у наведеній ситуації. Оцініть, чи може інформація про використання бюджетних коштів бути віднесена до державної таємниці. Визначте правові механізми захисту права журналіста на доступ до інформації.*

Рекомендована література:

1. Конституція України : офіц. текст. Київ : КМ, 2013. 96 с.
2. Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої

статті 34 Конституції України від 22.11.2006 № 12-рп/2006. URL: https://zakon.rada.gov.ua/laws/show/v012p606-06#Text (дата звернення: 12.12.2025).

3. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI. URL: https://zakon.rada.gov.ua/laws/show/2939-17 (дата звернення: 12.12.2025).

4. Про інформацію : Закон України від 02.10.1992 № 2657-XII. Дата оновлення: 14.06.2025. URL: https://zakon.rada.gov.ua/laws/show/2657-1 (дата звернення: 12.12.2025).

5. Про затвердження Порядку ведення та використання реєстрів : Постанова Кабінету Міністрів України від 08.09.2016 № 606. URL: https://zakon.rada.gov.ua/laws/show/606-2016-%D0%BF (дата звернення: 12.12.2025).

6. Про Національну програму інформатизації : Закон України від 01.12.2022 № 2807-IX. URL: https://zakon.rada.gov.ua/laws/card/2807-20 (дата звернення: 12.12.2025).

7. Про публічні електронні реєстри : Закон України від 18.11.2021 № 1907-IX. URL: https://zakon.rada.gov.ua/laws/show/1907-20 (дата звернення: 26.12.2025).

8. Про функціонування Реєстру публічних електронних реєстрів : Постанова Кабінету Міністрів України від 01.09.2023 № 969. URL: https://zakon.rada.gov.ua/laws/show/969-2023-%D0%BF (дата звернення: 26.12.2025).

9. Вебдоступність сайтів державних органів влади : Звіт за результатами моніторингу UNDP. URL: https://www.undp.org/sites/g/files/zskgke326/files/2025-03/undp-ua-basic_web_accessibility_of_100_websites-2024.pdf (дата звернення: 26.12.2025).

10. Про державну таємницю : Закон України від 21.01.1994 № 3855-XII. URL: https://zakon.rada.gov.ua/laws/show/3855-12 (дата звернення: 26.12.2025).

ТЕМА 3.
ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ. МІЖНАРОДНИЙ ОБМІН ІНФОРМАЦІЄЮ. АНГЛОМОВНА ПІДГОТОВКА КАДРІВ ПРАВООХОРОННИХ ОРГАНІВ ЯК ОСНОВА ЕФЕКТИВНОЇ КОМУНІКАЦІЇ

План

1. Повноваження правоохоронних органів у сфері забезпечення інформаційної безпеки.
2. Суб’єкти забезпечення інформаційної безпеки в Україні.
3. Кібербезпека як складова інформаційної безпеки держави.
4. Англомовна підготовка кадрів правоохоронних органів у контексті Закону України «Про застосування англійської мови в Україні» як основа ефективного міжнародного обміну інформацією, взаємодії з Інтерполом, Європолом та іншими міжнародними структурами.

Мета: систематизувати знання про правове регулювання доступу до інформації та захисту інформації з обмеженим доступом, основи кібербезпеки в діяльності органів державної влади та місцевого самоврядування, принципи відкритості та прозорості публічної інформації, види інформації та механізми їх правового захисту, а також сформувати практичні навички аналізу законності обмеження доступу до інформації та оцінки ризиків у цифровому середовищі.

Перелік ключових термінів і понять з теми: інформаційна безпека, правоохоронний орган, кібербезпека, інформація, інформаційні технології, персональні дані, суб’єкти забезпечення інформаційної безпеки, повноваження, взаємодія, відповідальність, Національний координаційний центр кібербезпеки, кібербезпека, національна безпека, кібератаки, критична інфраструктура, міжнародне співробітництво, державна політика, цифрові технології, кіберзагрози, кіберзахист, інформаційні системи.

1. Повноваження правоохоронних органів у сфері забезпечення інформаційної безпеки.

Забезпечення інформаційної безпеки є одним із ключових напрямів реалізації функцій сучасної держави та невід’ємною складовою системи національної безпеки. Особлива роль у цій сфері належить правоохоронним органам, які покликані захищати суспільство, державу та особу від протиправних посягань, у тому числі в інформаційному та кіберпросторі. У науковій доктрині інформаційна безпека розглядається як стан захищеності життєво важливих інтересів особи, суспільства і держави в інформаційній сфері.

Так, С. Усик визначає інформаційну безпеку суспільства й держави як ступінь їх захищеності та стійкості основних сфер життєдіяльності (економіки, науки, управління, військової сфери, суспільної свідомості тощо) від деструктивних інформаційних впливів, що загрожують національним інтересам [1, с. 271].

Захист інформації у правовому розумінні охоплює комплекс організаційних, правових, технічних і режимних заходів, спрямованих на:

- забезпечення цілісності, конфіденційності та доступності інформації;
- запобігання несанкціонованому доступу до інформації та її носіїв;
- обмеження незаконного поширення інформації з обмеженим доступом.

Як слушно зазначають С. Лихова та В. Сисоєва, саме правоохоронні органи як складова сектору безпеки і оборони відіграють провідну роль у протидії посяганням на інформаційну безпеку держави [2, с. 103].

Основоположні засади забезпечення інформаційної безпеки закріплено в Конституції України. Зокрема: ч. 1 ст. 17 Конституції України визначає захист інформаційної безпеки як одну з найважливіших функцій держави; ч. 2 ст. 34 Конституції України гарантує право кожного на вільне збирання, зберігання, використання та поширення інформації, водночас допускаючи законні обмеження з метою захисту національної безпеки.

Правовий компонент інформаційної безпеки, за визначенням Ю. Кунєва, полягає в наявності системи правових норм, які регламентують інформаційні відносини та забезпечують охоронну й регулятивну функції держави у сфері інформаційної діяльності [3, с. 98]. У науковій літературі повноваження правоохоронних органів у сфері забезпечення інформаційної безпеки доцільно класифікувати за функціональним критерієм. Таку систематизацію пропонує В. Макарчук [4, с. 325 - 326], зокрема:

Інформаційно-аналітичні. Збір, обробка, аналіз та використання інформації для виконання покладених законом завдань, тобто повноваження щодо створення та використання інформаційних систем. Так, наприклад, відповідно до ст. 24 Закону України «Про Службу безпеки України», СБУ здійснює інформаційно-аналітичну діяльність в інтересах національної безпеки [6]. Національна поліція України відповідно до ст. 23 Закону України «Про Національну поліцію» має право отримувати від органів державної влади, підприємств, установ, організацій та громадян інформацію, необхідну для виконання її повноважень, а також користуватися державними інформаційними базами даних [5]. Державна прикордонна служба України відповідно до законодавства створює та використовує інформаційні системи і банки даних щодо: осіб, які перетнули державний кордон; осіб, яким обмежено право в'їзду або виїзду; викрадених або втрачених документів [7].

Профілактично-запобіжні. Правоохоронні органи здійснюють комплекс заходів, спрямованих на попередження правопорушень у сфері інформаційної та кібербезпеки. Зокрема, СБУ відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» здійснює негласну перевірку готовності об'єктів критичної інфраструктури до кібератак [8].

Протидійно-реагувальні. Служба безпеки України протидіє кіберзлочинності, наслідки якої можуть створити загрозу життєво важливим інтересам держави; розслідує кіберінциденти та кібератаки щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури; забезпечує реагування на кіберінциденти у сфері державної безпеки [8]. Окрім того на неї покладено обов'язок протидіяти проведенню проти України спеціальних інформаційних операцій, спрямованих на підрив конституційного ладу, порушення суверенітету і територіальної цілісності України, загострення суспільно-політичної та соціально-економічної ситуації [9].

Оперативно-технічні. СБУ здійснює технічне регулювання у сфері спеціальних технічних засобів зняття інформації з каналів зв'язку [6], а Державна прикордонна служба має повноваження щодо протидії використанню безпілотних авіаційних систем [7].

Моніторингові - спрямовані на виявлення, фіксацію та обмеження доступу до інформації, поширення якої заборонено законом, а також на застосування санкцій та обмежень у сфері інформаційної та кібербезпеки [8]. *Моніторингові*, які проводяться з метою виявлення, фіксації, обмеження доступу та/або видалення з українського сегмента мережі Інтернет інформації, розміщення якої обмежено або заборонено законом. СБУ у межах компетенції здійснює: моніторинг спеціальними методами і способами вітчизняних та іноземних засобів масової інформації та Інтернету з метою виявлення загроз національній безпеці України в інформаційній сфері; протидію проведенню проти України спеціальних інформаційних операцій, спрямованих на підрив конституційного ладу, порушення суверенітету і територіальної цілісності України, загострення суспільно-політичної та соціально-економічної ситуації. Правоохоронні органи забезпечують проведення аудиту інформаційної безпеки, у тому числі на підпорядкованих об'єктах та об'єктах, що належать до сфери їх управління.

Правообмежуючі - правоохоронні органи мають повноваження щодо обмеження участі у заходах із забезпечення інформаційної безпеки та кібербезпеки будь-яких суб'єктів господарювання, які перебувають під контролем держави, визнані Верховною Радою України державою- агресором, або держав та осіб, стосовно яких діють спеціальні економічні та інші обмежувальні заходи (санкції), прийняті на національному або міжнародному рівні внаслідок агресії щодо України, а також обмеження використання

продукції, технологій та послуг таких суб'єктів для забезпечення технічного та криптографічного захисту державних інформаційних ресурсів, посилення державного контролю в цій сфері.

2. Суб'єкти забезпечення інформаційної безпеки в Україні.

В умовах цифровізації суспільних відносин та триваючої гібридної агресії проти України забезпечення інформаційної безпеки набуває системного, комплексного характеру та здійснюється сукупністю державних органів, об'єднаних у єдину національну систему. Правову основу функціонування цієї системи становлять Закон України «Про національну безпеку України», Закон України «Про основні засади забезпечення кібербезпеки України», а також Стратегія кібербезпеки України. Зазначені нормативно-правові акти визначають засади державної політики у сфері інформаційної та кібербезпеки, коло суб'єктів її забезпечення, їхні повноваження, а також механізми координації та взаємодії.

Національна система кібербезпеки України включає основних суб'єктів, кожен з яких виконує специфічні функції відповідно до своєї компетенції. Діяльність суб'єктів забезпечення інформаційної безпеки регулюється профільним законодавством, яке чітко окреслює межі їхніх повноважень, напрями відповідальності та форми взаємодії між собою.

1. ***Рада національної безпеки і оборони України (РНБО)*** є конституційним координаційним органом з питань національної безпеки і оборони при Президентові України. Ключова роль РНБО у сфері інформаційної безпеки реалізується через діяльність *Національного координаційного центру кібербезпеки (НКЦК),* який є її робочим органом. До основних повноважень НКЦК належать: координація та контроль діяльності всіх суб'єктів сектору безпеки і оборони у сфері кібербезпеки; аналіз стану кіберзахисту державних електронних інформаційних ресурсів та об'єктів критичної інфраструктури; прогнозування кіберзагроз; розроблення пропозицій щодо стратегічного розвитку національної системи кібербезпеки. Діяльність Центру спрямована на синхронізацію зусиль різних органів державної влади на стратегічному рівні та формування єдиної державної політики у сфері протидії кіберзагрозам.

2. ***Державна служба спеціального зв'язку та захисту інформації України*** є центральним органом виконавчої влади спеціального призначення, який забезпечує функціонування та розвиток державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, а також формування та реалізацію державної політики у сферах криптографічного та технічного захисту інформації, кіберзахисту, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку та активної протидії агресії у кіберпросторі. До ключових повноважень цього органу належать:

а) формування та реалізація державної політики у сферах кіберзахисту, криптографічного і технічного захисту інформації;

б) забезпечення функціонування Державного центру кіберзахисту та урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA;

в) проведення державних експертиз та аудитів інформаційної безпеки, зокрема на об'єктах критичної інфраструктури.

3. ***Служба безпеки України (СБУ)*** є головним органом у системі контррозвідувальної діяльності та протидії загрозам державній безпеці в інформаційній сфері. Повноваження СБУ у сфері забезпечення інформаційної безпеки України включають: виявлення, попередження та припинення розвідувально-підривної діяльності іноземних спеціальних служб в інформаційному просторі; боротьбу з такими протиправними діяннями, як кібертероризм та кібершпигунство; розслідування кримінальних правопорушень проти основ національної безпеки, вчинених із використанням комп'ютерних систем, інформаційно-комунікаційних мереж і технологій. Служба безпеки України зосереджує свою діяльність на виявленні та нейтралізації найбільш небезпечних загроз, що походять від іноземних спецслужб, терористичних організацій, кіберзлочинних угрупувань та інших суб'єктів, діяльність яких спрямована на підрив суверенітету, конституційного ладу, обороноздатності та інформаційної безпеки держави.

4. Одним із найбільш чисельних правоохоронних органів у системі забезпечення інформаційної безпеки є ***Національна поліція України***, у структурі якої функціонує спеціалізований підрозділ - *Департамент кіберполіції*. Він відповідно до законодавства України забезпечує реалізацію державної політики у сфері боротьби з кіберзлочинністю, а також організовує та здійснює оперативно-розшукову діяльність. До основних завдань Департаменту кіберполіції належать: участь у формуванні та реалізації державної політики щодо попередження та протидії кримінальним правопорушенням, механізм підготовки, вчинення або приховування яких пов'язаний з використанням електронно-обчислювальних машин, комп'ютерних систем, мереж і телекомунікаційних технологій; надання допомоги іншим підрозділам Національної поліції у виявленні, припиненні та розслідуванні кіберзлочинів.

Департамент кіберполіції Національної поліції України є правоохоронним органом, що спеціалізується на протидії загально кримінальній кіберзлочинності. До першочергових завдань кіберполіції належать:

а) протидія шахрайству з використанням електронно-обчислювальної техніки та несанкціонованому втручанню в роботу комп'ютерних мереж;

б) боротьба з розповсюдженням шкідливого програмного забезпечення, дитячої порнографії в мережі Інтернет та іншими видами кіберзлочинності.

При цьому слід зазначити, що кіберполіція переважно працює з кримінальними правопорушеннями загальнокримінального та інформаційного характеру, а не з політичними чи військовими загрозами.

До інших не менш важливих суб'єктів забезпечення інформаційної безпеки України належать: Міністерство оборони України та Збройні Сили України, які відповідають за кібероборону держави у військовій сфері; розвідувальні органи, що здійснюють кіберрозвідку; Національний банк України, який забезпечує кібербезпеку банківської та фінансової системи. Зважаючи на транснаціональний характер кіберзлочинності, Департамент кіберполіції Національної поліції України активно співпрацює з правоохоронними органами іноземних держав (США, Велика Британія, Франція, Німеччина, Польща, Італія тощо), а також з міжнародними правоохоронними організаціями, зокрема Європолом, Інтерполом, NCFTA та іншими, що є важливою складовою міжнародного обміну інформацією та протидії глобальним кіберзагрозам.

3. **Кібербезпека як складова інформаційної безпеки держави.**

Кібербезпека в сучасних умовах розвитку інформаційного суспільства та глобальної цифровізації є однією з ключових складових інформаційної безпеки держави та невід'ємним елементом системи національної безпеки. Інтенсивне впровадження інформаційно-комунікаційних технологій у сферу державного управління, економіки, фінансових відносин, оборони, енергетики, транспорту, охорони здоров'я та соціальних сервісів зумовлює істотне зростання залежності держави від стабільного та безпечного функціонування кіберпростору. За таких умов порушення роботи інформаційних систем або незаконне втручання в них може мати наслідки, співмірні з традиційними загрозами національній безпеці.

Кіберпростір сьогодні розглядається не лише як технологічне середовище обміну інформацією, а як окрема сфера суспільних відносин, у межах якої реалізуються політичні, економічні, військові та соціальні інтереси держав і недержавних суб'єктів. Саме тому кіберзагрози мають комплексний характер і включають кібератаки на державні інформаційні ресурси, об'єкти критичної інформаційної інфраструктури, фінансові та банківські системи, системи управління технологічними процесами, а також персональні дані громадян. До найбільш небезпечних форм кіберзагроз належать кібершпигунство, кібертероризм, організована кіберзлочинність, дезінформаційні кампанії та використання кіберінструментів у гібридних війнах.

У теоретико-правовому вимірі кібербезпека розглядається як складова інформаційної безпеки, що охоплює систему правових, організаційних, технічних, управлінських і міжнародних заходів, спрямованих на захист інформації, інформаційно-комунікаційних систем та цифрових ресурсів від несанкціонованого доступу, втручання, модифікації, блокування або знищення. На відміну від традиційних підходів, сучасна доктрина підкреслює, що кібербезпека не може обмежуватися виключно технічними засобами захисту, а

повинна інтегруватися у загальну систему державної безпекової політики та правового регулювання.

