UDC 343.985: 351.746.1
DOI https://doi.org/10.24144/2307-3322.2025.91.4.63

SPECIFICITIES OF THE APPLICATION OF API/PNR AS A TOOL OF OPERATIONAL AND SEARCH ACTIVITIES

Tuz O.S.,
PhD in Psychology
Associate Professor at the Department of Special Disciplines
National Academy of the State Border Guard Service of Ukraine
ORCID: 0000-0003-3879-4013

Basalyk S.A.,
PhD in law
Associate Professor at the Department of Special Disciplines
National Academy of the State Border Guard Service of Ukraine
ORCID: 0000-0002-4060-8673

Tuz O.S., Basalyk S.A. Specifics of using API/PNR as an instrument of operational and investigative activities.

The article provides a comprehensive analysis of the use of Advance Passenger Information (API) and Passenger Name Record (PNR) systems as significant instruments in the field of operational and investigative activities. The article highlights the historical development and legal framework governing the implementation of these systems, with a particular focus on international standards introduced by the United Nations Security Council, the International Civil Aviation Organization (ICAO), the European Union, the International Air Transport Association (IATA), and the World Customs Organization (WCO). The study examines in detail the practical experience of implementing API/PNR in the United States, Canada, Australia, and the European Union, underlining their crucial role in countering terrorism, illegal migration, human trafficking, drug smuggling, and other forms of transnational organized crime. API enables the transmission of identification data about passengers prior to their arrival, while PNR provides a wide range of additional information, including booking records, travel itineraries, personal data, and payment methods. The integration of API and PNR data therefore creates a powerful tool for risk assessment, detection of suspicious individuals, identification of criminal networks, and well-timed intervention by law enforcement agencies. The article also explores challenges associated with API/PNR implementation, such as the variable quality of data, technical interoperability issues between different systems, and the risks of human rights violating, particularly the right to privacy and data protection. Special emphasis is placed on the relevance of these systems for Ukraine, which is currently in the process of developing its own legal and institutional framework for API/PNR. The author argues that establishing a unified national API/PNR system in compliance with international standards will strengthen Ukraine's national security, improve border control, and foster deeper integration into global security and data exchange mechanisms.

Key words: API, PNR, operational and investigative activity, border control, international security, data protection.

Туз О.С., Басалик С.А. Специфіка застосування API/PNR як інструменту оперативно-розшукової діяльності.

У статті здійснено комплексний аналіз застосування систем Advance Passenger Information (API) та Passenger Name Record (PNR) як важливих інструментів у сфері оперативно-розшукової діяльності. Висвітлено основні етапи формування нормативно-правових засад їх функціонування, зокрема вимоги міжнародних організацій (Ради Безпеки ООН, ІСАО, ЄС, ІАТА, ВМО), які визначили стандарти обміну даними пасажирів між авіаперевізниками та державними органами. Проаналізовано практику впровадження API/PNR у США, Канаді, Австралії та

країнах Європейського Союзу, підкреслено їх значення для боротьби з тероризмом, нелегальною міграцією, торгівлею людьми, наркотрафіком та іншими формами транснаціональної злочинності. Показано, що API забезпечує можливість попереднього отримання ідентифікаційних даних пасажирів ще до прибуття рейсу, а PNR включає широкий спектр відомостей про бронювання, маршрути, контактні дані та способи оплати. Саме поєднання цих інформаційних масивів створює умови для ефективного аналізу ризиків, ідентифікації підозрілих осіб та своєчасного реагування правоохоронних органів. Окрему увагу приділено аналізу проблем, що виникають при використанні API/PNR: низька якість даних, складність технічної сумісності різних систем, ризики порушення прав людини та необхідність дотримання високих стандартів захисту персональної інформації. В контексті України окреслено завдання щодо створення національної системи збору й аналізу API/PNR, яка б відповідала міжнародним вимогам та дозволяла ефективно інтегруватися у глобальні механізми обміну даними. Підкреслено, що такий крок сприятиме підвищенню рівня національної безпеки, розвитку міжнародного співробітництва та забезпеченню надійного прикордонного контролю.

