Ярослав Шевчук

кандидат економічних наук,
доцент кафедри загальноправових дисциплін
Навчально-наукового гуманітарного інституту
Національної академії Служби безпеки України
(Київ, Україна)
ORCID ID: https://orcid.org/0009-0006-0585-3581
shevchuk.atc@ssu.gov.ua

DOI: 10.33498/louu-2026-01-277

УДК 342.951:656.072

ДОСВІД ПРАВОВОГО РЕГУЛЮВАННЯ ОБРОБКИ ІНФОРМАЦІЇ ПРО ПАСАЖИРІВ У ВЕЛИКІЙ БРИТАНІЇ ТА МОЖЛИВІ ШЛЯХИ ЙОГО ВПРОВАДЖЕННЯ В УКРАЇНІ

Анотація. Стаття присвячена аналізу досвіду правового регулювання обробки інформації про пасажирів у Великій Британії та можливим шляхам його впровадження в Україні. Актуальність статті зумовлена тим, що Велика Британія створила власну систему правового регулювання збирання попередньої інформації про пасажирів (API) та записів про бронювання пасажирів (PNR) ще у 2003 р., задовго до прийняття Директиви ЄС 2016/681. Тому цей досвід, зокрема, у створенні та функціонуванні Національного прикордонного таргетингового центру (NBTC) як Підрозділу обробки інформації про пасажирів (PIU) є цінним орієнтиром для України і може бути адаптовано для формування в Україні національного PIU, з урахуванням поточних законодавчих ініціатив щодо його інституціалізації, а також особливостей національного законодавства, зокрема Закону України "Про захист персональних даних" та Закону України "Про боротьбу з тероризмом".

На основі вивчення досвіду Великої Британії обґрунтовано висновок про доцільність напрацювання в Україні Концепції створення міжвідомчого мультимодального PIU для обробки інформації про пасажирів міжнародних рейсів залізничного, автомобільного (автобусного), морського та авіаційного транспорту, яка має містити такі аспекти: 1) структура та створення вітчизняного PIU, до складу якого мають входити, для забезпечення ефективної взаємодії та координації, Служба безпеки України, Державна прикордонна служба України, Державна митна служба України та Національна поліція України; 2) підготовка персоналу; 3) системи обробки даних; 4) аналіз і таргетинг для уникнення дискримінації за ознаками раси, релігії, сексуальної орієнтації тощо; 5) взаємодія вітчизняного PIU з органами держави та Європолом і Євроюстом; 6) захист інформації та конфіденційність, що передбачає знеособлення даних PNR через 6 місяців та призначення незалежного Уповноваженого з захисту даних у PIU; 7) контроль і нагляд з посиленням ролі Уповноваженого Верховної Ради України з прав людини для моніторингу за дотриманням законодавства, що стосується обробки інформації про пасажирів, з наданням доступу до даних і критеріїв моніторингу; впровадження громадського контролю, оприлюднення інформації про права пасажирів на офіційних вебсайтах уповноважених органів та ін.; 8) відповідальність за порушення законодавства про обробку інформації про пасажирів. Як орієнтир для визначення розміру штрафів за невиконання перевізниками зобов'язань щодо надання інформації PIU та форм передачі даних, можна використовувати Immigration Act 1971, PNR Regulations 2018, яке передбачає стягнення за вчинення порушень до 10 000 фунтів стерлінгів.

Доведено, що адаптація досвіду Великої Британії щодо правого регулювання обробки інформації про пасажирів, створення та функціонування PIU дасть змогу й Україні сформувати відповідну ефективну систему, що враховуватиме специфіку національних безпекових викликів, зокрема воєнні реалії та гібридні загрози. Це не лише посилить національну безпе-

© Ярослав Шевчук, 2026

ку через оперативну обробку API та PNR, а й сприятиме боротьбі з тероризмом, нелегальною імміграцією та організованою злочинністю, зберігаючи баланс із захистом прав людини та персональних даних. Акцентовано увагу на тому, що інтеграція міжвідомчого підходу, розвиток власної технологічної інфраструктури та впровадження пілотних проєктів забезпечать поступове впровадження вітчизняного бачення PIU, мінімізуючи ризики та оптимізуючи ресурси. Крім того, така модель сприятиме посиленню міжнародної співпраці з ЄС та іншими партнерами, наближаючи Україну до європейських стандартів у сфері боротьби з тероризмом, тяжкими злочинами та забезпечення належного прикордонного контролю. У довгостроковій перспективі це приведе до підвищення ефективності діяльності відповідних уповноважених державних органів, зниження рівня загроз і створення якісної системи правового регулювання обробки інформації про пасажирів, що відповідає як національним інтересам, так і міжнародним зобов'язанням України.

Ключові слова: інформація про пасажирів (API); реєстраційні записи пасажирів (PNR); правове регулювання обробки інформації про пасажирів; Підрозділ обробки інформації про пасажирів (PIU); Концепція створення міжвідомчого мультимодального PIU; європейські стандарти у сфері боротьби з тероризмом, тяжкими злочинами та забезпечення належного прикордонного контролю; Велика Британія; Служба безпеки України; Державна прикордонна служба України; Державна митна служба України; Національна поліція України.

