МІЖНАРОДНЕ ПРАВО

UDC 343.32:341.4
DOI https://doi.org/10.32782/chern.v5.2023.18

O. V. Batiuk
Doctor of Law, Associate Professor,
Professor at the Department of State Security
Lesya Ukrainka Volyn National University
orcid.org/0000-0002-2291-4247

A. V. Pasichnyk
Lecturer at the Department of Military Communications and Informatization
National Academy of National Guard of Ukraine
orcid.org/0000-0001-9570-9888

INTERNATIONAL EXPERIENCE IN INVESTIGATING CRIMES AGAINST THE FOUNDATIONS OF NATIONAL SECURITY

In the provisions of the scientific article, the study of foreign countries' regulatory legal acts, which reveal the main provisions of international approaches to the investigation of crimes against the foundations of national security, is carried out by the author. On this basis, the author proposes generalised scientific provisions for improving the national legislation of Ukraine. The author of the article comes to the conclusion that in the EU member states there are legal acts adopted by the EU which regulate the investigation of crimes that infringe on the legal order of several member states of the Union. Cooperation in the fight against crime is one of the most important areas of the common European policy. This area is regulated by the EU's constituent acts, namely the 1992 EU Treaty, the 1997 Treaty of Amsterdam, the 2001 Treaty of Nice, the Convention establishing a European Police Agency and acts of theoretical law. The priority tasks of cooperation between the police and judicial authorities of the EU member states in the criminal law sphere are to counter grave and especially grave crimes that pose an extreme danger to the EU member states. To fulfil this task, the EU established the European Police Office – Europol.

The authors determine that the success of the pre-trial investigation of crimes against the foundations of national security depends on the effective solution of the following tasks, namely: firstly, in connection with the detection of signs of a crime against the foundations of national security during the pre-trial investigation, a number of tasks arise which need to be addressed, namely: to establish whether a crime or a criminal offence against the foundations of national security has actually been committed, since the act committed does not have signs of criminal punishment; what kind of criminal offence against the foundations of national security was committed and by whom; what is the criminal qualification of the act against the foundations of national security; find out all the circumstances relevant to criminal proceedings against the foundations of national security; if there are sufficient grounds and verified evidence, formulate a suspicion and notify the person involved in the commission of a criminal offence against the foundations of national security; find out the causes and conditions that contributed to the commission of a crime against the foundations of national security.

Key words: security, government, sabotage, state, foreign experience, capture, criminality, forensics, espionage.

Батюк О. В., Пасічник А. В. **МІЖНАРОДНИЙ ДОСВІД РОЗСЛІДУВАННЯ ЗЛОЧИНІВ ПРОТИ ОСНОВ НАЦІОНАЛЬНОЇ БЕЗПЕКИ**

У положеннях наукової статті авторами проводиться дослідження нормативно-правових актів зарубіжних країн, які розкривають основні положення міжнародних підходів розслідування злочинів проти основ національної безпеки. На цій основі автори пропонують узагальнені наукові положення щодо удосконалення національного законодавства України. Автори наукової статті доходять висновку, що у державах – членах ЄС діють правові акти, прийняті ЄС та які регламентують діяльність із розслідування злочинів, що посягають на правовий порядок кількох країн – учасниць Союзу. При цьому одним із найважливіших напрямів єдиної загальноєвропейської політики виступає співпраця з питань боротьби зі злочинністю. Зазначений напрям регулюється установчими актами ЄС, а саме – Договором про ЄС 1992 р., Амстердамським договором 1997 р., Ніццьким договором 2001 р., Конвенцією про створення Європейського поліцейського відомства й актами теоретичного права. Пріоритетними завданнями співпраці поліції та судових органів держав – учасниць ЄС у кримінально-правовій сфері є протидія тяжким і особливо тяжким злочинам, що становлять надзвичайну небезпеку країнам – членам Союзу. Для виконання вказаного завдання в ЄС було створено Європейське поліцейське відомство – Європол.

