

DOI: <https://doi.org/10.18524/2411-2054.2021.43.240997>

УДК 351.746:342.9(477)

С. О. Філіппов, докт. юрид. наук, канд. психол. наук, доцент,
полковник, заступник начальника факультету правоохоронної діяльності
Національна академія Державної прикордонної служби України
вул. Шевченка, 46, Хмельницький, 29003, Україна
e-mail: nadpsu@i.ua
ORCID ID: <https://orcid.org/0000-0001-6700-4194>

ОКРЕМІ АСПЕКТИ ВИКОРИСТАННЯ ДАНИХ ПРО ПАСАЖИРІВ (API/PNR) В ІНТЕРЕСАХ ПРИКОРДОННОЇ БЕЗПЕКИ

У статті розкрито логіку, механізм та основні параметри використання даних про пасажирів (API/PNR) в інтересах прикордонної безпеки. Розкрито співвідношення понять «попередня інформація про пасажирів» та «запис реєстрації пасажирів». Підкреслено, що системи спрощення формальностей одночасно позитивним чином впливають й на безпеку. Наприклад, метою збору даних в ЄС визнається ефективна боротьба з нелегальною міграцією та посилення прикордонного контролю, а також запобігання, виявлення, розслідування і переслідування злочинів терористичної спрямованості і серйозних злочинів. Це стосується, як системи попередньої інформації про пасажирів (API), так і додаткових даних про пасажирів, таких, як дані реєстрації пасажирів (PNR). Беззаперечно, що успішне застосування обміну даними API і PNR залежить від єдиного підходу всіх учасників інформаційних відносин (як прикордонних відомств так і авіакомпаній в різних державах) до питання про стандарт даних та стандарт їх передачі. А забезпечення такого єдиного підходу є проблемою навіть тоді, коли наявна єдність правового регулювання щодо формату даних та процедур обміну даними.

У національному законодавстві відсутні спеціальні нормативно-правові акти, які б урегульовували відносини з приводу обігу даних про реєстрацію авіапасажирів, також не визначено єдиного оператора, який обробляє даний вид інформації. Отже, нарізла потреба у спеціальному нормативно-правовому регулюванні використання даних про авіапасажирів, які перетинають державний кордон України.

Ключові слова: протидія злочинності, прикордонна безпека, прикордонний контроль, пункти пропуску для повітряного сполучення, API/PNR, біометрія.

Постановка проблеми, її зв'язок з практичними завданнями. Активне застосування нових технологічних можливостей, у тому числі транскордонний обмін даними, є очевидною умовою ефективності протидії злочинності. У Резолюції 74/177 (2019) Генеральної асамблеї ООН особлива увага акцентується на міждержавному обміні даними для запобігання транскордонного переміщення іноземних бойовиків-терористів (FTF) [1]. Резолюція 2322 (2016) Ради Безпеки (РБ) ООН закликає держави-члени «запобігати переміщенню терористів, зокрема шляхом здійснення ефективного прикордонного контролю, і в зв'язку з цим оперативно обмінюватися інформацією і зміцнювати співробітництво між компетентними органами» [2]. Використання попередньої інформації про пасажирів (API) і записів реєстрації пасажирів (PNR) є одночасно важливим елементом забезпечення як авіаційної, так і прикордонної безпеки. Але запровадження в різних державах в інтересах прикордонної безпеки таких технологій, як, наприклад, система штучного інтелекту iBorderCtrl або API/PNR, породжують певні проблеми через розрив між впровадженням інновацій та їх нормативним врегулюванням.

Аналіз останніх досліджень і публікацій. Проблеми застосування технологій у різних аспектах адміністрування у прикордонній сфері, зокрема у прикордонному контролі, досліджувалися Дмитром Купрієнком, Миколою Литвином, Володимиром Нікіфоренком, Istvan Samu та ін. Аналіз праць зазначених вище дослідників свідчить про важливість проблеми.

Виділення невирішених раніше частин загальної проблеми. Натомість, аналіз наукових джерел свідчить про те, що незважаючи на очевидне практичне значення, ця

міждисциплінарна проблема в межах юридичної науки в Україні представлена лише на рівні поодиноких публікацій. Дослідження правових аспектів використання в інтересах прикордонної безпеки попередньої інформації про пасажирів (API) і записів реєстрації пасажирів (PNR) на маршрутах міжнародного повітряного сполучення практично відсутні в Україні. Дана обставина і обумовлює наш інтерес до заявленої теми.

