

Список використаних джерел

1. Конституція України: Закон України від 28 черв. 1996 р. № 254к/96-ВР. URL: <https://zakon.rada.gov.ua/laws/show/254k/96-вр>.
2. Закон України «Про медіа» від 13 груд. 2022 р. № 2849-ІХ. Дата оновлення: 01.01.2026. URL: <https://zakon.rada.gov.ua/laws/show/2849-20#Text>.
3. Стратегія інформаційної безпеки: Указ Президента України від 28 груд. 2021 р. № 685/2021. URL: <https://zakon.rada.gov.ua/laws/show/685/2021#Text>.
4. Дяковський О. С. Правові та інституційні механізми протидії дезінформації у розвинутих країнах світу. *Право і суспільство*. 2024. № 4. С. 210–214.
5. Інформаційна безпека суспільства в умовах дії правового режиму воєнного стану та повосенний період: збірник матеріалів міжвідомчого науково-практичного круглого столу (м. Київ, 29 трав. 2025 р.). Київ: Національна академія внутрішніх справ, 2025. 181 с.

Gaivaniuk Ivetta, cadet of the Dnipro State University of Internal Affairs

Research Supervisor – **Dekusar Ganna**, Senior Lecturer of Department of Language Training of Dnipro State University of Internal Affairs

INTERNATIONAL EXPERIENCE IN ENSURING NATIONAL SECURITY: INTEGRATION PROCESSES IN COUNTERING MODERN THREATS

The legal and organizational foundations of national security represent one of the most dynamic areas of contemporary legal scholarship, particularly in the context of the full-scale armed conflict in Ukraine and the growing complexity of hybrid threats worldwide. Ensuring national security requires not only effective domestic legislation but also active integration into international security frameworks, harmonization of national legal standards with international norms, and systematic exchange of experience with foreign partners. The relevance of this research is underscored by the fact that modern threats – including cyberattacks, disinformation campaigns, armed aggression, and terrorism – transcend national borders and demand coordinated multilateral responses.

The purpose of this study is to analyze the constitutional and legal foundations of Ukraine's national security, examine the role of law enforcement agencies in countering modern threats, and assess the integration processes that define international cooperation in the security domain.

The legal basis of the study includes: the Constitution of Ukraine of June 28, 1996 [1]; the Law of Ukraine «On National Security of Ukraine» of June 21, 2018 No. 2469-VIII [2]; the Law of Ukraine «On Combating Terrorism» of March 20, 2003 No. 638-IV [3]; the Criminal Code of Ukraine of April 5, 2001 No. 2341-III [4]; the National Security Strategy of Ukraine, approved by Decree of the President of Ukraine No. 392/2020 [5]; the HM Government Counter-Terrorism Strategy (CONTEST) 2023 [6].

I. Legal and Organizational Foundations of National Security

The constitutional framework of national security in Ukraine is established primarily by Articles 17 and 102 of the Constitution of Ukraine, which define the protection of sovereignty and territorial integrity as the most important functions of the state, entrusted to the President as Commander-in-Chief of the Armed Forces and the relevant security and defense sector institutions [1]. The Law of Ukraine «On National Security of Ukraine» (2018) consolidated a comprehensive legislative framework, defining the principles, objects, and subjects of national security, and establishing the National Security and Defense Council as the coordinating body in this sphere [2]. As V. Horbulin notes, the 2018 reform marked a paradigm shift from a reactive to a proactive model of national security governance, aligning Ukraine's institutional architecture more closely with NATO standards [7, p. 43].

The protection of the vital interests of individuals, society, and the state from internal and external threats is the central objective of national security policy. The National Security Strategy of Ukraine (2020) identifies a range of priority threats, including armed aggression, hybrid warfare, terrorism, cyberthreats, and corruption [5]. These threats are not isolated phenomena but form an interconnected complex that requires a whole-of-government response integrating law enforcement, intelligence, military, and civil society actors.