Автори визначають, що успіх досудового розслідування злочинів проти основ національної безпеки залежить від ефективного вирішення наступних завдань, а саме: встановити, чи справді було вчинено злочин або кримінальний проступок проти основ національної безпеки, або ж вчинене діяння не має ознак кримінальної караності; яке саме кримінальне правопорушення проти основ національної безпеки вчинено і ким саме; якою є кримінальна кваліфікація даного діяння проти основ національної безпеки; з'ясувати всі обставини, що мають значення для кримінального провадження проти основ національної безпеки; якщо є достатні підстави і перевірені докази,

то сформулювати підозру і повідомити про неї особу, яка причетна до вчинення кримінального правопорушення проти основ національної безпеки; з'ясувати причини й умови, що сприяли вчиненню злочину проти основ національної безпеки.

Ключові слова: безпека, влада, диверсія, держава, зарубіжний досвід, захоплення, злочинність, криміналістика, шпигунство.

A general description of the problem under analysis and its connection with important scientific or practical tasks. The relevance of the research topic is that, according to the official data of the Office of the Prosecutor General of Ukraine, the Unified Report on Criminal Offences for January-December 2022 officially disclosed 14,639 crimes against the foundations of national security of Ukraine, criminal offences in proceedings in which pre-trial investigation is carried out by security agencies. As of October 2023, 4,461 crimes against the foundations of Ukraine's national security were officially disclosed. In general, as of 4 December 2024, the Office of the Prosecutor General recorded 15,813 crimes against the national security of Ukraine committed since 24 February 2022, the date of the full-scale invasion of Ukraine by the Russian Federation [1].

Analysis of recent publications on the issue and identification of previously unresolved parts of the general problem. It should be noted that the problems of pre-trial investigation of crimes against the foundations of the national security of the State, the peculiarities of conducting investigative and covert investigative (detective) actions, as well as the detailing of the procedural order of their conduction and the development of specific ways to solve problematic issues in the field of criminalistics, criminal procedure, and the theory of operational and investigative activities were the subject of research by such domestic scholars as V.G. Honcharenko Hora I.V., Kolesnyk V.A., Loboyko L.M., Lukianchykova E.D., Nora V.T., Pogoretskyi M.A., Popelushko V.O., Shumyla M.E., Khodanovych V.O. Despite a significant number of works on the above-mentioned issues, we have every right to state that the issue of implementation of foreign experience in the practice of investigating crimes against the foundations of national security has been studied only superficially, which was a premise for the preparation of this scientific work.

Setting the objective. We consider it expedient, by analysing foreign scientific sources and relevant information reviews of forensic practice in the field of investigation of crimes against national security in foreign countries, to investigate the mechanisms and effective tools successfully used by foreign security agencies in the pre-trial investigation of crimes against the foundations of national security.

Official data of the Office of the Prosecutor General of Ukraine. 04.12.2023 [2]

Outline of the main material. The analysis of crimes against the national security foundations should begin with the United Kingdom of Great Britain and Northern Ireland.The main regulatory document of Great Britain in the field of National Security is- Security policy framework [3] date published April 2014 updated 2 December 2022 year.

The Security Policy Framework. The Prime Minister is ultimately responsible for the overall security of HMG. They are supported by the Cabinet Secretary, who chairs the Official Committee on Security (SO). Across HMG responsibility for the security of organisations lies with the respective Ministers, Permanent Secretaries and Management Boards.

This Framework describes the Cabinet Secretary and SO's expectations of how HMG organisations and third parties handling HMG information and other assets will apply protective security to ensure HMG can function effectively, efficiently and securely. There are some principles common to every area of security.

Protective security should reflect the UK's widest national security objectives and ensure that HMG's most sensitive assets are robustly protected.

Security must enable the business of government and should be framed to support HMG's objectives to work transparently and openly, and to deliver services efficiently and effectively, via digital services wherever appropriate.

