Дмитро Калюжний,
здобувач вищої освіти третього освітньо-наукового рівня (доктор філософії з Права) Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут», м. Харків. Україна
ORCID: 0009-0006-1709-8405
e-mail: dmitrijkoluznyj555@gmail.com

ПРАВОВІ ЗАСАДИ ВИКОРИСТАННЯ ІКТ В ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ: ЄВРОПЕЙСЬКИЙ ДОСВІД

Анотація: Реформування інформаційного забезпечення правоохоронних органів, яке здійснюється в контексті європейської інтеграції України, обумовлює важливість питань впровадження новітніх інформаційно-комунікаційних технологій, завдяки яким можна значно підвищити продуктивність правоохоронної діяльності У зв'язку з цим, незважаючи на вітчизняні досягнення у справі інформаційного забезпечення службового діяльності правоохоронних органів, особливого значення набуває вивчення європейського і міжнародного досвіду застосування інформаційних технологій та обліку його у вдосконаленні інформаційно-аналітичного забезпечення правоохоронної діяльності в Україні. У зв’язку з існуючим широким розмаїттям інституціоналізованого співробітництва всередині ЄС та з країнами, що не входять до ЄС, транскордонне співробітництво все ще залежить від готовності та бажання використовувати таке співробітництво. Інституційні можливості для ефективної співпраці правоохоронних органів відходять від визначення спільних викликів безпеці. Це призвело до розвитку інституційної, правової та технічної спроможності, що відповідає новим реаліям глобалізованого світу.

Ключові слова: правоохоронна діяльність, інформаційно-комунікаційні технології, міжнародне співробітництво, правове регулювання.

LEGAL BASIS FOR THE USE OF ICT IN LAW ENFORCEMENT: EUROPEAN EXPERIENCE

Abstract: Reforming the information support of law enforcement agencies, which is carried out in the context of Ukraine's European integration, determines the importance of introducing the latest information and communication technologies, which can significantly increase the productivity of law enforcement activities In this regard, despite domestic achievements in the field of information support of law enforcement agencies, the study of European and international experience in the use of information technologies is of particular importance Due to the existing wide variety of institutionalized cooperation within the EU and with non-EU countries, cross-border cooperation still depends on the readiness and willingness to use such cooperation. The

institutional framework for effective law enforcement cooperation is moving away from identifying common security challenges. This has led to the development of institutional, legal and technical capacities that meet the new realities of the globalized world.

Keywords: law enforcement, information and communication technologies, international cooperation, legal regulation.

Сьогодні інформаційне забезпечення правоохоронних органів України вимагає вдосконалення системи протидії злочинам проти життя та здоров'я людини, національної безпеки, а також в економічній, екологічній та інших сферах. Україна стала жертвою збройної агресії зі сторони Росії, тому особливої актуальності набувають питання використання ІКТ при обороні і захисті критичної інфраструктури країни, вдосконалення інформаційних технологій і інтеграція їх до міжнародних інформаційних систем. Це зумовлює необхідність удосконалення ІКТ відповідно до технологічного рівня вимог розвинутих країн і насамперед країн Європейського союзу [1].

4 грудня 2009 року у Києві підписано Угоду між Україною та Європейським поліцейським офісом про стратегічному співробітництві, яке було ратифіковано 5 жовтня 2010 року. Метою цієї угоди є посилення співробітництва держав-членів Європейського Союзу, які діють через Європол, з Україною у запобіганні міжнародній злочинності, їх виявленні, припиненні та розслідуванні таких злочинів у рамках мандату Європолу, зокрема, шляхом обміну стратегічною та технічною інформацією. Однак ця угода не дає повноважень на передачу даних, що належать до встановлення осіб, які вчинили злочини [2].

Державами, що входять до Європейського Союзу, у рамках Європолу організовано єдину автоматизовану систему обліку кримінальних відомостей, що діє з 2002 року. До складових комплексної інформаційно-аналітичної системи TECS (The Europol Computer System), крім власне AIC, також належать аналітичний центр та індексна підсистема. Комп'ютерна система TECS дозволяє одночасно обробити та проаналізувати майже мільйон записів. Вся інформація до системи надається безпосередньо державами-членами ЄС. Кожна з країн має власну організацію-представника у Гаазі, так звану ELOS. Тільки ці організації мають доступ до національних баз даних.

Якщо розглядати інформаційні системи країн Європейського Союзу загалом, то можна бачити, що вони утворені на загальнонаціональному рівні та забезпечують стратегічний аналіз даних, що стосуються функціонування злочинних угруповань. На центральному рівні ведуться узагальнені обліки осіб, які вчинили злочини, та їх дій, готуються пропозиції щодо удосконалення нормативного регулювання роботи кримінальної поліції підтримуються контакти з Інтерполом. І це цілком обґрунтовано, оскільки дозволяє краще спрямовувати та координувати зусилля, враховуючи розширення міжрегіональних та міжнародних контактів, а також міграцію організованих злочинців, що забезпечує більший рівень конспірації при значному вплив

криміналітету на політичні, економічні, а нерідко і правоохоронні структури на місцях, особливо у невеликих містах.

