European Journal of Sustainable Development (2025), **14**, 3, 703-714 ISSN: 2239-5938
Doi: 10.14207/ejsd.2025.v14n3p703

Ensuring National Security Through Effective Critical Data Management

By Nataliia Varenia[1], Oleksandr Rozvadovskyi[1], Vitalii Khodanovych[1], Tetiana Davydova[2], Ivan Draliuk[5]

ABSTRACT:
Emphasising the importance of protecting the information space, the article highlights the essence and challenges of the state' information sovereignty and its significance for national security. It also defines the main specific terms describing information security, such as: "information warfare", "destructive propaganda", "information confrontation", and others. In the context of irreversible information attacks, the state policy in the field of national security requires a targeted and reliable state decision.
Considering the documents of alienated countries and methods of optimising counter-propaganda activities of different states, the specifics of state activity are the basis for preserving information resources necessary for national security. The secrecy of information and manipulative information technologies are the basis for a rationalistic system of diverse use. Studies of state administrations and newly created information structures abroad open up new but critical communication approaches in combating the threats of unpredictable actions.
The analysis of private and public organisations in Ukraine was carried out in the following areas: operational activities, counterintelligence, intelligence, technical operations, protection of personal data of military and civilian personnel, anti-terrorist operations, international activities, internal reporting, finance, civil defence, territorial defence, housing and communal services. The article highlights that there is no unified approach to the classification of restricted information in these areas, which further complicates the information protection system in this area.

Keywords: information security, classified information, confidential information, media, destructive propaganda, disinformation, ideological expansion.

1. Introduction

The accelerating development of digital technologies makes it possible to effectively manage vast amounts of information, facilitating the creation of various types of information manipulation and influencing public sentiment in the global media arena. This is further compounded by the need to critically examine the importance of information security in the modern world. This phenomenon is closely related to the key element of political science - national security. Protecting the country's information infrastructure, including confidential information, and ensuring protection against ideological penetration and cyber aggression is an essential strategic task of the state and part of the national interest.

The interpretation of the term "sensitive information" can vary depending on the context but is generally understood to mean information important to a country's security,

[1] National Academy of Security Service of Ukraine, Kyiv, Ukraine.
[2] Sumy State Pedagogical University named after A.S.Makarenko, Sumy, Ukraine.
[3] Private researcher, Ukraine.

individuals' privacy, and other important issues. This information requires specific, unique methods to control who can access it, how it is protected and transmitted, and laws designed to prevent unauthorised disclosure or harmful use against certain people, organisations or even the country. It should be noted that Ukrainian legislation does not clearly define the legal status of classified information.

Today, in Ukraine, certain principles govern the security of information data or its processing, which has been and remains a legally important element of information policy. Nevertheless, the existing national strategy for information security in Ukraine needs to be further developed, as most of its fundamental principles focus exclusively on technical aspects of protection. Moreover, information security encompasses both political and psychological aspects. Politically, it pertains to national security, international diplomacy, and safeguarding state interests, frequently involving cyber warfare and espionage. Psychologically, it involves personal perceptions of safety, trust in technology, and vulnerability to misinformation and manipulation (Liu, 2022). Han et al. (2017) proposed an integrative model of information security policy compliance that incorporates the psychological contract, focusing on a bilateral perspective.

Moreover, the Copenhagen school's broadened approach to security and the societal security concept provides a fitting theoretical framework for analysis (Juurvee & Arold, 2021). The idea of positioning society as the focus of security is prominently reflected in the examined national security documents and in the practical implementation of strategies related to cybersecurity, psychological defence, and strengthening resilience against hybrid threats.

The global cyber war is intensifying and enlisting new players. Although the Russian-Ukrainian cyberwar continues to be a major factor in this conflict, the range of politically motivated hacker activity is growing. Russian hackers are now targeting military personnel's and security sector workers' personal mobile devices instead of Ukrainian businesses, according to international researchers. Activity is also escalating in the vicinity of Taiwan, where cyber gangs most likely associated with China are intensifying their attacks, in addition to the Russian-Ukrainian front (USAID, 2024).