Risk management is key and should be driven from Board level. Assessments will identify potential threats, vulnerabilities and appropriate controls to reduce the risks to people, information and infrastructure to an acceptable level. This process will take full account of relevant statutory obligations and protections, including data protection legislation, the Freedom of Information Act, the Official Secrets Act, Equality Act, and the Serious Organised Crime and Police Act.

Attitudes and behaviours are fundamental to good security. The right security culture, proper expectations and effective training are essential.

Security Outcomes. The Cabinet Secretary and SO expect all HMG organisations (and partners handling HMG information) to meet a range of mandatory security outcomes described below. These outcomes do not specify particular processes but describe what good security will look like. HMG organisations will consult the full range of policy, advice and guidance provided by the Cabinet Office, Centre for the Protection of National Infrastructure, National Cyber Security Centre, and other sources of good practice to shape their business specific approaches, mindful that:

Government organisations know their own business best, including how local risks should be managed to support operations and services.

Permanent Secretaries and Heads of Department are accountable to Parliament for the security of their organisations.

An annual reporting process (the Security Risk Management Overview) will ensure compliance and an appropriate level of commonality across government.

Effective leadership is a critical component of good security and accountability. The Permanent Secretary (or equivalent) will own the organisation's approach to security and ensure that these issues receive the attention and investment required.

Government organisations will have:

a. An appropriate security governance structure to support the Permanent Secretary, that is properly resourced with individuals who have been appropriately trained. These include:

– a Senior Information Risk Owner (SIRO);

– a Departmental Security Officer (DSO) who can manage day-to-day protective security;

– Information Asset Owners (IAOs) across distinct business units;

– Information risk assessment and risk management specialists;

– other specialists relevant and specific to the organisation's needs

b. Board-level oversight of security compliance and auditing processes.

c. Arrangements to determine and satisfy themselves that Delivery Partners, service providers and third party suppliers, apply proper security controls too (including List X accreditation for companies handling SECRET assets).

Everyday actions and the management of people, at all levels in the organisation, contribute to good security. A strong security culture with clear personal accountability and a mature understanding of managing risk, responsibility and reputation will allow the business to function most effectively.

Government organisations will have:

– a security culture that supports business and security priorities and is aligned to HMG's overarching priorities and the organisation's own appreciation of risk

– training which encourages personal responsibility and good security behaviours;

– processes, systems and incentives to deliver this;

– mechanisms to drive continuous improvement, tackle poor and inappropriate behaviour, enforce sanctions and encourage the sharing of best practice.

All HMG activities attract risk. Risks need to be assessed by government organisations so that they can make informed, practical and effective business enabling decisions.

Government organisations will have:

– a mature understanding of the security risks throughout the organisation, where appropriate

this will be informed by the National Technical Authorities;

– a clearly-communicated set of security policies and procedures, which reflect business objectives to support good risk management;

– mechanisms and trained specialists to analyse threats, vulnerabilities, and potential impacts which are associated with business activities;

– arrangements to determine and apply cost-effective security controls to mitigate the identified risks within agreed appetites;

– assurance processes to make sure that mitigations are, and remain, effective.

The security of information is essential to good government and public confidence. To operate effectively, HMG must maintain the confidentiality, integrity and availability of its information.

Government organisations will have:

– staff who are well trained to exercise good judgement, take responsibility and be accountable for the information they handle, including all partner information;

– mechanisms and processes to ensure assets are properly classified and appropriately protected;

– confidence that security controls are effective and that systems and services can protect the information they carry. There will be an overarching programme of information assurance driven by the Board.

The delivery of efficient public services, including the proper protection of citizen data, requires modern and functional technology. Resilience to cyber threats, compliance with data protection laws and management of national security-related information within these systems will require security to be integral to their design and implementation.

Government organisations will have:

a. Identified if technology and services are Critical National Infrastructure, and risk manage accordingly.

b. Risk-informed security controls which:

– mitigate applicable threats;

– are kept current and actively managed;

– protect against, detect and correct malicious behaviour;

– ensure that critical technology and services are resilient to disruptive challenges such as cyber attacks, and have the means to recover from these.