Проблематика кібербезпеки та її нормативно-правового забезпечення отримала широке висвітлення у вітчизняних і зарубіжних наукових дослідженнях. Теоретико-методологічну основу вивчення даного питання становлять фундаментальні положення інформаційного права, права національної безпеки, адміністративного та міжнародного права. Нормативну основу формують ключові законодавчі акти України, зокрема Закон України «Про основні засади забезпечення кібербезпеки України», Закон України «Про захист інформації в інформаційно-комунікаційних системах», Закон України «Про захист персональних даних», Стратегія кібербезпеки України, а також плани заходів з її реалізації.

Вагомий внесок у формування теоретико-правових засад забезпечення кібербезпеки зроблено у працях вітчизняних науковців, зокрема Б. Кормича, А. Марущака, А. Семенченка, В. Плескача та інших. У цих дослідженнях розкриваються питання правової природи кібербезпеки, механізмів правового регулювання кіберпростору, взаємодії суб'єктів забезпечення інформаційної та кібербезпеки, а також проблеми адаптації національного законодавства до міжнародних стандартів. У сфері державного управління кібербезпекою значну увагу приділено роботам О. Потія, Д. Мялковського та С. Кравченка, які акцентують на необхідності інституційного розвитку, удосконалення системи координації та управління кіберризиками.

Особливе місце у науковій розробці проблематики кібербезпеки посідають дослідження А. Зарубенка та О. Дєгтяря (2025 р.), у яких здійснено комплексний аналіз міжнародних і українських державних механізмів правового регулювання кібербезпеки. Науковці виходять з того, що кібербезпека має розглядатися як складова національної безпеки, яка потребує системного підходу, поєднання нормативно-правового регулювання, інституційної спроможності органів державної влади, належного фінансування та активної міжнародної співпраці. Обґрунтовують доцільність гармонізації національного законодавства з правом Європейського Союзу та міжнародними стандартами у сфері кіберзахисту [13, с. 691-704].

Національна система кібербезпеки України є багаторівневою та комплексною. Вона включає суб'єктів забезпечення кібербезпеки, сукупність правових норм, організаційних структур, технічних і криптографічних засобів, а також управлінські механізми реагування на кіберзагрози. До основних суб'єктів національної системи кібербезпеки належать Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національна поліція України, Міністерство оборони України, Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України та інші уповноважені органи.

Координацію діяльності у сфері кібербезпеки здійснює Державний центр кіберзахисту, який забезпечує функціонування національної команди реагування на комп'ютерні інциденти CERT-UA, проводить аудит кіберзахисту об'єктів критичної інформаційної інфраструктури та бере участь у формуванні політики реагування на кіберінциденти. Подальший розвиток інституційної складової кібербезпеки пов'язаний зі створенням у 2025 році Кіберцентру UA30, який функціонує як сучасна платформа моніторингу, аналізу кіберзагроз, підготовки кадрів та координації взаємодії держави з приватним сектором і громадянським суспільством.

Нормативно-правове забезпечення кібербезпеки України має багаторівневий характер. Центральне місце в цій системі займає Закон України «Про основні засади забезпечення кібербезпеки України», який визначає принципи державної політики у сфері кібербезпеки, суб'єктів національної системи кібербезпеки, механізми координації їх діяльності та напрями захисту критичної інформаційної інфраструктури. Закон встановлює обов'язки державних органів щодо впровадження заходів кіберзахисту, управління ризиками та відновлення функціонування інформаційних систем після інцидентів.

Стратегічні орієнтири державної політики у сфері кібербезпеки визначені Стратегією кібербезпеки України, затвердженою Указом Президента України № 447/2021. У Стратегії кібербезпека визначається одним із пріоритетів національної безпеки, а основними завданнями є формування системи кібероборони, протидія кіберзлочинності, підвищення кіберстійкості держави, розвиток кадрового та науково-технічного потенціалу, а також розширення міжнародного співробітництва. Практичну реалізацію Стратегії забезпечує План заходів на 2025 рік, який конкретизує завдання, строки їх виконання та відповідальних виконавців.

Важливим напрямом розвитку національної системи кібербезпеки є адаптація законодавства України до директив Європейського Союзу NIS та NIS2, які встановлюють підвищені вимоги до захисту критичної інфраструктури, управління кіберризиками та відповідальності операторів ключових послуг. Імплементація цих директив сприяє інтеграції України до європейського безпекового простору та підвищенню рівня довіри до національної системи кіберзахисту. Окрему роль у забезпеченні кібербезпеки відіграє міжнародне співробітництво. Україна активно взаємодіє з Європейським Союзом, НАТО, ENISA, ООН, ОБСЄ та Інтерполом, бере участь у спільних навчаннях, програмах технічної допомоги та обміну інформацією. Такі заходи сприяють підвищенню професійного рівня фахівців, запровадженню сучасних технологій кіберзахисту та формуванню ефективних механізмів реагування на транснаціональні кіберзагрози.

Отже, кібербезпека як складова інформаційної безпеки держави є складним, багатовимірним явищем, що потребує системного правового регулювання, ефективної інституційної моделі та постійного вдосконалення з урахуванням динаміки кіберзагроз. Забезпечення належного рівня кібербезпеки є необхідною умовою захисту національних інтересів, прав і свобод людини, стабільного функціонування державних інститутів та сталого розвитку інформаційного суспільства.

4. Англомовна підготовка кадрів правоохоронних органів у контексті Закону України «Про застосування англійської мови в Україні» як основа ефективного міжнародного обміну інформацією, взаємодії з Інтерполом, Європолом та іншими міжнародними структурами.

У сучасних умовах глобалізації, інтеграції України до європейського правового простору та активної міжнародної співпраці у сфері безпеки і правопорядку зростає потреба у фахівцях, спроможних до вербальної міжнародної комунікації. Англійською мовою як другою загалом володіють 743 555 740 осіб, і їх кількість постійно зростає. У Науково-практичному коментарі Закону України «Про застосування англійської мови в Україні» (2025 р.) за заг. ред. М. Ларкіна наголошується, що сьогодні англійська мова є офіційною де-юре у 58 зі 196 країн світу [14, с. 13]. Вона є однією з шести мов Організації Об'єднаних Націй, а також офіційною мовою Європейського Союзу, Ради Європи, Європейської комісії, Європейської асоціації вільної торгівлі та НАТО.

Наголошуючи на «особливому статусі» англійської мови як світової мови та мови сучасної науки, ділової комунікації, Конституційний Суд у справі за конституційним поданням 51 народного депутата України щодо відповідності Конституції України (конституційності) Закону України «Про забезпечення функціонування української мови як державної» від 14.07.2021 р. № 1-р/2021 у п. 6.3 мотивувальної частини зазначає, що «у нинішньому світі англійська мова відіграє роль глобального посередника в спілкуванні між народами. Такою самою є її роль у спілкуванні між представниками наукових і професійних спільнот» [15].

Англомовна підготовка кадрів у сфері безпеки набуває особливої актуальності в контексті п. 5 ст. 3 Закону України від 04.06.2024 р. «Про застосування англійської мови в Україні» [16], адже активізація професійної мобільності та міжнародної співпраці (зокрема, посилення ефективності взаємодії з міжнародними організаціями такими як Європол, Інтерпол, ОБСЄ, Місія ЄС з реформування сектору цивільної безпеки в Україні тощо), оперативний обмін інформацією, належний рівень обслуговування іноземних громадян, участь у спільних операціях, тренінгах, обмін досвідом на міжнародних конференціях, симпозіумах, нарадах та проходження професійного

навчання за участю іноземних інструкторів, потребує системної модернізації традиційних підходів як до організаційних моделей, так і до фінансово-правового забезпечення такої підготовки, що дозволить підвищити ефективність виконання службових обов'язків та належно представляти інтереси України на міжнародному рівні.

Відповідно до п. 5 ч. 1 ст. 3 ЗУ та «Про застосування англійської мови в Україні» вимога щодо обов'язковості володіння англійською мовою встановлюється до осіб, які претендують на заняття посад поліцейських середнього і вищого складу Національної поліції України, посад начальницького складу інших правоохоронних органів, посад начальницького складу служби цивільного захисту, перелік яких встановлюється Кабінетом Міністрів України (*набирає чинності через чотири роки з дня припинення або скасування воєнного стану в Україні, введеного Указом Президента України «Про введення воєнного стану в Україні» від 24 лютого 2022 року № 64/2022, затвердженим Законом України «Про затвердження Указу Президента України «Про введення воєнного стану в Україні» від 24 лютого 2022 року № 2102-IX*) [16].

Постановою КМУ від 24.12.2024 р. № 1488 затверджено перелік посад поліцейських середнього і вищого складу Національної поліції, посад начальницького складу інших правоохоронних органів, посад начальницького складу служби цивільного захисту, кандидати на зайняття яких зобов'язані володіти англійською мовою (*п. 2 зазначеної Постанови встановлено, що ця постанова набирає чинності через чотири роки з дня припинення або скасування воєнного стану в Україні*) [17]. Слід підкреслити, що зазначеною Постановою затверджено перелік відповідних посад без конкретизації рівня мовленнєвої компетенції володіння англійською мовою, що слід визнати суттєвим недоліком, який потребує усунення (більш виправданим вбачається підхід у Постанові КМУ від 27.12.2024 р. № 1522 при визначенні переліків посад військовослужбовців офіцерського складу, сержантського і старшинського складу, кандидати на зайняття яких з числа військовослужбовців за контрактом зобов'язані володіти англійською мовою, також прийнятою на виконання ЗУ «Про застосування англійської мови в Україні», в якій не лише затверджено перелік відповідних посад, але й передбачено рівень мовленнєвої компетенції) ї. Такий підхід є більш виправданим, з огляду на те, що створює підґрунтя для розробки концепції та практичної реалізації оптимального варіанта організаційно-правового забезпечення англомовної підготовки правоохоронців. Доцільно також звернути увагу на впровадження стимулюючих інструментів - Постанова КМУ від 7 березня 2025 р. № 257 «Про затвердження Порядку встановлення надбавки за володіння англійською мовою деяким категоріям осіб» [19].

Отже, англомовна підготовка правоохоронців професійно орієнтована та спрямована на формування практичних навичок використання мови у службовій діяльності. Йдеться не лише про загальне володіння англійською мовою, а про здатність працювати зі спеціалізованою правовою, кримінологічною та оперативною термінологією, складати службові документи, аналізувати інформаційні повідомлення, звіти та аналітичні матеріали, а також ефективно комунікувати в міжкультурному середовищі. У системі міжнародного обміну інформацією англійська мова відіграє ключову роль у забезпеченні оперативності та точності передавання даних. Недостатній рівень мовної підготовки може призводити до затримок у реагуванні на запити, помилок у тлумаченні інформації, обмеження доступу до міжнародних інформаційних ресурсів і, як наслідок, зниження ефективності правоохоронної діяльності. Важливе значення англомовна підготовка має у сфері інформаційно-аналітичної діяльності правоохоронних органів. Здатність аналізувати англомовні джерела інформації, у тому числі звіти міжнародних організацій, матеріали іноземних правоохоронних органів, судову практику та рекомендації експертних структур, сприяє підвищенню якості управлінських і процесуальних рішень.

Прийняття Закону України «Про застосування англійської мови в Україні» стало імпульсом для оновлення підходів до мовної підготовки кадрів правоохоронних органів у контексті їх професійної діяльності та міжнародної взаємодії [20, с. 366]. Системна модернізація нормативно-правових, організаційних та фінансових механізмів зазначеного процесу, а саме: конкретизація вимог до рівнів англомовної компетентності, інтегрування англомовної підготовки до системи професійної освіти та підвищення кваліфікації, впровадження сучасних освітніх моделей, зокрема на основі концепцій ESP (англійської для спеціальних цілей) з урахуванням специфіки службових обов’язків та реальних потреб правоохоронців у міжнародному комунікативному просторі, впровадження стимулюючих механізмів (надбавок за підтверджений рівень володіння), міжвідомча координація та створення єдиної інформаційно-освітньої платформи для системної підготовки та тестування дозволить забезпечити ефективну англомовну підготовку кадрів у сфері безпеки і правопорядку.

Використана література:

1. Усик С. Дослідження правового механізму забезпечення інформаційної безпеки в умовах надзвичайних ситуацій. *Науковий вісник: державне управління*. 2020. № 4 (6). С. 266-280.

2. Лихова С. Я., Сисоєва В. П. Діяльність правоохоронних органів України у сфері забезпечення інформаційної безпеки. *Наукові праці Київського авіаційного інституту. Сер. : Юридичний вісник.* 2022. № 1(64). С. 102-107.

3. Кунєв Ю. Д. Правове забезпечення інформаційної безпеки як предмет правового дослідження. *Наукові праці Національного авіаційного університету. Сер. : Юридичний вісник.* 2021. № 1(58). С. 95-102.

4. Макарчук В. В. Повноваження правоохоронних органів при реалізації державної політики щодо забезпечення інформаційної безпеки. *Юридичний науковий електронний журнал*. 2022. № 8. С. 324-326.

5. Про затвердження Положення про Національну поліцію : Постанова Кабінету Міністрів України від 28.10.2015 № 877. URL: https://zakon.rada.gov.ua/laws/show/877-2015-п#Text (дата звернення: 26.12.2025).

6. Про Службу безпеки України : Закон України від 25.03.1992 № 2229-XII. URL: https://zakon.rada.gov.ua/laws/show/2229-12#Text (дата звернення: 26.12.2025).

7. Про Державну прикордонну службу України : Закон України від 03.04.2003 № 661-IV. URL: https://zakon.rada.gov.ua/laws/show/661-15#Text (дата звернення: 26.12.2025).

8. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 26.12.2025).

9. 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. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text (дата звернення: 26.12.2025).

10. Про Національний координаційний центр кібербезпеки : Указ Президента України від 07.06.2016 № 242/2016. URL: https://zakon.rada.gov.ua/laws/show/242/2016#Text (дата звернення: 26.12.2025).

11. Про Державну службу спеціального зв'язку та захисту інформації України : Закон України від 23.02.2006 № 3475-IV. URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text6 (дата звернення: 29.12.2025)

12. Насонов М. І. Суб'єкти забезпечення інформаційної безпеки в Україні: повноваження, взаємодія, відповідальність. *Наука і техніка сьогодні*. *Сер. : Право*. 2025. № 8 (49). С. 149-157.

13. Зарубенко А. О., Дєгтяр О. А. Міжнародні та українські державні механізми правового регулювання кібербезпеки. *Успіхи і досягнення у науці.* 2025. № 11 (21). С. 691-704.

14. Закон України «Про застосування англійської мови в Україні»: науково-практичний коментар / В. І. Бояров та ін. ; за заг. ред. М. О. Ларкіна. Київ : Юрінком Інтер, 2025. 164 с.

15. Рішення Конституційного Суду України від 14.07.2021 № 1-р/2021 у справі за конституційним поданням 51 народного депутата України щодо відповідності Конституції України (конституційності) Закону України «Про забезпечення функціонування української мови як державної». URL:

https://zakon.rada.gov.ua/laws/show/v001p710-21#Text (дата звернення: 30.12.2025).

16. Про застосування англійської мови в Україні : Закон України від 04.06.2024 № 3760-IX. URL: https://zakon.rada.gov.ua/laws/show/3760-20#Text (дата звернення: 30.12.2025).

17. Про затвердження переліку посад поліцейських середнього і вищого складу Національної поліції, посад начальницького складу інших правоохоронних органів, посад начальницького складу служби цивільного захисту, кандидати на зайняття яких зобов'язані володіти англійською мовою: Постанова Кабінету Міністрів України від 24.12.2024 № 1488. URL: https://zakon.rada.gov.ua/laws/show/1488-2024-%D0%BF#Text (дата звернення: 30.12.2025).

18. Про переліки посад військовослужбовців офіцерського складу, сержантського і старшинського складу, кандидати на зайняття яких з числа військовослужбовців за контрактом зобов'язані володіти англійською мовою : Постанова Кабінету Міністрів України від 27.12.2024 № 1522. URL: https://www.kmu.gov.ua/npas/pro-pereliky-posad-viiskovosluzhbovtsiv-ofitserskoho-skladu-serzhantskoho-i-starshynskoho-skladu-t271224 (дата звернення: 26.07.2025).

19. Порядок встановлення надбавки за володіння англійською мовою деяким категоріям осіб : Постанова Кабінету Міністрів України від 07.03.2025 № 257. URL: https://zakon.rada.gov.ua/laws/show/257-2025-%D0%BF#Text (дата звернення 09.06.2025).

20. Пирожкова Ю. В., Ларкін М. О. Англомовна підготовка кадрів правоохоронних органів у контексті Закону України «Про застосування англійської мови в Україні»: організаційні моделі та фінансово-правове забезпечення. *Науковий вісник Ужгородського національного університету. Сер. : Право.* 2025. Випуск 90. Ч. 3. С. 360-366.

