

# Basic Principles of Public Administration of Critical Information Infrastructure: the Example of Ukraine

Maksym Sokiran<sup>1</sup>

Ph.D. in Law, Lawyer, Scientific and Research Institute of Public Law (Kyiv, Ukraine)

E-mail: maxim.sokiran@gmail.com

<https://orcid.org/0000-0002-1682-2012>

Sokiran, Maksym (2021) Basic Principles of Public Administration of Critical Information Infrastructure: the Example of Ukraine. *Advanced Space Law*, Volume 7, 63-72. <https://doi.org/10.29202/asl/7/7>

*The article considers the issues of stability of critical information infrastructures (CII), based on the analysis of current domestic legislation in the field of national security in general and cybersecurity – in particular; highlights the basic principles of administrative and legal support for the stability of critical information infrastructures. It is determined that the principles are enshrined in legal norms to establish a coordinate system in a particular area for its proper functioning. The analysis of the legal literature showed that most of the authors who studied the principles of administrative and legal support of a particular area, the main characteristics of these principles include: principles; defined in regulations; which create conditions; on which any activity is based; which is regulated and regulated. The analyzed regulations allow us to conclude that the activities in the field of protection of CII are based on a system of principles, which includes both general and special principles. However, we are interested only in the set of principles that regulate the sustainability of CII and not only their protection. To such a system, we include the following principles: the rule of law and respect for human and civil rights and freedoms; ensuring the national interests of Ukraine; openness, accessibility, stability and security; public-private partnership; proportionality and adequacy of protection measures to real and potential risks; priority of precautionary measures; objectivity and legal certainty of CII objects; standardization of procedures and standardization of technical requirements; cooperation and interaction. The author, under the system of principles of administrative and legal support for the stability of critical information infrastructure, means a set of basic guidelines that take into account the interests of man, society and state, based on which public policy is formed, which allows critical information infrastructure to withstand threats, recover quickly from violations functioning.*

*Keywords: stability, critical information infrastructure, public administration, legal support, system, principles*

Received: 4 March 2021 / Accepted: 12 April 2021 / Published: 29 June 2021

---

© Sokiran, Maksym, 2021

## **Introduction**

In recent years, in developed countries, the trend of expanding the context of measures related to the functioning of critical information infrastructure (CII) is growing: issues of protection (security) of CII are considered together with issues of its sustainability. At the same time, more and more attention is paid to the issues of ensuring stability in comparison with the issues of protection. This shift in the focus of the issue is due to the fact that the modern security environment is characterized by the emergence of new threats and dangers against the background of rapid processes of evolution and transformation of existing threats (The State, 2020). The possibility of cases of their various combinations should also be considered. Under such conditions, no established system of protection (security) can fully provide protection against all threats and dangers. After all, while the development of a protection system designed for certain threats continues, new threats and dangers appear in the world. Therefore, more and more attention is paid to the stability of CII – its ability to be ready and adapt to changing conditions and resist change and recover quickly after malfunctions. Thus, finding out the ability of critical information infrastructure to sustainability, we will analyze the system of principles of its administrative and legal support.

In the article, we will: consider the principles of administrative and legal support; we will pay attention to the protection of critical infrastructure, as well as the problems and prospects for the implementation of European practices in Ukraine; we will analyze the process of reforming the defense system and increasing the resilience of Ukraine's critical infrastructure in the context of modern threats. Let us dwell in detail on the modern model of administrative and legal regulation of the protection of critical infrastructure.