Мета статті. Виходячи з вищевикладеного, зосередимо увагу на уточненні наступних ключових аспектів використання даних про пасажирів в інтересах прикордонної безпеки: по-перше, виявлення правових проблем, що виникають у зв'язку з реалізацією системи API/PNR, по-друге, виявлення проблем у превентивному використанні біометричних баз даних з метою протидії транскордонній злочинності.

Виклад основного матеріалу. Зупинимось на вищезазначених дослідницьких проблемах. Зауважимо, що в умовах безпрецедентного глобального падіння обсягів пасажирських авіаперевезень через пандемію COVID-19 значення обміну інформацією про авіапасажирів, що перетинають державний кордон, не знижується. Крім того, що це важливий інструмент протидії загрозам тероризму і транскордонної злочинності, а також спрощення формальностей у міжнародних поїздках та забезпечення комфорту для пасажирів, Міжнародна організація цивільної авіації (ICAO) розглядає використання API/PNR як інструмент в контексті зусиль, спрямованих на підвищення стійкості галузі під час пандемії. Навіть за умови швидкого поновлення обсягів авіаперевезень, важко переоцінити значення API/PNR для аналізу даних про пасажирів, які починали свою подорож або проїжджали транзитом через країну з високим рівнем епідемічного ризику.

Використання даних про пасажирів за визначенням Володимира Нікіфоренка (попередніх даних реєстрації особи) – це нормативно визначений на міжнародному рівні спосіб передачі прикордонній службі вичерпного переліку даних про пасажирів, які придбали квитки та планують перетинати державний кордон, що також на підставі міжнародних угод можуть передаватися прикордонним відомствам інших держав, з гарантією збереження персональних даних від несанкціонованого витоку та використання [3, с. 68].

Такі засоби спрощення формальностей, як система API/PNR, неодноразово доводили свою користь для безпеки. Були і антиприкладі. Зокрема, 24 травня 2014 року в Єврейському музеї в Брюсселі бойовик Ісламської держави Мехді Немуш (Mehdi Nemmouche) розстріляв чотирьох людей. Хоча він був занесений у французьку розшукову базу, це не стало перешкодою для його вільного виїзду в 2013 р. у Сирію. Там він воював в рядах терористів. Попри те, що він був оголошений вже в міжнародний розшук, у березні 2014 року Немуш перетнув сухопутний кордон з Туреччиною, звідки безперешкодно вилетів до Малайзії, потім з Сінгапуру до Франкфурта. І тільки після вильоту з франкфуртського аеропорту був зафіксований факт його переміщення в Європі. Отже, систематична фіксація у всіх державах попередньої інформації і записів реєстрації пасажирів (API/PNR) від авіакомпаній, а також автоматична звірка з базами даних були б перешкодою для таких, як Мехді Немуш, вільно переміщатися через кордони для вчинення злочинів [4].

Система попередньої інформації про пасажирів (API) передбачає збір авіаперевізником біографічних даних пасажирів під час процесу реєстрації на рейс. Зазначена інформація передається в електронному вигляді органам прикордонного контролю в пункті призначення після вильоту рейсу. Ці органи можуть потім порівняти детальну інформацію про пасажирів зі своєю базою даних, виявляючи тих пасажирів, які підлягають більш ретельній перевірці після прибуття. Це також дає можливість ефективно і швидко здійснити оформлення осіб, які становлять мінімальний ризик [5]. Переважна більшість країн запитує дані формату API 1 – SSR DOCS, тобто тільки паспортні дані, які містять машинозчитувальні паспорти (та інші офіційні проїзні документи). США запитує дані формату API 2 – SSR DOCA – тобто дані про країну та адресу місця постійного проживання і адресу першої зупинки в США (крім громадян США та транзитних пасажирів). Більш сучасний варіант API – інтерактивна система API (iAPI) – забезпечує обмін електронними повідомленнями в режимі он-лайн щодо кожного пасажирів між перевізником і органом

прикордонного контролю в державі призначення (на відміну від спільного повідомлення API для всіх пасажирів рейсу). Повноважний орган прикордонного контролю пункту призначення направляє авіаперевізнику в режимі реального часу у відповідь електронне повідомлення, яке містить дозвіл або заборону посадки пасажирів на рейс [5].