People are an organisation's most important asset, so personnel assurance is fundamental to good security. Government organisations will deliver the appropriate combination of recruitment checks, vetting and on-going personnel security management to be assured, and to remain assured, about their people and to mitigate the risks from well-placed insiders.

Government organisations will have:

– joined-up HR and personnel security policies and processes, including recruitment checks (the Baseline Personnel Security Standard (BPSS)) for those with access to HMG assets;

– processes to evaluate areas of particular insider risk which require corresponding and proportionate levels of vetting;

– robust arrangements for managing the delivery of vetting services, and mechanisms to handle appeals;

– effective aftercare arrangements that include regular security appraisals, promote a security conscious culture, and drive staff and line management engagement.

Appropriate physical security measures will ensure a safe and secure working environment for staff that can protect against a wide range of threats (including theft, terrorism or espionage).

Government organisations will have:

– processes and plans in place, including those developed from the early stages of building design, to determine the appropriate physical security requirements through planning and risk assessment;

– mechanisms to implement internal and external security controls in a layered fashion that deter or prevent unauthorised access and protect assets, especially those that are critical or sensitive, against forcible or surreptitious attack;

– substantial controls for controlling access and proximity to the most high risk sites and Critical National Infrastructure assets.

Well-tested plans, policies and procedures will reduce organisations' vulnerability to security incidents (especially from the most serious threats of terrorism or cyber attack), but also leaks and other disruptive challenges.

Government organisations will have:

– business continuity arrangements aligned to industry standards, to maintain key business services, building resilience and security to facilitate a rapid and effective response to recover from incidents;

– processes in place to regularly conduct risk and vulnerability assessments and review resilience planning for critical assets, particularly those identified as Critical National Infrastructure;

– counter-terrorism contingency plans in place setting out procedures to be followed in the event of a terrorist threat, including procedures to immediately adjust security requirements around the Government Response Level system;

– effective management structures that ensure shared communications between HR and security teams and provide policies and procedures for detecting, reporting, responding to and handling incidents, including disciplinary measures that are well communicated and understood by staff;

– reporting mechanisms to the Cabinet Office Government Security Group, regarding incidents of unauthorised disclosure and breaches of official information, including incidents concerning classified information from foreign governments, agencies or organisations. In addition, such mechanisms should also exist to the Information Commissioner's Office for if and when a serious loss or breach of personal data occurs, in line with data protection legislation.

Protective security should always be approached in the round (holistically), but it is helpful to bear in mind specific areas of information, physical and people security. HMG policy across these three areas is set out below:

Information Security.

All information that HMG deals with has value. HMG handles the wide variety of information that it generates, collects, processes, stores and exchanges appropriately to ensure: the confidentiality of citizen data and commercial information; good government and the effective and efficient delivery of public services; the proper protection of national security-related information; and that obligations to international partners are met. HMG expects its' partners in the wider public sector, suppliers and other commercial partners who handle information on HMG's behalf to do the same.

HMG operates a Classification Policy to identify and value information according to its sensitivity and to drive the right protections. This comprises three levels: OFFICIAL, SECRET and TOP SECRET for which there are distinct security arrangements. OFFICIAL covers most of the day-to-day business of government, service delivery, commercial activity and policy development.

SECRET and TOP SECRET information will typically require bespoke, sovereign protection, but OFFICIAL information can be managed with good commercial solutions that mitigate the risks faced by any large corporate organisation. In this way government can deliver securely and efficiently, and shape its services to meet the user needs.

The effective management of information is critical to safeguarding it. Government organisations will consider good information management practice as the basis for their information security arrangements.

Technology and Services.

HMG will deliver services to the public digitally wherever it can. These services must be designed and delivered securely. A Public Services Network (PSN) offers an infrastructure across the public sector to increase efficiency and reduce overall expenditure. Organisations will utilise appropriate technologies (including mobile devices) and services (including Cloud) and secure these by default wherever possible. Contracts will specify security requirements clearly.