Питання для обговорення:

1. Особливості правової регламентації діяльності правоохоронних органів у сфері захисту інформації.
2. Роль та функції Національного координаційного центру кібербезпеки у забезпеченні захисту державних інформаційних ресурсів.
3. Повноваження правоохоронних органів щодо запобігання та розслідування кіберзлочинів: від оперативної діяльності до міжнародної співпраці.
4. Види інформаційної діяльності у правоохоронних органах: створення, поширення, використання та захист даних.
5. Особливості роботи з інформацією з обмеженим доступом: класифікація, строки дії рішень, правові наслідки порушень.

6. Практичні проблеми забезпечення кібербезпеки в правоохоронних органах: конфлікт між відкритістю даних та захистом державних інтересів.

7. Використання принципу пропорційності при обмеженні доступу до інформації: критерії оцінки законності та обґрунтованості обмежень.

8. Цифрові загрози інформаційній безпеці: кіберзлочини, несанкціонований доступ до державних електронних ресурсів, витоки даних.

9. Кейси порушень кібербезпеки та несанкціонованого доступу: аналіз реальних ситуацій, правові наслідки.

10. Обговорення організаційних моделей англомовної підготовки кадрів правоохоронних органів (проаналізувати Постанову КМУ від 27.12.2024 № 1522 «Про переліки посад військовослужбовців офіцерського складу, сержантського і старшинського складу, кандидати на зайняття яких з числа військовослужбовців за контрактом зобов'язані володіти англійською мовою»).

Тестові завдання:

Виберіть правильну відповідь з наступних варіантів. Свій вибір обґрунтуйте, посиланням на конкретну юридичну норму.

1. *Який принцип є базовим для інформаційної безпеки в правоохоронних органах?*

а) абсолютна секретність;

б) відкритий доступ до всіх даних;

в) баланс між захистом державних інтересів і доступом до інформації;

г) пріоритет міжнародних стандартів над національними законами.

2**.** *Який критерій визначає віднесення інформації до обмеженого доступу у кібербезпеці?*

а) формат документа;

б) суб'єкт, який володіє інформацією;

в) потенційна шкода національній безпеці у разі розголошення;

г) спосіб поширення інформації.

3**.** *До якого виду інформації належить внутрішня аналітична інформація правоохоронного органу щодо архітектури інформаційних систем?*

а) конфіденційна;

б) службова;

в) таємна;

г) персональні дані.

4. *Яка інформація відповідно до законодавства не може бути розголошена без обмежень?*

а) інформація про стан кіберзахисту критичної інфраструктури;
б) інформація про стан довкілля;
в) статистичні дані щодо злочинності;
г) законопроекти у відкритому доступі.

5. *Ключовим критерієм віднесення інформації до державної таємниці у сфері кібербезпеки є:*
а) рішення керівника органу влади;
б) суспільний інтерес;
в) потенційна шкода національній безпеці у разі розголошення;
г) наявність грифу секретності.

✍Практичні завдання:

1. Проаналізуйте офіційний веб-сайт правоохоронного органу та визначте, які розділи містять публічну інформацію про кіберзахист та безпеку. З'ясуйте наявність механізму подання запитів та оцініть доступність даних. *Форма виконання: аналітична таблиця з графами: назва розділу - вид інформації - нормативне обґрунтування - висновок щодо доступності.*

2. Керівник підрозділу кібербезпеки присвоїв документу гриф «таємно», мотивуючи це тим, що документ містить внутрішню аналітичну інформацію щодо вразливостей інформаційних систем. *Визначте, чи правомірне таке віднесення документа до державної таємниці. Форма виконання: письмовий правовий висновок (до 1 сторінки).*

3. Після кібератаки громадська організація вимагає оприлюднення службового документа, що описує архітектуру захисту інформаційних систем. *Відмежуйте службову інформацію від таємної та оцініть пропорційність обмеження доступу.*

4. Працівник державного органу отримав запит від громадянина щодо внутрішньої статистики ефективності роботи певного підрозділу. Частина інформації містить персональні дані співробітників та службову інформацію, а інша частина - загальні результати діяльності підрозділу. *Складіть правовий висновок щодо того, яку частину інформації можна надати, а яку - обмежити. Визначте правові підстави для обмеження доступу та запропонуйте алгоритм надання частково відкритої інформації.*

5. Виберіть одне або декілька рішень судів у відкритому судовому реєстрі (наприклад, Єдиний державний реєстр судових рішень), які стосуються

доступу до публічної інформації або обмеження доступу до інформації з обмеженим доступом. Проаналізуйте такі аспекти:

- предмет спору та сторони процесу;
- аргументи заявника та відповідача щодо права на інформацію;
- правову кваліфікацію інформації (публічна, службова, таємна, персональні дані);
- висновок суду та його обґрунтування;
- практичні наслідки рішення для забезпечення права на доступ до інформації.

Складіть аналітичну таблицю або звіт із посиланнями на номери рішень, дати та суди, що їх ухвалили. Форма виконання: аналітична таблиця або письмовий звіт (1-2 сторінки).

Рекомендована література:

1. Про національну безпеку : Закон України від 21.06.2018 № 2469-VII. URL: https://zakon.rada.gov.ua/laws/show/2469- 19#Text (дата звернення: 27.10.2024).

2. Про Національну поліцію : Закон України від 02.07. 2015 № 58-VIII. *Відомості Верховної Ради України.* 2015. № 40-41. Ст. 379.

3. Про Службу безпеки України: Закон України від 25.03.1992 № 2229-XII. *Відомості Верховної Ради України.* 1992. № 27. Ст. 382.

4. Про Державну прикордонну службу України : Закон України від 03.04.2003 № 661-IV. URL: https://zakon.rada.gov.ua/laws/show/661-15#Text (дата звернення: 27.10.2024).

5. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 26.12.2025).

5. 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. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text (дата звернення: 26.12.2025).

6. Про Національний координаційний центр кібербезпеки : Указ Президента України від 07.06.2016 № 242/2016. URL: https://zakon.rada.gov.ua/laws/show/242/2016#Text (дата звернення: 26.12.2025).

7. Про Державну службу спеціального зв’язку та захисту інформації України : Закон України від 23.02.2006 № 3475-IV. URL:https://zakon.rada.gov.ua/laws/show/3475-15#Text6 (дата звернення: 29.12.2025).

8. Про переліки посад військовослужбовців офіцерського складу, сержантського і старшинського складу, кандидати на зайняття яких з числа військовослужбовців за контрактом зобов’язані володіти англійською мовою :

Постанова Кабінету Міністрів України від 27.12.2024 № 1522. URL: https://www.kmu.gov.ua/npas/pro-pereliky-posad-viiskovosluzhbovtsiv-ofitserskoho-skladu-serzhantskoho-i-starshynskoho-skladu-t271224 (дата звернення: 27.10.2024).

9. Порядок встановлення надбавки за володіння англійською мовою деяким категоріям осіб : Постанова Кабінету Міністрів України від 07.03.2025 № 257. URL: https://zakon.rada.gov.ua/laws/show/257-2025-%D0%BF#Text (дата звернення: 27.10.2024).

10. Закон України «Про застосування англійської мови в Україні»: науково-практичний коментар / Бояров В. І., Ларкін М., Легких К. В., Лобода Ю. А., Макаренков О. Л., Пирожкова Ю. В. ; за заг. ред. М. О. Ларкіна. Київ : Юрінком Інтер, 2025. 164 с.

11. Зарубенко А. О., Дєгтяр О. А. Міжнародні та українські державні механізми правового регулювання кібербезпеки. *Успіхи і досягнення у науці.* 2025. № 11 (21). С. 691-704.

12. Насонов М. І. Суб’єкти забезпечення інформаційної безпеки в Україні: повноваження, взаємодія, відповідальність. *Наука і техніка сьогодні*. *Сер. : Право*. 2025. № 8 (49). С. 149-157.

13. Пирожкова Ю. В., Ларкін М. О. Англомовна підготовка кадрів правоохоронних органів у контексті Закону України «Про застосування англійської мови в Україні»: організаційні моделі та фінансово-правове забезпечення. *Науковий вісник Ужгородського національного університету. Сер. : Право*. 2025. Випуск 90. Ч. 3. С. 360-366.

ТЕМА 4.
ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ

План

1. Інформаційне забезпечення правоохоронної діяльності: поняття, елементи, принципи.
2. Джерела інформаційно-аналітичної діяльності. Використання відкритих джерел.
3. Автоматизовані інформаційні системи та інформаційно-аналітичні технології в діяльності правоохоронних органів.
4. Єдина інформаційна система Міністерства внутрішніх справ України як ключовий елемент сучасного інформаційно-аналітичного забезпечення правоохоронної діяльності.

Мета: систематизувати знання про організаційно-правові та технологічні аспекти інформаційно-аналітичного забезпечення правоохоронної діяльності, сформувати практичні навички з аналізу інформації, оцінки ризиків та прийняття рішень на основі аналітичних даних.

Перелік ключових термінів і понять з теми: правоохоронний орган, інформаційні системи, інформація, автоматизовані інформаційні системи, інформаційні технології, інформаційне забезпечення, аналітична діяльність, інформаційно-аналітичні технології, інформаційно-пізнавальна діяльність, криміналістичні обліки.

1. Інформаційне забезпечення правоохоронної діяльності: поняття, елементи, система.

Інформаційне забезпечення правоохоронної діяльності є комплексом організаційних, правових, технічних і технологічних заходів, засобів та методів, що забезпечують у процесі управління і функціонування системи сталий обмін інформацією між її елементами (суб'єктами та об'єктами) шляхом оптимальної організації інформаційних масивів, баз даних і знань. Будь-яка інформація набуває практичної цінності лише за умови можливості її використання та легалізації у встановленому законом порядку. За формою вона може бути представлена у числовому, графічному, текстовому вигляді, мати формат аудіо- або відеозапису. Ефективність діяльності правоохоронних органів безпосередньо залежить від якості інформаційного забезпечення заходів з протидії злочинності, що здійснюються відповідно до законодавчо визначених засад забезпечення національної безпеки та її складових - економічної, фінансової, соціальної, інноваційної, територіальної, правоохоронної тощо.

Важливою умовою результативності такої діяльності є професійна спроможність працівників правоохоронних органів щодо розроблення й застосування методик оброблення, узагальнення та аналізу інформації, творчого використання аналітичних результатів, формування обґрунтованих управлінських рішень, оцінювання їх наслідків у режимі реального часу, а також ефективного використання інформаційних ресурсів і сучасних інформаційних технологій.

Сучасні процеси глобалізації, інтеграції та динамічних змін у сфері безпеки зумовлюють підвищені вимоги до оперативності, ефективності та прозорості діяльності правоохоронних органів. В умовах зростання рівня злочинності, поширення організованих і транснаціональних злочинних угруповань, а також появи нових форм правопорушень, зокрема у сфері кіберзлочинності, актуалізується потреба у використанні сучасних управлінських підходів, заснованих на комплексному застосуванні інформаційно-аналітичних та організаційних методів. У цьому контексті Указом Президента України від 31 січня 2006 р. № 80/2006 «Про єдину комп'ютерну інформаційну систему правоохоронних органів у боротьбі зі злочинністю» було започатковано створення Єдиної комп'ютерної інформаційної системи правоохоронних органів [1]. Єдиний інформаційний простір включає бази та банки даних, технології їх формування і використання, а також інформаційно-телекомунікаційні системи та мережі. Саме інформаційно-аналітична діяльність у межах цього простору виступає підґрунтям для формування ефективних управлінських рішень, оскільки передбачає систематичний збір, перевірку, аналіз і використання відомостей про стан правопорядку та тенденції його розвитку.

Розвиток цифрових технологій, упровадження автоматизованих баз даних, геоінформаційних систем, інструментів прогнозної аналітики та елементів штучного інтелекту відкривають нові можливості для оперативного виявлення правопорушень, прогнозування ризиків і запобігання кримінальним проявам. Інформаційно-аналітичні та організаційні методи утворюють взаємодоповнювальну систему, у межах якої дані трансформуються у знання, а знання - в керовану дію. Ядром цієї системи є інтелектуально орієнтована модель діяльності правоохоронних органів, що передбачає пріоритет аналітики під час визначення оперативних і стратегічних рішень, розподілу ресурсів та оцінювання ризиків. Аналітичний цикл включає такі етапи: ідентифікацію проблеми, збирання та верифікацію даних, їх інтеграцію в єдине інформаційне середовище, багатовимірний аналіз, візуалізацію результатів, формування рекомендацій і моніторинг ефективності їх реалізації.

Джерелами інформації у практичній діяльності виступають відомчі реєстри, оперативно-розшукові матеріали, звернення громадян, відкриті дані, матеріали адміністративного нагляду, а також міжнародні канали обміну інформацією, зокрема системи Інтерполу. Для забезпечення якості інформації

критично важливими є стандартизація форматів запису, уніфікація класифікаторів подій і суб'єктів, а також процедури очищення даних, оскільки від точності вихідної інформації залежить валідність подальших аналітичних висновків.

У науковій літературі та нормативних актах широко використовуються поняття «інформаційне забезпечення», «інформаційно-аналітичне забезпечення», «інформаційно-аналітична діяльність», «аналітична робота», що зумовлює необхідність їх уточнення. Так, на думку В. Варненка, інформаційно-аналітична діяльність є специфічним різновидом інтелектуальної діяльності, у процесі якої шляхом послідовних дій із пошуку, накопичення, зберігання, обробки та аналізу первинної інформації формується вторинна аналітична інформація у вигляді довідок, звітів, оглядів, прогнозів тощо [2, с. 14]. С. Мазурик визначає інформаційно-аналітичну діяльність як вид соціальної діяльності, що полягає у роботі з інформацією із застосуванням логічних, математичних та інших методів, результатом якої є створення унікального інтелектуального інформаційного продукту [3]. В. Біла акцентує на доцільності виокремлення правової форми аналітичної діяльності, яка за своїм змістом є управлінським рішенням щодо наявності порушень чинного законодавства [4, с. 66]. Водночас О. Бандурка зазначає, що виявлення, запобігання та розслідування злочинів неможливі без попереднього отримання повної та всебічної інформації про діяльність суб'єкта правопорушення, що становить сутність процесу інформаційного забезпечення оперативно-розшукової діяльності [5, с. 281]. Є. Лук'янчиков розглядає інформаційне забезпечення як загальний метод організації діяльності та процес, пов'язаний зі збиранням, переробкою, використанням і збереженням інформації, яка відображає реальні події та явища [6, с. 111]. На завершення аналізу авторських підходів щодо природи «інформаційного забезпечення» наведемо позицію В. Лушера, який розглядає інформаційне забезпечення як комплекс нормативно-правових, організаційно-управлінських, науково-технічних та інших заходів поєднання усієї інформації, специфічних засобів і методів її оброблення, використання, дослідження, зберігання та захисту, а також включає в себе, роботу з інформаційними ресурсами, інформаційним програмним забезпеченням та інформаційно-аналітичну роботу [7].

Ядро інформаційно-аналітичної діяльності у правоохоронній сфері формується на основі комплексу сучасних аналітичних інструментів, зокрема: описової статистики, аналізу часових рядів, просторового аналізу, ризик-орієнтованого моделювання, соціально-мережевого аналізу для виявлення ключових вузлів злочинної взаємодії, а також кримінологічних «скриптів», що дозволяють реконструювати типові етапи вчинення правопорушень. Їх комплексне застосування забезпечує науково обґрунтовану підтримку управлінських рішень у сфері правоохоронної діяльності. Інформаційне

забезпечення правоохоронної діяльності має системний характер і включає три взаємопов'язані компоненти:

1. *Інформаційні системи* - сукупність технічних і програмних засобів, у межах яких здійснюється збирання, накопичення, системна обробка, зберігання та надання користувачам необхідної інформації.

2. *Аналітична робота* - комплекс організаційних заходів і методичних прийомів, спрямованих на обробку, узагальнення та синтез оперативної й іншої релевантної інформації з метою формування аналітичних продуктів.

3. *Управлінська діяльність* - процес ухвалення стратегічних і тактичних рішень у сфері протидії злочинності на основі результатів інформаційно-аналітичної обробки. Ефективність правоохоронної діяльності залежить від узгодженої взаємодії зазначених компонентів, що забезпечує трансформацію інформації в управлінські рішення та практичні дії щодо запобігання, виявлення й розслідування кримінальних правопорушень.

2. Джерела інформаційно-аналітичної діяльності. Використання відкритих джерел.

Авторами посібника «Основи кримінального аналізу» визначено основні види джерел інформації, це:

1) *Конфіденційні інформатори*: особи з безпосереднім доступом до інформації, що має відношення до незаконних форм діяльності і систем, які надають цю інформацію правоохоронним органам.

2) *Операції під прикриттям*: сплановане впровадження співробітників (необов'язково, щоб це були штатні співробітники правоохоронних органів) в злочинні групи, злочинні організації або їх інфраструктуру з метою отримання певних елементів інформації про систему.

