РОЗДІЛ 11. МІЖНАРОДНЕ ПРАВО

УДК 327:316
DOI https://doi.org/10.24144/2307-3322.2022.75.3.21

МІЖНАРОДНИЙ ДОСВІД ОРГАНІЗАЦІЇ ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ ДІЯЛЬНОСТІ: ТЕНДЕНЦІЇ НОРМАТИВНО ПРАВОВОЇ СПІВПРАЦІ УКРАЇНИ ТА ЗАРУБІЖНИХ КРАЇН

Адамовський В.І.,
кандидат історичних наук, доцент,
доцент кафедри археології, спеціальних історичних
та правознавчих дисциплін
Кам'янець-Подільського національного університету імені Івана Огієнка
https://orcid.org/0000-0002-9186-6234

Семенюк-Прибатень А.В.,
кандидат юридичних наук
старший викладач кафедри археології, спеціальних історичних та правознавчих дисциплін
Кам'янець-Подільського національного університету імені Івана Огієнка
https://orcid.org/0000-0003-0520-5083

Адамовський В.І., Семенюк-Прибатень А.В. Міжнародний досвід організації інформаційно-аналітичної діяльності: тенденції нормативно правової співпраці України та зарубіжних країн.

Стаття присвячена проблемам інформаційно-аналітичної діяльності крізь призму нормативно-правової співпраці України та зарубіжних держав. У статті визначено інформаційно-аналітичне забезпечення як один з основних елементів організації роботи системи органів державної влади. Ця діяльність зводиться, по-перше, до інформаційно-пошукової роботи, спрямованої на підтримку оперативно-розшукової діяльності, по-друге, до аналітичної роботи, спрямованої на підтримку ухвалення стратегічних рішень у цій сфері та координацію діяльності цих органів. Акцентовано на тому, що аналітичної діяльності є підвищена увага до захисту персональних даних. Особистий характер даних окремих видів інформації, а також використання для їх одержання методів, пов'язаних із вторгненням у приватне життя, надають особливу значущість механізмам нагляду і заходам щодо гарантування безпеки. Розвиток інформаційних технологій зумовив нову потребу захисту особистих даних. Зазначено, що аналітична робота є одним з основних елементів процесу пізнання, що здійснюється в процесі вирішення завдань органів державної влади. Аналітична робота дає змогу шляхом переробки певної недопрацьованої інформації в підсумку отримати знання, на основі яких можуть ухвалюватися відповідні рішення. При цьому обов'язковою умовою ефективного виконання аналітичних заходів є наявність відповідної інформаційної системи. Зроблено висновок, що національна інформаційно-аналітична система не може бути визнана повноцінною, призначеною для аналітичного забезпечення діяльності органів державної влади, без міжнародно-правової системи регламентації персональних даних. Розв'язком розглянутої проблеми може стати практична реалізація інформаційно-аналітичної системи, що охоплює набір сучасних інформаційних технологій у галузі аналітичної обробки даних, застосування підсистем штучного інтелекту, що дають змогу на основі багатокомпонентних модулів проводити зіставлення й аналіз інформації, прогнозувати дії осіб та місця їх можливого знаходження, давати рекомендації щодо організації діяльності органів державної влади.

Ключові слова: Угод про асоціацію між Україною та Європейським Союзом, законодавство ЄС, електронні комунікації, аналітична діяльність, інформаційні технології, відкриті дані, персональні дані, органи державної влади, міжнародна співпраця.

Adamovsky V.I., Semenyuk-Prybaten A.V. International experience of organizing information and analytical activities: trends in regulatory and legal cooperation of Ukraine and foreign countries.