У 2004 році **Європейський Союз (ЄС)** заснував Агентство ЄС з мережевої та інформаційної безпеки (ENISA) [3]. ENISA є експертним центром кібербезпеки в Європі. Він тісно співпрацює з державами-членами ЄС та приватним сектором, щоб сприяти «розвитку культури [безпеки мережі та інформації (NIS)] у суспільстві та з метою підвищення обізнаності про NIS» [4]. ISACA (Асоціація аудиту та контролю інформаційних систем) вважає, що структура для сертифікації кібербезпеки продуктів і послуг ІКТ має бути регіональною, а не національною, і повинна використовувати існуючі глобальні стандарти та найкращі практики. Крім того, слід переконатися, що при розробці продуктів і послуг на початку процесу проектування враховується кібербезпека, щоб уникнути створення нових вразливостей.

Зупинимося на інформаційному забезпеченні деяких країн-членів Європейського Союзу. У розробці та впровадженні корпоративної об'єднаної інформаційної моделі даних для потреб поліції, на нашу думку, на особливу увагу заслуговує досвід **Сполученого Королівства Великої Британії**. Як слушно зауважив В.О. Заросило, реалізація цих відносин під час попередження правопорушень та їх швидкого розкриття у Великій Британії забезпечується запровадженням новітніх комп'ютерних відеоспостережень, створених завдяки фінансуванню міських адміністрацій та приватних підприємств [5]. Так, з 2013 року до National Crime Agency (NCA) (Національного кримінального агентства) передано інформаційну систему The National Policing Improvement Agency (NPIA). Доступ до неї мають усі територіальні поліцейські сили Великої Британії, поліція Північної Ірландії (PSNI), Британська транспортна поліція (BTP), поліцейська служба Шотландії, Національна служба ідентифікації (NIS), Національне агентство зі злочинності (NCA), Служба безпеки (MI-5) і Секретна розвідувальна служба (MI-6), Асоціація начальників поліції (ACPO) та інші [6].

Національна база даних ДНК кримінальної розвідки Великої Британії National Criminal Intelligence DNA Database (NDNAD) створена 1995 року. Вона перебуває у віданні Міністерства внутрішніх справ Великої Британії. Дані, що містяться в NDNAD, належать поліцейському органу, який надав зразок для аналізу. Зразки зберігаються постійно компаніями, які аналізують їх за щорічну плату. NDNAD Великої Британії у своєму роді є головною і найбільшою у світі базою даних судових ДНК і містить дані щодо приблизно 10% населення, порівняно з 0,5% у США. Дані, що містяться в Національній базі даних ДНК, складаються з даних приватних осіб, відібраних на підставі Закону про поліцію і докази у кримінальних справах, і вилучених за нерозкритими злочинами у вигляді плям (наприклад, від крові, сперми, слини, волосся тощо, що залишилися на місці злочину). Щоразу, коли надходить новий профіль, відбувається автоматичний пошук на збіг серед записів NDNAD між даними фізичних осіб і даними нерозкритих злочинів [1].

У березні 2011 року **французький** парламент ухвалив закон, спрямований на забезпечення внутрішньої безпеки «Loppsi II», що став основою для

модернізації нормативно-правових актів, які стосуються інформаційно-телекомунікаційного забезпечення. Так, запроваджено кримінальну відповідальність за крадіжку особистих даних, поліції надано право підключення до Інтернету та телефонних ліній, а також звернення до провайдерів для фільтрації Інтернет-з'єднання тощо. Також ухваленим законодавчим актом дозволено створення інформаційної платформи, що з'єднує численні державні бази даних. Автоматизована система ідентифікації відбитків пальців осіб, які вчинили злочини або правопорушення - Système d'identification automatique par empreintes digitales (AFIS), створена 1987 року, перебуває у віданні Головного управління судової поліції Міністерства внутрішніх справ та під контролем Генерального прокурора і Апеляційного суду Парижа. Державний автоматизований банк даних судимостей перебуває у віданні міністра юстиції (Департамент у кримінальних справах і помилувань).

Правоохоронні органи **Федеративної Республіки Німеччина** також активно використовують телекомунікаційні засоби та запроваджують інноваційні комп'ютерні технології для ефективного та якісного інформаційного забезпечення своєї службової діяльності. Так, наприклад, інформаційно-пошукова система Федеральної кримінальної поліції - Informationssystem der Polizei (INPOL) - включає базу даних усіх осіб, оголошених у розшук, відомості про викрадені автомобілі, документи тощо. Дані щодо осіб, яких розшукує німецька поліція або судові органи, вже за кілька секунд після внесення до бази стають доступними для всіх користувачів зазначеної системи, а це всі відділення поліції та митні органів ФРН.