Велика Британія створила власну систему правового регулювання збирання попередньої інформації про пасажирів (API) та записів про бронювання пасажирів (PNR) ще у 2003 р., задовго до прийняття Директиви ЄС 2016/681[1]. Відтак цей досвід, зокрема, у створенні та функціонуванні Національного прикордонного таргетингового центру (NBTC) як Підрозділу обробки інформації про пасажирів (PIU) є цінним орієнтиром для України й може бути адаптовано для формування в Україні національного PIU, з урахуванням поточних законодавчих ініціатив щодо його інституціалізації, а також особливостей національного законодавства, зокрема Закону України "Про захист персональних даних" і Закону України "Про боротьбу з тероризмом". З таких міркувань звернення до обраної тематики дослідження видається актуальним.

Серед зарубіжних дослідників правового регулювання обробки інформації про пасажирів варто звернути увагу на роботи Ендрю Прістлі та Марка Бове[2], серед вітчизняних – наукові розвідки таких учених, як І. Бережнюк, О. Фрадинський[3], Л. Кисіль, Я. Шевчук, Н. Шевчук[4], С. Кудінов, О. Сукма-

[1] Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime <https://eur-lex.europa.eu/eli/dir/2016/681/oj/eng> (accessed 27.10.2025).

[2] Ендрю Прістлі, Марк Бове, *Міжнародний досвід та кращі практики у сфері попередньої інформації про пасажирів (API) та реєстраційних записів пасажирів* (PNR) (2021) 52 <https://www.osce.org/sites/default/files/f/documents/a/6/510620.pdf> (дата звернення 19.10.2025)

[3] І Бережнюк, О Фрадинський, 'Системи реєстрації пасажирів (PNR), як джерело інформації на авіаційному транспорті' [2017] 1 Митна безпека 6–12.

[4] Л Кисіль, Я Шевчук, 'Інституційно-правові засади реалізації функції збирання інформації про пасажирів' [2023] 3 Часопис Київського університету права 85–91; Л Кисіль, Я Шевчук, 'До питання про модель реалізації функції збирання інформації про пасажирів усіх видів транспорту, зокрема API/PNR' [2024] 34 Правова держава 467–469; Л Кисіль, Н Шевчук, 'Обробка інформації про пасажирів (API) та даних запису реєстрації пасажирів (PNR): європейські стандарти та вітчизняні реалії' [2024] 9 Право України 104–121.

нова[5], Б. Леонов[6], А. Марчук, С. Філіппов, В. Нікіфоренко, В. Фігура[7] та ін. Водночас слід визнати, що на сьогодні британський досвід правового регулювання збирання інформації про пасажирів (API) та записів про бронювання пасажирів (PNR) та можливі шляхи його використання в Україні переважно залишалися поза увагою науковців.

Мета дослідження – на підставі аналізу досвіду правового регулювання обробки інформації про пасажирів у Великій Британії запропонувати можливі напрями його впровадження в Україні, зокрема шляхом напрацювання Концепції створення міжвідомчого мультимодального PIU в Україні для обробки інформації про пасажирів міжнародних рейсів залізничного, автомобільного (автобусного), морського та авіаційного транспорту.

На сьогодні обробка інформації про пасажирів у Великій Британії ґрунтується, зокрема, на Додатку 2 до Закону про імміграцію 1971 р.; Наказі про імміграцію та поліцію (інформація про пасажирів, екіпаж та службову інформацію) № 1227 2024 р.; Законі про захист даних 2018 р.; Положенні про дані реєстраційних записів пасажирів та інші зміни № 598 2018 р. (далі – Положення 2018 р.); Директиві "Імміграція (форма та спосіб надання інформації про пасажирів)" 2023 р.; Схемі надання дозволу на перевезення 2023 р.; Положенні про Схему надання дозволу на перевезення та цивільно-правові санкції 2023 р. № 326; Положенні щодо інформації про пасажирів, екіпаж та службову інформацію (цивільні штрафи) 2015 р. № 961[8].

Формування у Великій Британії власного бачення системи правового регулювання обробки інформації про пасажирів, який спочатку стосувався лише попередньої інформації про пасажирів (API) як інструменту для боротьби з незаконною імміграцією та покращення прикордонного контролю, розпочалося у 2003 р. А вже у 2009–2010 рр. Велика Британія змінила підхід до відслідковування пасажирів, оскільки виявляти тих осіб, які потенційно можуть становити загрозу для національної та міжнародної безпеки, безпосередньо на кордоні може бути занадто пізно для реагування відповідних служб. Відтак 11 березня 2010 р. Прикордонним агентством Великої Британії (UK Border Agency / UKBA) був створений Національний прикордонний таргетинговий центр (NBTC), що реалізував повний комплекс аналітичної діяльності, пізніше зафіксованої у Директиві ЄС 2016/681,

[5] С Кудінов, О Сукманова, 'Попередня реєстрація пасажирів як засіб протидії тероризму' [2024] 40 Наукові записки Львівського університету бізнесу та права. Серія економічна. Серія юридична 326–332.

[6] Б Леонов, Я Шевчук, 'Обробка інформації про пасажирів як ефективний інструмент протидії тероризму' [2024] 1(48) Інформація і право 170–179.

[7] С Філіппов, А Марчук, 'Практичні рекомендації щодо впровадження системи обробки попередньої інформації про пасажирів (API/PNR) як інструменту протидії транскордонним загрозам' [2021] 44 Правова держава 70–77; С Філіппов, 'Кримінологічні засади протидії транскордонній злочинності' (дис д-ра юрид наук, 2019) 561; В Нікіфоренко, 'Адміністративна відповідальність авіаперевізників за невиконання обов'язку передачі попередніх даних реєстрації особи' [2020] 5 Право і суспільство 90–96; В Фігура, 'Особливості правового статусу Національного центру обробки попередніх даних в контексті функціонування системи API/PNR' [2024] 1(3) Закон і кордон 201–219.