Останнім часом деякі країни вийшли за рамки API і запровадили законодавство, що вимагає від перевізників додаткових даних, що стосуються пасажирів, у формі даних PNR, які становлять собою більш широкий набір даних, що використовуються для оцінки ризиків: дані про пасажирів і маршрути/рейси з систем бронювання / продажу квитків авіаперевізників і систем управління відправленнями, що передаються за кілька днів (24–48–72 годин) і за кілька годин (1–8 годин) до початку реєстрації. Існує п'ять основних пунктів PNR, які необхідні для здійснення бронювання: ім'я пасажирів, контактна інформація агентства, яка здійснила бронювання; дані про дату продажу, яка використовується агентом для продажу або анулювання; деталі маршруту (польотні сегменти); ім'я особи, на запит якої здійснено бронювання. З метою протидії злочинності в деяких країнах вимагають від перевізника надання і таких даних про пасажирів, як дата і місце народження, стать, громадянство пасажирів, інформація про інвалідність, стан здоров'я пасажирів, телефони, деталі тарифу, форма оплати, дані платіжних карт.

В ЄС на підставі Директиви Європейського Парламенту і Ради від 27 квітня 2016 року № 2016/681 дані записів реєстрації пасажирів (PNR) використовуються з метою «ефективної боротьби з нелегальною міграцією та посилення прикордонного контролю», а також «запобігання, виявлення, розслідування і переслідування злочинів терористичної спрямованості і серйозних злочинів». У додатку до документа – перелік 26 таких злочинів [6].

Керівні принципи API розроблені Всесвітньою митною організацією (WCO) у співпраці з Міжнародною асоціацією повітряного транспорту (IATA). Згодом до процесу приєдналася Міжнародна організація цивільної авіації (ICAO). Щоб допомогти своїм членам запровадити систему API, ці три організації опублікували Керівництво WCO/IATA/ICAO з попередньої інформації про пасажирів. Керівні принципи, що стосуються PNR, також розроблені ICAO у співпраці з IATA і WCO.

Важливою є роль ООН у сфері просування API / PNR. Резолюція 2178 (2014) РБ ООН, створює основу для міжнародних дій у відповідь на загрозу тероризму. У Резолюції, серед іншого, міститься заклик до держав-членів «вимагати, щоб авіакомпанії, що працюють на їх території, надавали попередню інформацію про пасажирів відповідним національним органам» [7]. Резолюція 2396 (2017) РБ ООН встановлює, що «відповідно до пункту 9 резолюції 2178 і стандарту, введеному ICAO, держави – члени ICAO повинні починаючи з 23 жовтня 2017 року створити системи попереднього збору інформації про пасажирів... вимагати, щоб авіаційні компанії, що діють на їх території, надавали відповідним національним органам відповідно до внутрішнього законодавства і міжнародних зобов'язань попередню зібрану інформацію про пасажирів» [8].

В Україні це питання частково врегульовано Законом, яким 21 березня 2017 року затверджено Державну програму авіаційної безпеки цивільної авіації». Даним Законом встановлено, що під час виконання міжнародних рейсів з/до України або транзитних рейсів через аеропорти України авіаперевізник зобов'язаний надавати органу охорони державного кордону, митним органам та головному органу у загальнодержавній системі боротьби з терористичною діяльністю інформацію про пасажирів таких міжнародних рейсів, що включає прізвище, ім'я пасажирів, його стать, громадянство, дату народження, серію, номер документа, що посвідчує особу [9]. Дана інформація надається авіаперевізником за 72 години до запланованого часу виконання міжнародного рейсу та у разі зміни цієї інформації авіаперевізник зобов'язаний надати оновлену інформацію не пізніше як за 30 хвилин до посадки повітряного судна в аеропорту України або після завершення реєстрації на міжнародний рейс, що виконується з аеропорту України [9].

Водночас, цей перелік даних, які надаються, не відповідає формату API / PNR. Зокрема, не передаються дані про вид, державу видачі і термін дії документа, назву

авіаліній, номер міжнародного рейсу, дату і час вильоту (посадки) повітряного судна, назву аеропорту, в якому відбулися виліт і посадка. Це, у свою чергу, не повною мірою сприяє виконанню завдання інформаційного забезпечення протидії злочинності [10].