A number of closely related concepts, some with precise definitions and some rather ambiguous (e.g. election meddling, fake news, subversive leverage, information disorder, asymmetric war (fare), fourth-generation warfare, non-linear war (fare), non-traditional warfare, and grey zone activities) have been the subject of a heated public and scholarly debate in recent years. All this landscape determines the multidimensionality of information security and national strategy. There should be a set of good-practice elements that can make the national strategy comprehensive and effective, while allowing for tailoring to the national context. Accordingly, internal vulnerabilities, such as disjointed institutional frameworks, negatively affect implementation across government sectors, leading even to entropy effect. Social entropy even presents information measure of institutional complexity (van Stokkum, 2024).

Counteraction to complex information and psychological influences on the country is very low. This is due to the overly simplified security system that exists today. This threatens national security, especially in areas particularly vulnerable to aggression and conceptual manipulation - the external one. Given the dominance of the Internet and alternative networks in shaping public opinion, in the postmodern context, strategic management measures should be taken to ensure the information sovereignty and

resilience of the state against external threats.

2. Theoretical Background

Even though social reality is closely related to communication, and indeed it is, there is still classified information controlled to prevent unlawful disclosure, as well as materials of various levels that can harm the interests of a person, organisation or even the state (Bakyumenko, 2022). Back in the days of Aristotle, he defined information and communication as one of the most developed forms of human social activity, which refers to the state in which he lives as a social construct (Gorbulin, 2010).

From the point of view of Zaverbnyi (2022),"an open forum for an ongoing discourse on mutual tolerance and access to central life values" describes what communication is (Zaverbnyi, 2022).

Also important are the works of Vynohradov and Mykhailutsa (2019), which are devoted to the communicative approach in political science. These scholars have made a significant contribution - the impact of communication processes on forming and maintaining a political community (Vynohradov & Mykhailutsa, 2019). It is known that all modern conceptions of communication emphasise its information and communication nature and its dominant position in social relations (Gorshkov, 2018).

Deutsch emphasises the importance of social communication in governance processes, calling it the "nervous system of public administration" (Verba-Sydor & Fedyk, 2016). This system responds quickly to changes while ensuring the receipt, analysis, evaluation, information processing, decision-making, implementation and feedback (Akchurin, 2018).

The monograph "Public Administration and Governance in the Information Society" states that managerial communications form a system of managerial functions for anybody, as they are a universal means of regulating the management process (Verbenskyi et al., 2020).

The authors Yevseiev et al. (2021), study in depth the methods of access control and encryption of information, as well as special conditions for storing and processing information (Yevseiev et.al., 2021).

In her article, Mikhailova (2023), analyses the rules governing the status of confidential information, protection rules, and mechanisms for its use (Mikhailova, 2023).

Aims. Assessment of the use and justification of confidential information in the context of the national security system. Research and development of information security systems to counter propaganda based on foreign experience.

3. Methods

The study analyses confidential information as an essential resource in the formation of information security in different countries of the world. Retrospective studies of the integration of new technologies in recent years have been conducted with a special focus on the suspected use of such technologies in the Integration with Europe campaign framework. Particular attention is paid to communication as a means of countering propaganda. Historical and logical analysis methods, comparative, expert evaluation, and systemic forecasting were used. The research used lower-level resources, concepts, and

proprietary intangible assets to help in the effective fight against propaganda.

4. Results

One of today's primary and essential tasks is to ensure the sovereignty and territorial integrity of the state. This issue is directly related to other aspects of national security, which are generally of primary importance for public administration. In the scientific discourse, security is one of the issues that need to be discussed on the political agenda, as its provision requires political action and the formulation of organisational and legal measures by state bodies. These constitute a comprehensive state security policy. Figure 1 summarises one of the most critical issues - the potential leakage of confidential information from state institutions (Orlyk & Hrytsenko, 2022).