For new policies or projects that include the use of personal information, an initial assessment on the privacy risks to individuals in the collection, use and disclosure of the information, is made. All ICT systems that manage government information or that are interconnected to them are assessed to identify technical risks. Proportionate assurance processes will provide confidence that these identified risks are being properly managed. This also takes account of risks originating from within the organisations, which could arise from poor behaviours and malicious insiders.

Accountability.

HMG organisations are responsible for the information they handle under appropriate governance structures, including at Board level lead. A SIRO is accountable and responsible for information risk across the organisation, supported by IAOs from distinct business units. The SIRO will ensure that everyone is aware of their personal responsibility to exercise good judgement, and to safeguard and share information appropriately. HMG continues to remind the public of the importance of protecting their own information online and when accessing government services.

Physical Security.

HMG has a wide, diverse estate at home and abroad, including administrative HQs, military bases, Embassies, public offices, and service centres. To ensure: the proper protection of citizen data, commercial confidences, and national security related information; good government and the efficient delivery of public services; and a safe working environment for staff and visitors, a range of physical security controls are required. HMG assets held or managed by third parties must be similarly protected.

The range of physical controls will vary depending upon circumstances and business requirements, and the type of threats (including natural hazards, other disruptive challenges, crime, terrorism, and espionage). Organisations will layer their security, including: perimeter controls and guarding; building design features; limiting, screening or otherwise controlling access; appropriate fittings and office furniture; and the use of separate areas in buildings for particularly sensitive work. Controls should not be onerous but proportionate to ensure the safety and security of staff and visitors.

HMG organisations should also have in place arrangements to adapt and enhance security measures if there is an increase in threats, especially from terrorism. In such circumstances, it may be necessary to limit non-essential access; to increase the frequency of staff and visitor checks and bag

searches; and to establish additional perimeter controls and other guarding activities. Response mechanisms and contingency plans are in place to respond to possible critical security incidents and to enable the continuity of services.

Personnel Security and National Security Vetting.

Personnel security controls confirm the identity of individuals (employees and contractors) and provide a level of assurance as to their trustworthiness, integrity and reliability. Whilst HMG personnel security controls cannot provide guarantees, they are sensible and important precautions.

It is HMG's policy that all areas of government and the national infrastructure should include in their recruitment processes certain basic checks. These checks include verification of the applicant's identity, employment history, their right to work in the UK and, if appropriate, checks of any unspent criminal records. Within government these controls are described in the Baseline Personnel Security Standard.

National Security Vetting.

National security vetting comprises a range of additional checks and may be applied where policy or a bespoke risk assessment indicates it is proportionate to do so. The risk assessment process takes account of the access an individual may have to sensitive assets (physical, personnel or information) at risk from a wide range of threats. These threats will include: terrorism, espionage, or other actions that could threaten the UK.

There are five main levels of national security vetting clearance: Accreditation Check (AC), Counter-Terrorist Check (CTC), Level 1B, Security Check (SC), and Developed Vetting (DV). Before any such clearance is undertaken the requirements of the Baseline Personnel Security Standard, or equivalent background checks for the AC, must be met. Whilst the information required and the range and depth of checks undertaken at each level may vary, they are all intended to allow Government departments and agencies, the Armed Forces and police forces to assess whether individuals who are to be employed in sensitive posts or critical functions might represent a security risk either directly or indirectly.

Ongoing Personnel Security Management.

The national security vetting process provides an assessment of the vetting subject at the time the process is carried out, but active, ongoing personnel security management is required to ensure that a security clearance maintains its currency. As a minimum, this will involve active consideration of the vetting subject's continuing conduct in respect of security matters; it will also require checks to be repeated at regular intervals.