[8] Див: Прістлі, Бове (н 2).

проводив перевірку осіб за 48, 24 години, а також під час check-in (тобто з використанням PNR). Хоча формально NBTC входив до складу Прикордонної служби, він працював як міжвідомчий орган, центр якого був розташований у приміщенні Розвідувального управління Прикордонної служби.

Після прийняття Директиви ЄС 2016/681 (про використання реєстраційних записів пасажирів – PNR), яка зобов'язала кожну державу-учасницю заснувати або призначити уповноважений орган із запобігання, виявлення, розслідування та переслідування терористичних та інших тяжких злочинів, який функціонуватиме як Національний орган з обробки інформації про пасажирів (Passenger Information Unit – PIU), у Великій Британії, для забезпечення сумісності з іншими країнами ЄС, було визначено, що національний PIU – NBTC, є міжвідомчим і мультимодальним Підрозділом обробки інформації про пасажирів Великої Британії, органом, який уповноважений запобігати, виявляти, розслідувати або переслідувати терористичні та тяжкі злочини, і входить до складу британського аналогу Міністерства внутрішніх справ (Home Office).

На сьогодні метою діяльності NBTC є обробка й аналіз інформації про пасажирів і екіпаж, а також пов'язаної службової інформації для міжнародних авіарейсів, морських подорожей і залізничних сполучень у Тунелі під Ла-Маншем, які прибувають (або очікуються їх прибуття) до або відправляються (або очікуються їх відправлення) з Великої Британії. До прикладу, NBTC отримує та обробляє дані від понад 200 перевізників, які обслуговують понад 7000 напрямів; для понад 280 мільйонів пасажирів і членів екіпажів щорічно; для 100 % запланованих авіаційних маршрутів; для 94 % усіх комерційних маршрутів, включаючи морські та залізничні.

NBTC захищає Сполучене Королівство шляхом виявлення та запобігання від прибуття до або вибуття з нього осіб високого ступеню ризику, які можуть завдати шкоди національним інтересам, а також шляхом попередження співробітників охорони кордону про цільові об'єкти інтересів, які залишають або прибувають у Сполучене Королівство.

Пріоритетними напрямами діяльності NBTC є національна безпека та боротьба з тероризмом; виявлення організованої іммиграційної злочинності та запобігання сприянню нелегальній імміграції та торгівлі людьми; незаконний обіг наркотиків і відмивання грошей.

NBTC працює 24/7, до його складу входять близько 250 співробітників таких агентств, як:

– *антитерористична поліція* (Counter-Terrorism Policing, CTP), яка забезпечує розповсюдження оперативних сповіщень для реагування до або під час подорожі, пошук у базах даних за дорученням слідчих, збирання доказів і надання рекомендацій поліцейським силам та іншим органам, що займаються боротьбою зі злочинністю, та національною безпекою. Команда CTP реалізує у своїй діяльності декілька стратегій на державному рівні, пов'яза-

pravoua.com.ua

них з різними сферами поліцейської діяльності, включаючи Стратегію боротьби з тероризмом у Великій Британії (CONTEST);

– *прикордонна та імміграційна розвідки* (Home Office Intelligence, розвідка МВС), які забезпечують надання дозволу на перевезення (АТС); зосереджені на ідентифікації та обробці осіб, які є об'єктом імміграційних, товарних або національних записів у списку спостереження, та які подорожують до та з Великої Британії; керують Підрозділом координації інформації про пасажирів (Passenger Information Coordination Unit, PICU), що є основним контактним пунктом у NBTC для зовнішніх агентств; Службою підтримки перевізників, яка є цілодобовою контактним центром для всіх перевізників, системних провайдерів і наземних операторів, які відчувають технічні труднощі з передачею даних і поданням їх до NBTC. Прикордонна та імміграційна розвідки мають у своїй структурі Групу даних, аналізу та звітності, яка забезпечує продуктивність і аналітичну підтримку для управління NBTC;

– *Національне агентство боротьби зі злочинністю* (National Crime Agency, NCA), місія якого полягає в захисті громадськості від серйозної та організованої злочинності;

– *Паспортний офіс та Податкове і митне управління Його Величності* (HM Passport Office, HMPO; HM Revenue & Customs, HMRC), які надають консультації та здійснюють експертизу з митних і паспортних питань для NBTC, а також аналізують дані подорожей;

– *незалежна Група управління розвідувальними даними МВС* (Home Office Intelligence Data Governance Team, DGT) під керівництвом спеціаліста із захисту даних (Data Protection Officer, DPO), які контролюють обробку даних NBTC, щоб переконатися, що вся обробка даних є законною, а всі дані захищені та їх розголошення відбулось у рамках закону. NBTC аналізує інформацію про пасажирів, екіпаж і службову інформацію, як попередню інформацію про пасажирів (API), так і дані запису реєстрації пасажирів (PNR). Ця інформація надходить в електронному вигляді та обробляється (збагачується, доповнюється) державними базами даних.

NBTC DGT має законодавчу роль щодо моніторингу та забезпечення безпеки даних PNR. Вона також контролює роботу засобів захисту даних щодо API і відповідає за проведення аудиту та перевірок. Інші сфери роботи з управління даними під керівництвом NBTC DGT включають відповідь на запити щодо свободи інформації, на доступ до даних та оцінку інцидентів із даними, нагляд за незалежним адміністративним органом (Independent Compliance Governance Team NBTC), призначеним для схвалення використання або передачі даних PNR в ЄС, згідно з вимогами Угоди про торгівлю та співпрацю між Великою Британією та ЄС. При цьому старший офіцер NBTC є керівником відділу агентурної розвідки (of People Intelligence) Міністерства внутрішніх справ.