### **Theoretical definition of the concept “principles of administrative and legal support”**

One of the fundamental foundations of administrative and legal support for the sustainability of critical information infrastructure in Ukraine is the principles of such activities. This is due to the fact that any legal, economic or social phenomenon has its origins. It is about its formation and development, about what underlies it. With the help of the category “principles,” the core, the primordial basis is revealed. However, we need to find out what the “foundation” is. In the beginning, it should be noted that the term “principle” comes from the Latin word “principium,” which means the beginning, the basis. At the same time, the principle is what underlies a certain theory of science, the inner conviction of man, the basic rule of conduct (Principle, 2021). The word “principle” means a scientific or moral principle, basis, rule, from which do not deviate. In legal doctrine, when defining the concept of principles of law, scholars use such categories as the initial theoretical provisions, basic, guiding principles (ideas), general regulations, leading foundations, patterns, essence, coordinate system and more. Many categories are homogeneous. Therefore, the principles are general, guiding (basic, main, starting, initial theoretical, general normative-guiding, guiding) provisions. As for the “principles of law,” there is no stable definition of this phrase; different scholars in their works bring different characterizing data and features. In addition, the term “principles of law” uses the term “legal principles.” These two concepts differ in that first, there are legal principles, and only then, with the advent of the system of law and legislation, the principles of law appear (Sokiran, 2020).

The principles of law are enshrined directly in legislative acts (articles, preambles of constitutions, laws) or follow from the content of specific legal norms. For example, the Doctrine of Information Security states that it is based on the principles of respect for human and civil rights and freedoms, respect for human dignity, protection of its legitimate interests, as well as the legitimate interests of society and the state, ensuring the sovereignty and territorial integrity of Ukraine (Decree, 2017).

Thus, the principles are enshrined in legal norms, to establish a coordinate system in a particular area for its proper functioning.

Recently, more and more attention in society has been paid to the relationship between the state and civic institutions, which are based on updated principles. We agree with the position of Victor Tsymbal, who noted that the peculiarity of modern management practice is to build relations between the state, civil society and business on the principles of partnership, effective interaction, transparency, decentralization, implementation of the participatory mechanism of public administration. Civil society institutions and business structures have the opportunity to express their views on certain socially significant issues and participate directly in the development and adoption of management decisions (Tsymbal, 2016).

Thus, public authorities should take into account these principles when forming relations with non-governmental structures, because this is the only way to build an effective, sustainable and inclusive state policy of socio-economic development of Ukraine.

Examining the principles of administrative and legal support of voting rights of citizens of Ukraine Eugene Serdyuk concludes that they should be understood as the basic initial, objectively determined principles on which the activities of subjects of administrative law to ensure the voting rights of citizens of Ukraine, the normal functioning of the state and civil society as a whole (Serdiuk, 2014: 73). Principles in the field of administrative and legal support for the circulation and use of weapons were studied by Sergey Didenko, who determined that these are the main initial, objectively determined principles on which the activities of public administration entities to ensure the circulation and use of weapons to ensure citizens' rights for self-defense, defense of Ukraine from external aggression, normal functioning of the state and civil society. He justifies the expediency of principles in the field of administrative and legal support for the circulation and use of weapons by the fact that such activities require the state to clearly regulate the actions of public administration in order to properly, timely, impartial and objective regulation of this sphere of public life (Didenko, 2016: 71). Arthur Zamryga understands the principles of administrative and legal support of economic activity in Ukraine as a set of normatively fixed framework, objectified in the form of instructions, guidelines and guarantees that determine the direction of the impact of regulatory, administrative norms on public relations between the state and business entities, as well as procedures for their interaction and general functioning of the economic market of the country (Zamryha, 2019).

These authors to the main characteristics of the principles of administrative and legal support include principles, defined in regulations, which create conditions; on which any activity is based; which is regulated.

## **The regulatory definition of the principles of ensuring the sustainability of CII**

There is no special law that would regulate legal relations and establish a system of principles to ensure the sustainability of CII. The issue of CII is regulated in the field of critical infrastructure protection and cybersecurity.

Thus, the concept of creating a state system of critical infrastructure protection, approved by order of the Cabinet of Ministers of Ukraine dated December 6, 2017, No 1009-r, determined that the problems of ensuring the protection of critical infrastructure should be solved by: creating a regulatory framework for the organization of state bodies and economic entities in the field of critical infrastructure protection; creation of the organizational and institutional structure of the state system of critical infrastructure protection; determination of powers, tasks and responsibilities of the subjects of the state system of critical infrastructure protection (On approval, 2017).