Ключові слова: API, PNR, оперативно-розшукова діяльність, прикордонний контроль, міжнародна безпека, захист персональних даних.

Problem statement. The growth of population mobility and cross-border transportation, as well as the escalation of terrorist threats, necessitate the implementation of modern information systems for controlling the movement of persons. Among such systems, API/PNR, which have proven effective in combating crime in many countries of the world, holds a key place [1; 2].

Analysis of recent research and publications. The API/PNR issue has been reflected in the works of foreign scholars, including N. Vavoula, M. Tzanou, R. Bellanova, as well as in reports of the European Commission and studies of ICAO, IATA and WCO [3; 4; 5]. In Ukraine, the issues of legal regulation of API/PNR are at the stage of formation and are mostly considered in the context of integration into EU standards and strengthening border security.

Purpose of the study. Comprehensive study of the specifics of the use of API/PNR as a tool of operational and investigative activities; analysis of international experience, international legal acts in the field of API/PNR, determination of the prospects for implementation in Ukraine; study of the practice of using API/PNR in other countries; outline of the problems and risks of implementing API/PNR in Ukraine.

Presentation of the main material. In today's conditions, effective management of migration processes and ensuring the security of international transportation are of particular importance. Air transport, being the fastest and one of the most widespread means of transportation between states, at the same time represents increased vulnerability in terms of cross-border crime and terrorist attacks. That is why information systems for preliminary screening of passengers are increasingly being implemented in world practice, among which API (Advance Passenger Information) and PNR (Passenger Name Record) play a key role.

API involves the transfer of data contained in passengers' travel documents by airlines to border and law enforcement agencies before the flight arrives. PNR is a set of information about ticket reservations, travel itinerary, contact details and additional services that a passenger orders when purchasing a ticket. The combination of these two systems allows states to conduct preliminary risk analysis, identify suspicious persons, combat illegal migration, human trafficking and drug trafficking and terrorist financing.

The relevance of API/PNR research is due to several factors. First, international organizations, in particular the International Civil Aviation Organization (ICAO) and the UN Security Council, require member states to develop national systems for collecting and processing passenger data. In particular, UN Security Council Resolution 2396 (2017) directly obliges states to use API/PNR information in the fight against foreign terrorist fighters. Second, the European Union adopted Directive (EU) 2016/681, which obliges airlines to provide PNR data to competent authorities for the analysis of security threats. Third, in the practice of leading states (USA, Canada, Australia, Great Britain), API/PNR have become an integral element of the national and regional security system [6].

The purpose of this article is a comprehensive study of the specifics of the application of API/PNR systems and a generalization of international experience in their use to ensure aviation and national security.

To achieve the goal, the following tasks have been defined: 1) To analyze the regulatory and legal framework for the functioning of API/PNR at the international level; 2) To reveal the features of the practical application of API and PNR in leading countries of the world; 3) To identify key problems in the implementation of the API/PNR system (personal data protection, standardization, technical compatibility); 4) To assess the status of API/PNR implementation in Ukraine and development prospects in the context of European integration.

The object of the study is the systems for collecting and using API/PNR data in the field of international air transportation, and the subject is the legal, organizational, and practical aspects of their application in the context of ensuring the security of states and international aviation.

The scientific novelty of the article lies in the attempt to combine the analysis of international experience and the regulatory framework with the practical challenges facing Ukraine in the process of integration into the European aviation safety system.

The practical significance of the results obtained lies in the possibility of using the developments to improve national legislation, train specialists in the field of aviation and border security, as well as in increasing the effectiveness of international cooperation between Ukraine and the EU and other states in the field of countering terrorism and cross-border crime.

The main international imperatives for the collection and processing of passenger data are enshrined in UN documents and international aviation organizations. UNSCR 2396 (2017) explicitly calls on States to use API/PNR as an element in the fight against foreign terrorist fighters and strengthens the requirements for data exchange and integration of watch lists. In parallel, ICAO is working on the unification of concepts and technical approaches to API/PNR, and regional initiatives (in particular EU directives and regulations) define legal safeguards and control mechanisms.