Функції NBTC включають:

1) *створення списків спостереження* ("вочлистів"), виявлення суб'єктів списків спостереження або реагування на потрапляння до списків спостереження відомих осіб і документів. API надсилається до NBTC перевізниками та автоматично перевіряється за списками спостереження. Групи в NBTC, які працюють зі списками спостереження, відповідають за перевірку співпадінь і прийняття рішень щодо подальших дій, таких як запобігання поїздкам до Великої Британії або сповіщення портів про об'єкти зацікавленості.

2) *використання інформації (розвідданих) від різних агенцій для обробки даних PNR відповідно до заздалегідь визначених критеріїв,* також відомих як таргетинг, для ідентифікації інших невідомих осіб, які представляють інтерес. Заздалегідь визначені критерії або правила таргетингу, які використовує NBTC, забезпечують надійність, цілеспрямованість, пропорційність і конкретність діяльності NBTC; захист прав людини та їх рівність перед законом; нормативну визначеність діяльності та підконтрольність NBTC компетентним органам влади Великої Британії. Обробляючи переважно дані PNR, NBTC може здійснювати пошук у великих обсягах даних про пасажирів, щоб визначити ризики за допомогою розвідки та аналітики даних;

3) *можливість заборони польотів.* NBTC керує Схемою надання дозволу на перевезення (Authority to Carry Scheme) 2023 (ATC), яка фактично є схемою заборони польотів Великої Британії. Мета полягає в тому, щоб перешкодити певним особам подорожувати до або з Великої Британії, коли це необхідно в суспільних інтересах. Якщо особа підпадає під дію ATC, зв'язуються з перевізником і йому відмовляють у дозволі перевезти особу до Великої Британії. У наданні ATC відмовляють особам, яким заборонено в'їзд до Сполученого Королівства, наприклад, якщо вони видворені зі Сполученого Королівства, були депортовані з Великої Британії або вони використовують проїзний документ, щодо якого є інформація про втрату чи викрадення, чий дозвіл на подорож або дозвіл на в'їзд скасовані або анульовані, або якщо особи становлять пряму загрозу безпеці літака, корабля чи поїзда.

У правовому регулюванні обробки інформації про пасажирів у Великій Британії важлива увага приділяється захисту інформації про пасажирів, про що свідчать такі положення нормативно-правових актів:

– *існування заборони на обробку спеціальних категорій персональних даних.* Так, Положення 14 Положення 2018 р. передбачає, що PIU не повинен обробляти та повинен назавжди видаляти дані PNR, що стосуються раси, етнічного походження, політичних поглядів, філософських переконань, членства у профспілках, стану здоров'я, статевого життя або сексуальної орієнтації особи;

– *дані PNR необхідно знеособити через 6 місяців* (Положення 13 Положення 2018 р.), починаючи з дати передачі даних PNR авіаперевізником або PIU ЄС, шляхом маскування таких елементів даних: а) імені, включаючи імена інших пасажирів у PNR та кількість подорожуючих, які подорожують разом

pravoua.com.ua

по PNR; b) адреси та контактної інформації; c) всіх видів платіжної інформації, включаючи адресу виставлення рахунку; d) інформації про пасажирів, які часто літають; e) загальні зауваження; f) будь-які дані API, (g) іншої службової інформації (OSI) та h) системної службової інформації (SSI), інформації про запити на системні послуги (SSR);

– дані PNR можуть бути повторно персоналізовані лише за наявності конкретних умов;

– дані PNR повинні зберігатися не довше 5 років (Положення 13 Положення 2018 р.) з моменту передачі даних, PIU зобов'язаний остаточно видаляти ці дані після закінчення цього періоду.

Водночас Положення 13AA встановлює умови для збереження певних даних PNR ЄС, якщо вони стосуються особи, яка виїхала з Великої Британії, на основі оцінки ризиків, що базується на об'єктивно встановлених критеріях.

Ці положення про зберігання даних не впливають на випадки, коли дані PNR були передані компетентному органу Великої Британії і використовуються в контексті конкретних справ з метою запобігання, виявлення, розслідування або переслідування терористичних або тяжких злочинів.

Велика Британія отримує дані PNR за допомогою методу "пуш", щоб захистити персональні дані, які містяться в системах операторів, і щоб оператори зберігали контроль над своїми системами. Це зазначено в Загальному ICD Великої Британії: дані PNR повинні надсилатися (передаватися) щодо запланованого часу відправлення Перевізника і в терміни, визначені відповідним законодавством Великої Британії. "Пуш" визначається в ICD як повідомлення, що передаються системою перевізника / постачальника послуг до системи Великої Британії[9].