У зв'язку з цим, як зазначає Володимир Нікіфоренко, з метою «запровадження системи використання механізму попередньої перевірки пасажирів прикордонниками у пунктах пропуску для повітряного сполучення в Україні вивчається можливість щодо впровадження кращих світових практик, які дозволили би здійснювати автоматизовану обробку даних реєстрації особи шляхом порівняння попередніх даних реєстрації особи з персональними даними, зібраними у відповідних базах даних або профілів даних реєстрації особи, що проводиться кожного разу під час передачі попередніх даних реєстрації особи авіаперевізниками» [3, с. 68].

Додаток 9 (Спрощення формальностей) до Чиказької Конвенції про міжнародну цивільну авіацію визначає, що «договірним державам слід включати біометричні дані в свої машинозчитувальні паспорти, візи та інші офіційні проїзні документи» [11]. В Україні з 2016 року в усіх міжнародних пунктах пропуску застосовуються біометричні сканери та сканери документів. Але з'явилися нові способи підроблення документів, тому актуальним є підвищення надійності біометричної верифікації та ідентифікації. Застосовувані в більшості паспортів стандарту ІКАО елементи захисту паспортів і біометрії вже є уразливими на нинішньому технічному рівні, який досягнуто криміналітетом [12]. Це означає, що з розвитком технологій (морфінг біометричних зразків, 3-D біопринтинг, створення штучної сітківки ока) вже не можна стверджувати про 100% надійність біометричної ідентифікації та її зв'язку з даними пасажира [13]. Наприклад, злиття біометричних зразків (морфінг), тобто трансформація зображень, що належать двом і більше особам, може забезпечити успішну верифікацію будь-якої з них. Серед способів підроблення дактилоскопічної біометрії є виготовлення шляхом 3-D біопринтингу фальшивих пальців, навмисне пошкодження шкіри хімічними речовинами або абразивними матеріалами; використання посмертних відбитків пальців.

Незважаючи на те, що розпізнавання по райдужній оболонці ока є точною і надійною біометричною модальністю (в зв'язку з тим, що райдужна оболонка ока не змінюється з часом), але і вона має свої уразливості. До їх числа належать: використання косметичних контактних лінз з надрукованою райдужною оболонкою; використання високоякісних зображень облич, доступних в Інтернеті, для отримання роздрукованих зображень очей; хірургічне вживлення по-іншому пофарбованої райдужної оболонки поверх справжньої райдужної оболонки ока людини [14, с. 38].

Висновки і пропозиції. Отже, нами розкрито логіку доцільності системи використання даних про пасажирів (API/PNR) в інтересах прикордонної безпеки. В Україні як на рівні закону [9], так і на підзаконному рівні існує певне нормативне підґрунтя для обробки попередньої інформації [15]. Разом із тим, підкреслено, що система обробки та обміну даними записів реєстрації пасажирів для повноцінного функціонування в Україні потребує врегулювання з урахуванням нижчезазначених обставин:

1. Беззаперечно, що успішне застосування обміну даними API і PNR залежить від єдиного підходу всіх учасників інформаційних відносин (як прикордонних відомств, так і авіакомпаній в різних державах) до питання про стандарт даних та стандарт їх передачі. А забезпечення такого єдиного підходу є проблемою і в ЄС, навіть незважаючи на єдність правового регулювання щодо формату даних та процедур обміну даними.

2. З практичної точки зору це обумовлює необхідність для органів прикордонного контролю у всіх державах прийняти стандартний формат даних API/PNR та їх передачі.

3. Через низку причин (деякі зазначено вище) біометрична ідентифікація, яка є частиною збору даних про пасажира, підлягає постійному вдосконаленню.

4. Серед іншого, важливим є визначення єдиного оператора даних, який відповідає за координацію. Наприклад, Киргизьким законодавством визначено, що оператором системи API / PNR є Антитерористичний центр Державного комітету національної безпеки Киргизької Республіки, який обробляє і зберігає ці дані. Це покликано мінімізувати ризики,

пов'язані із забезпеченням конфіденційності персональних даних громадян. Прикладом тут може бути норма Загального регламенту щодо захисту даних (GDPR) Європейського Союзу, згідно з якою носій персональних даних має право не бути суб'єктом такого рішення, що створює для нього правові наслідки, яке засноване виключно на автоматичній обробці даних, у тому числі профілювання ризиків щодо суб'єкта даних [16]. Так, на сучасному етапі навіть за умови максимальної технологізації правоохоронної діяльності, технологічні інструменти включно зі штучним інтелектом, не можуть застосовуватися без здорового глузду компетентного і грамотного співробітника правоохоронного органу, який володіє обстановкою і розуміє специфічний контекст місцевих умов [12].