The article is devoted to the problems of information and analytical activity through the prism of regulatory and legal cooperation between Ukraine and foreign countries. The article defines information and analytical support as one of the main elements of the organization of the system of state authorities. This activity is reduced, firstly, to information and research work aimed at supporting operative and investigative activities, and secondly, to analytical work aimed at supporting strategic decision-making in this area and coordinating the activities of these bodies. Emphasis is placed on the fact that analytical activity has increased attention to the protection of personal data. The personal nature of certain types of information, as well as the use of privacy-intrusive methods to obtain them, place particular importance on surveillance mechanisms and measures to ensure security. The development of information technologies led to a new need for personal data protection. It is noted that analytical work is one of the main elements of the process of cognition, which is carried out in the process of solving the tasks of state authorities. Analytical work makes it possible, by processing certain unfinished information, to obtain knowledge on the basis of which appropriate decisions can be made. At the same time, a necessary condition for the effective performance of analytical measures is the availability of an appropriate information system. It was concluded that the national information and analytical system cannot be recognized as full-fledged, intended for analytical support of the activities of state authorities, without an international legal system of regulation of personal data. The solution to the considered problem can be the practical implementation of an information and analytical system, which includes a set of modern information technologies in the field of analytical data processing, the use of artificial intelligence subsystems, which make it possible to compare and analyze information on the basis of multi-component modules, predict the actions of persons and their locations possible location, give recommendations on the organization of activities of state authorities.

Key words: Association Agreement between Ukraine and the European Union, EU legislation, electronic communications, analytical activity, information technologies, open data, personal data, state authorities, international cooperation.

Постановка проблеми. Рівень розвитку сучасного суспільства, процеси інтеграції та глобалізації, які тривають, взаємодія між суб'єктами права за межами територіальних кордонів окремих держав не можуть не враховуватися в організації роботи органів державної влади і окремо країни, і на міжнародному рівні. Нагадаємо, в Угоді про асоціацію між Україною та Європейським Союзом (далі – ЄС) вказано зобов'язання спільно працювати над узгодженням законодавства України із законодавством ЄС про електронні комунікації, у якому BEREC (Орган європейських регуляторів електронних комунікацій) відіграє важливу роль. Угода сприяє співпраці між національним регулятором України та національними регуляторами країн-членів ЄС [1]. Особливе значення це має для інформаційної аналітики як напряму діяльності державних органів.

Інформаційно-аналітичну діяльність традиційно розуміють як сукупність цілеспрямованих дій дослідницько-пізнавального характеру, які здійснюються спеціалізованими підрозділами правоохоронних органів за допомогою інформаційних технологій, системи організаційних заходів і методичних прийомів під час вивчення явищ, що становлять оперативний інтерес [2]. Інформаційно-аналітичне забезпечення як один з основних елементів організації роботи системи органів державної влади загалом зводиться, по-перше, до інформаційно-пошукової роботи, спрямованої на підтримку оперативно-розшукової діяльності, по-друге, до аналітичної роботи, спрямованої на підтримку ухвалення стратегічних рішень у цій сфері та координацію діяльності цих органів. До слова, 1 серпня 2022 року відновив роботу Єдиний державний вебпортал відкритих даних (*data.gov.ua*). Розпорядники інформації вже публікують та оновлюють свої набори даних. Одним із пріоритетів розвитку відкритих даних в Україні є стимулювання їх використання [3].

Особлива актуальність і важливість аналітичної роботи були відзначені Міністерством цифрової трансформації України у 2022 році: «Цифровізація всіх сфер – нові реалії світу. Для побудови успішної цифрової держави потрібно постійно залучати нових кваліфікованих спеціалістів. Зокрема, у сферах кіберзахисту, аналізу даних, штучного інтелекту, роботи з державними реєстрами та захистом персональних даних» [4].

Упродовж останніх кількох десятків років неухильно зростала необхідність у використанні інформації. Державні інформаційні системи, що раніше існували у вигляді архівів з інформаційними картотеками, розвивалися разом з інформаційними технологіями в рамках спеціального програмного забез-

печення і навичок професійного аналізу тієї чи іншої сфери діяльності. У стратегічному і тактичному плані дані можуть бути використані для ухвалення більш точних і виправданих рішень.