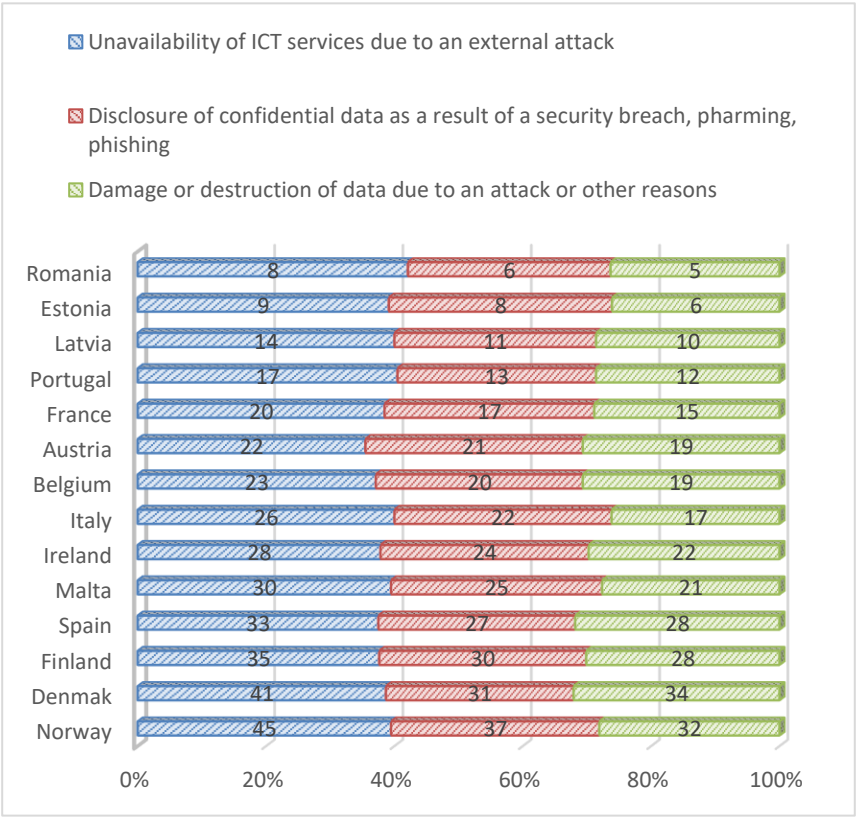

Figure 1: *Percentage of companies in EU member states by type of risk of confidential information leakage*
Source: Nakonechna, 2023

Businesses in a variety of industries in Ukraine are vulnerable to numerous kinds of leaks of sensitive data. These risks can be broadly divided into three categories: insider threats, cyber threats, and data breaches brought on by human error or insufficient security measures. Because of the sensitive nature of the data they manage, certain industries - like IT, finance, and healthcare - are especially vulnerable. Businesses in Ukraine are vulnerable to a range of online dangers, such as malware, DDoS attacks, and data breaches. DDoS

attacks make up 68.1% of all attacks, making them especially common. Despite being less common, malware and data breaches are still quite dangerous. Notable dangers include ransomware and phishing (Anishchuk, 2023). These attacks, which target corporations, government organizations, and critical infrastructure, can come from a variety of sources, including state-sponsored actors.

Over the past four years, hundreds of thousands of personal papers have been made public by Ukrainian car inspections due to inadequate cyber security, putting reams of personal data at danger of being exploited by hackers and Russian intelligence, among other bad actors. The documents, which mostly consist of scans of passports, driver's licenses, taxpayer identity numbers, and vehicle registrations, cover a wide range of Ukrainian geography and demographics. They mostly identify individuals who are purchasing or selling secondhand autos abroad. The records were accessible, unprotected and unencrypted, on a server belonging to one of the biggest cloud storage providers in the world until April 1, 2025. While difficult for ordinary users to access, malicious actors can easily locate them (Post, 2025).

Moreover, in the digital era, protecting personal and service-related data is critical, especially for military personnel. Adversary intelligence relentlessly pursues methods to access critical data that could jeopardize plans, locations, or personal information of military personnel. Digital technologies have both complicated and simplified intelligence gathering. On one hand, data can be protected using advanced encryption methods; on the other, users frequently unknowingly disclose sensitive information via social media, messaging apps, and other communication channels.