In turn, the Cyber Security Strategy of Ukraine of March 15, 2016, No 96/2016, cybersecurity of Ukraine should be based on the principles (Cybersecurity, 2016):

- a) The rule of law and respect for human and civil rights and freedoms;
- b) Ensuring the national interests of Ukraine;
- c) Openness, accessibility, stability and security of cyberspace;
- d) A public-private partnership, broad cooperation with civil society in the field of cybersecurity and cyber defense;
- e) Proportionality and adequacy of cybersecurity measures to real and potential risks;
- f) Priority of precautionary measures; невідворотності покарання за вчинення кіберзлочинів;
- g) Priority development and support of domestic scientific, scientific-technical and production potential;
- h) International cooperation in order to strengthen mutual trust in the field of cybersecurity and develop joint approaches to counter cyber threats, consolidate efforts in the investigation and prevention of cybercrime, prevent the use of cyberspace for illegal and military purposes;
- i) Ensuring democratic civilian control over military formations and law enforcement agencies of the state formed in accordance with the laws of Ukraine, operating in the field of cybersecurity.

The application of legislation in the field of cybersecurity and the adoption of decisions by the subjects of power to implement the provisions of the Law of Ukraine “On Basic Principles of Cybersecurity of Ukraine” are carried out in compliance with the principles of (On the basic, 2017):

1. The minimum necessary regulation, according to which the decisions (measures) of the subjects of power must be necessary and minimally sufficient to achieve the goals and objectives defined by this law.
2. Objectivity and legal certainty, the maximum possible application of national and international law in relation to the powers and responsibilities of state bodies, enterprises, institutions, organizations, citizens in the field of cybersecurity.
3. Ensuring the protection of users’ rights of communication systems and/or consumers of electronic communications services and/or information protection

services, cybersecurity, including the right to privacy and protection of personal data.

4. Transparency, according to which the decisions (measures) of the subjects of power must be duly substantiated and communicated to the subjects to which they relate before their entry into force (their application).
5. A balance of requirements and responsibilities, according to which a balance must be struck between establishing liability for non-compliance with cybersecurity and cybersecurity requirements, as well as for imposing excessive requirements and restrictions.
6. Non-discrimination, according to which the decisions, actions and omissions of the subjects of power may not lead to a legal or factual scope of rights and obligations of a person, which is: different from the scope of rights and obligations of others in similar situations, if only the difference is not necessary and minimally sufficient to satisfy the general public interest; as well as the scope of rights and responsibilities of others in dissimilar situations, if such equality is not necessary and minimally sufficient to meet the public interest.
7. Equivalence of requirements for cybersecurity of critical infrastructure, according to which the application of legal norms should be as equivalent as possible to cyber protection of communication and technological systems of critical infrastructure belonging to one sector of the economy and/or performing similar functions.

Thus, these regulations indicate that the activities in the field of protection of CII are based on a system of principles, which includes both general and special principles. However, we are only interested in the set of principles that govern sustainability, not protection, namely the sustainability of CII. To such a system, we include the following principles:

1. The rule of law and respect for human and civil rights and freedoms.
2. Ensuring the national interests of Ukraine.
3. Openness, accessibility, stability and security.
4. Public-private partnership.
5. Proportionality and adequacy of protection measures to real and potential risks.
6. Priority of precautionary measures.
7. Objectivity and legal certainty of CII objects.
8. Standardization of procedures and standardization of technical requirements.
9. Cooperation and interaction.

Given the amount of work, we will briefly explore some of these principles.

*The principle of the rule of law and respect for human and civil rights and freedoms* is one of the basic general principles. Thus, Alexandra Rudneva attributed the principle of the rule of law to “mega-principles,” human rights standards of the highest value level (Rudneva, 2012); the principle of the rule of law is often widely interpreted through the selection of its individual components (“integrated” approach), in particular, through eight such elements: 1) accessibility of the law (in the sense that the law must be clear, concise and predictable); 2) issues of legal rights should be resolved by law, not on the basis of discretion; 3) equality before the law; 4) power must be exercised in a lawful, fair and reasonable manner; 5) human rights must be protected; 6) means must be provided for resolving disputes without excessive

material costs or excessive duration; 7) the court must be fair; 8) compliance with the state as its international legal obligations and those conditioned by national law (Rule, 2011: 176).