Перспектива подальших розвідок у даному напрямі пов'язана з ключовим елементом дієвості механізму використання інформації про пасажирів, а саме налагодження каналу міждержавного взаємообміну даними за єдиним стандартом. Невиконання цієї умови, очевидно, негативним чином впливатиме на ефективність використання даних в інтересах прикордонної безпеки.

Список використаної літератури

1. Strengthening the United Nations crime prevention and criminal justice programme, in particular its technical cooperation capacity. Resolution 74/177 adopted by the General Assembly on 18 December 2019. URL: <https://undocs.org/en/A/RES/74/177>.
2. Resolution 2322 (2016) Adopted by the Security Council UN at its 7831st meeting, on 12 December 2016. URL: [https://undocs.org/S/RES/2322\(2016\)](https://undocs.org/S/RES/2322(2016)).
3. Нікіфоренко В. С. Організаційні та правові засади виявлення потенційних загроз національній (прикордонній) безпеці на основі обробки попередніх даних реєстрації особи. *Вчені записки ТНУ імені В. І. Вернадського. Серія: юридичні науки*. 2020. № 5. Т. 31(70). С. 64–69.
4. Deignan S. Advance Passenger Information for Aviation Security. *Security Community*. OSCE. 2016. № 4. 11 January 2017. URL: <https://www.osce.org/ru/magazine/315286>.
5. Advance passenger information (API) and its role in aviation security. working paper ICAO. High-Level conference on aviation security (HLCAS). Montréal, 12 to 14 September 2012. URL: <https://cutt.ly/OEp6VPq>.
6. 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. URL: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32016L0681>.
7. Resolution 2178 (2014) Adopted by the Security Council UN at its 7272nd meeting, on 24 September 2014. URL: [https://undocs.org/S/RES/2178\(2014\)](https://undocs.org/S/RES/2178(2014)).
8. Resolution 2396 (2017) Adopted by the Security Council UN at its 8148th meeting, on 21 December 2017. URL: [https://undocs.org/en/S/RES/2396\(2017\)](https://undocs.org/en/S/RES/2396(2017)).
9. Про Державну програму авіаційної безпеки цивільної авіації: Закон України від 21 березня 2017 р. URL: <https://zakon.rada.gov.ua/laws/show/1965-19#Text>.
10. Філіппов С. О. Інформаційне забезпечення протидії транскордонній злочинності. *Visegrad Journal on Human Rights*. 2018. № 4(2). С. 102–112.
11. Convention on International Civil Aviation. Annex 9. ICAO. URL: http://www.icscc.org.cn/upload/file/20200508/20200508100922_97215.pdf.
12. Филиппов С. А. Противодействие трансграничной преступности: дуэль технологий. *Сучасне право в епоху соціальних змін: Матер. XI Міжнар. наук.-практ. конф., м. Київ, Нац. авіац. ун-т, 26.02.2021*. Т.: Вектор, 2021. С. 357–360.
13. Філіппов С. О. Біометричні технології: значення для протидії транскордонній злочинності. *Вісник Національної академії Державної прикордонної служби України. Юридичні науки*. 2018. Вип. 2. URL: http://nbuv.gov.ua/UJRN/vnadrpcurn_2018_2_6.
14. Сборник практических рекомендаций Организации Объединенных Наций по ответственному использованию биометрических данных и обмену ими в рамках борьбы с терроризмом. URL: https://www.unodc.org/pdf/terrorism/Compendium-Biometrics/__.pdf.
15. Про затвердження Порядку подання авіаперевізниками або уповноваженими ними особами попередньої інформації про пасажирів, імпорتنі та транзитні вантажі, які перевозяться повітряними суднами, органом охорони державного кордону та митним органам: Наказ від 27.04.2012 № 291/506/228 АДПСУ, Мін. фінансів України, Мін. інфраструктури України. URL: <https://zakon.rada.gov.ua/laws/show/z0740-12#Text>.
16. EU GDPR «Automated individual decision-making, including profiling». Article 22. URL: <https://www.privacy-regulation.eu/en/article-22-automatedindividual-decision-making-including-profiling-GDPR.htm>.