In Ukraine, during the ongoing war, confidential information leakage poses a significant risk, potentially impacting both military operations and civilian safety. Cyberattacks, disinformation campaigns, and the spread of harmful information can have severe consequences, requiring careful management and mitigation. Understanding the methods employed by the enemy to gather intelligence, along with a solid grasp of essential cybersecurity protocols, enables effective defense against data breaches. The Ministry of Defence provides detailed insights into key threats and offers practical recommendations for safeguarding personal and service-related information. However, leakages still take place.

The modern world is undoubtedly a dangerous place. Tensions in the international arena are constantly growing, turning global conflicts into more serious threats. The dispute between the two major superpowers is increasingly becoming an information war. Classical wars, acts of violence and terrorism are giving way to the media. Modern media and the endless flow of the Internet are becoming tools of power that manipulate public opinion and political decisions (Oracle Corporation, 2019). Information warfare, as a powerful tool of neo-imperialism, is known to almost everyone, as there has never been and will never be such tight control over the public consciousness and its superstructure, especially regarding decision-making mechanisms in public administration. This trend in using modern information propaganda is increasing globally (Laptiev et al., 2023).

In order to further an agenda, propaganda uses inaccurate or biased information to sway public opinion. It exerts influence through repetition, passion, and targeted messaging. Propaganda, as used in public policy, is described as carefully crafted public

discourse on political matters that asserts a monopoly of truth and discredits opposition (Kavanagh, 2024). This is applicable in a high-choice digital information world where viewers have access to a multitude of conflicting claims, and it goes far beyond particular circumstances (such as a crisis or war), internal politics, and authoritarian regimes. Propaganda and politics are closely related in today's world, and internet platforms are crucial to its spread.

Therefore, what people find credible and important in these kinds of settings is more important than what they are exposed to. There is a choice here, and certain people and groups will choose extremely biasedly what they absorb and incorporate into their worldview. There are several levels at which this occurs: at the level of the persistent meta-narrative that shapes their story world and establishes their normative polarity; at the level of adaptive communication campaigns that concentrate on the issues that need to be discussed in practice at the moment and offer compelling justifications for important issues along with identity defenses and behavioral guidance; and at the lowest level of daily (dis)information flows that directly address current events and encourage tactical mobilization or demobilization (Aziz et al., 2024).

In order to provide ontological security, a performance of loyalty, and the obligation to apologize for any transgressions against this identity, propaganda takes advantage of a social mechanism that is founded on the perception of threats to one's own identity. This leads to a monopoly of truth that is ingrained in the culture.

Al-Rodhan (2017) discusses post-truth politics in his writing. The Oxford Dictionaries chose "post-truth" as their 2016 "word of the year", however the term describes a "era" rather than a year: one of unrestricted internet communication in which politics thrives on a rejection of reality and common sense. "Post-truthness" blurs new boundaries: political disagreements appear to be more about the conflict between truth and fiction than ideology. One basic characteristic of post-truth politics worldwide is that it prioritizes gut instinct and emotion over logic and facts. In just a few hours, conspiracy theories and fake news can spread widely, generating false realities and being used for propaganda. Post-truth reveals the fragility of the liberal order while also posing a threat to liberal democracy and its institutions. Additionally, it is a sign of a bigger issue: accountability in online communities. The recurring theme throughout the term's history is that lies propagated by politicians on a regular basis with negligible or no repercussions for their credibility and reputation are what constitute post-truth. However, there are unavoidable repercussions for both democracy and humanity's future: a future where scientific realities are denied can only be unstable.

These contemporary advances include, on the one hand, attempts to preserve liberal democratic procedures and ensure fair elections, yet state-sanctioned news censorship and filtering has historically been linked to authoritarian governments. However, there are risks and shortcomings associated with state-led efforts. First of all, the accusation of "fake news" can be used as a pretext to impose censorship and so further undermine public confidence in the government. Another issue is that citizens must exercise caution and vigilance when it comes to the information they are exposed to in nations that lack the institutional capacity and resources to combat the menace of false news. Assuming that every citizen possesses the necessary literacy abilities to evaluate the veracity of the news is just one of the many reasons why this idealistic idea is unfeasible.