Стан дослідження. На сучасному етапі розвитку правової науки дедалі більше уваги вчені приділяють питанням інформаційного забезпечення діяльності органів державної влади. Найважливішу роль у цьому процесі відіграє аналітична робота, що має на озброєнні свої спеціальні види аналізу. Аналітична робота є одним з основних елементів процесу пізнання, що здійснюється в процесі вирішення завдань органів державної влади. Аналітична робота дає змогу шляхом переробки певної недопрацьованої інформації в підсумку отримати знання, на основі яких можуть ухвалюватися відповідні рішення. При цьому обов'язковою умовою ефективного виконання аналітичних заходів є наявність відповідної інформаційної системи. Однак одним із виявлених під час аналізу наукових джерел проблемних питань є недосконаліть наявної інформаційної системи. На важливість удосконалення інформаційної системи державної інформації звертали увагу у своїх працях, зокрема, такі вчені: О.А. Мандзюк, Т.Д. Ганцюк, О.А. Дєгтяр, О.Половцев, М.Ю. Дітковська та ін. Відповідно, соціальні процеси, що постійно ускладнюються, зумовлюють потребу створення спеціалізованих систем зберігання й обробки інформації. Розв'язком цієї проблеми є створення автоматизованих систем використання технічних засобів обробки інформації.

У межах цієї статті не ставимо собі завданням здійснити глибокий аналіз сутності інформаційних систем, натомість наведемо наявні в науковій літературі узагальнені дані щодо поняття інформаційно-аналітичної діяльності в Україні та зарубіжних країнах. З огляду на це, **метою статті** є дослідження міжнародно-правової співпраці України та зарубіжних країн у сфері інформаційно-аналітичної діяльності.

Означене питання становить інтерес не тільки в рамках діяльності державних органів конкретної держави, а й на міжнародному рівні загалом.

Відзначимо, що на сьогодні розроблено низку міжнародних нормативно-правових актів, спрямованих на вироблення загальних принципів і підходів до організації інформаційно-аналітичної діяльності в системі органів державної влади, що дають змогу в оптимальний спосіб збалансувати захист інтересів суспільства щодо запобігання і стримування кримінальних злочинів та підтримання правового порядку, з одного боку, та інтересів особистості і її права на недоторканність приватного життя, з іншого боку. До них варто зарахувати Конвенцію Ради Європи 1981 року про захист фізичних осіб у зв'язку з автоматизованою обробкою персональних даних (ратифікована Україною 2010 року) (далі – Конвенція) [5], Рекомендацію Комітету Міністрів Ради Європи № R(87)15 1987 року про використання персональних даних у діяльності поліції (далі – Рекомендація) [6], Додатковий протокол 2001 року до Конвенції Ради Європи 1981 року про захист фізичних осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних (ратифікований Україною 2010 року) [7] та ін.

У рамках Європейського Союзу зазначене питання врегульовано в положеннях низки директив. Наприклад, у Директиві 95/46/ЄС про захист прав фізичних осіб при обробці персональних даних і про вільне переміщення таких даних наведено критерії для легітимації обробки даних (ст. 7) [8], розширено випадки обмеження права на захист персональних даних (ст. 13), передбачено створення органів нагляду тощо, а в Директиві 2002/58/ЄС щодо обробки персональних даних і захисту конфіденційності в секторі електронних засобів зв'язку закріплено принцип конфіденційності (ст. 15) [9], що забороняє прослуховування, перехоплення, зберігання та інші види втручання або спостереження з боку третіх осіб без згоди заінтересованої особи, передбачено винятки з принципу конфіденційності для випадків захисту національної безпеки, громадського порядку тощо. Також для запобігання, виявлення і розслідування терористичних дій та інших тяжких злочинів Рішенням Ради Європейського Союзу 2008/633/ЈНА передбачено консультаційний доступ до Візової інформаційної системи (ВІС) уповноваженими службовцями держав-членів Європолу [10].

Для Співдружності Незалежних Держав (далі – СНД) правове регулювання розглядуваного питання зосереджено в положеннях модельного закону країн СНД «Про персональні дані», прийнятого постановою на чотирнадцятому пленарному засіданні Міжпарламентської асамблеї держав-учасників СНД від 16 жовтня 1999 року [11]. У цьому законі докладно розкрито правовий режим персональних даних (ст 4), наведено основні форми державного регулювання дій власників персональних даних, а саме ліцензування дій з персональними даними, реєстрація баз персональних даних, реєстрація власників персональних даних, сертифікація інформаційних систем, призначених для обробки персональних даних (ст. 5), пропонується створити спеціальні органи, діяльність яких доповнює наявні можли-

вості захисту прав суб'єктів (ст. 16), описано права суб'єкта персональних даних, права й обов'язки зберігачів персональних даних (ст. 12, 13), низку інших норм, пов'язаних з названим інститутом [11]. Зауважимо, що тільки в деяких державах СНД (Республіка Молдова, Вірменія, Україна, Азербайджан) розроблено та прийнято спеціальні нормативні правові акти, спрямовані на захист персональних даних [12].