Judicial and investigative practice determines what in the case of Chahal v. the United Kingdom [UK], the UK authorities wished to deport the applicant, an Indian citizen suspected of involvement in terrorist activities related to Sikh separatism, for reasons of national security and on other grounds, namely the international fight against terrorism. The applicant relied on Article 3 because of the risks of torture to which he would be exposed again if he were returned to India. The Government argued that Article 3 contained an implicit restriction which allowed a Contracting State to deport an individual to another country, even in the event of a real risk of ill-treatment, when that deportation was necessary in the interests of national security. The Court rejected this view of things. In its opinion, the prohibition of ill-treatment set out in Article 3 was equally absolute in deportation cases. Thus, whenever substantial grounds had been shown for believing that an individual would face a real risk of being subjected to treatment contrary to Article 3 if removed to another State, the responsibility of the Contracting State to safeguard him or her against such treatment was engaged in the event of deportation. The activities of the individual in question, however undesirable or dangerous, could not be a material consideration, and this has been reaffirmed subsequently on many occasions by the Court (see, for example, Auad v. Bulgaria; in respect of the principles for assessing the risk of exposure to ill-treatment, see Saadi v. Italy [GC]) [4].

National security considerations may affect the safeguards provided by Article 5, but the Court is far from willing to give carte blanche to the authorities every time they invoke national security.

This absence of carte blanche for the authorities recurs even in some cases connected with security problems outside national territory, as in the case of Al-Jedda v. the United Kingdom [UK], which concerned the preventive detention of an Iraqi national by the British forces in Iraq on the basis of a UN Security Council resolution. The Court concluded that the resolution authorised the United Kingdom to take steps to contribute to the maintenance of security and stability in Iraq, without, however, requiring the United Kingdom to imprison, without any time limit or charge, an individual considered to be a security risk. In these conditions, in the absence of a binding obligation to make use of internment, the Court considered that there was no conflict between the obligations imposed on the United Kingdom by the United Nations Charter and those deriving from Article 5 § 1 of the Convention, which should therefore be complied with. The Court concluded that the applicant's detention constituted a violation of Article 5 § 1 [4].

The analysis of crimes against the national security foundations should begin with the Germany.

The paramount task of German security policy is to ensure that we can continue to live in our

country in peace, freedom and security. Germany's security is indivisible from that of our European partners and allies. Our commitment to NATO and the EU is unshakeable. We stand resolutely by the mutual defence pledge under Article 5 of the North Atlantic Treaty. We are strengthening the Bundeswehr as a cornerstone of defence in Europe. National and collective defence is the core task of the Bundeswehr, and this task includes our contribution to NATO's deterrence capabilities. We will allocate two percent of our GDP, as an average over a multi-year period, to reaching NATO capability goals, initially in part via the newly created special fund for the Bundeswehr. At the same time, we will bolster investments in critical-infrastructure protection, cyber capabilities, effective diplomacy, civil protection, stabilising our partners, and dedicated humanitarian assistance and development cooperation.

We aim to strengthen civil preparedness and protection through a comprehensive approach involving the whole of society, with the Federal Government, the Länder, the municipalities, the business sector and the public taking on responsibility together. We are improving Federal Government support for the Länder in the field of disaster prevention and relief and making our critical infrastructure more resilient.

Our goal remains a Europe united in peace and freedom. We want to ensure that the European Union (EU) is able to act geopolitically and to uphold its security and sovereignty for the coming generations. The Federal Government supports further EU integration, cohesion, and enlargement to include the Western Balkan states, Ukraine, the Republic of Moldova and, in the longer term, Georgia. In order to prepare the EU for this enlargement and to ensure its continued ability to act, reforms within the EU are essential.

Our security is lnked to the security and stability of other regions in the world. The EU's Common Security and Defence Policy plays a key role in our crisis management. Integrated Security means joining up civilian, military and police capabilities in crisis prevention, conflict management and peacebuilding and including these capabilities in our actions at international and multilateral level.

In this context, the Federal Government will also take particular account of the interests of women and disadvantaged groups, in line with a feminist foreign and development policy.