References

1. Strengthening the United Nations crime prevention and criminal justice programme, in particular its technical cooperation capacity. Resolution 74/177 adopted by the General Assembly on 18 December 2019. URL: <https://undocs.org/en/A/RES/74/177>.
2. Resolution 2322 (2016) Adopted by the Security Council UN at its 7831st meeting, on 12 December 2016. URL: [https://undocs.org/S/RES/2322\(2016\)](https://undocs.org/S/RES/2322(2016)).
3. Nikiforenko V. S. (2020). Orhanizatsiyni ta pravovi zasady vyvavlennya potentsiynkh zahroz natsional'niy (prykordonniy) bezpetsi na osnovi obrobky poperednikh danykh reyestratsiyi osoby. *Vcheni zapysky TNU imeni V.I. Vernads'koho. Seriya: yurydychni nauky*. № 5. V. 31(70). P. 64–69. [in Ukrainian]
4. Deignan S. (2016). Advance Passenger Information for Aviation Security. *Security Community*. OSCE. № 4. 11 January 2017. URL: <https://www.osce.org/ru/magazine/315286>.
5. Advance passenger information (API) and its role in aviation security. working paper ICAO. High-Level conference on aviation security (HLCAS). Montréal, 12 to 14 Septmber 2012. URL: <https://cutt.ly/OEp6VPq>.
6. 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. URL: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32016L0681>.
7. Resolution 2178 (2014) Adopted by the Security Council UN at its 7272nd meeting, on 24 September 2014. URL: [https://undocs.org/S/RES/2178\(2014\)](https://undocs.org/S/RES/2178(2014)).
8. Resolution 2396 (2017) Adopted by the Security Council UN at its 8148th meeting, on 21 December 2017. URL: [https://undocs.org/en/S/RES/2396\(2017\)](https://undocs.org/en/S/RES/2396(2017)).
9. Pro Derzhavnu prohramu aviatsiynoyi bezpeky tsyvil'noyi aviatsiyi: Zakon Ukrayiny vid 21 bereznaya 2017 r. URL: <https://zakon.rada.gov.ua/laws/show/1965-19#Text>. [in Ukrainian]
10. Filippov S. (2018). Information support for counteraction to cross-border crime. *Visegrad Journal on Human Rights*. № 4(2). P. 102–112. [in Ukrainian]
11. Convention on International Civil Aviation. Annex 9. ICAO. URL: http://www.icscc.org.cn/upload/file/20200508/20200508100922_97215.pdf.
12. Filippov S. A. (2021). Protivodeystvie transgranychnoy prestupnosti: duél' tekhnologiy. Suchasne pravo v epokhu sotsial'nykh zmin: Materialy XI Mizhnarodnoyi naukovo-praktychnoyi konferentsiyi, m. Kyiv, Natsional'nyy aviatsiynyy universytet, 26 lyutoho 2021. Ternopil': Vektor. P. 357–360. [in Ukrainian]
13. Filippov S. O. (2018). Biometrychni tekhnolohiyi: znachennya dlya protydyiyi transkordonniy zlochynnosti. Visnyk Natsional'noyi akademiyi Derzhavnoyi prykordonnoyi sluzhby Ukrayiny. Yurydychni nauky. Vyp. 2. URL: http://nbuv.gov.ua/UJRN/vnadcurn_2018_2_6. [in Ukrainian]
14. United Nations Compendium of recommended practices for the responsible use and sharing of biometrics in counter-terrorism URL: https://www.unodc.org/pdf/terrorism/Compendium-Biometrics/Compendium-biometrics-final-version-LATEST_18_JUNE_2018_optimized.pdf. [in Russian]
15. Pro zatverdzhennya Poryadku podannya aviapereviznykamy abo upovnovazhenymy nymy osobamy poperedn'oyi informatsiyi pro pasazhyriv, importni ta tranzytni vantazhi, yaki perevozyat'sya povitryanymy sudnamy, orhanam okhorony derzhavnoho kordonu ta mytnym orhanam. Nakaz vid 27.04.2012 № 291/506/228 Administratsiyi Derzhavnoyi prykordonnoyi sluzhby, Min. Fin., Min. infrastruktury Ukrayiny. URL: <https://zakon.rada.gov.ua/laws/show/z0740-12#Text>. [in Ukrainian]
16. EU GDPR «Automated individual decision-making, including profiling». Article 22. URL: <https://www.privacy-regulation.eu/en/article-22-automatedindividual-decision-making-including-profiling-GDPR.htm>.