In the context of ensuring the sustainability of CII, the principle of the rule of law and respect for human and civil rights and freedoms is as follows:

First, there is a need to change the prevailing view that human rights are an obstacle to security. Perhaps the most widely cited example of human rights that interfere with security is the claim that encryption, which is critical to the exercise of the right to privacy, prevents law enforcement from carrying out its work. Therefore, some governments are arguing to reduce the encryption to provide access to encrypted communications for law enforcement. However, experts agree that it is impossible to provide access to encrypted communications for a single government without doing so for all governments or for attackers (Brown & Esterhuysen, 2019). In other words, the weakening of cybersecurity for law enforcement purposes cannot be done without weakening security for all and without endangering human rights. This is because cybersecurity is inextricably linked to human security, which is a fundamental human right. Cybersecurity and human rights are complementary and interdependent. In order to effectively ensure freedom and security, it is necessary to strive to protect the former and the resilience of the latter.

Second, it is critical to apply human rights-based approaches to cybersecurity laws, policies and practices. Cybersecurity should never be an excuse for human rights violations. Instead, recognizing that individual and collective security is at the heart of cybersecurity means that the protection of human rights must be at the heart of cybersecurity policy-making. For example, the Freedom Online Coalition's Internet Free and Secure Working Group (Freedom, 2021) has developed a set of recommendations on cybersecurity and human rights to ensure that cybersecurity policies and practices are based and fully in line with human rights.

The advantage of human rights in the field of information security was pointed out by the European Court of Human Rights (ECHR). Thus, in its judgment of March 25, 1983, in *Silver and other* ECHR, it stated that "a law conferring discretion must determine the limits of the exercise of such a right." However, detailed rules and conditions must be contained in substantive law (*ibid.*, series A, No 61, pp. 33–34, pp. 88–89). The accuracy of the wording required by the "law in this regard will depend on the specific situation ... granting the executive power by law"- or a judge – "unrestricted discretion would be contrary to the principle of the rule of law. Therefore, the law should clearly define the limits of any such powers conferred on the competent authorities, as well as the manner in which they are exercised ..., in order to ensure adequate protection of the individual against arbitrary interference" (Series A, 82, pp. 32-33, pp. 67-68) (European, 2001).

Thus, the principle of the rule of law and respect for human and civil rights and freedoms is to ensure a balance of protection of the individual from arbitrary interference by public authorities and the stability of a critical information structure by creating certain restrictions set out in law.

*The principle of ensuring the national interests of Ukraine.* It should be noted that this principle should not contradict the above principle, because as we have already determined, observance of the rule of law and respect for human and civil rights and freedoms is one of the basic fundamental rights. However, this does not mean that national interests in ensuring the sustainability of CII should "suffer" from this.

National interests – an integral expression of the interests of all members of society, realized through the political system of the state as a compromise in the combination of the demands of each person and society as a whole (Babkina & Gorbatenko, 2006). In addition, the combination of interests in the construction of national interests should not only be a guide, but also unite the nation around certain central ideas. For Ukraine, the search for a new system of ideals and guidelines is today a difficult but important task, because without this stage of cognitive and ideological search it is impossible to develop programs of economic, political and other reforms and overcome the systemic crisis (Dashutin & Mikhalchenko, 2001). And, as the Ukrainian human rights activist and co-founder of the Ukrainian Helsinki Group Myroslav Marynovych rightly noted, “we do not know how to unite in peacetime in order to implement good deeds” (The Ukrainians, 2014). Therefore, the author agrees with Larysa Soroka, who, defining national space interests, pointed out that these are “fundamental interests of the individual, civil society and the state, the provision of which is the basis for sustainable development of Ukraine, the welfare of its citizens and security” (Soroka, 2020). Thus, in the formation of any measures aimed at ensuring national interests, in the first place should be the interests of the individual, and only then society and the state.