II. National Security Mechanisms: Challenges for the Law Enforcement System in Crisis Conditions

Modern hybrid threats present particular challenges for the law enforcement system. Hybrid warfare – combining conventional military operations, cyberattacks, disinformation, and political subversion – blurs the traditional distinction between internal and external security, placing law enforcement agencies at the intersection of policing and national defense. R. Thornton defines hybrid warfare as «the use of a tailored mix of conventional weapons, irregular tactics, terrorism, and criminal behavior in the same time and battlespace to obtain political objectives» [8, p. 12]. Ukraine's experience since 2014, and particularly since February 2022, has confirmed this definition in practice and highlighted the need for law enforcement agencies to develop capabilities beyond traditional policing.

The role of law enforcement in shaping national security policy has expanded significantly. The National Police of Ukraine, the Security Service of Ukraine, and the State Bureau of Investigation now operate not only as law enforcement bodies but as integral components of the national security architecture. Article 258 of the Criminal Code of Ukraine establishes criminal liability for terrorist acts with imprisonment ranging from five years to life, depending on the severity of consequences [4]. Article 258-5 addresses financing of terrorism, while Article 258-6, introduced in 2023, establishes liability for crossing the state border with terrorist intent [4]. These legislative developments reflect the growing intersection of criminal law and national security.

The training of security sector personnel emerges as a critical challenge in crisis conditions. The full-scale war has demonstrated that effective national security requires not only well-equipped and legally empowered agencies but also personnel capable of operating in complex, rapidly evolving environments. S. P. Kolesnik emphasizes that the development of professional competencies in counter-terrorism and national security among law enforcement personnel must be treated as a strategic priority, embedded in institutional training programs rather than addressed reactively [9, p. 30].

III. International Experience in Ensuring National Security: Integration Processes

The adaptation of national legislation to international standards is a defining feature of Ukraine's security reform trajectory. Ukraine's Euro-Atlantic integration aspirations have driven significant legislative harmonization, particularly following the Association Agreement with the European Union and the intensification of NATO cooperation. The 2018 National Security Law explicitly references Euro-Atlantic integration as a strategic objective [2], while the National Security Strategy (2020) identifies membership in NATO and the EU as priority foreign policy goals [5].

International experience offers valuable models for institutional design. The United Kingdom's CONTEST strategy – structured around the four pillars of Prevent, Pursue, Protect, and Prepare – is widely regarded as a benchmark for comprehensive counter-terrorism and national security policy [6]. The Prevent strand, focused on countering radicalization at an early stage, and the Channel program, which provides individualized support to persons assessed as vulnerable to extremist influence, represent approaches with direct relevance for Ukraine's post-war reconstruction of security governance [6].

Mutual exchange of information and experience with international partners constitutes another essential dimension of modern national security. Ukraine's cooperation with Europol, Eurojust, Interpol, and bilateral partners has intensified significantly since 2022. This cooperation encompasses intelligence sharing, joint investigations, capacity building, and technical assistance. As the U.S. Department of State Country Report on Terrorism (2023) notes, effective counter-terrorism increasingly depends on the quality of real-time information exchange between allied agencies rather than on unilateral national capabilities alone [10, p. 47].

The implementation of joint security initiatives reflects the growing institutionalization of multilateral security cooperation. Ukraine's participation in EU advisory missions, NATO trust funds, and bilateral security assistance programs has created frameworks for the transfer of best practices in areas ranging from cybersecurity to border management. Cybersecurity merits particular attention as a domain where international cooperation is indispensable: the UK Online Safety Act 2023 and similar legislative instruments in EU member states establish legal obligations for technology platforms to remove terrorist and harmful content, creating a regulatory environment that no single state can replicate unilaterally [11].

The integration of Ukraine into international security frameworks also raises questions of legal harmonization. Adapting national legislation to international standards while preserving constitutional traditions and rule of law principles requires careful legislative design. The principle of the rule of law,

enshrined in Article 8 of the Constitution of Ukraine [1], must remain the foundational constraint on all national security measures, including those adopted under martial law conditions.