Так, в Україні ці питання регулює Закон України «Про захист персональних даних» від 1 червня 2010 року № 2297-VI [13].

Наявний досвід дає змогу визначити основні загальні тенденції та проблеми, що виникають під час організації інформаційно-аналітичної діяльності в Україні. При цьому одним із ключових аспектів є підвищена увага до захисту персональних даних. Особистий характер даних окремих видів інформації, а також використання для їх одержання методів, пов'язаних із вторгненням у приватне життя, надають особливу значущість механізмам нагляду і заходам щодо гарантування безпеки [14]. Розвиток інформаційних технологій зумовив нову потребу захисту особистих даних [15, с. 50; 16, с. 27]. Саме з цієї причини у наведених вище нормативно-правових актах міжнародного характеру розробці поняття персональних даних та принципів поводження з ними, зокрема у сфері діяльності органів державної влади, приділено особливу увагу.

Так, відповідно до Конвенції під персональними даними розуміють будь-яку інформацію про певну фізичну особу, або особу, яка підлягає визначенню («суб'єкт даних») [5]. Якщо персональні дані піддаються автоматизованій обробці, мають бути дотримані такі правила: персональні дані збираються й обробляються на справедливій і законній основі; зберігаються для визначених і законних цілей та не використовуються з іншою метою; є адекватними, не надмірними для зберігання, точними, стосуються справи, за потреби оновлюються; зберігаються у формі, що дозволяє ідентифікувати суб'єкти даних не довше, ніж вимагається для зберігання таких даних.

Міжнародні стандарти у сфері захисту персональних даних зараховують більшість персональних даних, що обробляються правоохоронними органами, з огляду на певну специфіку їх діяльності, до категорії так званих «чутливих» персональних даних, зокрема про расове або етнічне походження людини, політичні, релігійні та світоглядні переконання, членство в політичних партіях або професійних спілках тощо. Цим, зокрема, й пояснюється важливість застосування особливих та додаткових правових гарантій захисту персональних даних під час їх обробки правоохоронними органами, адже що більша чутливість та особливість персональних даних, то більшим стає ризик порушення прав осіб на їх приватне життя [17].

Відповідно до ст. 6 Конвенції та Додаткового протоколу до неї стосовно органів нагляду та транскордонних потоків даних, які Україна ратифікувала 2010 року (Закон № 2438-VI від 06.08.2010 [18]), персональні дані, що свідчать про расову належність, політичні, релігійні чи інші переконання, а також дані, що стосуються здоров'я або статевого життя, не можуть піддаватись автоматизованій обробці, якщо внутрішнє законодавство не забезпечує відповідних гарантій [5]. Це правило також застосовується до персональних даних, що стосуються засудження в кримінальному порядку. Проте ст. 9 Конвенції допускає винятки зі ст. 6, коли таке відхилення передбачене законодавством Сторони та є в демократичному суспільстві необхідним заходом, спрямованим на захист державної та громадської безпеки, фінансових інтересів держави або на боротьбу з кримінальними правопорушеннями [5].

Персональні дані, що стосуються расової належності, політичних поглядів або релігійних чи інших переконань, а також здоров'я або статевого життя, не можуть піддаватися автоматизованій обробці, якщо законодавство не встановлює відповідних гарантій. Це положення діє також щодо персональних даних, що стосуються судимості. Особисті дані використовують тільки за наявності згоди суб'єкта таких даних. При цьому допускається відступ від названого вище режиму, якщо це (відступ) передбачено законодавством конкретної держави і є необхідним засобом у демократичному суспільстві задля: а) захисту безпеки держави, громадської безпеки, валютно-кредитних інтересів держави або припинення кримінальних злочинів; б) захисту суб'єкта даних або прав і свобод інших осіб.

Практика реалізації цього конвенційного положення в різних державах показує, що якщо дані необхідні для запобігання злочинам чи боротьбі зі злочинністю, допускаються винятки щодо згоди суб'єкта, але інші обмеження залишаються в силі.