The priority of the interests of the individual in the formation of national interests is discussed in the Doctrines of Information Security of Ukraine, which determines that the national interests of Ukraine in the information sphere are:

1) Vital interests of the person: ensuring the constitutional rights and freedoms of human to collect, store, use and disseminate information; ensuring constitutional human rights to the protection of privacy; protection from destructive information and psychological influences;

2) Vital interests of society and the state: protection of Ukrainian society from the aggressive influence of destructive propaganda, primarily by the Russian Federation; protection of Ukrainian society from the aggressive informational influence of the Russian Federation, aimed at propaganda of war, incitement of national and religious enmity, change of the constitutional order by force or violation of the sovereignty and territorial integrity of Ukraine; comprehensive satisfaction of the needs of citizens, enterprises, institutions and organizations of all forms of ownership in access to reliable and objective information; ensuring the free circulation of information, except as provided by law; development and protection of national information infrastructure; preservation and increase of spiritual, cultural and moral values of the Ukrainian people; ensuring the comprehensive development and functioning of the Ukrainian language in all spheres of public life throughout Ukraine; free development, use and protection of national minority languages and promotion of the language of international communication; strengthening information ties with the Ukrainian diaspora, promoting the preservation of its ethnocultural identity; development of media culture of society and socially responsible media environment; formation of an effective legal system to protect the individual, society and the state from destructive propaganda influences; creation taking into account norms of the international law of system and mechanisms of protection against negative external information and psychological influences, first of all propaganda; development of the information society, in particular its technological infrastructure; safe functioning and development of the national information space and its integration into the European and world information space; development of the system of strategic communications of Ukraine; effective interaction of public authorities and civil society institutions during the formation and implementation of state policy in the information sphere; ensuring the development of information and communication technologies and information resources of Ukraine; protection of state secrets and other information, the requirements for

the protection of which are established by law; formation of a positive image of Ukraine in the world, communication of operative, reliable and objective information about events in Ukraine to the international community; development of the system of foreign broadcasting of Ukraine and ensuring the presence of a foreign-language Ukrainian channel in cable networks and in satellite broadcasting outside Ukraine (Decree, 2017).

In some normative legal acts, national interests are formed, taking into account the priority of state interests. Thus, in the Law of Ukraine “On National Security of Ukraine,” the fundamental national interests of Ukraine are (On the National, 2018):

1. State sovereignty and territorial integrity, democratic constitutional order, prevention of interference in the internal affairs of Ukraine.
2. Sustainable development of the national economy, civil society and the state to ensure the growth of the level and quality of life of the population.
3. Ukraine’s integration into the European political, economic, security, legal space, membership in the European Union and the North Atlantic Treaty Organization, the development of equal mutually beneficial relations with other states.

Thus, under the principle of ensuring the national interests of Ukraine, we understand the creation of conditions for the safe, sustainable operation of critical information infrastructures, their use in the interests of the individual, society and the state.

## Conclusions

Thus, the analysis of various scientific approaches to understanding such categories as “principles,” “legal principles,” “principles of administrative and legal support,” as well as current regulations of Ukraine allowed to state that activities in the field of administrative and legal support of sustainability CII is based on a system of principles that includes both general and special principles. To such a system, we include the following principles: the rule of law and respect for human and civil rights and freedoms; ensuring the national interests of Ukraine; openness, accessibility, stability and security; public-private partnership; proportionality and adequacy of protection measures to real and potential risks; priority of precautionary measures; objectivity and legal certainty of CII objects; standardization of procedures and standardization of technical requirements; cooperation and interaction.

Thus, under the system of principles of administrative and legal support for the stability of critical information infrastructure, we understand a set of basic guidelines, regulations that take into account the interests of man, society and state, which form the state policy of administrative and legal regulation of critical information infrastructure, which allows the latter to withstand threats and recover quickly in the event of a malfunction.