3) *Попередні розслідування*: висновки, зроблені на основі попереднього збору і аналізу інформації про відповідні заходи боротьби з кримінальною діяльністю, організаціями і особами.

4) *Правові інструменти*: застосування таких інструментів як арешт і повістки в суд для отримання інформації із захищених джерел або осіб, що відмовляються від співпраці.

5) *Системи по отриманню та зберіганню інформації*: застосування даних, які вже зібрані й зберігаються в сховищі даних, таких як картотека або комп'ютерна база даних.

6) *Речові докази*: інформація про фізичне положення, одержана з місця злочину, про жертву, про підозрювану особу і його оточення.

7) *Аудіо-, відеоконтроль особи*: таємне спостереження за діяльністю особи.

8) *Технічне спостереження*: приховане спостереження за діяльністю і фіксація із застосуванням технічних засобів.

9) *Взаємний обмін*: інформація, яка одержана або обмінена з іншим правоохоронним органом.

10) *Регіональні мережі «кримінальної розвідки»:* агентства по обміну інформацією, які надають певні послуги з підтримки в конкретному регіоні.

11) *Відкриті джерела:* залучення інформації, вже зібраної державними відомствами та іншими установами, у тому числі й даних держустанов.

12) *Відкриті посилання*: наукові роботи і інші джерела, такі як газети, журнали, ЗМІ.

13) *Інтерв'ю:* інформація, одержана шляхом використовування запланованого, але неформального діалогу, при цьому учасники не відносяться один до одного вороже.

14) *Допит:* аналогічно інтерв'ю, але з виключенням, що між сторонами може бути атмосфера ворожості та недовіри.

5) *Дебрифінг:* офіційна сесія питань і відповідей між членами того ж підрозділу, агентства або професії [8, с. 28].

Сучасні технології та інформаційні ресурси надають національним правоохоронним органам нові можливості для ефективного виконання їхніх завдань. *Використання відкритих джерел інформації* (Open Source Intelligence - OSINT) стає все більш важливим елементом інформаційно-аналітичної діяльності поліції України. Різні агенції по-різному дають визначення OSINT, але одне загальноприйняте визначення походить від Довідника НАТО з відкритих джерел розвідки, який визначає OSINT як «розвідувальну інформацію, яка створюється на основі загальнодоступної інформації та своєчасно збирається, використовується та поширюється належним чином для відповідної аудиторії з метою вирішення конкретної розвідувальної та інформаційної вимоги» [9]. Протокол Берклі про розслідування цифрових відкритих джерел *визначає інформацію з відкритих джерел* як «інформацію, яку будь-який член громадськості може переглядати, купувати або запитувати, не вимагаючи спеціального правового статусу або несанкціонованого доступу. Цифрова інформація з відкритих джерел - це загальнодоступна інформація в цифровому форматі, яку зазвичай отримують з Інтернету» [10].

OSINT передбачає використання загальнодоступних джерел, таких як газети, телефонні довідники, телебачення, радіопередачі, і, що найважливіше, цифрових джерел, таких як веб-сайти, блоги, форуми та платформи соціальних мереж, для збору інформації, яка може сприяти аналізу розвідданих. Деякі джерела можуть розглядати платні набори даних, які можна отримати через покупку, як інформацію з відкритих джерел, а інші - ні. Але головне, щоб інформація була доступна у відкритих джерелах.

Методи OSINT широко використовуються в кіберрозслідуваннях. Величезна кількість і різноманітність відкритих джерел, особливо в Інтернеті, мають великий обсяг інформації, яку можна зібрати. Від IPадрес, інформації про

веб-сайти та заголовків електронних листів до публікацій у соціальних мережах і онлайнових баз даних дослідники можуть використовувати OSINT для збору інформації та виявлення моделей діяльності. Оскільки він покладається на загальнодоступні джерела, інформацію з відкритих джерел можна збирати без попередження суб'єктів розслідування, що робить його ефективним підходом для початкових запитів або коли потрібна обережність. OSINT широко використовується в приватному секторі, а також для збору інформації про ділових партнерів, співробітників або потенційних загроз.

3. Автоматизовані інформаційні системи та інформаційно-аналітичні технології в діяльності правоохоронних органів.

Указом Президента України від 11 травня 2023 року № 273/2023 було схвалено Комплексний стратегічний план реформування органів правопорядку як частини сектору безпеки і оборони України на 2023 - 2027 роки [11]. Цим документом передбачено комплексну цифрову трансформацію, зокрема:

1. Здійснення консолідованої поетапної цифрової трансформації органів правопорядку та прокуратури на основі інструментів стратегічного менеджменту, які відповідають найкращим практикам ЄС.

2. Подальше впровадження в діяльність органів правопорядку та прокуратури інноваційних технологічних досягнень, що забезпечують гнучкість операційних процесів, ІТ-рішення, цифрову спроможність оперативно реагувати на події та зміни й здобувати результат, орієнтований на інтереси суспільства.

3. Поетапне впровадження електронної системи управління кримінальними провадженнями шляхом комплексної заміни та модернізації обладнання, забезпечення сумісності ІТ-систем, безперебійності роботи, доступу усіх учасників кримінального провадження та Інтер операбельності.

4. Підвищення ефективності діяльності органів правопорядку та прокуратури через забезпечення більшої доступності й повноти інформації, розроблення і впровадження сервісів на Єдиному державному веб-порталі електронних послуг.

5. Впровадження заходів безпеки і захисту персональних даних відповідно до стандартів ЄС.

6. Удосконалення та впровадження більш безпечних, гнучких, спроможних і доступних систем зв'язку між усіма органами право- порядку та іншими екстреними службами (включаючи цифрове радіо: голосовий зв'язок і широкосмугове передавання даних).

7. Запровадження в усіх органах правопорядку та прокуратури уніфікованої системи особистої автентифікації та системи біометричного зіставлення із поступовим забезпеченням її сумісності з європейськими системами. Широке використання під час здійснення досудового розслідування, а також для обробки даних та аналітичної діяльності органів правопорядку і

прокуратури штучного інтелекту, блокчейну, хмарних обчислень та інших інноваційних рішень.

8. Оновлення операційних процесів за допомогою ІТ-систем, придатних для обміну даними з інституціями ЄС відповідно до стандартів ЄС.

9. Надання органам правопорядку та прокуратури для забезпечення виконання покладених на них функцій права на безпосередній спільний доступ до автоматизованих інформаційних і довідкових систем, реєстрів і баз даних, держателем (адміністратором) яких є інші державні органи.

Інформаційні системи - це організаційно-технічні системи, в яких реалізуються технології обробки інформації з використанням технічних і програмних засобів. До складу інформаційних систем можуть входити інформаційні підсистеми, які містять банки даних, поєднані технологією обміну інформацією. В аналітичній роботі використовується: аналіз (аналіз даних, аналіз справ, порівняльний аналіз); тактичний аналіз (кримінальний аналіз, аналіз кримінальних тенденцій, геопросторовий аналіз, аналіз місць концентрації злочинності, часовий аналіз, МО-аналіз, кримінальні моделі, профілі підозрюваних/жертв); стратегічний аналіз (SWOT-аналіз, PEST-аналіз, аналіз моделей/форм злочинності та профілювання, аналіз тенденцій, аналіз з використанням географічного профілювання); аналіз даних з відкритих джерел (OSINT); аналіз даних з багатьох джерел (Multi-Source Analysis). Для проведення аналізу застосовуються аналітичні інструменти, відповідне програмне забезпечення, а також наявні інформаційні ресурси.

Автоматизована інформаційна система (АІС) визначається як організаційно-технічна система, що реалізує технологію обробки інформації за допомогою технічних і програмних засобів. Автоматизовані інформаційні системи, що використовуються правоохоронними органами у своїй діяльності, можна класифікувати таким чином [12]:

– АІС, призначені для збору та обробки облікової, реєстраційної та статистичної інформації;

– АІС, призначені для обробки інформації оперативного призначення;

– АІС, що використовуються для оперативно-розшукової діяльності;

– АІС, що використовуються для криміналістичного опрацювання інформації;

– АІС, що використовуються для експертної діяльності;

– АІС для адміністративного призначення.

Автоматизовані інформаційні системи за рівнем складності обробки інформації можуть мати певну класифікацію:

– автоматизовані інформаційно-довідкові системи (АІДС);

– автоматизовані системи управління (АСУ);

– автоматизовані робочі місця (АРМ);

– автоматизовані інформаційно-пошукові системи (АІПС);

– автоматизовані системи обробки даних (АСОД);

– експертні системи (ЕС), експертні консультаційні системи, а також системи підтримки прийняття управлінських рішень.

Відповідно до Закону України «Про Національну поліцію» від 02.07.2025 р. №580-VIII, «Поліція здійснює інформаційно-аналітичну діяльність виключно для реалізації своїх повноважень, визначених законом». Засобами реалізації інформаційно-аналітичної діяльності є системи передачі даних та зв’язку, створення баз даних правової інформації, застосування інформаційно-телекомунікаційних технологій та інформаційних систем, використання правових, технічних, програмних, інформаційних та організаційних засобів.

Системою інформаційного забезпечення Національної поліції України є сукупність взаємодіючих та взаємопов'язаних технічних засобів та організаційних елементів, які здійснюють інформаційне забезпечення діяльності поліції України. В основу системи інформаційного забезпечення поліції покладено формування галузевих та відомчих інформаційних підсистем, які функціонують за такими принципами: нормативно-правового забезпечення; достовірності даних; розширення та розвитку; функціонального призначення (слідчого призначення, оперативно-розшукового призначення, інформаційної підсистеми кримінального призначення, підсистеми розвідки, інформаційної підсистеми, що становить основу системи інформаційного забезпечення Національної поліції України).

Основним органом, відповідальним за формування інформаційної підсистеми поліції, є *Департамент інформатизації Міністерства внутрішніх справ України.* Відповідно до законодавства України та нормативно-правових актів центральних органів виконавчої влади, цей Департамент виступає структурним підрозділом апарату МВС, який здійснює організацію, спрямовану на інформаційно-аналітичне забезпечення правоохоронної діяльності в органах і підрозділах Міністерства внутрішніх справ України та захист персональних даних під час їх обробки. Органом, який відповідає за формування розвідувальних ресурсів національної поліції в регіонах, є Департамент інформаційно-аналітичного забезпечення (ДІАЗ). Він є структурним підрозділом обласних головних управлінь Національної поліції України (далі - ГУНП). Департамент інформаційно-аналітичного забезпечення є структурним підрозділом Головного управління Національної поліції в області (ГУНП) і організовує та здійснює заходи, спрямовані на забезпечення правоохоронної діяльності поліції області. Основними напрямами його діяльності є:

– збір, обробка, зберігання та архівування статистичної, слідчої, оперативної, довідкової, криміналістичної та облікової інформації;

– організація створення, розвитку та експлуатації автоматизованих та інтелектуальних інтегрованих інформаційних систем;

– розробка корпоративної інформаційної мережі для обласних управлінь поліції;

– інформаційне забезпечення органів поліції, надання інформації фізичним та юридичним особам;

– облік правопорушників, скоєних злочинів, ведення кримінальної статистики злочинності; – інформаційна підтримка органів поліції щодо зберігання та захисту ділової документації;

– впровадження сучасних інформаційних технологій та інформаційних систем у діяльність Головного управління поліції;

– підготовка національних та галузевих статистичних звітів про стан діяльності в області, регіоні та країні. Оптимізація вирішення завдань пошуку, відбору та систематизації інформації, необхідної для діяльності поліції, є ключовим елементом системи МВС.

Інформаційний простір системи МВС України можна визначити наступним чином. Він базується на побудові єдиного інформаційного простору системи МВС України, суб'єктів інформаційно-аналітичної діяльності, технології ведення та використання спеціалізованих баз даних, а також на інформаційно-комунікаційних системах та мережі банку даних, які мають єдиний принцип функціонування та побудови для забезпечення інформаційної взаємодії системи Міністерства внутрішніх справ України.

Інформаційно-аналітичне забезпечення є одним із засобів виявлення проблем, їх оцінювання та ефективності впроваджених в діяльність органів поліції змін. Із зростанням рівня злочинності в Україні у діяльності правоохоронних органів та в Національній поліції запроваджено сучасні інформаційно-аналітичні системи. Саме застосування сучасних технологій при виконанні інформаційно-аналітичної роботи мінімізує витрачений робочий час оперативного працівника та підвищує якість його роботи.

Інформаційно-аналітичне забезпечення є важливим елементом діяльності Національної поліції України, зокрема кримінального аналізу. Це включає організаційні, правові та технологічні засоби, які дозволяють збирати, обробляти, аналізувати та використовувати інформацію, необхідну для виконання завдань поліції, визначених законодавством. Сучасне суспільство вимагає інформаційно-аналітичної діяльності як ключового чинника стабільності та життєздатності країни. Кримінальний аналіз полягає у виявленні та аналізі зв'язків між інформацією про злочини, їх виконавців і даними з різних джерел. Це дозволяє правоохоронним органам, прокуратурі та судам оцінити і використовувати цю інформацію для подальших дій. Основною метою кримінального аналізу є розробка нових підходів до ефективної слідчої роботи та досудового розслідування, а також поліпшення оперативно-розшукової та профілактичної діяльності у боротьбі зі злочинністю.

4. Єдина інформаційна система Міністерства внутрішніх справ України як ключовий елемент сучасного інформаційно-аналітичного забезпечення правоохоронної діяльності.

Відповідно до Положення про Єдину інформаційну систему Міністерства внутрішніх справ України, затвердженого Постановою Кабінету Міністрів України від 14 листопада 2018 р. № 1024 (у редакції постанови Кабінету Міністрів України від 15 серпня 2023 р. № 866), *Єдина інформаційна система МВС* (далі - ЄІС МВС) є інтегрованою інформаційною системою, що безпосередньо забезпечує реалізацію функцій її суб'єктів, інформаційну підтримку та супроводження їх діяльності [13].

ЄІС МВС становить сукупність взаємопов'язаних функціональних підсистем, сервісів, програмно-інформаційних комплексів, програмно-технічних і технічних засобів електронної комунікації, які забезпечують логічне поєднання та інтеграцію електронних інформаційних ресурсів, обробку та захист інформації, а також внутрішню і зовнішню інформаційну взаємодію. Власником і розпорядником ЄІС МВС є держава в особі Міністерства внутрішніх справ України.

ЄІС МВС призначена для автоматизації та технологічного забезпечення обміну даними між суб'єктами системи в інтересах національної безпеки, захисту прав і законних інтересів громадян, суспільства і держави у сферах:

- забезпечення охорони прав і свобод людини, протидії злочинності, підтримання публічної безпеки і порядку;
- захисту державного кордону та охорони суверенних прав України у виключній (морській) економічній зоні;
- цивільного захисту, запобігання та ліквідації надзвичайних ситуацій, пожежної і техногенної безпеки, рятувальної справи;
- міграції, громадянства, протидії нелегальній міграції, реєстрації фізичних осіб, біженців та інших категорій мігрантів.

Основними завданнями ЄІС МВС є:

1. Створення єдиного інформаційного простору системи МВС та центральних органів виконавчої влади, діяльність яких координується через Міністра внутрішніх справ.

2. Інформаційна підтримка діяльності суб'єктів ЄІС МВС під час виконання ними законодавчо визначених функцій.

3. Забезпечення електронної взаємодії суб'єктів ЄІС МВС з метою оперативного виконання завдань у сфері національної безпеки.

4. Зменшення часових і фінансових витрат на управлінські, інформаційно-пошукові та аналітичні процеси.

5. Інтеграція електронних інформаційних ресурсів, реєстрація суб'єктів ЄІС МВС та надання доступу до них.

До основних функціональних підсистем ЄІС МВС належать:

- національна система біометричної верифікації та ідентифікації;
- інформаційний портал Національної поліції України;
- Єдиний державний реєстр транспортних засобів;
- Реєстр адміністративних правопорушень у сфері безпеки дорожнього руху;
- система автоматичної фіксації правопорушень у сфері безпеки дорожнього руху;
- інтегрована міжвідомча інформаційно-комунікаційна система контролю осіб, транспортних засобів і вантажів на державному кордоні;
- інформаційно-комунікаційна система прикордонного контролю «Гарт-1»;
- інформаційно-комунікаційна система екстреної допомоги 112;
- Електронний реєстр геномної інформації людини;
- Єдиний реєстр осіб, зниклих безвісти за особливих обставин;
- Єдиний реєстр зброї;
- Система управління силами та засобами цивільного захисту;
- інші реєстри, бази даних і системи, створені суб'єктами ЄІС МВС у межах їх повноважень.