Існує поняття «закрита інформація», яка є секретною. На таких даних ставиться відповідна відмітка для їх захисту. У зв'язку з відмінностями між позначками і грифами, які використовуються в різних країнах, в урядових і військових організаціях, що діють на міжнародній основі (таких як ЄС або НАТО), увійшли в практику «таблиці відповідності» із зазначенням найменування всіх рівнів секрет-

ності та розшифруванням кожного терміна, наприклад: «restricted» (для службового користування), «confidential» (конфіденційно), «secret» (таємно) та «top secret» (цілком таємно) тощо [19].

Якщо інформація позначається одним із цих грифів, використання даних визначається спеціальними обмеженнями, а доступ до них можуть отримати лише особи з відповідним рівнем допуску. Спеціальні обмеження щодо роботи з інформацією можуть стосуватися не тільки осіб, які мають право отримувати закриту інформацію, але й умов її отримання, носіїв, способів передачі та порядку її знищення. Можливі варіанти, коли за державним законодавством про діяльність правоохоронних органів інформація, яка є у їх віданні або зібрана ними, автоматично вважається закритою, хоча її зміст не є конфіденційним.

У країнах, де діють закони про захист персональних даних і недоторканність приватного життя, створюється офіційний незалежний орган контролю, до якого можна подати скаргу і який уповноважений проводити перевірки та давати обов'язкові до виконання вказівки щодо поводження з особистими даними [20]. Наприклад, у країнах СНД такий орган діє в Республіці Молдова (Національний центр захисту персональних даних Республіки Молдова). У цьому контексті можна згадати такі інституції: Федеральну комісію із захисту персональних даних, створену в Німеччині, і комісарів із захисту персональних даних, які призначаються практично в кожній з німецьких земель; Комісара із захисту персональної інформації в Канаді, який є спеціальним чиновником, що призначається парламентом і відповідальний перед ним; Комісаріат із захисту інформації у Великобританії, який виступає незалежним агентством, забезпечує дотримання дії законодавства в розглядуваній сфері; Національну комісію з інформатики та свобод у Франції [21].

Крім того, суб'єкт даних має право на захист у суді у разі неналежного використання його особистих даних у тій чи іншій формі. На міжнародному рівні зазначене право може бути реалізовано шляхом звернення суб'єкта, наприклад, до Європейського суду з прав людини (далі – ЄСПЛ). Аналіз практики ЄСПЛ, що склалася сьогодні щодо захисту персональних даних суб'єктів від незаконного втручання з боку правоохоронних органів, свідчить про прагнення ЄСПЛ знайти баланс між приватними інтересами кожної людини і суспільними інтересами, захищеними правоохоронними органами.

Ще одним важливим питанням інформаційно-аналітичної діяльності системи органів державної влади різних країн є кадрове забезпечення [22]. Оцінювання значущості інформації, надійності джерела її отримання, сумісності з іншими даними здійснює аналітик. Існує дві основні категорії аналізу: стратегічний аналіз, що забезпечує більш детальний огляд і має довгострокову перспективу, і тактичний аналіз, який фокусується на безпосередніх оперативних питаннях. Стратегічна інформація та дані відображають тенденції потенційних загроз. Тактична інформація і дані відображають конкретну ситуацію або поточну операцію, часто в режимі реального часу. Якісно проведений аналіз дає змогу аналітикові зробити висновок у контексті всіх даних, передбачити розвиток подій і сформувати рекомендації щодо можливих варіантів дій.

Аналіз може розпочати аналітик зі самостійного виявлення аномалій, тенденцій або зв'язків у процесі загального дослідження, проте частіше цю роботу регулюють керівники, які задають питання або ставлять певні завдання. Результати можуть бути представлені в різних форматах залежно від вимог та установок. Вони можуть варіюватися від докладних звітів про складні стратегічні питання до короткої усної доповіді про конкретну операцію. Якісний аналіз має бути переконливим, коротким і доступним, з чіткими і недвозначними рекомендаціями, переконливими доказами. На жаль, якщо інформаційні потоки, джерела та навички аналітика виявляються недостатніми, аналітичний продукт буде неякісним.