У Європі та в усьому світі все частіше розробляються та впроваджуються системи ШІ для різних форм державного стеження і забезпечення правопорядку. Однак, такі тенденції викликають занепокоїння і заперечення з богу окремих фахівців і правозахисних організацій. Від використання біометрії для ідентифікації, розпізнавання та категоризації до систем прогнозування в різних можливостях прийняття рішень і розподілу ресурсів, штучний інтелект у правоохоронних органах непропорційно націлений на вже маргіналізовані спільноти, підриває юридичні та процесуальні права та уможливлює масове стеження. Це означає, що існує ще більший ризик заподіяння шкоди та порушення основних прав і верховенства права. Так, прийняття Акту про штучний інтелект [7] в Європі спричинило звернення Організації громадянського суспільства закликають прийняти цей документ в такій редакції, що запобігатиме неконтрольованим формам дискримінаційного та масового стеження. Щоб захистити права людини та запобігти шкоді від використання штучного інтелекту в поліцейській діяльності, міграційному контролі та національній безпеці, Закон ЄС про штучний інтелект повинен:

- включіть юридичні обмеження, що забороняють ШІ для використання, яке створює неприйнятний ризик для основних прав. Це включає законодавчу заборону на різні форми біометричного стеження, інтелектуальну поліцію та шкідливе використання ШІ в контексті міграції;

- забезпечити публічну прозорість і нагляд, коли поліція, міграційні служби та органи національної безпеки використовують штучний інтелект «високого ризику», дотримуючись однакового обов'язку цих органів реєструвати випадки використання високого ризику в базі даних штучного інтелекту ЄС;

- переконайтеся, що Закон про штучний інтелект належним чином регулює використання штучного інтелекту в поліцейській діяльності, міграції та національній безпеці, що становить загрозу правам людини, зокрема повний перелік штучного інтелекту в міграційному контролі, а також забезпечення того, щоб національна безпека не була виключена зі сфери застосування [8].

Висновки. Спроможність і готовність країн визначати спільні виклики безпеці є однією з передумов ефективної співпраці правоохоронних органів. У зв'язку з існуючим широким розмаїттям інституціоналізованого співробітництва всередині ЄС та з країнами, що не входять до ЄС, транскордонне співробітництво все ще залежить від готовності та бажання використовувати таке співробітництво. Інституційні можливості для ефективної співпраці правоохоронних органів відходять від визначення спільних викликів безпеці. Це призвело до розвитку інституційної, правової та технічної спроможності, що відповідає новим реаліям глобалізованого світу. Ми вважаємо, що ефективна відповідь на майбутні виклики безпеці окремих країн і світової спільноти, спричинені збройними конфліктами, потребує процесу обміну інформацією правоохоронних органів у режимі реального часу та спільної відданості у визначенні загальних викликів безпеці. Таким чином, Україні, з огляду на необхідність створення умов для інтеграції вітчизняних програмних комплексів в інформаційні системи Європейського Союзу, необхідно налагодити співробітництво з правоохоронними відомствами Європейського Союзу з метою удосконалення наявних вітчизняних аналогів та розробки нових, що відповідають світовим стандартам.

Список використаних джерел:

1. Катеринчук І. Міжнародний та зарубіжний досвід застосування інформаційних технологій у діяльності правоохоронних органів // Національний юридичний журнал: теорія та практика. - Червень. - 2015. - С. 22-26. – Режим доступа: https://dspace.oduvs.edu.ua/server/api/core/bitstreams/efd04dce-59c5-49cd-b868-a14881450289/content

2. Угода між Україною та Європейським поліцейським офісом про стратегічне співробітництво: Закон України від 5 жовтня 2010 року № 2576-VI // Офіційний вісник України. –2010. – № 96/№ 84. – Ст. 2934/3432

3. European Union Agency for Network and Information Security (ENISA), 'ENISA: 15 years of building cybersecurity bridges together', Press release, 20 March 2019. URL: https://www.enisa.europa.eu/news/enisa-news/enisa-15-years-of-building-cybersecurity-bridges-together

4. ENISA, About ENISA. URL: https://www.enisa.europa.eu/about-enisa

5. Заросило В. О. Порівняльний аналіз адміністративної діяльності міліції України та поліції зарубіжних країн (Великобританії, США, Канади та Франції) : дис. … канд. юрид. наук : спец. 12.00.07 / В.О. Заросило. – К., 2002. – 250 с. – Режим доступа : http://www.irbis-nbuv.gov.ua/aref/20081124035695

6. Официальный веб-сайт National Crime Agency [Електронний ресурс]. – Режим доступу : http://www.nationalcrimeagency.gov.uk.

7. Regulation of the european parliament and of the council laying down harmonised rules on artificial intelligence (ARTIFICIAL INTELLIGENCE ACT) and amending certain union legislative acts. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206

8. EU policymakers: regulate police technology! URL: https://www.accessnow.org/press-release/eu-regulate-police-technology/