До пріоритетних електронних інформаційних ресурсів ЄІС МВС належать відомості, що формуються та використовуються:

- Державною міграційною службою України (ЄДДР, біометричні та міграційні реєстри);
- Офісом Генерального прокурора (ЄРДР);
- Державною судовою адміністрацією (реєстри судових рішень);
- Міністерством внутрішніх справ та Національною поліцією (обліки зброї, дактилоскопічні, криміналістичні, персонально-довідкові обліки);
- Адміністрацією Державної прикордонної служби України (дані про перетин кордону, заборони в'їзду, транспортні засоби);
- Державною службою України з надзвичайних ситуацій (облік надзвичайних ситуацій і пожеж).

Окрему групу інформаційних ресурсів ЄІС МВС становлять відомості, що формуються у процесі здійснення оперативно-розшукової діяльності відповідно до законодавства. Така інформація використовується для виявлення, запобігання та розкриття кримінальних правопорушень, розшуку осіб, забезпечення публічної безпеки та підтримання правопорядку.

ЄІС МВС є ключовим елементом сучасного інформаційно-аналітичного забезпечення правоохоронної діяльності. Її функціонування забезпечує інтеграцію розрізнених інформаційних ресурсів, підвищує обґрунтованість управлінських рішень, сприяє ефективній міжвідомчій взаємодії та створює умови для дотримання принципів законності, захисту персональних даних і інформаційної безпеки. З метою підвищення ефективності інформаційно-

аналітичного забезпечення діяльності суб'єктів МВС, Наказом Міністерства внутрішніх справ України від 06 жовтня 2025 року № 677 було затверджено Положення про інформаційно-комунікаційну систему «Автоматизована аналітична платформа» єдиної інформаційної системи МВС [14].

ІКС «Автоматизована аналітична платформа» є функціональною підсистемою ЄІС МВС і створена для автоматизації, інтеграції, обробки та аналізу даних з різних джерел у реальному часі. *Мета та завдання* - забезпечення аналітичної підтримки управлінських рішень керівництва МВС та суб'єктів системи, прогнозування стану безпекового середовища, обробка даних про криміногенну ситуацію, надзвичайні події, міграційні процеси та інші аспекти діяльності МВС.

Структура - до складу ІКС входять: центральне сховище даних, сервери обробки та рольових моделей, сервери додатків, засоби файлового обміну, шлюзові сервери, електронний кабінет користувача, автоматизовані робочі місця, інтерфейси програмної взаємодії та інші технічні та програмні засоби.

Суб'єкти та користувачі - суб'єктами ІКС є структурні підрозділи МВС, Національна поліція, Держприкордонслужба, ДСНС, ДМС та Нацгвардія. Користувачами є уповноважені особи цих підрозділів із визначеними правами доступу, які здійснюють обробку та внесення даних відповідно до законодавства.

Організаційні положення - власником та розпорядником інформації є держава в особі МВС, технічним адміністратором - державне підприємство у сфері управління МВС. Розподіл прав доступу, моніторинг достовірності та захист даних здійснюються згідно з Положенням та чинним законодавством.

Функції - автоматизоване формування, збереження, систематизація та аналіз даних, створення аналітичних звітів, візуалізація та прогнозування стану безпекового середовища, обмін інформацією з ЄІС МВС та іншими державними ресурсами, використання сучасних технологій, включно зі штучним інтелектом, забезпечення інформаційної безпеки та контролю доступу. Впровадження цієї системи забезпечує інтеграцію інформаційних ресурсів, підвищує ефективність міжвідомчої взаємодії та сприяє оперативності та обґрунтованості управлінських рішень у сфері безпеки, правопорядку та цивільного захисту.

Використана література:

1. Про єдину комп'ютерну інформаційну систему правоохоронних органів у боротьбі зі злочинністю : Указ Президента України від 31.01.2006 № 80/2006. URL: https://zakon.rada.gov.ua/laws/show/80/2006#Text (дата звернення 07.01.2026).

2. Варенко В.М. Інформаційно-аналітична діяльність : навч. посіб. Київ, 2014. 417 с.

3. Мазурик С. Інформаційно-аналітична діяльність органів прокуратури. *Науковий вісник Херсонського державного університету*. 2016. №

5. С. 56-59. URL: http://nbuv.gov.ua/ UJRN/Nvkhdu_jur_2016_5%282%29__15 (дата звернення 07.01.2026).

4. Біла В. Р. Форми аналітичної діяльності правоохоронних органів. *Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика)*. 2018. Вип. 1-2. С. 61-67. URL: http://nbuv.gov.ua/UJRN/muvnudp_2018_1-2_15 (дата звернення 07.01.2026).

5. Бандурка О. М. Оперативно-розшукова діяльність. Частина І : підруч. Харків : НУВС, 2002. 336 с.

6. Лук'янчиков Є. Д. Методологічні засади інформаційного забезпечення розслідування злочинів : монографія. Київ, 2005. 320 с.

7. Лушер В. В. Поняття інформаційного забезпечення органів прокуратури України. *Форум права*. 2014. № 1. С. 338-341. URL: http://nbuv.gov.ua/UJRN/FP_index (дата звернення 07.01.2026).

8. Основи кримінального аналізу : посіб. з елементами тренінгу / О. Є. Користін та ін. Одеса : ОДУВС, 2016. 112 с.

9. Bazzell M. OSINT Techniques: Resources for Uncovering Online Information. CreateSpace Independent Publishing Platform, 2023. 550 p.

10. Borges D. Adversarial Tradecraft in Cybersecurity: Offense versus defense in real-time computer conflict. Packt. 2021. 246 p.

11. Про Комплексний стратегічний план реформування органів правопорядку як частини сектору безпеки і оборони України на 2023-2027 роки : Указ президента України від 11.05.2023 № 273/2023. URL: https://www.president.gov.ua/documents/2732023-46733 (дата звернення 07.01.2026).

12. Інформаційно-аналітичне забезпечення правоохоронної діяльності : навч. посіб. / Е. В. Рижков, Ю. П. Синиціна, С. О. Прокопов та ін. Дніпро, 2024. 180 с.

13. Положення про Єдину інформаційну систему Міністерства внутрішніх справ України : Постанова Кабінету Міністрів України від 14.11.2018 № 1024 (у редакції постанови Кабінету Міністрів України від 15 серпня 2023 р. № 866). URL: https://zakon.rada.gov.ua/laws/show/1024-2018-%D0%BF#n124 (дата звернення 07.01.2026).

14. Положення про інформаційно-комунікаційну систему «Автоматизована аналітична платформа» єдиної інформаційної системи МВС : Наказ Міністерства внутрішніх справ України від 06.10.2025 № 677. URL: https://zakon.rada.gov.ua/laws/show/z1522-25/sp:dark#Text (дата звернення 07.01.2026).

Питання для обговорення:

1. Охарактеризуйте організаційно-правові засади інформаційно-аналітичного забезпечення діяльності правоохоронних органів України.

2. Розкрийте сутність основних напрямків та критеріїв оцінки ефективності аналітичної роботи у сфері правоохоронної діяльності.

3. Охарактеризуйте принципи збору, обробки та використання інформації у правоохоронних органах.

4. Назвіть умови та обмеження використання відкритих джерел інформації (OSINT) під час аналітичної діяльності.

5. Охарактеризуйте призначення та завдання автоматизованих інформаційних систем у правоохоронній діяльності.

6. Розкрийте сутність аналітичного циклу: ідентифікація проблеми, збір даних, аналіз, синтез, формування рекомендацій та моніторинг.

7. Дотримання законності та прав людини у процесі інформаційно-аналітичного забезпечення: основні вимоги та стандарти.

8. Охарактеризуйте роль Єдиної інформаційної системи МВС у забезпеченні аналітичної підтримки та оперативної взаємодії між підрозділами.

9. Розкрийте сучасні технології аналітичної роботи (штучний інтелект, геоінформаційні системи, блокчейн) та їх застосування у правоохоронній діяльності. Оцініть практичну значимість інформаційно-аналітичного забезпечення для запобігання злочинам та прийняття управлінських рішень.

10. Інформаційно-аналітичне забезпечення оперативно-розшукової діяльності у протидії молодіжній злочинності: правові та організаційно-технологічні аспекти.

<u>Тестові завдання:</u>

1**.** *Яке завдання інформаційно-аналітичного забезпечення правоохоронної діяльності?*

а) Збір статистичних даних без їх подальшого аналізу;

б) Забезпечення керівництва та підрозділів аналітичними даними для прийняття рішень;

в) Ведення архівів документів;

г) Виключно контроль за виконанням службових обов’язків.

2. *Що таке OSINT?*

а) Закрита база даних правоохоронного органу;

б) Дані, отримані незаконним шляхом;

в) Розвідувальна інформація з відкритих джерел;

г) Тільки інформація з соціальних мереж.

3. *Яка мета Єдиної інформаційної системи МВС України?*

а) Зберігати інформацію тільки про транспортні засоби;

б) Інтегрувати інформаційні ресурси, забезпечувати аналітичну підтримку і оперативну взаємодію;

в) Створювати статистичні звіти без доступу користувачів;

г) Забезпечувати доступ лише для Національної поліції.

4. *Який етап аналітичного циклу включає візуалізацію даних та формування рекомендацій?*

а) Збирання даних;

б) Ідентифікація проблеми;

в) Аналітична обробка та синтез;

г) Моніторинг.

5. *Яке твердження про використання сучасних аналітичних технологій у правоохоронних органах є правильним?*

а) Використовуються для статистики;

б) Підвищують ефективність аналізу та прийняття рішень;

в) Використовуються тільки у розслідуваннях.

✍Практичні завдання:

1**.** Ви отримали інформацію про потенційний конфлікт у регіоні через соціальні мережі та новини. Проведіть збір і систематизацію даних, визначте ключові ризики та підготуйте аналітичну довідку.

2. Використовуючи умовну автоматизовану систему обліку правопорушень, визначте тренди по типах злочинів за останній місяць. Підготуйте рекомендації щодо пріоритетних заходів поліції.

3. Отримано оперативні дані про серію квартирних крадіжок у місті. Пройдіть всі етапи аналітичного циклу: ідентифікація проблеми, збір даних, верифікація, аналіз, формування рекомендацій та моніторинг. Складіть короткий звіт.

4. На прикладі ЄІС МВС оцініть, як інтеграція даних з різних підсистем допомагає запобігти злочинам та підвищує швидкість прийняття рішень. Складіть короткий звіт.

5. Виявлено витік персональних даних з регіональної бази МВС. Складіть план дій із захисту інформації та забезпечення безпеки даних, враховуючи принципи законності та захисту персональних даних.

Рекомендована література:

1. Про Національну поліцію : Закон України від 02.07.2015 № 580-VIII. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text (дата звернення: 21.12.2025).

2. Про оперативно-розшукову діяльність : Закон України від 18.02.1992 № 2135-XII. URL: https://zakon.rada.gov.ua/laws/show/2135-12/card2#Card (дата звернення: 21.12.2025).

3. Про єдину комп'ютерну інформаційну систему правоохоронних органів у боротьбі зі злочинністю : Указ Президента України від 31.01.2006 № 80/2006. URL: https://zakon.rada.gov.ua/laws/show/80/2006#Text (дата звернення: 21.12.2025).

4. Про Комплексний стратегічний план реформування органів правопорядку як частини сектору безпеки і оборони України на 2023-2027 роки : Указ президента України від 11.05.2023 № 273/2023. URL: https://www.president.gov.ua/documents/2732023-46733 (дата звернення: 21.12.2025).

5. Положення про Єдину інформаційну систему Міністерства внутрішніх справ України : Постанова Кабінету Міністрів України від 14.11.2018 № 1024 (у редакції постанови Кабінету Міністрів України від 15 серпня 2023 р. № 866). URL: https://zakon.rada.gov.ua/laws/show/1024-2018-%D0%BF#n124 (дата звернення: 21.12.2025).

6. Положення про інформаційно-комунікаційну систему «Автоматизована аналітична платформа» єдиної інформаційної системи МВС : Наказ Міністерства внутрішніх справ України від 06.10.2025 № 677. URL: https://zakon.rada.gov.ua/laws/show/z1522-25/sp:dark#Text (дата звернення: 21.12.2025).

7. Інформаційно-аналітичне забезпечення правоохоронної діяльності : навч. посіб. / Е. В. Рижков, Ю. П. Синиціна, С. О. Прокопов та ін. Дніпро, 2024. 180 с.

ТЕМА 5.
ОРГАНІЗАЦІЙНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ПРОТИДІЇ МОЛОДІЖНІЙ ЗЛОЧИННОСТІ: СТРАТЕГІЯ, ТАКТИКА, ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ

План

1. Протидія молодіжній злочинності як елемент забезпечення національної безпеки в умовах воєнного стану.
2. Роль правоохоронних органів у протидії молодіжній злочинності в умовах правового режиму воєнного стану: інформаційно-аналітичне забезпечення ОРД, тактика отримання достовірної інформації, етичні та правові межі її використання.
3. Організаційні та тактичні особливості проведення допиту підозрюваних при розслідуванні групових злочинів неформальної молоді: особливості отримання інформації, забезпечення законності, недопущення порушень прав людини.
4. Захист прав потерпілих під час розслідування злочинів проти життя та здоров’я особи, учинених членами молодіжних неформальних груп (об’єднань).
5. Спеціальна техніка та інформаційне забезпечення розслідування групових злочинів неформальної молоді.

Мета: систематизувати знання про організаційно-правові засади протидії молодіжній злочинності як складової забезпечення національної безпеки України в умовах воєнного стану, сформувати практичні навички з застосування інформаційно-аналітичних технологій, спеціальної техніки, тактичних прийомів оперативно-розшукової діяльності та досудового розслідування з урахуванням принципів законності, дотримання прав людини і потерпіло-орієнтованого підходу при розслідуванні групових злочинів неформальної молоді.

Перелік ключових термінів і понять з теми: інформація, кримінальна аналітика, автоматизовані інформаційні системи, інформаційні технології, інформаційно-аналітичне забезпечення, програмне забезпечення, оперативно-розшукова діяльність, молодіжна злочинність, спеціальна техніка, цифрові технології, молодь, молодіжне угрупування, молодіжна злочинність, кримінальне правопорушення, потерпілий, розслідування, захист прав потерпілих, підхід орієнтований на потерпілого.

1. Протидія молодіжній злочинності як елемент забезпечення національної безпеки в умовах воєнного стану.

Протидія молодіжній злочинності є одним із пріоритетних напрямів державної політики у сфері забезпечення національної безпеки України, особливо в умовах воєнного стану. Вона має комплексний соціально-правовий характер і безпосередньо пов'язана із завданнями демократизації, реформування правоохоронної системи та зміцнення інституційної спроможності держави. Воєнна агресія Російської Федерації проти України істотно загострила криміногенну ситуацію в державі. Політична нестабільність, економічні втрати, масове внутрішнє переміщення населення, руйнування соціальної інфраструктури та психологічна травматизація молоді створили сприятливі умови для поширення злочинності, зокрема у молодіжному середовищі.

Молодь України стикається з безпрецедентними викликами, обумовленими соціально-економічною нестабільністю, вимушеним переміщенням, втратою родинних зав'язків і друзів, перебуванням на окупованих територіях, а також масштабними соціальними трансформаціями, спричиненими повномасштабною війною в Україні. За результатами комплексного дослідження «Молодь України: виклики та адаптація в умовах воєнного стану» (2025 р.), 82% опитаних молодих людей зазначили, що зазнали тих чи інших втрат через війну, зокрема: зниження або втрату доходу (36%), погіршення психічного здоров'я (28%), розрив стосунків або розлуку з сім'єю (по 18%), вимушене переміщення (16%), смерть близьких (14%), пошкодження житла чи травмування внаслідок бойових дій (по 6%) [1, с. 13 - 14]. Крім того, 40% респондентів вказали на недостатність коштів навіть для задоволення базових потреб, 19% - на відсутність можливостей самореалізації, ще 19% - на неможливість працевлаштування. Наведені дані демонструють зростання соціальної напруги, що безпосередньо впливає на девіантну поведінку молоді та формування криміногенних ризиків. Аналітичний центр дослідження соціальних трансформацій Cedos у дослідженні «Вплив війни на молодь в Україні» (2024 р.) наголошує, що молоді люди, які втратили стабільність і соціальні зв'язки, стають більш уразливими до проявів агресії, стресових розладів і девіантної поведінки, що потребує системної уваги з боку правоохоронних органів [2], адже сучасна злочинність демонструє стійку тенденцію до «омолодження». Молоді особи віком від 14 до 35 років дедалі активніше залучаються до кримінальної діяльності, зокрема до:

- особливо тяжких злочинів проти основ національної безпеки;
- колабораційної діяльності та державної зради;
- незаконного обігу зброї і наркотичних засобів;
- торгівлі людьми;
- кіберзлочинності та шахрайства в мережі Інтернет;

- сприяння незаконному перетину державного кордону особами призовного віку.