Meanwhile, effective public diplomacy requires ethical communication. It promotes trust and enduring ties between countries by requiring integrity, openness, and respect for differing viewpoints. To establish credibility and accomplish long-lasting collaboration, practitioners should place a high value on telling the truth, refraining from manipulation, and having sincere conversations.

Due to the development of information technologies, information wars are becoming increasingly relevant. By attacking the enemy's information security, these wars aim to destabilise the state's domestic policy in a situation of important decision-making. The main goals of the opposing sides are changing public opinion, controlling people's behaviour, and imposing certain ideological postulates. This goal is achieved through manipulative models that form the desired picture of reality in the information space (Bondarenko & Lytvynenko, n.d.).

As Ukraine seeks to integrate into the Euro-Atlantic region, alignment with EU and NATO standards is integral to this process. In particular, the focus of reforms aimed at ensuring the security of document flow is becoming increasingly important. Discussion of these issues in the context of public control over the authorities' activities is becoming an essential step in strengthening the country's information resilience (Voitovskyi, 2022).

A decision that will serve the interests of the government, citizens, and society as a whole and enshrine precise approaches to this issue should be made in the legislation. In particular, there is a need to define confidential information as a separate category and establish a preliminary classification system for such information. In general, this type of information needs to be systematically arranged into classifications by established agreements, see Table 1.

Table 1: Transparent data and the hierarchy of encryption of confidential information

DPAPI	DPAPI encrypts SMK	
SMK	SMK encrypts the DMK	
DMK	DMK secures the private key	DMK secures the entire user database
Asymmetric keys	The asymmetric key protects DEK	
DEK	DEK is used to protect user data	

Currently, data on the movement of certain security goods is continuously processed, including technical support, tactical deployment of military units, movement of equipment, and protection of specific strategic facilities and law enforcement agencies. Recently, Ukraine has been actively considering information about the possible accumulation of the Russian army in Belarus and other countries and the deployment of defence, which poses serious risks. This information calls for avoiding any measures that, in the worst-case scenario, could seriously threaten national security (Regulation (EU) 2016/679 of the European Parliament and of the Council, 2016).

Effective use of information flows and turning them to one's advantage is the leading quality of Ukraine's security policy. Measures against unlawful interference in the

state's information space, in turn, threaten the main pragmatic goals of the state. The basic principles of the state policy in information security are defined in Article 21 of the Law of Ukraine, "On State Secrets," and Article 9 of the Law of Ukraine, "On Access to Public Information". According to the Order of the Central Office of the Security Service of Ukraine No. 383 dated 23.12.2020, information security is the protection of the interests of the individual, society and the state in the information space. Thus, the state is responsible for citizens' access to destructive content (Kravchuk, 2022).

The most acceptable balance between society, the individual and the state emphasises national security. Today, in times of global political tension, information protection is a fundamental part of a country's overall security strategy. Propaganda information campaigns, fake news and content management that distort reliable information require an adequate neutralising response (Nakonechna, 2023).

Ukraine, like its neighbouring countries, is often subjected to information attacks from Russia, which are mainly aimed at socio-political destabilisation, inter-ethnic conflicts and social discord. To effectively counter such information threats, it is essential to ensure adequate information security. In the academic environment, this concept is called the policy of information counteraction, which, along with information influences, forms the experience of information warfare (Halushka & Tikhonov, 2021).

5. Discussion

Ukraine and other countries already have some experience in information assurance and the relevant legislative, organisational, and institutional elements created for its implementation. However, these structures are primarily focused on ensuring state control and protection of information systems and networks of strategic importance. The need to combat ideological expansion is not sufficiently developed. Most countries mentioned in this article do not currently have a developed and coordinated strategy to fight fake news and propaganda, which poses a serious threat to national security (List of NoSQL Database Management Systems, 2019).