У зв'язку з делікатним характером, важливістю інформації, співробітники для роботи з нею повинні мати більш високий рівень ділових якостей. Перевірка здійснюється за допомогою системи безпеки, яка вивчає психологічний стан й оцінює ризик. Кваліфіковані і досвідчені аналітики стають ключем до досягнення ефективного використання інформації і розвідки. Навчання аналітиків досить дороге, і якщо їхня робота недооцінюється, то вони переходять у приватний сектор, де можуть отримувати більшу винагороду за свої послуги. Збереження кадрів – це важливе завдання для будь-якого керівника.

Із зазначеною проблемою тісно пов'язані достатність і своєчасність матеріально-технічного забезпечення інформаційно-аналітичної діяльності. Інформаційний продукт, підготовлений аналітиком, слугує основою у розслідуванні злочинів. Комп'ютерні бази даних, які часто недооцінюються, вимагають значних інвестицій. Так, незважаючи на повсюдне використання ДНК у розслідуванні злочинів, досвід діяльності правоохоронних органів різних держав свідчить про те, що цей відносно новий напрям не отримує необхідної технічної підтримки, і це є перешкодою для ефективної реалізації всіх

її можливостей. Щоправда, ця проблема не стосується такої міжнародної правоохоронної організації як Інтерпол, який має також бази даних відбитків пальців, щодо втрати або крадіжки проїзних документів (SLTD), сексуального насильства над дітьми, копії викрадених творів мистецтва, бази даних викрадених транспортних засобів тощо [23].

Не останнє місце серед актуальних проблем інформаційно-аналітичної діяльності в системі органів державної влади в рамках міжнародного масштабу поідає організація взаємодії, обмін відповідною інформацією. Обмін інформацією є зворотною стороною організації інформаційно-аналітичної діяльності, основаною на взаємній вигоді. Питанням обміну інформацією між, наприклад, правоохоронними органами присвячені положення деяких нормативно-правових актів. Приміром, у ст. 5.1 Рекомендації (про яку ми вище згадували) прямо встановлено, що передача даних між поліцейськими органами для надання допомоги в досягненні цілей поліції дозволяється тільки у випадках, якщо існує правомірний інтерес до такої передачі інформації в межах повноважень зазначених органів. При цьому передача даних іншим публічним установам або приватним особам дозволяється тільки в особливих випадках, таких як: наявність відповідного дозволу на передачу інформації, необхідність в отриманні подібних даних для здійснення одержувачем своїх законних обов'язків, без дозволу суб'єкта даних або обставин, що дозволяють очевидно припустити можливість такої згоди; впевненість у тому, що передача інформації є необхідною умовою для запобігання серйозній небезпеці.

Щодо міжнародного обміну інформацією Рекомендація встановлює заборону для органів поліції на передачу даних закордонним установам (ст. 5.4). Вона стає можливою тільки за наявності національного або міжнародного законодавства із цього питання, а також у випадку, якщо передача інформації є необхідною для відвернення серйозної небезпеки або запобігання серйозному кримінальному правопорушенню згідно з нормами загального права, за умови, що не порушується національне законодавство щодо захисту людини.

Так, Міністерство цифрової трансформації України розширює співпрацю з найбільшою розвідувально-аналітичною компанією у світі Recorded Future. Команда підписала Меморандум у сфері захисту критичної інфраструктури в Україні від військової та кіберагресії з боку Росії. Також домовилися про спільну роботу над створенням нових продуктів і технологій для захисту критичної інфраструктури, які зможуть використовувати в усьому світі. Україна і Recorded Future давно співпрацюють у сфері кібербезпеки. Підписаний меморандум дасть змогу підсилити партнерство та використовувати розвідувальні дані для захисту України у фізичному та кіберпросторі [24].