Цілком логічним є висновок В. Бабакіна, що криміналізація молодіжного середовища становить реальну загрозу як обороноздатності держави, так і стабільності післявоєнного суспільного розвитку [3, с. 24]. Вчений наводить наступні дані: за даними Офісу Генерального прокурора України, у 2021 - 2022 роках спостерігається різке зростання кількості кримінальних правопорушень проти основ національної безпеки, зокрема:

- державна зрада - 208 (2021) / 1957 (2022);
- колаборційна діяльність - 0 / 3851;
- пособництво державі-агресору - 0 / 379;
- шпигунство - 9 / 40;
- диверсія - 18 / 64;
- перешкоджання діяльності ЗСУ - 7 / 76 [3].

При цьому молоді особи становлять переважну більшість серед суб'єктів зазначених злочинів. Їх питома вага у загальній кількості зареєстрованих кримінальних правопорушень у 2021 - 2022 рр. у середньому становила 79,2 %, а у структурі тяжких та особливо тяжких злочинів проти основ національної безпеки - 82,4 %.

Найпоширенішими видами злочинів, вчинених молоддю, залишаються:

- крадіжки - 91,7 %;
- незаконний обіг наркотиків - 84,9 %;
- шахрайства (у т.ч. під виглядом допомоги військовим та переселенцям) - 57,1 %;
- умисні вбивства - 30,5 %;
- колаборційна діяльність - 69,8 %.

Зазначені показники свідчать про формування стійкої кримінальної субкультури серед частини молоді, яка швидко адаптується до змін оперативної обстановки та використовує воєнні умови для розвитку нових злочинних схем.

Протидія цьому негативному соціальному явищу - важлива суспільна справа, складова системи забезпечення внутрішньої безпеки держави, побудованої на основі і в дотримання гуманістичних цінностей. Протидія не зводиться тільки до діяльності правоохоронних органів із виявлення, розкриття та розслідування кримінальних правопорушень, учасниками яких були представники цієї категорії осіб. Вона включає в себе цілий комплекс заходів, що запобігають криміналізації молоді. Причому ці заходи не повинні зводитися тільки до заходів кримінально-правового впливу, а мають передбачати й дії, що лежать в іншій площині, тобто провадиться державою і суспільством у сфері виховання, зайнятості тощо. Особливістю системної діяльності з протидії є те, що вона має бути орієнтована не тільки на виявлення фактів злочинів, запобігання їх наслідкам, притягнення винних до відповідальності, а й на

профілактику цих злочинів, яка повинна передбачати такий вплив із боку правоохоронних органів на потенційних правопорушників, результатом якого була б їх відмова від злочинної діяльності.

2. Роль правоохоронних органів у протидії молодіжній злочинності в умовах правового режиму воєнного стану: інформаційно-аналітичне забезпечення ОРД, тактика отримання достовірної інформації, етичні та правові межі її використання.

В умовах воєнного стану правоохоронні органи України виконують не лише класичні функції із забезпечення правопорядку, а й додаткові завдання, пов'язані з обороною держави, зокрема:

- участь у територіальній обороні;
- ідентифікація воєнних злочинців;
- розшук безвісти зниклих осіб;
- розмінування територій;
- розшук активів держави-агресора;
- забезпечення евакуації цивільного населення.

Разом із тим, протидія молодіжній злочинності здійснюється в надзвичайно складних умовах, особливо на територіях, наближених до зони бойових дій або тимчасово окупованих.

Звертаємо увагу на проблеми в зазначеному питанні, які окреслює В. Бабакін в матеріалах Всеукраїнської науково-практичної конференції (м. Кропивницький, 7 липня 2023 року), зокрема вчений цілком справедливо зазначає, що покладені на правоохоронні органи України завдання щодо запобігання та протидії кримінальним правопорушенням, зокрема серед молоді, реалізуються недостатньо результативно. У протидії вказаним злочинам не повною мірою використовуються можливості оперативно-розшукової діяльності, яка забезпечує припинення злочинної діяльності молоді та молодіжних злочинних угруповань на стадії замислу, підготовки і замаху. Також правоохоронним органам необхідно удосконалювати стратегію і тактику, методи і форми ОРД у дослідженому напрямі. Також під час воєнного стану правоохоронним органам потрібно проводити постійний моніторинг, прогнозування дії окремих кримінально налаштованих молодих осіб, груп та угрупувань, які можуть нанести шкоду для життя та здоров'я людини та громадянина, а також надавати ворогу інформацію щодо дислокації Збройних Сил України та критичної інфраструктури міст; здійснювати постійний контроль стану оперативної обстановки на території, лінії, напрямі оперативного обслуговування і недопущення створення неформальних та інших незаконних чи криміналізованих молодіжних об'єднань; здійснювати збір значимої інформації

відносно кримінально активних молодих осіб, зокрема й раніше засуджених, а також осіб, які підтримують збройну агресію 27 проти України та ін. [3, с. 25-27].

Отже, сучасні соціально-економічні та воєнно-політичні умови в Україні зумовлюють істотне зростання криміногенних ризиків у молодіжному середовищі. Молодь є однією з найбільш соціально та психологічно вразливих категорій населення, що підвищує імовірність її залучення до протиправної діяльності, зокрема:

- злочинів майнового і насильницького характеру;
- незаконного обігу наркотичних засобів;
- участі у деструктивних інтернет-спільнотах;
- діяльності організованих молодіжних угруповань.

З урахуванням сучасних викликів для підвищення ефективності протидії молодіжній злочинності, правоохоронним органам необхідно:

- удосконалювати стратегію і тактику оперативно-розшукової діяльності;
- здійснювати постійний моніторинг криміногенної ситуації;
- прогнозувати поведінку кримінально налаштованих молодих осіб;
- здійснювати контроль за формуванням неформальних та криміналізованих молодіжних об’єднань;
- проводити системну індивідуальну та загальну профілактику;
- розширювати міжвідомчу взаємодію.

Протидія молодіжній злочинності в умовах воєнного стану є складовою системи національної безпеки та одним із ключових чинників збереження державності, громадянської стабільності й правопорядку в Україні.

За таких умов особливого значення набуває своєчасне виявлення криміногенних тенденцій та формування ефективної системи запобігання злочинності серед молоді.

Інформаційно-аналітичне забезпечення оперативно-розшукової діяльності (ІАЗ ОРД) у сфері протидії молодіжній злочинності доцільно розглядати як комплекс взаємопов’язаних організаційних, інформаційних та аналітичних заходів, що здійснюються уповноваженими суб’єктами з метою:

- збирання оперативно-розшукової інформації;
- її накопичення, перевірки та систематизації;
- аналітичної обробки та узагальнення;
- прогнозування криміногенних процесів у молодіжному середовищі.

Основним призначенням ІАЗ ОРД є забезпечення оперативних підрозділів достовірною, повною, актуальною та структурованою інформацією, необхідною для прийняття обґрунтованих тактичних і управлінських рішень. Отримання оперативно-розшукової інформації є початковим і базовим етапом інформаційно-аналітичної роботи. Воно полягає у пошуку, фіксації та первинній перевірці відомостей про:

- підготовку, вчинення або вчинені злочини;
- осіб, причетних до протиправної діяльності;
- криміногенні процеси в молодіжному середовищі.

До традиційних джерел оперативної інформації належать:

- звернення громадян;
- матеріали оперативних обліків;
- агентурні повідомлення;
- результати оперативно-розшукових заходів;
- матеріали досудового розслідування;
- інформація інших правоохоронних органів.

Сучасна молодь є високодиджиталізованою соціальною групою, основна комунікація якої відбувається у цифровому середовищі. Соціальні мережі, месенджери та онлайн-платформи виступають не лише каналами спілкування, а й середовищем поширення криміногенного та деструктивного контенту [5].

Цифрове комунікативне середовище молодіжних груп характеризується:

- високою інтенсивністю комунікації;
- швидким поширенням інформації;
- автономністю та анонімністю користувачів;
- глобальним доступом до інформаційних ресурсів.

У зв’язку з цим особливого значення набуває аналіз так званих «цифрових слідів», зокрема:

- моніторинг соціальних мереж та інтернет-спільнот;
- аналіз контенту, що пропагує насильство, наркотики, екстремізм;
- виявлення каналів вербування молоді до злочинної діяльності;
- ідентифікація лідерів та координаторів молодіжних угруповань.

Моніторинг цифрової комунікації молодіжних груп є важливим елементом початкового етапу інформаційно-аналітичної роботи.

Його основними завданнями є:

- раннє виявлення криміногенних тенденцій;
- ідентифікація груп підвищеного ризику;
- фіксація каналів поширення протиправного контенту;
- формування профілю загроз;
- підготовка аналітичних висновків для прийняття управлінських рішень.

Моніторинг здійснюється шляхом аналізу відкритих джерел [22]:

- публічних профілів у соціальних мережах;
- відкритих груп і форумів;
- доступних статистичних та аналітичних звітів;
- матеріалів громадських і дослідницьких організацій.

Систематизація оперативно-розшукової інформації полягає в упорядкуванні отриманих відомостей із використанням технічних і програмних

засобів. Інформаційну основу діяльності оперативних підрозділів становлять автоматизовані інформаційні системи, які забезпечують:

- облік оперативної інформації;
- накопичення та зберігання масивів даних;
- пошук та узагальнення відомостей;
- формування аналітичних продуктів;
- оцінювання криміногенних ризиків.

Поєднання даних ЄРДР, оперативно-криміналістичних обліків, звернень громадян, інформації інших органів та відкритих джерел створює основу для комплексного аналізу криміногенної ситуації в молодіжному середовищі.

Інформаційно-аналітичне забезпечення ОРД здійснюється виключно в межах чинного законодавства України з дотриманням принципів:

- законності;
- поваги до прав і свобод людини;
- конфіденційності;
- пропорційності втручання у приватне життя.

До основних правових і етичних обмежень належать:

- недопустимість незаконного втручання в особисте і сімейне життя;
- заборона збору інформації без правових підстав;
- дотримання режиму захисту персональних даних;
- використання інформації виключно в цілях ОРД та кримінального провадження;
- забезпечення балансу між публічними та приватними інтересами.

Особливого значення набуває захист прав неповнолітніх як найбільш уразливої категорії населення.

Ефективне ІАЗ ОРД дозволяє:

- своєчасно виявляти криміногенні тенденції;
- прогнозувати розвиток злочинних проявів;
- ідентифікувати організаторів та активних учасників угруповань;
- запобігати злочинам на ранніх стадіях;
- формувати обґрунтовані управлінські рішення.

Таким чином, інформаційно-аналітичне забезпечення є ключовим інструментом сучасної оперативно-розшукової діяльності у сфері протидії молодіжній злочинності та важливою складовою державної політики у сфері безпеки.

3. Організаційні та тактичні особливості проведення допиту підозрюваних при розслідуванні групових злочинів неформальної молоді: особливості отримання інформації, забезпечення законності, недопущення порушень прав людини.

Не занурюючись у детальний аналіз підходів до розуміння теоретичної сутності допиту, зазначимо, що ознайомлення із юридичною літературою демонструє одностайність у підходах вчених-криміналістів щодо цієї слідчої (розшукової) дії, яка традиційно розглядається як інформаційно-психологічний процес спілкування, спрямований на отримання інформації (фактичних даних, усних відомостей) про відомі допитуваному обставини справи, які мають доказове значення. При цьому мета, об'єкт, форма отримання відомостей обумовлюється загальним тактичним завданням - отримання повних і правдивих показань і зведення до мінімуму можливостей мимовільних перекручень. Окрім цього, як цілком слушно зауважують М. Климчук та Я. Фурман, окреслюючи тактичні особливості допиту як слідчої дії [6, с. 175], слід враховувати, що інформація, яка передається під час допиту не позбавлена «особистісного» відтінку, оскільки її сприйняття, фіксування у пам'яті має низку особливостей, обумовлених віковими особливостями, психічним та психологічним станом, моральними принципами та освітнім рівнем особи, що допитується, часом та місцем проведення тощо.

Виходячи із загальних положень криміналістичної тактики допит, як і будь-яка інша слідча (розшукова) дія, складається з трьох етапів:

- *підготовка до проведення (підготовчий*), спрямований на вирішення слідчим організаційних питань та детальну алгоритмізацію дій (організаційно-підготовчі заходи дозволять уникнути його поверховості та безрезультативності);
- *безпосередній (робочий)* - безпосередня процесуальна форма спілкування, змістом якої є одержання інформації, що стосується розслідуваної події;
- *заключний*, під час якого аналізується та фіксується хід та результат допиту.

Окреслюючи підготовчий етап проведення допиту особи, яка є підозрюваною у вчиненні кримінального правопорушення, слід підтримати слушне зауваження М. Климчука, Я. Фурман, В. Шепітько, які зазначають, що з метою поставлених цілей слідчий повинен підготуватися до проведення допиту, і враховуючи той факт, що допит є найбільш індивідуальною слідчою (розшуковою) дією залежно від ситуації правильно обрати найбільш раціональний та ефективний спосіб дій або найбільш доцільну лінію поведінки, тобто тактичні прийоми, які за своєю сутністю мають сприяти виявленню інформаційного матеріалу та встановленню істини у справі [6, с. 175, 7 с. 82].

Враховуючи напрацювання криміналістичної літератури щодо організаційно-підготовчих заходів до проведення допиту (дослідження А. Волобуєва, М. Климчука, О. Кремінського, Л. Омельчук, А. Плосконоса, К. Чаплинського та ін.), а також поділяючи позицію К. Чаплинського, який слушно пропонує у підготовці до допиту виділяти три рівні:

- пізнавальний (вивчення матеріалів кримінальної справи та особи злочинця, ознайомлення з оперативно-розшуковою інформацією);

- прогностичний (визначення кола осіб, які підлягають допиту та послідовність їх проведення);

- синтезуючий (визначення місця і часу проведення слідчої дії, способу виклику на допит, складання плану допиту) [8, с. 143].

Вважаємо за доцільне слідчому застосовувати комплекс організаційно-підготовчих заходів до допиту підозрюваної особи при розслідуванні групових злочинів неформальної молоді, серед яких:

1) *ретельне і всебічне вивчення слідчим матеріалів справи*, що містяться у протоколах слідчих дій та інших матеріалах справи, пов'язані з оглядом місця події, відеозаписи та фотографії, протоколи огляду речових доказів та допитів потерпілих. Слід зауважити, що при розслідуванні даної категорії справ, слід приділи увагу аналізу наявної інформації щодо місця вчинення дій, оскільки це дозволить не лише визначитися із майбутньою тактикою допиту, але й «намітити» можливі шляхи отримання інформації, якої бракує для подальшого розслідування.

2) визначення предмету допиту. Це дозволить заздалегідь сформувати найбільш важливі запитання, продумати майбутній допит підозрюваного до дрібних деталей та визначитися із системою найбільш доцільних тактичних прийомів. Враховуючи специфіку допиту підозрюваних, які вчиняють кримінальне правопорушення одноособово або у складі угруповання, при визначенні предмету допиту необхідно вивчити та враховувати обставини щодо особи підозрюваного (вік, рівень інтелекту, схильності, темперамент, спосіб життя, особливості поведінки осіб, які вчиняють такі злочини тощо), проаналізувати причини та умови, що сприяли вчиненню злочину.

Як слушно зауважує А. Масалітін інформацію про підозрюваного 16-22 років можна отримати з Інтернету, соціальних мереж, відео сервісів [9, с. 145]. Цю інформацію, як і інформацію, отриману під час інших допитів, (свідків, потерпілих), огляду місця події, обшуків та інших процесуальних дій, слідчий використовує під час допиту підозрюваних.

Враховуючи той факт, що допит є слідчою (розшуковою) дією, без якої не може обійтися розслідування майже жодного кримінального правопорушення, адже показання підозрюваних є тим джерелом доказів, від якого найчастіше залежать подальші перспективи та хід розслідування, встановлення «цілісної картини» кримінального правопорушення, а його тактичним прийомам

присвячено досить велику кількість наукових праць (дослідження І. Биховського, Л. Карнєєвої, В. Комаркова, В. Коновалової, К. Чаплинського, М. Яблокова та ін.), вважаємо за доцільне окреслити ключові підходи до допиту підозрюваних при розслідуванні групових злочинів неформальної молоді крізь призму можливостей, які створює впровадження процесуального інтерв'ю, адже згідно з дослідженням «Розкажи мені, що сталося, або зізнайся» (2020 р.), 61% слідчих повністю або радше погоджуються з тезою, що успішним допит можна вважати лише тоді, коли підозрювана особа розповіла про всі обставини вчиненого нею злочину, тобто зізналася. І таке ставлення до допиту як інструменту досудового розслідування має свої окремі причини, однією з яких є фрагментарна та застаріла система підготовки правоохоронців з питань проведення допитів [11, с. 114-115]. Беручи до уваги особистість правопрушника (зазвичай це особи чоловічої статі віком від 14 до 35 років, не одружені, мають середню освіту, іноді вищу та є членами офіційного або неформального клубу). Непоодинокими є випадки, коли зазначені особи мають розлади психіки, можна навіть казати про «дефекти психічного самовладання» [11, с. 109], враховуючи складність і специфіку допиту підозрюваних, які входять до молодіжного угрупування, вважаємо за доцільне зупинитися на ключових аспектах зміни парадигми комунікації при безпосередньому проведенні зазначеної процесуальної дії. Цілком справедливим вбачається зауваження Ю. Бєлоусова, А. Орлеана, Т. Філоненка, які наголошують на тому, що в Україні практика проведення допитів є спадком обвинувального (accusatorial) підходу, який притаманний країнам з тоталітарним та посттоталітарним режимом, коли слідчий, з метою економії часу, підходить до вибору тактичних прийомів допиту, виходячи з позиції винуватості особи, використовуючи різноманітні психологічні маніпулятивні тактики для отримання згоди підозрюваного у формі зізнання [10].