The article considers vulnerable Russian propaganda narratives in the Ukrainian media to confirm Ukraine's insufficient information security. It is also proposed to create a system of early warning of information attacks, modern cyber sabotage, manipulations, and a comprehensive automated system for neutralising threats. In addition, the article considers the legislative framework's adjustment and the development of a comprehensive information security policy for Ukraine and other fairly powerful countries, such as China and the United States. This policy should include sub-policies to strengthen the capacity of national media to counter destructive propaganda (Bilij & Mykhalchuk, 2021).

Confidential data requires special attention when processing, as sometimes the law prohibits working with such data, even if there is consent. Other more severe cases include mandatory data encryption before transmission over open networks or complete suppression of such information (Snihir, 2008).

The Law "On Principles and Guarantees of Freedom of Information" of 12 December 2002, which regulates information security in Uzbekistan, defines "information security" as the protection of the interests of citizens, society, and the state in the information environment. This means that the state is at least obliged to protect itself and

its citizens from destructive information (Pavliutin, 2020).

Unlike other countries, the United States does not have a single regulatory act governing state secrets. However, in 2009, the US President signed Executive Order 13526, which established a classification system for classified documents that is still in place today (Shcherbak, 2017).

Therefore, simple procedures for protecting and handling information containing personal data should be introduced at all levels of society's organisation in accordance with the basic legal provisions of laws and other regulations (Shevtsov & Mernikov, 2008).

Stakeholder interviews and practical case studies are absent from the article, which examines institutional arrangements and laws. One limitation is the lack of up-to-date material from Ukraine's recent information crises, which could provide support or context for its assertions.

6. Implications and further research

In an effort to provide better and more effective public services, governments are among the biggest producers and consumers of data worldwide. The use of data analytics can be used to monitor, assess, and offer real-time insights on the movements of public resources (such as monitoring gender equality, resource leakage or waste, or the spread of viral infections) or to prompt a public service provider to take action (such as during a disaster or in response to high demand for public transportation). Utilizing data can reduce resource waste and enhance public results.

However, strong frameworks for data collection, storage, and usage are necessary to maximize the potential of public sector data while maintaining data security and privacy. Many governments find it difficult to build and implement data governance and management frameworks because of the subject's complexity and the quick advancements in digital technologies. Among the difficulties are a lack of knowledge and comprehension of the relevant frameworks and standards, insufficient financial and human resources, and poor coordination between ministries and agencies within the same nation.

Information was analysed in the following areas: operational search, counterintelligence and intelligence activities, operational and technical measures, protection of personal data of employees and military personnel, activities of participants in anti-terrorist operations and hostilities, international cooperation, internal audit, financial reporting, civil protection, territorial defence and housing and communal services. However, there is almost no unified approach to determining the information categories that require access restrictions in these areas.

A coherent approach to discussing the systematisation of public resources about any information whose sovereignty is protected by Article 6 of the current Law of Ukraine, "On Access to Public Information", means that depending on this information, control schemes in different agencies will change, which can lead to significant problems.

In Ukraine, given the current observations of terrorist activities by Russia and the aggressor's activities in the country's information space, the Law of Ukraine "On Access to Public Information" and its integration into electronic resources and systems, unfortunately, do not provide for the establishment of appropriate control measures over confidential information. In addition, the established hierarchical checklists for state and

official organisations do not comply with the law.

Though the impact on national security, political security, ideological security, and social public security are frequently overlooked, the impact of big data on national security encompasses many facets of national security, including evident science and technology security and information security.

Information and data management techniques frequently intersect with national security policies, as the research clearly demonstrates. These regulations seek to protect private data, guarantee its accessibility for permitted uses, and stop illegal access or abuse. By safeguarding sensitive data and preserving the integrity of vital systems, effective data management is essential to preserving national security. Today, there is a need to study national security in Big Data era. The creation of national security management rules in the big data era has emerged as a pressing and practical significant issue from a national security standpoint, and this discourse should determine the vectors of further research.