Але визначальним для правового регулювання обробки інформації про пасажирів у Великій Британії є, поза сумнівом, принцип верховенства права, повага до прав людини та основоположних її свобод, тому:

1) законодавство чітко визначає складові інформації про пасажирів, екіпаж та службової інформації, які використовуються в операційній діяльності. Так, дані PNR визначені в Додатку 3 до Наказу про імміграцію та поліцію (інформація про пасажирів, екіпаж та службову інформацію) 2024 р. (далі – Наказ 2024 р.). У Положенні 2018 р. дані PNR означають один або кілька елементів персональних даних, перелічених у Додатку 3 до Наказу 2024 р.;

[9] Довідково: натепер існує два можливих методи передавання даних: метод "згори" (або "пулл"), за яким компетентні органи держави-члена, яким необхідні дані PNR, отримують доступ до системи бронювання авіаперевізника та самостійно формують витяг необхідних даних; та метод "знизу" (або "пуш"), за яким авіаперевізники самі передають необхідні дані органу, який здійснює на них запит, що дає їм змогу контролювати, які саме дані вони надають. Вважають, що другий метод забезпечує вищий рівень захисту даних.

2) чітко визначено цілі, для яких органи влади можуть використовувати дані PNR. Зокрема, Положення 2018 р. передбачає, що дані PNR не повинні оброблятися, за винятком цілей запобігання, виявлення, розслідування та переслідування терористичних або тяжких злочинів, а також захисту життєво важливих інтересів осіб (що включає захист осіб, які перебувають або можуть перебувати під загрозою смерті або серйозного поранення, або від значних загроз для здоров'я населення) (положення 6);

3) обмежено розкриття даних PNR іншим органам влади Великої Британії чи іншої країни, які виконують функції, пов'язані з метою, для якої обробляються дані PNR. Положення 2018 р. встановлює умови щодо розкриття даних PNR, результатів обробки даних PNR або аналітичної інформації, що містить дані PNR, які можуть бути розкриті лише певним чітко визначеним суб'єктам:

– органам Великої Британії, уповноваженим запобігати, виявляти, розслідувати та переслідувати за терористичні або тяжкі злочини, а також захищати життєво важливі інтереси осіб (положення 7);

– Підрозділу обробки інформації про пасажирів (PIU) держави – члена ЄС, якщо це необхідно для запобігання, виявлення, розслідування або переслідування терористичних або тяжких злочинів (положення 11A);

– Європолу та Євроюсту, якщо це необхідно для цілей запобігання, виявлення, розслідування або переслідування терористичних або тяжких злочинів (положення 11B). Так, PIU повинен якнайшвидше передати інформацію PNR до Європолу або Євроюсту в конкретному випадку, якщо Європол або Євроюст направив належним чином обґрунтований запит на отримання інформації PNR, і PIU переконаний, що необхідно передати цю інформацію PNR для цілей запобігання, виявлення, розслідування та переслідування терористичних або тяжких злочинів. Також PIU повинен якомога швидше передавати аналітичну інформацію, що містить дані PNR, до Європолу або Євроюсту в конкретному випадку, коли PIU вважає за необхідне передати цю аналітичну інформацію з метою запобігання, виявлення, розслідування та переслідування терористичних або тяжких злочинів;

– органам третіх країн, компетентним у сфері запобігання, виявлення, розслідування та переслідування терористичних і тяжких злочинів або захисту життєво важливих інтересів осіб (положення 12);

4) у контексті запобігання несанкціонованому доступу, розголошенню та використанню даних PNR у Великій Британії, Шостий принцип захисту даних, викладений в пункті 40 Закону про захист даних 2018 р., встановлює, що персональні дані, які обробляються для будь-яких правоохоронних цілей, повинні оброблятися таким чином, щоб забезпечити належну безпеку персональних даних із застосуванням відповідних технічних або організаційних заходів (і в цьому принципі "належна безпека" включає захист від

pravoua.com.ua

несанкціонованої або незаконної обробки, а також від їх випадкової втрати, знищення або пошкодження);

5) встановлена юридична відповідальність у вигляді покарання за зловживання, несанкціонований доступ та несанкціоноване розголошення даних PNR. Будь-яке порушення даних, таке як несанкціонований доступ до персональних даних, несанкціоноване розголошення або використання даних, може бути покаране Комісаром з інформації. Контролери даних зобов'язані за законом повідомляти про будь-які порушення даних. Пункт 170 Закону про захист даних 2018 р. передбачає конкретний склад злочину – незаконне отримання, розголошення, придбання або зберігання персональних даних;

6) на уповноважені органи покладено обов'язок інформування осіб про збір, використання, обробку та захист даних PNR і пов'язаних з ними стандартів конфіденційності, що застосовуються. Зокрема, п. 44 Закону про захист даних 2018 р. встановлює загальні обов'язки контролерів даних, які включають інформацію, яку вони повинні оприлюднювати, а саме: ідентифікаційні та контактні дані контролера; цілі, для яких контролер обробляє персональні дані; наявність прав суб'єктів даних вимагати доступу до даних, виправлення даних, видалення даних або обмеження обробки, а також інформацію про правові підстави для обробки даних та про зберігання даних. Уряд Великої Британії опублікував інформацію про збір, використання, обробку та захист даних PNR, а також про права суб'єктів даних PNR відповідно до Закону 2018 р. на вебсайті www.gov.uk (Додаток 2). Велика Британія також вжила заходів для забезпечення того, щоб оператори повітряних суден інформували своїх клієнтів про передачу даних PNR. Так, ст. 13 Загального регламенту про захист даних у Великій Британії (UK GDPR)[10] зобов'язує авіакомпанії надавати пасажирам інформацію про обробку їхніх персональних даних;