Обираючи тактику допиту підозрюваних при розслідуванні групових злочинів неформальної молоді, доцільно враховувати світові стандарти його проведення, які, перш за все базуються на використанні непримусових, таких, що відповідають етичним принципам практиках, спрямованих запобігти отриманню зізнання «будь-якою ціною», в тому числі і шляхом порушення прав людини (ізоляції підозрюваного у невеликій кімнаті для переживання тривоги, незахищеності, невпевненості; психологічного тиску, залякування та погроз, використання обману, маніпулювання фактами тощо).

При допиті підозрюваних, які входять до складу молодіжного угруповання, доцільним є застосування методики процесуального інтерв'ю, тобто входження у комунікацію без жодних упереджень шляхом демонстрації доброзичливого та неупередженого ставлення, щирої зацікавленості цінностями відповідного угрупування та встановлення психологічного контакту.

4. Забезпечення прав потерпілих на доступ до інформації під час розслідування злочинів проти життя та здоров'я особи, учинених членами молодіжних неформальних груп (об'єднань).

Враховуючи євроінтеграційний вектор розвитку нашої держави, необхідно зауважити, що однією з вимог до кримінального процесуального законодавства є його функціональна спроможність бути реальним процедурним механізмом попередження негативних наслідків кримінальної процедури для потерпілого [13, с. 69]. Сучасний розвиток правничої науки характеризується тенденціями, які, як цілком справедливо наголошують І. Антюк, Д. Клепка, А. Крижановський, О. Новіков, С. Сорока, А. Хоцька, О. Щиголь, наразі спостерігаються у кримінальному процесі: поступовим переходом від обвинувального характеру кримінального провадження, де вся увага сфокусована на підозрюваному/обвинуваченому, до компенсаційного характеру, який передбачає, що саме потерпілий та його права і свободи є пріоритетними (окремі науковці навіть пропонують виокремити самостійну засаду кримінального провадження - процесуальний віктимоцентризм, змістом якої є закріплення механізмів якнайкращого забезпеченні прав та законних інтересів потерпілого у ході здійснення кримінального провадження) [14, с. 184], акцентують увагу на необхідності реалізації принципів «потерпіло-орієнтованого» підходу в кримінальному правосудді та комплекс заходів для його реалізації, зокрема, при розслідуванні воєнних кримінальних правопорушень [15, с. 260].

Враховуючи специфіку злочинів, що вчиняються членами молодіжних неформальних груп (об'єднань) проти життя та здоров'я особи, розглянемо рекомендації, розроблені міжнародними та національними інституціями, науковцями, юристами, які можуть стати базисом для формування підходу, орієнтованого на потерпілого, що дозволить ліквідувати диспропорцію обсягів процесуальних прав потерпілого та обвинуваченого при розслідуванні злочинів зазначеної категорії.

Серед найбільш суттєвих прогалин у законодавстві, що суттєво ускладнюють, а іноді унеможливлюють ефективний захист прав потерпілого визнаються:

- відсутність чітко врегульованої процедури визнання особи потерпілою у рамках кримінального провадження, що ускладнює набуття особою відповідного процесуального захисту з метою своїх прав та законних інтересів, ситуації відмови фактичним потерпілим у визнанні їх потерпілими у рамках кримінального провадження через невідповідність встановленим критеріям [16, с. 201];

- формальний характер прав потерпілого (так, видається цілком слушним зауваження С. Сороки, А. Крижановського, які зазначають, що хоча потерпілому і вручають пам'ятку про процесуальні права та обов'язки, але потерпілі не завжди користуються своїми правами [17]);

- відсутність професійного адвоката, що впливає на активність потерпілих щодо захисту своїх прав. У разі необхідності потерпілому слід надати соціальну допомогу, оскільки він повинен мати доступ до спеціальних систем підтримки (медичної, соціальної, психологічної допомоги [18]);

- дисбаланс у питанні збору доказів (поділяємо позицію О. Щиголь, що поза увагою законодавця залишається питання пошуку та збору потерпілим доказів, які згодом можуть бути подані на підставі п. 3 ч. 1 ст. 56 КПК України. Наразі у КПК України центральними суб'єктами збирання доказів є саме органи досудового розслідування [18, с. 290-291]. Зважаючи на незворотність європейського курсу України, отримання Україною статусу кандидата на членство в ЄС, варто звернути увагу на європейські стандарти виміру прав потерпілих, що можуть стати орієнтиром як для удосконалення вітчизняного кримінально-процесуального законодавства, так і слідчої практики при розслідуванні злочинів проти життя та здоров'я особи, учинених членами молодіжних неформальних груп (об'єднань). Передусім зауважимо на ключових пріоритетах задекларованих у Стратегії ЄС щодо прав потерпілих (2020-2025), серед яких:

1) ефективна комунікація з потерпілими та безпечне середовище для повідомлення про злочини;

2) покращення підтримки та захисту найбільш уразливих потерпілих;

3) кращі можливості потерпілих у питанні виплати компенсації;

4) зміцнення співпраці та координації між усіма відповідними учасниками/цями;

5) посилення міжнародного виміру прав потерпілих [19].

Основними документами, що містять міжнародні стандарти фізичного та психологічного захисту потерпілих, є: Директива 2012/29/ЄС Європейського Парламенту та Ради від 25 жовтня 2012 року (надалі - Директива), що встановлює мінімальні стандарти щодо прав, підтримки та захисту постраждалих від злочинів і замінює Рамкове рішення Ради 2001/220/ЈНА (Директива про права потерпілих) - передбачає **право на доступ до інформації**, право на підтримку та захист відповідно до індивідуальних потреб потерпілих, а також комплекс процесуальних прав; Директива Ради 2004/80/ЄС від 29 квітня 2004 року щодо компенсації постраждалим від злочинів (Директива про компенсацію), Директива 2011/99/ЄС Європейського Парламенту та Ради від 13 грудня 2011 року про Європейський захисний ордер та рекомендація Rec (2005) 9 комітету міністрів ради Європи державам-членам щодо захисту свідків та осіб, які співпрацюють з правосуддям.

Перш за все зупинимося на аналізі положень Директиви для взаємодії з потерпілим під час розслідування злочинів проти життя та здоров'я особи, учинених членами молодіжних неформальних груп (об'єднань): право на отримання інформації з першого контакту з компетентним органом задля

забезпечення можливості користуватися правами, зокрема надання основної інформації про доступ до медичної підтримки, будь-якої фахової підтримки, в тому числі психологічної підтримки та альтернативного житла (ст. 4), право на доступ до служб підтримки постраждалих та підтримку служб підтримки постраждалих: інформаційну, консультаційну, емоційну (ст.ст. 8, 9), права у разі прийняття рішення про відмову в порушенні кримінальної справи (ст. 11), право на гарантії в контексті послуг відновного правосуддя (ст. 12), право на захист, втому числі від вторинної та повторної віктимізації, від залякування та помсти, у тому числі від ризику емоційної чи психологічної шкоди, а також для захисту гідності постраждалих під час допиту та надання свідчень (ст. 18), право уникати контакту між постраждалою особою та правопорушником (ст. 19).

Особливу увагу слід зосередити на правилах захисту потерпілих, передбачених ст. 20 Директиви: забезпечення проведення опитування постраждалих без невиправданої затримки після того, як скарга щодо кримінального правопорушення була подана до компетентного органу; кількість допитів постраждалих повинна бути зведена до мінімуму, а допити проводяться лише тоді, коли це вкрай необхідно для цілей кримінального розслідування; медичні огляди повинні бути зведені до мінімуму та проводитися лише у випадках, коли це вкрай необхідно для цілей кримінального провадження. Зазначені правила повинні бути дотримані правоохоронними органами при взаємодії з потерпілими при розслідуванні злочинів проти життя та здоров'я особи, учинених членами молодіжних неформальних груп (об'єднань).

Крім того, нові контури цілісного підходу до прав потерпілих в контексті подальшого розвитку та розширення прав потерпілих та послуг для них поза межами кримінального провадження, сформульовані у Рекомендації CM/Rec(2023)2 Комітету міністрів державам-членам щодо прав, послуг і підтримки жертв злочинів, яку було прийнято Комітетом міністрів 15 березня 2023 р. на 1460-му засіданні заступників міністрів, в якій наголошено на важливості забезпечення індивідуальної оцінки жертв злочинів, яка повинна, зокрема, враховувати особисті характеристики потерпілого, вид або характер злочину та обставини його вчинення, з метою визначення конкретних потреб у захисті та питань ефективності процесуальних засобів щодо конкретного потерпілого (ст. 4), та визначено фундаментальні права жертв кримінальних правопорушень.

Розслідування злочинів проти життя та здоров'я, учинених членами молодіжних неформальних груп (об'єднань), має бути зорієнтовано, насамперед, на забезпечення прав та законних інтересів потерпілого [21, с. 830]. Аналіз міжнародних правових принципів і стандартів дозволяє виокремити комплекс заходів за допомогою яких вбачається можливим реалізація зазначеного підходу: інформованість та надання першочергової правової, соціальної та медичної допомоги (зокрема, надання постраждалим особам

інформації стосовно їх процесуальних прав, зокрема на захист та отримання компенсації, а також можливості звернення до спеціалізованих служб підтримки, надання інформації про заходи, які можуть бути застосовані правоохоронними органами для захисту від залякування); фізичний та психологічний захист потерпілих; спеціальна тактика допиту та мінімізація повторної віктимізації (зокрема, слідчим мають враховуватися вікові та психологічні особливості, стан здоров'я та місце проведення допиту (вдома у потерпілого, у закладі охорони здоров'я, де він проходить лікування або у кабінеті слідчого)); використання аудіовізуальних записів для мінімізації допитів; забезпечення відшкодування шкоди.

5. Спеціальна техніка та інформаційне забезпечення розслідування групових злочинів неформальної молоді.

Розслідування злочинів, учинених членами молодіжних неформальних груп, вимагає застосування спеціальних технічних засобів. *Спеціальна техніка* - це обладнання, технічні пристрої, транспортні та криміналістичні засоби, які підвищують ефективність розслідування в умовах обмеженості часу, потенційної протидії та тактичних ризиків.

Усталеною є думка, що спеціальну техніку, яка використовується оперативними та слідчими підрозділами, можна поділити на три групи [12, с. 327]:

спеціальна техніка, яка надходить у готовому вигляді (деякі види автотранспорту, апаратура зв'язку, оптико-механічні прилади спостереження, вимірювальні прилади, фото- і відеотехніка, обчислювальна та інша налаштована на спеціальні потреби техніка);

спеціальна техніка, модернізована для виконання специфічних завдань і умов діяльності оперативно-слідчих підрозділів (автозасоби, обладнані радіостанціями, засобами підсилення звуку; засоби маскування та дистанційного управління для різних фото- та відеокамер; персональні ЕОМ, на базі яких створені автоматизовані робочі місця для співробітників оперативних і слідчих підрозділів органів державної безпеки);

спеціальна техніка, розроблена та виготовлена спеціально для оперативно-слідчих органів з найбільш повним урахуванням специфіки їхніх завдань та умов роботи.

Завдяки використанню спеціальної техніки вирішують такі основні завдання:

- ✓ Запобігання злочинам (охоронні сигналізації, оперативні обліки).
- ✓ Припинення порушень громадського порядку та хуліганських дій (засоби захисту особового складу, спецоперації).
- ✓ Виявлення речових доказів (пошукові прилади, хімічні пастки під час огляду).

- ✓ Отримання та документування достовірних даних про осіб, причетних до злочинів (апаратура звуко- та відеозапису, прилади спостереження, радіоактивні ізотопи).
- ✓ Проведення оперативно-розшукових заходів щодо затримання правопорушників (радіозв'язок, прилади нічного бачення, оперативне дактилоскопіювання).
- ✓ Ефективне управління оперативними групами (радіостанції для мобільності та маневреності).

Аналіз причин скоєння злочинів та умов, що сприяють їх вчиненню (обчислювальна техніка для аналізу даних та прогнозування).

Застосування деяких видів спеціальної техніки під час розслідування групових злочинів неформальної молоді:

- Водомети, бронемашини та інші спецзасоби - використовуються для припинення масових заворушень, групових нападів, затримання озброєних осіб (ЗУ «Про національну поліцію», ст. 45).
- Електрошокери - застосовуються для зупинки групових дій, відбиття нападу, з можливістю комбінованого використання з іншими засобами.
- Засоби індивідуального захисту - бронежилети (клас від 1до 6+, захист від куль та уламків), шоломи (протиударні та балістичні), респіратори, протигази, спеціальне взуття та наколінники.

Інформаційне забезпечення – це аналітична діяльність слідчих, прокурорів та оперативних співробітників, спрямована на виявлення, документування та аналіз злочинної діяльності молодіжних неформальних груп.

Джерела інформаційного забезпечення:

1. Інформаційні системи - криміналістичні обліки, бази даних.
2. Матеріали кримінального провадження - протоколи, свідчення, результати експертиз.
3. Матеріали оперативно-розшукової справи - інформація, зібрана під час слідчих та оперативних заходів.
4. Відкриті джерела інформації - соціальні мережі, Інтернет-ресурси, публічні бази даних.

Завдання інформаційного забезпечення:

- встановлення осіб, причетних до злочинів;
- аналіз причин та умов, що сприяють вчиненню злочинів;
- підготовка матеріалів для ефективного планування оперативних заходів;
- використання сучасних аналітичних методів для прогнозування та профілактики правопорушень.

Використана література:

1. Молодь України: виклики та адаптація в умовах воєнного стану: інформаційно-аналітичні матеріали до державної доповіді про становище молоді в Україні / В. О. Радкевич, М. А. Пригодій, Т. М. Герлянд, О. А. Тітова, В. А. Кручек, О. В. Лапа, Д. О. Закатнов, Л. А. Лупаренко. Київ : Інститут професійної освіти НАПН України, 2025. 37 с.

2. Cedos. Центр досліджень соціальних трансформацій 2024. Вплив війни на молодь в Україні. URL: https://cedos.org.ua/researches/vpliv-vijni-na-molod-v-ukrayini/ (дата звернення: 11.12.2025).

3. Бабакін В. Протидія молодіжній злочинності як елемент національної безпеки в умовах воєнного стану. О*рганізаційно-правове забезпечення національної безпеки в умовах воєнного стану :* матеріали Всеукр. наук.-практ. конф. (м. Кропивницький, 7 липня 2023 р.). Кропивницький, 2023. С. 23-27.

4. Офіс Генерального прокурора України. Статистичні дані URL: https://new.gp.gov.ua/ua/posts/statistika (дата звернення: 22.06.2023).

5. Пирожкова Ю. В., Ларкін М. О., Мельковський О. В. Інформаційно-аналітичне забезпечення оперативно-розшукової діяльності у протидії молодіжній злочинності: правові та організаційно-технологічні аспекти. *Електронне наукове видання «Аналітично-порівняльне правознавство»*. 2026. № С. 345-354.

6. Климчук М. П., Фурман Я. В. Тактичні особливості допиту підозрюваних - членів організованих злочинних угруповань. *Юридичний науковий електронний журнал.* 2017. № 1. С. 174-177. URL: http://www.lsej.org.ua/1_2017/45.pdf (дата звернення: 22.06.2023).

7. Настільна книга слідчого / М. П. Панов, В. М. Шепітько, В. О. Коновалова та ін. Київ : Вид. дім «Ін Юре», 2011. 736 с.

8. Чаплинський К. О. Тактика проведення окремих слідчих дій : монографія. Дніпропетровськ : РВВ ДДУВС, 2006. 416 с.

9. Масалітін А. О. Розслідування злочинів, що вчиняються учасниками угруповань футбольних уболівальників : дис. … канд. юрид. наук : 12.00.09. Київ, 2019. 190 с.

10. Пирожкова Ю. В. Допит при розслідуванні хуліганства, вчиненого футбольними вболівальниками крізь призму дотримання прав людини. *Забезпечення правопорядку та протидії злочинності в Україні та у світі: проблеми та шляхи їх вирішення.* матеріали ІІІ Міжнар. наук.-практ. конф. (м. Дніпро, 16 черв. 2023 р.). Дніпро, 2023. С. 113-115.