Досить високий рівень організації взаємодії між відомствами щодо обміну інформацією можна простежити на прикладі Італії. Зокрема, у МВС Італії створено підрозділ – Центр з обробки оперативної інформації, головним завданням якого є обмін даними, що надходять, щодо діяльності мафіозних груп зі службою Верховного комісара з боротьби з мафією, Корпусом карабінерів, Фінансовою гвардією, місцями позбавлення волі і з центрами координації і планування оперативної діяльності підрозділів МВС, що розташовані у 12 найбільших містах Італії (Римі, Турині, Мілані, Неаполі та ін.). Крім того, оперативно-технічний підрозділ МВС Італії Центр із вивчення обстановки здійснює різноманітну діяльність, зокрема із застосуванням технічних засобів для збору оперативної інформації про організовану злочинність та її передачу до оперативних підрозділів міністерства. На нього покладено також підтримання постійного зв'язку з розташованими в Італії представництвами ФБР, Управлінням боротьби з наркотиками та Митного управління США, а також з аналогічними службами країн Євросоюзу для забезпечення чіткого й оперативного обміну інформацією про організовану злочинність [21, с. 41].

Водночас варто також враховувати і той факт, що більшість держав не завжди має змогу легко встановити взаємодію з іншими відомствами всередині країни або за кордоном. Основними причинами є правові норми, що обмежують обмін даними (особливо персональними даними), або побоювання з міркувань безпеки, а також відмінності в цілях і завданнях таких відомств, відсутність необхідної координації їхньої діяльності.

Висновки. Отже, можна зробити висновок про необхідність комплексного підходу до вирішення питання про підвищення ефективності інформаційно-аналітичної діяльності в органах державної влади. Вжиті заходи мають бути спрямовані на забезпечення відповідного рівня нормативного правового регулювання, кадрового, матеріального і технічного забезпечення, а також сприяти своєчасній й ефективній взаємодії між різними структурами і всередині держави, і на міжнародному рівні.

Проаналізувавши наведені відомості про побудову, цілі та завдання інформаційно-аналітичної діяльності, можна зробити висновок, що національна інформаційно-аналітична система не може бути

визнана повноцінною, призначеною для аналітичного забезпечення діяльності органів державної влади, без міжнародно-правової системи регламентації персональних даних. Розв'язком розглянутої проблеми може стати практична реалізація інформаційно-аналітичної системи, що охоплює набір сучасних інформаційних технологій у галузі аналітичної обробки даних, застосування підсистем штучного інтелекту, що дають змогу на основі багатокомпонентних модулів проводити зіставлення й аналіз інформації, прогнозувати дії осіб та місця їх можливого знаходження, давати рекомендації щодо організації діяльності органів державної влади, зокрема і правоохоронних.

Список використаних джерел:

1. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони від 27.06.2014. *База даних «Законодавство України»* / ВР України. URL: https://zakon.rada.gov.ua/laws/show/984_011#Text (дата звернення: 09.12.2022).
2. James G. McGann. 2020 Global Go To Think Tank Index Report / University of Pennsylvania. Pennsylvania, 2021. 366 p. URL: https://repository.upenn.edu/cgi/viewcontent.cgi?article=1019&context=think_tanks (viewed on 09.12.2022).
3. Держслужбовців навчили працювати з відкритими даними завдяки програмуванню. *Офіц. вебсайт Міністерства цифрової трансформації*. 2022. 11 серп. URL: https://thedigital.gov.ua/news/derzhsluzhbovtsiv-navchili-pratsyuvati-z-vidkritimi-danimi-zavdyaki-programuvannyu (дата звернення: 09.12.2022).
4. В Україні з'явиться Президентський університет. Навчання почнеться у 2023 році. *Офіц. вебсайт Міністерства цифрової трансформації*. 2021. 31 трав. URL: https://thedigital.gov.ua/news/v-ukraini-zyavitsya-prezidentskiy-universitet-navchannya-pochnetsya-u-2023-rotsi (дата звернення: 09.12.2022).
5. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних: міжнар. док. від 28.01.1981. *База даних «Законодавство України»* / ВР України. URL: https://zakon.rada.gov.ua/laws/show/994_326#Text (дата звернення: 09.12.2022).
6. Рекомендація Комітету Міністрів Ради Європи № R(87)15 про використання персональних даних у діяльності поліції від 17.09.1987. URL: http://cyberpeace.org.ua/files/rekomendacia_km_radi_evropi_sodo_vikoristanna_personal_nih_danih__sektori_policii.pdf (дата звернення: 09.12.2022).
7. Додатковий протокол до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних від 08.11.2001. *База даних «Законодавство України»* / ВР України. URL: https://zakon.rada.gov.ua/laws/show/994_363#Text (дата звернення: 09.12.2022).
8. Директива 95/46/ЄС Європейського Парламенту і Ради про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних від 24.10.1995. *База даних «Законодавство України»* / ВР України. URL: https://zakon.rada.gov.ua/laws/show/994_242#Text (дата звернення: 09.12.2022).
9. Директива 2002/58/ЄС Європейського Парламенту й Ради ЄС щодо обробки персональних даних і захисту конфіденційності в секторі електронних засобів зв'язку від 12.07.2002. URL: https://ips.ligazakon.net/document/MU02283 (дата звернення: 09.12.2022).
10. Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32008D0633 (viewed on 09.12.2022).
11. Модельный закон «О персональных данных» (принят на 14-м пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ, постановлением от 16.10.1999 № 14–19). URL: https://online.zakon.kz/Document/?doc_id=30076334 (дата обращения: 09.12.2022).
12. Труш О., Гудима О.П., Новік І.С. Інформаційно-аналітичні засоби забезпечення державного управління у провідних країнах світу: досвід для України. *Теорія та практика державного управління.* 2014. Вип. 3. С. 287–295.
13. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. *База даних «Законодавство України»* / ВР України. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 09.12.2022).