7) існують адміністративні та судові механізми правового захисту від незаконної обробки даних PNR органами державної влади. Зокрема, п. 167 Закону 2018 р. передбачає, що якщо суд визнає, що мало місце незаконне порушення прав суб'єкта даних, то суд може винести постанову з метою забезпечення дотримання законодавства про захист даних, яка зобов'язує контролера, що здійснює обробку, або обробника, який діє від імені цього контролера, а) вжити заходів, зазначених у постанові, або b) утриматися від вжиття заходів, зазначених у постанові. Стаття 82 GDPR Великої Британії та п. 169 Закону 2018 р. надають фізичним особам право на компенсацію за будь-яку шкоду, завдану діями контролера або обробника даних;

8) передбачено механізми для того, щоб особи могли отримати доступ до їхніх даних PNR та вимагати, за необхідності, їх виправлення, видалення або внесення приміток. Так, право доступу суб'єкта даних викладено в ст. 45 Закону 2018 р. Суб'єкт даних має право отримати від контролера

[10] UK General Data Protection Regulation <https://uk-gdpr.org/chapter-3-article-13> (accessed 27.10.2025).

a) підтвердження того, чи обробляються його персональні дані, і б) якщо так, то доступ до персональних даних та наступної інформації: a) цілі та правові підстави для обробки; b) категорії відповідних персональних даних; c) одержувачі або категорії одержувачів, яким було розкрито персональні дані (включаючи одержувачів або категорії одержувачів у третіх країнах або міжнародних організаціях); d) період, протягом якого передбачається зберігати персональні дані, або, якщо це неможливо, критерії, використані для визначення цього періоду; e) наявність прав суб'єкта даних вимагати від контролера i) виправлення персональних даних (ст. 46) та ii) видалення персональних даних або обмеження їх обробки (ст. 47); (f) наявність права суб'єкта даних подати скаргу до Комісара та контактні дані Комісара; g) повідомлення про персональні дані, що підлягають обробці, та будь-яку наявну інформацію про їхнє походження. Комісар з інформації опублікував інструкцію для фізичних осіб щодо їхніх прав на персональні дані та механізмів реалізації суб'єктами даних своїх прав;

9) Комісар з інформації є відповідним компетентним наглядовим органом Великої Британії у сфері захисту даних і відповідає за моніторинг застосування Закону 2018 р. щодо обробки даних правоохоронними органами з метою захисту основних прав і свобод осіб у зв'язку з обробкою даних компетентним органом для будь-яких правоохоронних цілей (як визначено в ч. 3 Закону 2018 р.) та сприяння вільному потоку персональних даних. Згідно із законом Комісар з інформації та його співробітники є незалежними від уряду. Додаток 12 до Закону 2018 р. передбачає, що Комісар, його співробітники та персонал не повинні розглядатися як слуги або агенти Корони.

Відповідно до положення 14 Положення 2018 р. PIU повинен вести документацію, що стосується всіх систем і процедур обробки, які знаходяться під його відповідальністю, та надавати її Комісару на його вимогу. Така документація повинна містити щонайменше: a) ім'я та контактні дані персоналу PIU, якому доручено обробляти дані PNR; (b) відповідні рівні повноважень цього персоналу для доступу до даних PNR; c) деталі запитів, зроблених PIU ЄС, Європолом або Євроюстом, та d) деталі всіх запитів на передачу даних PNR до третьої країни.

Досвід правового регулювання Великої Британії у створенні та функціонуванні Національного прикордонного таргетингового центру (NBTC) як Підрозділу обробки інформації про пасажирів (PIU) є цінним орієнтиром для України. Проведений нами його аналіз дає змогу зробити висновок про доцільність напрацювання Концепції створення і в Україні міжвідомчого мультимодального PIU для обробки інформації про пасажирів міжнародних рейсів залізничного, автомобільного (автобусного), морського та авіаційного транспорту. Ця Концепція має містити такі важливі аспекти:

– *Структура та створення PIU*. З урахуванням функцій, структури та повноважень британського PIU (NBTC), яке забезпечує ефективну обробку

pravoua.com.ua

даних з акцентом на пріоритети (національну безпеку, боротьбу з тероризмом, нелегальною імміграцією та організованою злочинністю), рекомендується створити вітчизняний PIU на базі незалежної інституції, яка виконуватиме функцію "Єдиного вікна" для збору, структурування та розподілу даних до компетентних органів.

В Україні ключовими стейкхолдерами щодо обробки попередньої інформації про пасажирів (API) та даних реєстрації пасажирів (PNR) є Служба безпеки України, Державна прикордонна служба України, Державна митна служба України та Національна поліція України. Представників цих відомств доцільно делегувати до PIU для забезпечення ефективної взаємодії та координації. Реалізацію проєкту рекомендується розпочати з пілотної ініціативи, фокусуючись на одній категорії перевізників з подальшим масштабуванням на інші види транспорту.

– *Підготовка персоналу.* У Великій Британії персонал PIU починав з виконання простих завдань і проходив навчання на практиці. В Україні доцільно впровадити аналогічний підхід, доповнивши його обов'язковими тренінгами з питань прав людини, захисту персональних даних та запобігання дискримінації.

– *Система обробки даних.* Велика Британія використовує систему EBorders для обробки даних від понад 200 перевізників (обсяг – близько 280 млн пасажирів щорічно), з залученням послуг компанії IBM (вартість – мільйони фунтів стерлінгів на рік). Водночас планується перехід на власну технічну систему за сприяння спеціалістів Міністерства внутрішніх справ для забезпечення незалежності та підвищення ефективності. Зважаючи на безпекові виклики в Україні, зокрема постійні гібридні загрози, рекомендується зосередитися на розробці власної системи обробки даних. Додатково доцільно створити службу підтримки для перевізників у режимі 24/7.