International technical standards and recommendations for the format, content and transmission of API/PNR have been developed and disseminated by organizations such as IATA and WCO. IATA has published detailed "Guidelines" and an API/PNR toolkit that serve as a practical standard for airlines and booking agents. These standards cover the message format (e.g. PAXLST/PAXLST symbology), business processes for data transmission and recommendations for information security at the transport layer [7, 8].

National implementation models (state practice). In the practice of leading states, different but related models have been formed: the USA (APIS / eAPIS, Secure Flight, CBP - emphasis on pre-target sorting and immigration control), Canada (CBSA API / PNR - integrated targeting and interactive task program), the EU (regulation of PNR Directive 2016/681; current initiatives for total integration of API with EU regulations), the UK and Australia - each has its own transfer and storage procedures, but they share the desire to combine preliminary risk identification with operational interaction of law enforcement agencies. Practical reviews and government reports show that the success of the system depends on integration with local databases, high-quality targeting and cooperation with the aviation industry [12; 13; 14].

The scientific and analytical literature highlights the constant tension between the effectiveness of API/PNR for ensuring security and the risks to privacy, personal data protection and legal protection procedures (data retention, third-party access, automatic "rule-based" sorting algorithms). European court cases and analyses have shown the need for clear guarantees, data minimization and transparent control procedures. The authors also talk about the problem of "extraterritoriality" of data access (transfers between jurisdictions) and the difficulty of harmonizing different protection standards in the US, the EU and other regions.

Challenges include standardizing formats (to reduce the burden on airlines), ensuring the cybersecurity of the transmitted data, ensuring the quality and completeness of PNR (PNR often contains non-standardized free text fields), and developing methods for the legal and ethical use of machine learning/AI for targeting. New initiatives (including EU efforts on API regulation and projects to generate synthetic PNR datasets for research) aim to mitigate these issues [15; 17].

Literature and official documents demonstrate that API/PNR is already an established international security tool with developed technical standards and significant practice of use. At the same time, issues of compatibility of legal regimes, guarantees of privacy and transparency of data processing remain key for the reversible legitimization of such systems in democratic states. For Ukraine, it is important to simultaneously resolve technical compatibility with European mechanisms and ensure reliable legal and institutional guarantees of data protection.

API and PNR systems are considered in modern international practice as key tools for ensuring aviation and national security. Their importance is especially growing in the context of increased international crime and terrorist threats, when the preventive nature of information allows for proactive action. According to UN Security Council Resolution 2396 (2017), states are obliged to create appropriate conditions for the collection, analysis and use of API/PNR data to counter terrorist threats [2]. In the European Union, similar requirements are enshrined in Directive (EU) 2016/681 [1], which establishes the procedure for the use of PNR information for the prevention, detection and investigation of terrorist and serious criminal offences.

API provides basic identification data (name, date of birth, passport number, citizenship, flight, date and time of arrival), which allows to verify the identity even before the actual arrival of the plane. PNR, in turn, contains extended information about the booking: travel route, contact details, companions, payment methods, baggage, and changes in booking. For operational and investigative activities, such a combination creates the basis for preliminary targeting and identification of risky passengers; building connections and network structures (co-travel, frequent-co-booking); reconciliation with national and international databases (wanted lists, sanction lists, stolen document databases); verification of operational information received from other sources (agent, technical, financial).

Thus, API/PNR functions as a multi-layered tool for initial verification and confirmation of available operational data.

Operational model of application in operational and investigative activities. The process of using API/PNR in the practice of operational units includes the following stages: 1) Data receipt - structured API fields and unstructured PNR records from airlines; 2) Normalization and cleaning - bringing data to a unified format, eliminating duplicates, selecting relevant fields; 3) Automatic sorting - applying risk scoring algorithms (rule-based, ML); 4) Analytical work - checking and interpreting results by an operative, reconciliation with other databases; 5) Response - organizing operational measures: additional examination, temporary detention, arrest.

The success of this process depends on the technical compatibility of data transmission channels, the quality of the entered PNR records, as well as the availability of interdepartmental cooperation protocols (MoU).

The use of API/PNR in ORD involves a balance between efficiency and respect for human rights.