References

Akchurin, S. (2018). *Concept of "Data Centric Security" protection*. LinkedIn. https://www.linkedin.com/pulse/концепция-защиты-data-centric-security-akchurin-sergei

Al-Rodhan, N. (2017, June 7). *Post-truth politics, the Fifth Estate and the securitization of fake news*. Global Policy. https://www.globalpolicyjournal.com/blog/07/06/2017/post-truth-politics-fifth-estate-and-securitization-fake-news

Anishchuk, V. (2023). Information security as an object of crimes against the foundations of national security of Ukraine. *Uzhhorod National University Herald. Series: Law*, *2*(77), 139–143. https://doi.org/10.24144/2307-3322.2023.77.2.23

Aziz, F., Alam, M., Khan, M., & Mehmood, K. (2024). Political propaganda on the internet: A systematic review. *Migration Letters*, *21*(S8), 1077–1088. https://doi.org/10.59670/ml.v21iS8.9539

Bilij, V. I., & Mykhalchuk, V. M. (2021). Main directions of ensuring the national security of the state. *Investments: Practice and Experience*, *17*, 92–98. https://doi.org/10.32702/2306_6814.2021.17.92

Bondarenko, V., & Lytvynenko, O. (n.d.). Information security of the modern state: Conceptual reflections. Lviv Polytechnic National University. https://science.lpnu.ua/uk/shv/vsi-vypusky/tom-2-chyslo-1-2016/informaciyna-bezpeka-ukrayiny-suchasni-vyklyky-zagrozy-ta

Gorbulin, V. P. (2010). *Strategic planning: Solving national security problems* [Monograph]. NISD. http://repositsc.nuczu.edu.ua/bitstream/123456789/9018/1/Zb%D1%96rnik%20NUCZU_2019_1%20%2810%29_%20NEW-64-69.pdf

Gorshkov, S. (2018). Unified access point to company data. *Open Systems. DBMS*, *04*. https://csecurity.kubg.edu.ua/index.php/journal/article/view/116

Halushka, V., & Tikhonov, H. (2021). Peculiarities of legal regulation of protection of state secrets in Ukraine and abroad. *Enterprise, Economy and Law*, *1*, 205–209. https://doi.org/10.32849/2663-5313/2021.1.36

Han, J., Kim, Y., & Kim, H. (2017). An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective. *Computers & Security*, *66*, 52–65. https://doi.org/10.1016/j.cose.2016.12.016

Juurvee, I., & Arold, U. (2021). Psychological defence and cybersecurity: Two integral parts of Estonia's comprehensive approach for countering hybrid threats. *Íconо 14*, *19*(1), 70–94. https://doi.org/10.7195/ri14.v19i1.1628

Kavanagh, R. (2024). *Understanding modern propaganda: A comprehensive guide to public persuasion*. Grin Verlag.

Kravchuk, V. O. (2022). Protection of personal data in wartime. *Legal Scientific Electronic Journal*, *9*, 319–321. https://doi.org/10.32782/2524-0374/2022-9/77

Laptiev, O., Sobchuk, V., Sobchuk, A., Laptiev, S., & Laptieva, T. (2021). An improved model for estimating the economic costs of the information protection system in social networks. *Cyber Security: Education, Science, Technology*, *4*(12), 19–28. https://doi.org/10.28925/2663-4023.2021.12.1928

List of NoSQL database management systems. (2019). *List of NoSQL database management systems*. https://csecurity.kubg.edu.ua/index.php/journal/article/view/116

Liu, X. (2022). The study on national security in big data era. *Frontiers in Business Economics and Management*, *5*(3), 191–200. https://doi.org/10.54097/fbem.v5i3.2006

Mikhailova, O. (2023). Communication strategies in public management and administration: State and problems in implementation. *International Science Journal of Management, Economics & Finance*, *2*(2), 93–99. https://doi.org/10.46299/j.isjmef.20230202.10

Nakonechna, I. V. (2023). Guarantees of ensuring Ukraine's national security in the context of European integration: The aspect of identifying the essence. *Kyiv Law Journal*, *1*, 391–396. https://doi.org/10.32782/klj/2023.1.60