– *Аналіз та таргетинг.* У Великій Британії дані API/PNR аналізуються NBTC з використанням державних баз даних, формується список спостереження (watchlist) та застосовується таргетинг на основі об'єктивних правил без дискримінації. Для України рекомендується адаптувати цю модель з акцентом на ризики, пов'язані з тероризмом та серйозними злочинами. Ключовими елементами цієї моделі мають також стати об'єктивні критерії та зовнішній контроль для уникнення дискримінації за ознаками раси, релігії, сексуальної орієнтації тощо.

– *Взаємодія PIU з органами держави.* Необхідно забезпечити належний обмін даними з національними компетентними органами (Службою безпеки України, Державною прикордонною службою, Державною митною службою, Національною поліцією) та міжнародними структурами (Європолом та Євроюстом), подібно до практики Великої Британії (PNR Regulations 2018). Перед кожною передачею інформації слід проводити оцінку рівня захисту даних у відповідних країнах.

ПРАВО УКРАЇНИ • 2026 • № 1 • 277-290

– *Захист інформації та конфіденційність.* У Великій Британії нормативно забезпечений захист персональних даних, PNR знеособлюються через 6 місяців, існують заборона на обробку чутливих даних і незалежний нагляд за дотриманням означеного законодавства (Комісар з інформації). На нашу думку, в Україні профільний закон має містити аналогічні норми щодо знеособлення даних через 6 місяців та передбачати призначення незалежного Уповноваженого з захисту даних у PIU.

– *Контроль та нагляд.* У Великій Британії функціонує незалежний контроль через Home Office Intelligence Data Governance Team, з регулярними аудитами та перевірками. Для України доцільно адаптувати цю модель, посилюючи роль Уповноваженого Верховної Ради України з прав людини для моніторингу за дотриманням законодавства, що стосується обробки інформації про пасажирів, з наданням доступу до даних та критеріїв моніторингу. Додатково рекомендується впровадити громадський контроль за дотриманням законодавства, що стосується обробки інформації про пасажирів, оприлюднювати інформацію про права пасажирів на офіційних вебсайтах уповноважених органів.

– *Відповідальність за порушення законодавства про обробку інформації про пасажирів.* Як орієнтир для визначення розміру штрафів за невиконання перевізниками зобов'язань щодо надання інформації PIU та форм передачі даних можна використовувати британське законодавство (Immigration Act 1971[11], PNR Regulations 2018[12]), яке передбачає стягнення за вчинення порушень до 10 000 фунтів стерлінгів.

Висновок. Адаптація досвіду Великої Британії щодо правового регулювання обробки інформації про пасажирів, створення та функціонування PIU дасть змогу й Україні сформувати відповідну ефективну систему, що враховуватиме специфіку національних безпекових викликів, зокрема воєнні реалії та гібридні загрози. Це не лише посилить національну безпеку через оперативну обробку API та PNR, а й сприятиме боротьбі з тероризмом, нелегальною імміграцією та організованою злочинністю, зберігаючи баланс із захистом прав людини та персональних даних. Інтеграція міжвідомчого підходу, розвиток власної технологічної інфраструктури та впровадження пілотних проєктів забезпечать поступове впровадження вітчизняного бачення PIU, мінімізуючи ризики та оптимізуючи ресурси. Крім того, така модель сприятиме посиленню міжнародної співпраці з ЄС та іншими партнерами, наближаючи Україну до європейських стандартів у сфері боротьби з тероризмом, тяжкими злочинами та забезпечення належного прикордонного контролю. У довгостроковій перспективі це приведе до підвищення ефективності діяльності відповідних уповноважених державних органів,

[11] Immigration Act 1971 <https://www.legislation.gov.uk/ukpga/1971/77/contents> (accessed 27.10.2025).
[12] The Passenger Name Record Data and Miscellaneous Amendments Regulations 2018 <https://www.legislation.gov.uk/uksi/2018/598> (accessed 27.10.2025).

зниження рівня загроз і створення якісної системи правового регулювання обробки інформації про пасажирів, що відповідає як національним інтересам, так і міжнародним зобов'язанням України.

REFERENCES

Bibliography

Journal articles

1. Berezhniuk I, Fradynskyi O, 'Systemy reiestratsii pasazhyriv (PNR), yak dzherelo informatsii na aviatsiinomu transporti' [2017] 1 Mytna bezpeka 6–12 (in Ukrainian).
2. Kysil L, Shevchuk N, 'Obrobka informatsii pro pasazhyriv (API) ta danykh zapysu reiestratsii pasazhyriv (PNR): yevropeiski standarty ta vitchyzniani realii' [2024] 9 Pravo Ukrainy 104–121 (in Ukrainian).
3. Kysil L, Shevchuk Ya, 'Do pytannia pro model realizatsii funktsii zbyrannia informatsii pro pasazhyriv usikh vydiv transportu, zokrema API/PNR' [2024] 34 Pravova derzhava 467–469 (in Ukrainian).
4. Kysil L, Shevchuk Ya, 'Instytutsiino-pravovi zasady realizatsii funktsii zbyrannia informatsii pro pasazhyriv' [2023] 3 Chasopys Kyivskoho universytetu prava 85–91 (in Ukrainian).
5. Kudinov S, Sukmanova O, 'Poperednia reiestratsiia pasazhyriv yak zasib protydii teroryzmu' [2024] 40 Naukovi zapysky Lvivskoho universytetu biznesu ta prava. Seriia ekonomichna. Seriia yurydychna 326–332 (in Ukrainian).
6. Leonov B, Shevchuk Ya, 'Obrobka informatsii pro pasazhyriv yak efektyvnyi instrument protydii teroryzmu' [2024] 1(48) Informatsiia i pravo 170–179 (in Ukrainian).
7. Nikiforenko V, 'Administratyvna vidpovidalnist aviapereviznykiv za nevykonannia obov'iazku peredachi poperednikh danykh reiestratsii osoby' [2020] 5 Pravo i suspilstvo 90–96 (in Ukrainian).
8. Fihura V, 'Osoblyvosti pravovoho statusu Natsionalnoho tsentru obrobky poperednikh danykh v konteksti funktsionuvannia systemy API/PNR' [2024] 1(3) Zakon i kordon 201–219 (in Ukrainian).
9. Filippov S, Marchuk A, 'Praktychni rekomendatsii shchodo vprovadzhennia systemy obrobky poperednoi informatsii pro pasazhyriv (API/PNR) yak instrumentu protydii transkordonnym zahrozam' [2021] 44 Pravova derzhava 70–77 (in Ukrainian).