The Federal Government will increase its engagement to fight poverty, hunger, social inequality and the climate crisis. Where governments undermine security and the rule of law, we will focus our cooperation to a greater extent on non-state actors, the local level and multilateral approaches. At the same time, we will strengthen those partner governments that, like us, are committed to upholding the international order based on international law. The Federal Government will align its development policy to an even greater extent with its strategic goals.

We will increase our efforts to uphold the global arms-control architecture, nuclear disarmament and non-proliferation on the basis of the Non-Proliferation Treaty. Our goal remains a safe world free of nuclear weapons.

As regards the control of arms exports, the Federal Government will continue to adhere to its restrictive baseline policy. When deciding on arms exports, it will take into account in particular human rights, democracy and the rule of law in the importing country. At the same time, the Federal Government takes into account alliance and security interests, the geostrategic situation and the needs of enhanced European arms cooperation [5].

We agree with V.O. Khodanovych that knowledge of the actual circumstances of crimes against the foundations of national security begins even before the pre-trial investigation and often within the framework of counterintelligence and operational search activities. However, evidence in criminal proceedings, as an element of cognition, cannot arise objectively before the relevant procedural procedures are completed, as this requires procedural mediation. The investigator's assessment of the results of operational cognition of the actual circumstances of espionage, treason, etc. may become an impetus for the development of criminal procedural cognition and influence the investigator's decision to enter information about the detected crime into the Unified Register of Pre-trial Investigations and initiate criminal proceedings. The main subject of operational and investigative cognition is an operative unit officer who carries out such activities and has certain powers determined by his/her official status [6].

The conclusion of this study allows us to generalise:

– firstly, in the context of detecting signs of a crime against the foundations of national security during the pre-trial investigation, a number of tasks arise that need to be addressed, namely

– to establish whether a crime or criminal offence against the foundations of national security has actually been committed or the act does not have signs of criminal punishment;

– what kind of criminal offence against the foundations of national security was committed and by whom;

– what is the criminal qualification of the act against the foundations of national security;

– find out all the circumstances relevant to the criminal proceedings against the foundations of national security;

– if there are sufficient grounds and verified evidence, formulate a suspicion and notify the person involved in the commission of a criminal offence against the foundations of national security;

– to find out the reasons and conditions that contributed to the commission of a crime against the foundations of national security.

Secondly, we believe that in the EU member states there are legal acts adopted by the EU that regulate the investigation of crimes that infringe on the legal order of several member states of the Union. Cooperation in the fight against crime is one of the most important areas of the common European policy. This area is regulated by the EU's founding acts, namely the 1992 EU Treaty, the 1997 Treaty of Amsterdam, the 2001 Treaty of Nice, the Convention establishing a European Police Agency and acts of theoretical law. The priority tasks of cooperation between the police and judicial authorities of the EU member states in the criminal law sphere are to counter grave and especially grave crimes that pose an extreme danger to the EU member states. To fulfil this task, the EU established the European Police Office – Europol.

Bibliography

1. Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування. Офіс генерального прокурора України URL: *https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2 (дата звернення 20.11.2023)*

2. Злочини вчиненні в період повномаштабного вторгнення російської федерації. Офіс генерального прокурора України URL: https://gp.gov.ua *(дата звернення 04.12.2023)*

3. Security policy framework. Date published April 2014. URL: https://www.gov.uk/government/organisations/national-security *(date of application 19.11.2023)*

4. National security and European case-law. URL: *https://rm.coe.int/168067d214 (date of application 21.11.2023)*

5. Robust. Resilient. Sustainable. Integrated Security for Germany. National Security Strategy. URL: *https://www.nationalesicherheitsstrategie.de/National-Security-Strategy-EN.pdf (date of application 21.11.2023)*

6. Ходанович В.О. Окремі питання виявлення й досудового розслідування злочинів проти основ національної безпеки України. *Вісник Академії адвокатури України.* Число 38. Том. 14. № 1. 2017. С. 177–185. URL: *file:///C:/Users/Admin/Downloads/vaau_2017_14_1_24.pdf (дата звернення 22.11.2023)*