Thus, ensuring national security in the contemporary context demands a comprehensive approach that unites constitutional guarantees, effective law enforcement mechanisms, and deep integration into international security frameworks. The Ukrainian experience under martial law offers both lessons and challenges that are of broader relevance for the development of national security doctrine. Further research should focus on the empirical assessment of institutional reforms undertaken since 2022 and on the development of evidence-based recommendations for the post-war reconstruction of Ukraine's security sector, with particular attention to the harmonization of domestic legislation with EU and NATO standards and the institutionalization of preventive security approaches.

References

1. Constitution of Ukraine of June 28, 1996. URL: <https://zakon.rada.gov.ua/laws/show/254к/96-вр>
2. Law of Ukraine «On National Security of Ukraine» of June 21, 2018 No. 2469-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2469-19>
3. Law of Ukraine «On Combating Terrorism» of March 20, 2003 No. 638-IV. URL: <https://zakon.rada.gov.ua/laws/show/638-15>
4. Criminal Code of Ukraine of April 5, 2001 No. 2341-III. URL: <https://zakon.rada.gov.ua/laws/show/2341-14>
5. National Security Strategy of Ukraine, approved by Decree of the President of Ukraine No. 392/2020 of September 14, 2020. URL: <https://zakon.rada.gov.ua/laws/show/392/2020>
6. HM Government. Counter-Terrorism Strategy (CONTEST) 2023. London : Home Office, 2023. 116 p.
7. Horbulin V. P. National Security of Ukraine: Challenges and Priorities. Kyiv : NISD, 2021. 224 p.
8. Thornton R. Asymmetric Warfare: Threat and Response in the 21st Century. Cambridge : Polity Press, 2021. 256 p.
9. Kolesnik S. P. Legal Provision of Prevention of Terrorism by National Police. *European Reforms Bulletin*. 2019. No. 3. P. 28–32.
10. U.S. Department of State. Country Reports on Terrorism 2023. Washington : Bureau of Counterterrorism, 2024. 312 p.
11. Online Safety Act 2023, c. 50 (UK). URL: <https://www.legislation.gov.uk/ukpga/2023/50>.

Ганусяк Богдан Володимирович, курсант ХНУВС

Науковий керівник – **Тімошин Анатолій Сергійович**, доцент кафедри інформаційних систем та технологій ХНУВС, кандидат фізико-математичних наук, доцент

ВИЯВЛЕННЯ ПІДОЗРІЛИХ ШАБЛОНІВ У ДОМЕННИХ ІМЕНАХ ВЕБРЕСУРСІВ

У сучасних умовах стрімкого розвитку інформаційних технологій питання забезпечення кібербезпеки набуває особливої актуальності [1, с. 205]. Значна частина сучасних кіберзагроз пов'язана із використанням шкідливих вебресурсів, які створюються з метою викрадення конфіденційної інформації та отримання несанкціонованого доступу до облікових записів користувачів. Одним із важливих елементів будь-якого вебресурсу є доменне ім'я, яке виконує роль унікального ідентифікатора ресурсу в мережі Інтернет. Саме тому аналіз доменних імен є ефективним інструментом для виявлення потенційно небезпечних вебресурсів і протидії кіберзлочинності.

Сьогодні зловмисники активно використовують різноманітні методи маскуванню шкідливих сайтів під легітимні вебресурси. Найчастіше такі домени створюються таким чином, щоб бути максимально схожими на адреси популярних сервісів, банківських установ або соціальних мереж. Основною метою подібних дій є введення користувача в оману та спонукання його перейти на фальшивий ресурс. Після переходу користувач може несвідомо ввести персональні дані, логіни чи банківські реквізити, які надалі використовуються зловмисниками [2, с. 53]. Такі атаки є одними з найпоширеніших способів реалізації фішингових схем у мережі Інтернет.

Одним із найбільш поширених способів створення підозрілих доменів є тайпсквотинг. Цей метод полягає у реєстрації доменних імен, які містять навмисні помилки у написанні відомих вебадрес. Наприклад, замість адреси «google.com» може використовуватись