Basic requirements: legal basis for data collection and processing (national legislation, international treaties); proportionality and minimization of the amount of information used; data storage periods with subsequent anonymization; access control and audit; protection of personal data in accordance with the principles of the GDPR in the EU [9].

The Court of Justice of the European Union in case C-817/19 emphasized that the processing of PNR data must be carried out within the framework of clearly defined legal guarantees [10]. Data quality: PNR records may be incomplete or contain errors. 2. Format incompatibility: different GDS systems (Amadeus, Sabre, and Galileo) generate PNRs differently. 3. Cybersecurity: large amounts of personal data are an attractive target for attackers. 4. Algorithmic risks: automated systems risk creating “false positives” and biased decisions [17; 18].

Conclusions. In conclusion, it can be stated that API/PNR have become an integral element of operational and investigative activities in the aviation sector. Their effectiveness lies in the possibility of preventive response, testing hypotheses and identifying network connections of criminals. At the same time, their application requires strict legal guarantees, technical compatibility and independent supervision. The implementation of API/PNR systems in Ukraine is an important step towards strengthening national security and integration into the European space. However, a number of problems, including imperfect legislation, high financial costs and technical challenges, accompanies this process. Significant risks are associated with the protection of personal data and possible cyber threats, which requires comprehensive solutions in the field of information security. It is important to ensure a balance between the state’s needs for control and compliance with citizens’ rights to privacy. Therefore, the success of the implementation will depend on effective coordination of state bodies, proper legal regulation and compliance with international standards.

Further research will be aimed at improving data quality, developing transparent risk assessment algorithms, and improving international cooperation in information exchange.

REFERENCES:

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. Official Journal of the European Union. 2016. L119/132–L119/149.
2. United Nations Security Council. Resolution 2396 (2017) [on threats to international peace and security caused by terrorist acts]. S/RES/2396 (2017). New York: UN, 2017.
3. Vavoula N. EU Passenger Name Records (PNR): A Privacy Test for the European Union. Computer Law & Security Review. 2018. Vol. 34, No. 6. P. 1277–1291.
4. Tzanou M. Data Protection, Privacy and European PNR Data-sharing: A New Era of Mass Surveillance in the EU? Common Market Law Review. 2017. Vol. 54, No. 3. P. 807–841.
5. Bellanova R., de Goede M. The Algorithmic Regulation of Security: An Infrastructural Perspective. Regulation & Governance. 2022. Vol. 16. P. 91–107.
6. International Civil Aviation Organization (ICAO). Guidelines on Passenger Name Record (PNR) Data. Montreal: ICAO, 2010.
7. International Air Transport Association (IATA). Passenger Data Toolkit: API/PNR Guidelines. Montreal: IATA, 2019.
8. World Customs Organization (WCO). WCO/IATA/ICAO Guidelines on Advance Passenger Information (API). Brussels: WCO, 2014.
9. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation, GDPR). Official Journal of the European Union. 2016. L119/1–L119/88.
10. Judgment of the Court of Justice of the European Union (Grand Chamber) of 21 June 2022. Ligue des droits humains v Conseil des ministres. Case C-817/19. ECLI:EU:C:2022:491.
11. U.S. Customs and Border Protection (CBP). Advance Passenger Information System (APIS) Guide. Washington, DC: CBP, 2019.
12. Canada Border Services Agency (CBSA). Passenger Protect Program and API/PNR Framework. Ottawa: CBSA, 2018.
13. European Commission. Report on the Implementation of Directive (EU) 2016/681 on the Use of PNR Data. Brussels: European Commission, 2020.
14. European Data Protection Supervisor (EDPS). Opinion on PNR Directive Implementation. Brussels: EDPS, 2018.
15. Privacy International. PNR and API Systems: Surveillance of Travellers. London: Privacy International, 2019.
16. International Civil Aviation Organization (ICAO). Annex 9 to the Chicago Convention – Facilitation. 15th ed. Montreal: ICAO, 2017.
17. European Union Agency for Fundamental Rights (FRA). Fundamental Rights and the PNR Directive: Report. Vienna: FRA, 2019.
18. Council of the European Union. EU Strategy for Passenger Data and API/PNR Interoperability. Brussels: Council of the EU, 2021.