Theses

10. Filippov S, 'Kryminolohichni zasady protydii transkordonnii zlochynnosti' (dys d-ra yuryd nauk, 2019) (in Ukrainian).

Websites

11. Pristli E, Bove M, Mizhnarodnyi dosvid ta krashchi praktyky u sferi poperednoi informatsii pro pasazhyriv (API) ta reiestratsiinykh zapysiv pasazhyriv (PNR) (2021) 52 <https://www.osce.org/sites/default/files/f/documents/a/6/510620.pdf> (accessed 19.10.2025) (in Ukrainian).

Yaroslav Shevchuk

EXPERIENCE OF LEGAL REGULATION OF PASSENGER INFORMATION PROCESSING IN THE UNITED KINGDOM AND POSSIBLE WAYS OF ITS IMPLEMENTATION IN UKRAINE

Abstract. The article is devoted to the analysis of the experience of legal regulation of passenger information processing in the United Kingdom and possible ways of its implementation in Ukraine.

The relevance of the article is due to the fact that the United Kingdom created its own system of legal regulation of the collection of advance passenger information (API) and passenger name record (PNR) back in 2003, long before the adoption of EU Directive 2016/681. Therefore, this experience, including in the creation and operation of the National Border Targeting Centre (NBTC) as a Passenger Information Unit (PIU), is a valuable reference for Ukraine and can be adapted for the formation of a national PIU in Ukraine, taking into account current legislative initiatives on its institutionalization, as well as the specifics of national legislation, in particular the Law of Ukraine "On Personal Data Protection" and the Law of Ukraine "On Combating Terrorism".

Based on the study of the experience of Great Britain, the conclusion is substantiated on the feasibility of developing in Ukraine the Concept of creating an interdepartmental multimodal PIU for processing information about passengers of international flights of railway, road (bus), sea and air transport, which should contain the following aspects: 1) structure and creation of a domestic PIU, which should include, to ensure effective interaction and coordination, the Security Service of Ukraine, the State Border Guard Service of Ukraine, the State Customs Service of Ukraine and the National Police of Ukraine; 2) personnel training; 3) data processing systems; 4) analysis and targeting to avoid discrimination on the grounds of race, religion, sexual orientation, etc.; 5) interaction of the domestic PIU with state bodies and Europol and Eurojust; 6) information protection and confidentiality, which provides for the depersonalization of PNR data after 6 months and the appointment of an independent Data Protection Officer in the PIU; 7) control and supervision with a strengthened role of the Commissioner for Human Rights of the Verkhovna Rada of Ukraine to monitor compliance with legislation on the processing of passenger information, with access to data and monitoring criteria; introduction of public control, publication of information on passenger rights on the official websites of authorized bodies, etc.; 8) liability for violations of legislation on the processing of passenger information. As a guideline for determining the amount of fines for failure by carriers to fulfil their obligations to provide PIU information and data transfer forms, the Immigration Act 1971, PNR Regulations 2018, which provides for penalties for violations of up to 10,000 pounds sterling, can be used.

It has been proven that the adaptation of the experience of the United Kingdom in the legal regulation of passenger information processing, the creation and functioning of PIU will allow Ukraine to form an appropriate effective system that will take into account the specifics of national security challenges, in particular military realities and hybrid threats. This will not only enhance national security through the expeditious processing of API and PNR, but will also contribute to the fight against terrorism, illegal immigration and organized crime, while maintaining a balance with the protection of human rights and personal data. Attention is focused on the fact that the integration of an interagency approach, the development of our own technological infrastructure, and the implementation of pilot projects will ensure the gradual implementation of the domestic vision of PIU, minimizing risks and optimizing resources. In addition, such a model will contribute to strengthening international cooperation with the EU and other partners, bringing Ukraine closer to European standards in the fight against terrorism, serious crime and ensuring proper border control. In the long term, this will lead to increased efficiency of the relevant authorized state bodies, reduced threats and the creation of a high-quality legal regulation system for the processing of passenger information, which meets both national interests and international obligations of Ukraine.

Keywords: advance passenger information (API); passenger name record (PNR); legal regulation of passenger information processing; Passenger Information Unit (PIU); Concept of creating an interdepartmental multimodal PIU; European standards in the field of combating terrorism, serious crimes and ensuring proper border control; Great Britain; Security Service of Ukraine; State Border Guard Service of Ukraine; State Customs Service of Ukraine; National Police of Ukraine.