Кропивницька В.,
здобувач ступеня вищої освіти бакалавра
Національної академії внутрішніх справ
Консультант з мови: **Гіпська Т.**

ENSURING INFORMATION SECURITY FOREIGN EXPERIENCE

The current stage of the development of information technologies is characterized by the possibility of massive informational influence on individual and public consciousness up to large-scale information wars, as a result of which the principle of information security becomes an inevitable counterbalance to the principle of freedom of information. This principle is due to the global information revolution, rapid development, and widespread implementation of the latest information technologies and global means of telecommunications. Penetrating all spheres of life activity of states, the information revolution expands the possibilities of development of international cooperation and forms a planetary information space in which information acquires the properties of the most valuable element of national property, its strategic resource [1].

One of the most urgent problems in the world today is the problem of legal regulation on the Internet. The global information and telecommunications network Internet, along with the objective benefits it provides to humanity, has absorbed many societal problems that have manifested themselves in the emergence of new forms (types) of illegal activity and the emergence of new threats incompatible with the tasks of maintaining global stability and security. The tasks of countering terrorism and extremism are reflected in the state policy of many foreign states, and the analysis of legal regulation in this area allows us to conclude the tendency to strengthen responsibility for cyberterrorism and the spread of illegal information [1].

Cybersecurity is the desired state of information technology security, in which risks to cyberspace are reduced to an acceptable minimum (German Cybersecurity Strategy) [2].

Among the main threats to national cyberspace, the strategies of most countries define as:

- Cyber espionage and military actions carried out with the support or knowledge of the state. All technologically advanced states and corporations become the target of cyber espionage, which aims to acquire state or industrial secrets, personal data, or other valuable information. Thus, one of the most high-profile cyberattacks in recent times was the actions of the DPRK against Sony Pictures Entertainment, as a result of which the attackers took possession of confidential data, including information about the company’s commercial operations.
- Using the Internet for terrorist purposes. Terrorist groups use the Internet for propaganda, fundraising, and recruiting.

- Cybercrime: theft of personal data and laundering of illegally obtained funds. Criminals sell information about bank card numbers, and passwords from computer servers, and malware.

Accordingly, the national legislation of countries, as a rule, regulates the following issues:

- Protection of personal data (Canada, the Netherlands, Estonia, Sweden, Finland, Spain);
- Protection of e-commerce and security of electronic transactions and payment instruments (USA, Canada, Poland, Estonia, Italy);
- Protection of children (USA);
- Protection of important infrastructure facilities and information systems (France).

For this study, data from the «Cyberwellness profiles» of the International Telecommunication Union were used [2].

Among the numerous international legal acts, the thesis that information and network security is understood as the ability of a network or system to resist with a certain level of reliability accidents or malicious actions that can violate the availability, integrity, and confidentiality of information that is stored or transmitted, as well as services, provided by a network or information system. Compliance with security is defined as the availability, identification, integrity, and confidentiality of information. Special attention is paid to the legislative framework covering the issue of interception and decryption of information [2].

Yes, in the US Information Security Management Act of 2002 year, information security is defined as the protection of information and information systems from unauthorized access, use, disclosure, distribution, modification, or destruction; ensuring the integrity of information from unauthorized alteration or destruction, including guarantees of its authenticity; ensuring confidentiality, which means maintaining the established restrictions on access and dissemination of information, including the closure of data about private life and property; availability, which means fast and reliable access to information [1].

Today, the U.S. government promotes the active use of information technology and digital communications to maintain a strong foundation for cooperation, the exchange of ideas and information, the review of the electoral process, the fight against corruption, and the promotion of civil democracy. Within the framework of this policy, the US government is guided by the goals of providing a favorable environment for the development of constitutional law and real opportunities for the use of information technologies by non-governmental organizations, human rights defenders, and journalists. Cooperation with the public sector, in general, and individual organizations to increase the level of society's resistance to modern information risks [3].

An example of the effectiveness of ISC security is the practical implementation of a non-governmental, non-profit project – the Centre for Cybersecurity and Education. The center promotes careers in this field by providing scholarships to women, and students of higher educational institutions. Countering information threats to the national security of the state is one of the main goals of the project, which is implemented in two main areas:

– research of topical issues of cybersecurity and formation of appropriate recommendations for government agencies;

– promoting the professional development of information security professionals, who later became state personnel sources [4].

A similar field of activity is implemented by the Information Systems Security Association (ISSA), which is a non-profit international organization that unites specialists in the field of information security. The main tools of the organization are holding scientific conferences, educational forums, and publication of relevant materials, as well as creating conditions for interaction between specialists and experts in this field [5].

Thus, the US experience in involving civil society in information security and interaction with the state is based not only on the formation of mechanisms for effective cooperation between government and nongovernmental actors but also on ensuring broad membership of nongovernmental actors in security structures. If there is a developed system of non-governmental organizations, public authorities have the necessary sources of resources to implement security policy in the information sphere.

Список використаних джерел

1. Зарубіжний досвід правового регулювання забезпечення інформаційної безпеки. URL: http://el-zbirn-du.at.ua/2020_1/4.pdf.
2. Законодавство та стратегії у сфері кібербезпеки країн європейського союзу США, Канади та інших: інформаційна довідка, підготовлена Європейським інформаційно-дослідницьким центром. Європейський інформаційно-дослідницький центр. URL: http://euinfocenter.rada.gov.ua/uploads/documents/28982.pdf.
3. Кіберпростір як новий вимір геополітичного суперництва. URL: https://niss.gov.ua/sites/default/files/2015-02/Dubov_mon-89e8e.pdf
4. About Information Security Education & Certification Leader. URL: https://www.isc2.org/aboutus/default.aspx.
5. About Centre for Strategic and International Studies. URL: https://www.csis.org/about-us.

Кузнєцова В.,
здобувач ступеня вищої освіти бакалавра
Національної академії внутрішніх справ
Консультант з мови: **Сторожук О.**

LAW OF ITALY

The **law of Italy** is the system of law across the Italian Republic. The Italian legal system has a plurality of sources of production. These are arranged in a hierarchical scale, under which the rule of a lower source cannot conflict with the rule of an upper source (hierarchy of sources) [1].