Стаття надійшла 10.09.2021 р.

С. А. Филиппов, докт. юрид. наук, канд. психол. наук, доцент, полковник
Заместитель начальника факультета правоохранительной деятельности
Национальная академия Государственной пограничной службы Украины
ул. Шевченко, 46, Хмельницкий, 29003, Украина
e-mail: nadpsu@i.ua
ORCID ID: <https://orcid.org/0000-0001-6700-4194>

НЕКОТОРЫЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ ДАННЫХ О ПАССАЖИРАХ (API/PNR) В ИНТЕРЕСАХ ПОГРАНИЧНОЙ БЕЗОПАСНОСТИ

Резюме

В статье раскрыта логика, механизм и основные параметры использования данных о пассажирах (API/PNR) в интересах пограничной безопасности.

Раскрыто соотношение понятий «предварительная информация о пассажирах» и «записи регистрации пассажиров». Подчеркнуто, что системы упрощения формальностей одновременно положительным образом влияют и на безопасность. Например, целью сбора данных в ЕС признается эффективная борьба с нелегальной миграцией и усиление пограничного контроля, а также предупреждение, выявление, расследование преступлений террористической направленности и серьезных преступлений. Это касается как системы предварительной информации о пассажирах (API), так и дополнительных данных о пассажирах, таких, как данные регистрации пассажиров (PNR). Бесспорно, что успешное применение обмена данными API / PNR зависит от единого подхода всех участников информационных отношений (как пограничных ведомств так и авиакомпаний в разных государствах) к вопросу о стандарте данных и стандарте их передачи. А обеспечение такого единого подхода является проблемой даже тогда, когда имеется единое правовое регулирование по формату данных и процедуре обмена данными.

В национальном законодательстве отсутствуют специальные нормативно-правовые акты, которые бы регулировали отношения по поводу обмена данными о регистрации авиапассажиров, также не определен единый оператор данных. Итак, существует необходимость в специальном нормативно-правовом регулировании обмена данными об авиапассажирах, пересекающих государственную границу Украины.

Ключевые слова: противодействие преступности, пограничная безопасность, пограничный контроль, пункты пропуска для воздушного сообщения, API / PNR, биометрия.

S. O. Filippov, Doctor of Juridical Sciences, Associate Professor, Colonel,
Deputy Dean of the Law Enforcement Faculty
the National Academy of the State Border Guard Service of Ukraine
Shevchenka Str., 46, Khmelnytskyi, 29003, Ukraine
e-mail: nadpsu@i.ua
ORCID ID: <https://orcid.org/0000-0001-6700-4194>

SOME ASPECTS OF USING PASSENGER DATA (API/PNR) IN SUPPORT OF BORDER SECURITY

Summary

The article reveals with the logic, mechanism and main parameters for using passenger data (API/PNR).

The interrelation of the concepts of “Advance Passenger Information” and “Passenger Name Record” has been revealed. It has been determined that the systems of simplification of formalities also have a positive effect on security. For example, the purpose of data collection in the EU is to effectively combat illegal migration and strengthen border control, as well as to prevent, detect, investigate and prosecute terrorist and serious crimes. This applies to both the Passenger Information System (API) and additional passenger data, such as Passenger Name Record (PNR) data. There is no doubt that the successful application of API and PNR data exchange depends on a unified approach of all participants in information relations (both border agencies and airlines in different countries) regarding the question of data standard and standard of their transmission. Ensuring such a unified approach is a problem even when there is unity of legal regulation on data format and data exchange procedures.

There are no special regulations in the national legislation that would regulate the relationship regarding the circulation of passenger registration data, nor is there a specific entity that processes this type of information. Thus, there is a need for special legal regulation of the circulation of information about airline passengers crossing the state border of Ukraine. In particular, the legislation must regulate the procedure, grounds, purpose of obtaining, processing, transmission, storage and destruction of information about passengers (its content), protection of the right to confidential information of persons operating international flights, establish a responsible controller of such information.

Keywords: crime counteraction, border security, border control, aviation checkpoints, API/PNR, biometrics.