Orlyk, V., & Hrytsenko, A. (2022). Key provisions of the new U.S. national security strategy. *National Institute for Strategic Studies*. https://niss.gov.ua/sites/default/files/2022-10/171022_us_nss_pdf.pdf

Oracle Corporation. (2019). *Comprehensive defense in depth: Oracle database security capabilities, what's new in database security*. https://csecurity.kubg.edu.ua/index.php/journal/article/view/116

Pavliutin, Y. M. (2020). The national security system: Political and legal analysis. *Honor and Law*, *3*, 84–90. http://nbuv.gov.ua/UJRN/Chiz_2020_3_14

Post, K. (2025, April 1). Exclusive: Massive data leak potentially exposes Ukrainian IDs to Russian intelligence, hackers. *Kyiv Independent*. https://kyivindependent.com/ukrainian-vehicle-inspections-expose-trove-of-passports-drivers-licenses-and-vehicle-registries-through-sloppy-cyber-practices-for-over-4-years/

Regulation (EU) 2016/679 of the European Parliament and of the Council. (2016). On the protection of natural persons with regard to the processing of personal data and on the free movement of such data. *Official Journal of the European Union*. https://eur-lex.europa.eu/eli/reg/2016/679/oj

Shcherbak, S. V. (2017). Legal regulation of executive process principles: Problematic issues. In *Reforming the legal system in the context of European integration processes: Conference proceedings* (pp. 233–236). http://www.pgp-journal.kiev.ua/archive/2019/3/14.pdf

Snihir, O. (2008). Trends and priorities in the development of EU security and defense policy. *National Institute for Strategic Studies*. https://ipacs.knu.ua/pages/dop/336/files/7148e643-1410-42f1-a6b6-f4cf15aeb638.pdf

Shevtsov, A., & Mernikov, H. (2008). Formation and implementation of national security policy in EU member states. *National Institute for Strategic Studies*. https://ipacs.knu.ua/pages/dop/336/files/7148e643-1410-42f1-a6b6-f4cf15aeb638.pdf

United States Agency for International Development. (2024). *Review of cybersecurity news in Ukraine, tendencies, and world events related to the First World Cyber War*. https://www.rnbo.gov.ua/files/2024/NATIONAL_CYBER_SCC/20240916/2024%2008%20Cyber%20digest_ENG.pdf

van Stokkum, R. (2024). Social entropy: An information measure of institutional complexity for social psychology. *Advances in Social Sciences Research Journal*, *11*(2), 33–53. https://doi.org/10.14738/assrj.112.16387

Vynohradov, A. K., & Mykhailutsa, M. I. (2019). Political and legal analysis of criminal liability for the disclosure of state secrets and for the disclosure of information of a high nature, constituting a state secret, or the loss of documents or materials containing such information. *South Ukrainian Legal Journal*, *3*, 46–49. https://doi.org/10.32850/sulj.2019.3-11

Verbenskyi, M. H., Kulyk, O. H., & Naumova, I. V. (2020). Criminal situation in Ukraine: Main trends. *Yurinkom Inter*. https://doi.org/10.36486/np.2022.1(55)

Verba-Sydor, O. B., & Fedyk, S. E. (2016). Principles of executive proceedings under new draft laws No. 2507-a and No. 2506-a. *Legal Scientific Electronic Journal*, *2*, 21–24. http://www.lsej.org.ua/2_2016/6.pdf

Voitovskyi, K. (2022). Israel's report on the formation of the national security strategy. *National Institute for Strategic Studies*. http://newukrainianlaw.in.ua/index.php/journal/article/download/328/290/647

Yevseiev, S., Laptiev, O., Lazarenko, S., Korchenko, A., & Manzhul, I. (2021). Modeling the protection of personal data from trust and the amount of information on social networks. *EUREKA: Physics and Engineering*, *1*, 24–31. https://doi.org/10.21303/2461-4262.2021.001615

Zaverbnyi, A. (2022). Communication strategies: Problems and prospects of formation and implementation in the context of European integration. *Innovation and Sustainability*, *1*, 13–19. https://doi.org/10.31649/ins.2022.1.13.19