11. Ларкін М. О. Криміналістична характеристика хуліганства, що вчиняється футбольними уболівальниками (фанами). *Вісник Запорізького національного університету*. 2018. № 4. С. 107-111.

12. Ларкін М. О., Пирожкова Ю. В. Спеціальна техніка та інформаційне забезпечення розслідування групових злочинів неформальної молоді. *Науковий вісник Ужгородського національного університету. Сер. : Право.* 2025. Вип. 92(4). С. 326-331.

13. Єдність судової практики у вимірі стандартів якості кримінального процесуального законодавства України : монографія / за заг. ред. О. Г. Шило. Харків : Право, 2021. 351 с.

14. Щиголь О. В. Нова концепція процесуального становища потерпілого та його представників у кримінальному провадженні з урахуванням засади процесуального віктимоцентризму. *Юридичний вісник*. 2021. № 2. С. 177-185.

15. Клепка Д., Новіков О. Питання забезпечення прав потерпілих під час розслідування воєнних злочинів. *Вісник кримінологічної асоціації України*. 2024. № 1 (31). С. 253-26.

16. Антюк І. П., Хоцька А. А. Забезпечення прав та законних інтересів потерпілого у кримінальному провадженні. *Наукові записки. Сер. : Право*|. Вип. 16. 2024. С. 198-203.

17. Сорока С. О., Крижановський А. С. Захист прав потерпілого під час досудового розслідування. *Вісник Національного університету "Львівська політехніка". Сер. : Юридичні науки*. 2019. Вип. 23. С. 114-122.

18. Нор В. Т. Удосконалення процесуального статусу потерпілого від злочину та системи гарантій захисту його прав і закон-них інтересів. URL: http://radnuk.info/ component/content/ article/24955 (дата звернення 12.12.2025).

19. Щиголь О. Забезпечення прав потерпілого на збирання та подання доказів під час досудового розслідування. *Підприємництво, господарство і право*. 2021. № 3. С. 289-295.

20. Стратегія ЄС щодо прав потерпілих (2020-2025). URL: https://jurfem.com.ua/wp-content/uploads/2023/09.1(дата звернення 12.12.2025).

21. Пирожкова Ю. В. Верлос Н. В., Мельковський О. В. Захист прав потерпілих під час розслідування злочинів проти життя та здоров'я особи, учинених членами молодіжних неформальних груп (об'єднань). *Електронне наукове видання «Аналітично-порівняльне правознавство»*. 2024. № 5. Т. 1. С. 825-830.

22. Пирожкова Ю. В. Моніторинг ризиків цифрової комунікації молодіжних груп як інформаційно-аналітичний інструмент на початковому етапі роботи оперативних підрозділів: баланс безпеки та прав людини. *Актуальні проблеми правової науки та правоохоронної діяльності :* матеріали Всеукр. наук.-практ. конф. (м. Запоріжжя, 22 грудня 2025 р.). Запоріжжя, 2025. С. 38-40.

Питання для обговорення:

1. Охарактеризуйте молодіжну злочинність як соціально-правове явище та чинник криміногенної дестабілізації суспільства.
2. Проаналізуйте сучасний стан та тенденції молодіжної злочинності в Україні в умовах воєнного стану.
3. Охарактеризуйте систему суб'єктів протидії молодіжній злочинності та їх функціональні повноваження.
4. Розкрийте організаційно-правові засади діяльності правоохоронних органів у сфері протидії злочинності серед молоді.
5. Охарактеризуйте роль оперативно-розшукової діяльності у системі протидії молодіжній злочинності.
6. Проаналізуйте інформаційно-аналітичне забезпечення як інструмент запобігання та протидії злочинам, що вчиняються молоддю.
7. Розкрийте значення спеціальної техніки та цифрових технологій у діяльності правоохоронних органів.
8. Охарактеризуйте тактичні особливості отримання достовірної інформації у молодіжному середовищі.
9. Назвіть та проаналізуйте основні джерела інформації про злочинну діяльність молоді.
10. Розкрийте правові та етичні межі використання інформації у протидії молодіжній злочинності.

Тестові завдання:

1. *Молодіжна злочинність у системі національної безпеки України розглядається як:*

а) соціальне явище, що не має правового значення;
б) елемент кримінальної статистики без стратегічного впливу;
в) загроза внутрішній безпеці держави;
г) виключно проблема органів освіти.

2. *Інформаційно-аналітичне забезпечення ОРД спрямоване на:*

а) контроль за діяльністю громадських організацій;
б) формування доказової бази у цивільних справах;
в) забезпечення оперативних підрозділів достовірною інформацією;
г) проведення судових експертиз.

3. *Основною метою інформаційно-аналітичної діяльності є:*

а) архівування кримінальних справ;
б) збір статистичних показників;
в) прийняття обґрунтованих управлінських і тактичних рішень;

г) формування звітності для органів прокуратури.

4. *До відкритих джерел оперативної інформації належать:*

а) агентурні повідомлення;

б) оперативні обліки;

в) соціальні мережі та публічні інтернет-ресурси;

г) матеріали негласних слідчих дій.

5. *Спеціальна техніка в діяльності правоохоронних органів використовується з метою:*

а) забезпечення побутових умов служби;

б) підвищення ефективності розслідування;

в) навчання курсантів;

г) адміністративного управління.

✍Практичні завдання:

1. На підставі офіційних статистичних даних Офісу Генерального прокурора України та МВС України:

- проаналізуйте динаміку злочинності серед осіб віком 14-35 років за останні два роки;
- визначте основні види кримінальних правопорушень, вчинюваних молоддю;
- сформулюйте висновки щодо основних тенденцій розвитку молодіжної злочинності в умовах правового режиму воєнного стану.

Форма звіту: аналітична довідка (2-3 стор.).

2. Розробіть модель інформаційно-аналітичного забезпечення протидії молодіжній злочинності для територіального підрозділу поліції.

У моделі відобразіть:

- суб’єктів інформаційного забезпечення;
- джерела інформації;
- канали збору та обробки даних;
- аналітичні продукти (довідки, зведення, прогнози);
- механізми реагування.

Форма звіту: структурна схема + пояснювальна записка.

3. Група осіб віком 18 - 23 роки через соціальні мережі поширює інформацію про місця дислокації підрозділів ЗСУ, а також збирає кошти нібито на потреби військових, які фактично використовує у власних інтересах.

Необхідно:

1. Дати кримінально-правову кваліфікацію дій осіб.
2. Визначити можливі напрями оперативно-розшукової роботи.

3. Запропонувати першочергові заходи реагування.

Форма звіту: письмове рішення ситуаційної задачі.

4. На основі відкритих джерел інформації (соціальні мережі, форуми, месенджери):

1. Опишіть алгоритм виявлення кримінально активних молодіжних груп.

2. Визначте ризики та правові обмеження використання OSINT.

3. Запропонуйте заходи щодо документування протиправної діяльності.

Форма звіту: методична інструкція (1-2 стор.).

5. Розробіть проєкт комплексної міжвідомчої програми протидії молодіжній злочинності для територіальної громади.

У програмі передбачте:

- профілактичні заходи;
- освітні та інформаційні кампанії;
- роботу з групами ризику;
- залучення органів місцевого самоврядування, закладів освіти та громадських організацій.

*Форма звіту***:** проєкт програми (3-4 стор.).

Рекомендована література:

1. Про Національну поліцію : Закон України від 02.07.2015 № 580-VIII. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text (дата звернення: 23.12.2025).

2. Про оперативно-розшукову діяльність : Закон України від 18.02.1992 № 2135-XII. URL: https://zakon.rada.gov.ua/laws/show/2135-12/card2#Card (дата звернення: 23.12.2025).

3. Про єдину комп’ютерну інформаційну систему правоохоронних органів у боротьбі зі злочинністю : Указ Президента України від 31.01.2006 № 80/2006. URL: https://zakon.rada.gov.ua/laws/show/80/2006#Text (дата звернення: 23.12.2025).

4. Інформаційно-аналітичне забезпечення правоохоронної діяльності : навч. посіб. / Е. В. Рижков, Ю. П. Синиціна, С. О. Прокопов та ін. Дніпро, 2024. 180 с.

5. Верлос Н. В., Пирожкова Ю. В., Мельковський О. В. Особливості проведення оперативно-розшукових заходів та негласних слідчих (розшукових) дій при розслідуванні хуліганства, вчиненого футбольними вболівальниками. *Аналітично-порівняльне правознавство*. 2022. № 5. С. 351-355.

6. Ларкін М. О., Пирожкова Ю. В. Спеціальна техніка та інформаційне забезпечення розслідування групових злочинів неформальної молоді. *Науковий*

вісник Ужгородського національного університету. Сер. : Право. 2025. Вип. 92 (4). С. 326-331.

7. Пирожкова Ю. В., Ларкін М. О., Мельковський О. В. Інформаційно-аналітичне забезпечення оперативно-розшукової діяльності у протидії молодіжній злочинності: правові та організаційно-технологічні аспекти. *Електронне наукове видання «Аналітично-порівняльне правознавство»*. 2026. № С. 345-354.

2. Пирожкова Ю. В. Допит при розслідуванні хуліганства, вчиненого футбольними вболівальниками крізь призму дотримання прав людини. *Забезпечення правопорядку та протидії злочинності в Україні та у світі: проблеми та шляхи їх вирішення.* матеріали III Міжнар. наук.-практ. конф. (м. Дніпро, 16 черв. 2023 р.). Дніпро, 2023. С. 113-115.

3. Сорока С. О., Крижановський А. С. Захист прав потерпілого під час досудового розслідування. *Вісник Національного університету "Львівська політехніка". Сер. : Юридичні науки*. 2019. Вип. 23. С. 114-122.

1. Нор В. Т. Удосконалення процесуального статусу потерпілого від злочину та системи гарантій захисту його прав і законних інтересів. URL: http://radnuk.info/ component/content/ article/24955 (дата звернення: 23.12.2025).

4. Щиголь О. Забезпечення прав потерпілого на збирання та подання доказів під час досудового розслідування. *Підприємництво, господарство і право*. 2021. № 3. С. 289-295.

5. Пирожкова Ю. В. Верлос Н. В., Мельковський О. В. Захист прав потерпілих під час розслідування злочинів проти життя та здоров'я особи, учинених членами молодіжних неформальних груп (об'єднань). *Електронне наукове видання «Аналітично-порівняльне правознавство»*. 2024. № 5. Т. 1. С. 825-830.

6. Пирожкова Ю. В. Моніторинг ризиків цифрової комунікації молодіжних груп як інформаційно-аналітичний інструмент на початковому етапі роботи оперативних підрозділів: баланс безпеки та прав людини. *Актуальні проблеми правової науки та правоохоронної діяльності :* матеріали Всеукр. наук.-практ. конф. (м. Запоріжжя, 22 грудня 2025 р.). Запоріжжя, 2025. С. 38-40.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Бандурка О. М. Оперативно-розшукова діяльність. Частина І : підруч. Харків : НУВС, 2002. 336 с.
2. Бєляков К. І. Інформація в праві: теорія і практика : монографія. Київ : КВІЦ, 2006. 116 с.
3. Єдність судової практики у вимірі стандартів якості кримінального процесуального законодавства України : монографія / за заг. ред. О. Г. Шило. Харків : Право, 2021. 351 с.
4. Закон України «Про застосування англійської мови в Україні»: науково-практичний коментар / Бояров В. І., Ларкін М., Легких К. В., Лобода Ю. А., Макаренков О. Л., Пирожкова Ю. В. ; за заг. ред. М. О. Ларкіна. Київ : Юрінком Інтер, 2025. 164 с.
5. Зарубенко А. О., Дєгтяр О. А. Міжнародні та українські державні механізми правового регулювання кібербезпеки. *Успіхи і досягнення у науці.* 2025. № 11 (21). С. 691-704.
6. Інформаційно-аналітичне забезпечення правоохоронної діяльності : навч. посіб. / Е. В. Рижков, Ю. П. Синиціна, С. О. Прокопов та ін. Дніпро, 2024. 180 с.
7. Ковалів М. В., Єсімов С. С., Ярема О. Г. Інформаційне право : навч. посіб. Львів : ЛьвДУВС, 2016. 280 с.
8. Ларкін М. О. Криміналістична характеристика хуліганства, що вчиняється футбольними уболівальниками (фанами). *Вісник Запорізького національного університету*. 2018. № 4. С. 107-111.
9. Ларкін М. О., Пирожкова Ю. В. Спеціальна техніка та інформаційне забезпечення розслідування групових злочинів неформальної молоді. *Науковий вісник Ужгородського національного університету. Сер. : Право.* 2025. Вип. 92(4). С. 326-331.
10. Лук’янчиков Є. Д. Методологічні засади інформаційного забезпечення розслідування злочинів : монографія. Київ : НАВСУ, 2005. 320 с.
11. Лушер В. В. Поняття інформаційного забезпечення органів прокуратури України. *Форум права*. 2014. № 1. С. 338-341. URL: http://nbuv.gov.ua/UJRN/FP_index (дата звернення 07.01.2026).
12. Масалітін А. О. Розслідування злочинів, що вчиняються учасниками угруповань футбольних уболівальників : дис. … канд. юрид. наук : 12.00.09. Київ, 2019. 190 с.
13. Насонов М. І. Суб’єкти забезпечення інформаційної безпеки в Україні: повноваження, взаємодія, відповідальність. *Наука і техніка сьогодні*. *Сер. : Право*. 2025. № 8 (49). С. 149-157.
14. Настільна книга слідчого / М. П. Панов, В. М. Шепітько, В. О. Коновалова та ін. Київ : Вид. дім «Ін Юре», 2011. 736 с.

15. Основи кримінального аналізу : посіб. з елементами тренінгу / О. Є. Користін та ін. Одеса : ОДУВС, 2016. 112 с.

16. Пирожкова Ю. В. Верлос Н. В., Мельковський О. В. Захист прав потерпілих під час розслідування злочинів проти життя та здоров'я особи, учинених членами молодіжних неформальних груп (об'єднань). *Електронне наукове видання «Аналітично-порівняльне правознавство»*. 2024. № 5. Т. 1. С. 825-830.

17. Пирожкова Ю. В. Допит при розслідуванні хуліганства, вчиненого футбольними вболівальниками крізь призму дотримання прав людини. *Забезпечення правопорядку та протидії злочинності в Україні та у світі: проблеми та шляхи їх вирішення.* матеріали III Міжнар. наук.-практ. конф. (м. Дніпро, 16 черв. 2023 р.). Дніпро, 2023. С. 113-115.

18. Пирожкова Ю. В. Моніторинг ризиків цифрової комунікації молодіжних груп як інформаційно-аналітичний інструмент на початковому етапі роботи оперативних підрозділів: баланс безпеки та прав людини. *Актуальні проблеми правової науки та правоохоронної діяльності :* матеріали Всеукр. наук.-практ. конф. (м. Запоріжжя, 22 грудня 2025 р.). Запоріжжя, 2025. С. 38-40.

19. Пирожкова Ю. В., Ларкін М. О. Англомовна підготовка кадрів правоохоронних органів у контексті Закону України «Про застосування англійської мови в Україні»: організаційні моделі та фінансово-правове забезпечення. *Науковий вісник Ужгородського національного університету. Сер. : Право*. 2025. Випуск 90. Ч. 3. С. 360-366.

20. Про Комплексний стратегічний план реформування органів правопорядку як частини сектору безпеки і оборони України на 2023-2027 роки : Указ президента України від 11.05.2023 № 273/2023. URL: https://www.president.gov.ua/documents/2732023-46733 (дата звернення 07.01.2026).

21. Стратегія ЄС щодо прав потерпілих (2020-2025). URL: https://jurfem.com.ua/wp-content/uploads/2023/09.1(дата звернення 12.12.2025).

22. Хахановський В., Корнейко О. Актуальні питання інформаційного права : навч. посіб. Київ : Право, 2024. 148 с.

23. Чаплинський К. О. Тактика проведення окремих слідчих дій : монографія. Дніпропетровськ : РВВ ДДУВС, 2006. 416 с.

24. Bazzell M. OSINT Techniques: Resources for Uncovering Online Information. CreateSpace Independent Publishing Platform, 2023. 550 p.

25. Borges D. Adversarial Tradecraft in Cybersecurity: Offense versus defense in real-time computer conflict. Packt. 2021. 246 p.

Навчальне видання
(українською мовою)

Юлія Володимирівна Пирожкова
Михайло Олександрович Ларкін

ПРАВОВЕ РЕГУЛЮВАННЯ ВИКОРИСТАННЯ ТА ЗАХИСТУ ІНФОРМАЦІЇ

Навчальний посібник

для здобувачів ступеня вищої освіти бакалавра
спеціальності «Правоохоронна діяльність»
освітньо-професійної програми «Правоохоронна діяльність»

Рецензент *О.В. Мельковський*
Відповідальний за випуск *Р.В. Бараннік*
Коректор *Ю.В. Пирожкова*