14. Мандзюк О.А. Аналітична діяльність в Україні: адміністративно-правові засади регулювання: монографія. Херсон: Вид. дім «Гельветика», 2019. 488 с.
15. Бисага Ю.М., Палінчак М.М., Бєлов Д.М., Данканич М.М. Права людини. Ужгород, 2003. 189 с.
16. Войтович Є. М. Проблемні питання судового контролю в кримінальному процесі України. *Науковий вісник Ужгородського національного університету*. 2021. Вип. 63. С. 284–287.
17. Мервінський О., Мельник К. Правові аспекти організації захисту персональних даних у сфері правоохоронної діяльності відповідно до міжнародних стандартів. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. 2012. Вип. 1 (23). URL: https://ela.kpi.ua/bitstream/123456789/8607/1/23_p5.pdf (дата звернення: 09.12.2022).
18. Про ратифікацію Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додаткового протоколу до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних стосовно органів нагляду та транскордонних потоків даних: Закон України від 06.07.2010 № 2438-VI. *База даних «Законодавство України»* / ВР України. URL: https://zakon.rada.gov.ua/laws/show/2438-17#Text (дата звернення: 09.12.2022).
19. Law Enforcement Analytic Standards (2004), U.S. Dept of Justice and IALEIA. URL: http://it.ojp.gov/ documents/law_enforcement_analytic_standards (viewed on 09.12.2022).
20. Мандзюк О.А. Міжнародний досвід правового регулювання діяльності аналітичних спільнот. *Наукові праці Національного університету «Одеська юридична академія».* 2019. № 25. С. 49–58.
21. Порівняльно-правове дослідження відповідності законодавства України законодавству ЄС у сфері персональних даних / В.М. Брижко, А.І. Радянська, М.Я. Швець. Київ: Тріумф, 2006. 256 с.
22. Ганцюк Т.Д. Інформаційно-аналітичне забезпечення діяльності органів публічної влади в Україні: джерелознавчий аналіз дискурсного поля. *Державне управління: удосконалення та розвиток*. 2018. № 8. URL: http://www.dy.nayka.com.ua/?op=1&z=1287 (дата звернення: 09.12.2022).
23. Brown S.D. Criminal Intelligence: Data Prospecting or Seeking Significance. *International Association of Law Enforcement Intelligence Analysts (IALEIA) Journal*. 2006. № 17, vol. 1.
24. Мінцифра співпрацюватиме з найбільшою розвідувальною компанією у світі Recorded Future у сфері кіберзахисту – підписано Меморандум. *Офіц. вебсайт Міністерства цифрової трансформації*. 2022. 6 груд. URL: https://thedigital.gov.ua/news/mintsifra-spivpratsyuvatime-z-naybilshoyu-rozviduvalnoyu-kompanieyu-u-sviti-recorded-future-u-sferi-kiberzakhistu-pidpisano-memorandum (дата звернення: 09.12.2022).