## References

- Babkina, Olga and Vladimir Gorbatenko (2006) *Political Science*. Tutorial. VTs.
- Brown, Deborah and Anriette Esterhuysen (2019) *Why cybersecurity is a Human Rights Issue, and it is Time to Start Treating it Like one*. Association for Progressive Communications (APC). Available online: <https://www.apc.org/en/news/why-cybersecurity-human-rights-issue-and-it-time-start-treating-it-one#:~:text=Cybersecurity%20and%20human%20rights%20are,cybersecurity%20laws%2C%20policies%20and%20practices>

- Cybersecurity Strategy of Ukraine* (2016) Decree of the President of Ukraine of March 15, No 96/2016. Available online: <https://zakon.rada.gov.ua/laws/show/96/2016#n11>
- Dashutin, Gregory and Nikolay Mikhailchenko (2001) *Ukrainian Experiment on the Scales of Humanism*. Parlam. Type.
- Decree of the President of Ukraine No 47/2017* (2017) On the decision of the National Security and Defense Council of Ukraine “On the Doctrine of Information Security of Ukraine.” February 25. Available online: <https://zakon.rada.gov.ua/laws/show/47/2017#Text>
- Didenko, Sergey (2016) *Administrative and legal support for the circulation and use of weapons in Ukraine*. Candidate’s thesis. Kyiv.
- European Court of Human Rights (Kruslin Case)* (2001) Ukrainian Portal of the Case Law of the European Court of Human Rights. No 4. Available online: <http://www.eurocourt.in.ua/Article.asp?AIdx=432>
- Freedom Online Coalition* (2021) Available online: <https://freedomonlinecoalition.com/about-us/foc-documents/>
- On Approval of the Concept of Creation of the State System of Protection of Critical Infrastructure* (2017) The Order of the Cabinet of Ministers of Ukraine from December 6, No 1009-r. Available online: <https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80#Text>
- On the Basic Principles of Cybersecurity of Ukraine* (2017) Law of Ukraine from October 5, No 2163-VIII. Available online: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>
- On the National Security of Ukraine* (2018) Law of Ukraine from June 21, No 2469-VIII. Available online: <https://zakon.rada.gov.ua/laws/card/2469-19>
- Principle (2021) Oxford English Dictionary, Synonyms. *Lexico.com*. Available online: <https://www.lexico.com/definition/principle>
- Rudneva, Alexandra (2012) International Standards of Human Rights and the Principle of the Rule of Law: to the Problem of the Relationship of Legal Phenomena. *Legal Ukraine*. Vol. 4 (112), 15-19.
- Rule of Law (2011) Report Approved by the Venice Commission at the 86th plenary session on March 25-26, 2011. *Law of Ukraine*. No 10, 168–184.
- Serdiuk, Eugene (2014). Principles of administrative and legal support of voting rights of citizens of Ukraine. *Informatsiia i pravo*, 2, 72-78.
- Sokiran, Maksim (2020) System of Principles of Administrative and Legal Support of Critical Information Infrastructure of Ukraine. *Scientific Notes. Series: Law*. Vol. 8, 73-77.
- Soroka, Larysa (2020) Space Doctrine and Guidelines for Long-Term Sustainability of Outer Space Activities as Basis for Sustainable Earth Development. *Philosophy and Cosmology*, Vol. 25, 43-56. <https://doi.org/10.29202/phil-cosm/25/4>
- The State System of Critical Infrastructure Protection in the System of National Security: an Analytical Report* (2020) National Institute for Strategic Studies. Available online: [https://niss.gov.ua/sites/default/files/2020-08/dopovid-systema-zahystu-krytychnoyi-infrastruktury\\_0.pdf](https://niss.gov.ua/sites/default/files/2020-08/dopovid-systema-zahystu-krytychnoyi-infrastruktury_0.pdf)
- The Ukrainians: Conversation with Myroslav Marynovych* (2014) Ukrainian Catholic University. Available online: <https://ucu.edu.ua/news/the-ukrainians-rozмова-iz-myroslavom-marynovychem/>
- Tsymbal, Victor (2016) *Improving the tools of public management of the contract system*. Available online: <https://www.dissercat.com/content/sovershenstvovanie-instrumentariyapublichnogo-upravleniya-kontraktnoi-sistemoi>
- Zamryha, Arthur (2019) On the definition of the principles of administrative and legal support

of economic activity in Ukraine. *Aktualni Problemy Vitchyznianoï Yurysprudentsii*. Vol. 3, 83-86. Available online: [http://apnl.dnu.in.ua/3\\_2019/21.pdf](http://apnl.dnu.in.ua/3_2019/21.pdf)