УДК 351.746:323(520)

Vozniuk Eugenia, Lesya Ukrainka Eastern European National University

PRINCIPLES AND FEATURES OF JAPAN'S INFORMATION SECURITY SYSTEM

Japan has been described as one of the most advanced information systems in the world. The modern ways of the government's struggle with all possible cyber threats to the national security of the state are highlighted, as well as a sufficiently detailed documentary background of the country's information confrontation is emphasized.

Author analyzed Japan's Cyber security Strategy (2013), the main provisions of the strategy for information security – the following four main objectives of the information security system can be singled out: ensuring the free and secure exchange of information; an attempt to overcome the problem of cyber security at a higher level; optimization of response actions aimed at solving this problem; developing a plan of action and strengthening cooperation based on the principles of social responsibility.

The influence of full informatization on all sectors of economy is revealed. The emphasis is on outsourcing information security, Internet industry within the Japanese society.

The essence of the «information society» of Japan and its sixty year old path of formation, «the right to access information» (in accordance with the Constitution), «hidden state censorship» – its advantages and disadvantages are revealed.

Key words: *Japan, information security system, cyber attacks, national security, threats, cyber security.*

Cyberspace has become an integral part of the life of any modern nation. It contributes to the solution of social problems and has great potential in terms of economic growth and innovation activity, the world community regards it as a stimulus for development and will undoubtedly continue to develop it. In view of this, cyber attacks on information infrastructure have become a real threat and have become one of the top priority problems of national security and risk management.

Japan claims to be one of the most developed information countries in the world, and in order to maintain its reputation, it needs to ensure a decent level of cybersecurity. The range of groups exposed to cyber attacks (from individuals and individual families to complex social infrastructure enterprises) is expanding rapidly. Despite all the efforts of the Japanese government, the risk of information attack increases. This risk affects such areas as national security, risk management and the competitiveness of a country and is a constant concern for citizens.

The information security strategy was developed to create an information-protected nation. Within the framework of this strategy, the following four main objectives can be distinguished: ensuring the free and secure exchange of information; an attempt to bring the problem of cybersecurity to a higher level; optimization of the response actions aimed at solving this problem; Develop an action plan and strengthen cooperation based on the principles of social responsibility. The strategy also clearly defines the roles of all stakeholders (state, infrastructure enterprises, commercial organizations (research institutes), individual users and companies operating through the Internet).

The problem of regulating relations regarding the access, obtaining, exchanging and protecting information, as well as determining the legal basis for the information rights of citizens in the Ukrainian and Russian scientific literature on Japan, has not yet been thoroughly studied. Thus, at present there is no wide range of works devoted to the study of the newest legal framework for regulating information relations and information rights, as well as regulating the activities of the media and the development trends of the Japanese model of the information society. Proceedings concerning the problems of the development of the information society in Japan and the legal regulation of the information and telecommunications sphere are few and do not cover the problems of constitutional and legal regulation of information relations.

In Japan – a country where in the 1960s the term «information society» was introduced into circulation and for the first time attention was focused on the notions of informatization, information industry, – the norms of the information legislation were not adopted immediately. Until 1999, Japan's legislation was not able to regulate new information relations regarding the access, receipt and dissemination of information, virtually no legal acts were adopted that would timely regulate not only the scope of electronic media, but also the information and telecommunications sphere [5]. Since 1999, Japan's legislation in the information and telecommunications industry has begun to change rapidly, and today the country already has all the prerequisites for creating a comprehensive industry of information legislation. In Japan, at present, there is an *information legislation* that *fully regulates the information and telecommunications sphere and information relations* in such areas as: Regulation of the basis for the development of the information society in Japan; Regulation of TV and radio broadcasting; Legal regulation of the protection of users of telecommunications services; Regulation of network communication and the process of introduction of information and telecommunication technologies; Legal regulation of Internet content; Regulation of the procedure for accessing, receiving, transferring and protecting information [6].

In Japan, «the right to access information» (the right to information, or the right to know (sirukenri)) also means «the right of the people to know», that is, the right to freely obtain and demand information from the executive authorities. Right to receive information under the jurisdiction of state authorities and local self-government bodies, is not directly stipulated in the Constitution of Japan of 1947. Nevertheless, the Constitution of Japan guarantees the right to receive (access) information (even in the presence of all contradictions) in Article 13, which has an extensive interpretation and is the basis for the Japanese concept of public welfare [7].

In Japan, the constitutional legal doctrine of determining the guarantees of information rights of citizens and the regulation of information relations consists of such sources as the Constitution, international documents, normative legal acts, judicial precedents, interpretations and professional opinions of jurists, as well as traditions and social regulators of society. Information rights of citizens include such rights as the right to access to information and the right to privacy of a person, including the right to protect personal information. Information relations are relations regarding the receipt, distribution, access, exchange and protection of information using information technology, i.e. various operations with information that are separated from other public relations by the availability of information and the purpose of its use.

In Japan, there is a system of implicit state censorship, which, on the one hand, promotes compliance with the law and journalistic ethics, and on the other – restricts freedom of information, because the government source of information controls the content of the information it provides to a journalist who is part of the press club that plays a key role in information exchange in the country press clubs are the link between official sources of information (government, other authorities and local governments, as well as the largest commercial organizations that are business leaders) and the media that provide the society with already «filtered» information [8]. Such a form of covert censorship, despite many attempts by both Japanese and foreign journalists working in Japan, and by civil society, cannot be abolished in any way.

It is planned that the government will ensure the reliability and stability of cyberspace, increasing the level of information security and providing protection against cyber attacks; create new structures that promote the dynamic development of cyberspace, aimed at stimulating research and development, attracting new personnel on a competitive basis to ensure cybersecurity and educating citizens about cybersecurity; and will formulate tasks in relation to cyberspace, based on diplomatic principles, the global development of this space and international cooperation.

For Japan, the problem of cybersecurity is inextricably linked to its role as a sovereign, independent state. Japan occupies the fourth largest export income in the world and is the most difficult economy in terms of the Economic Complexity Index (ECI). In 2013, Japan exported goods and services by 862.5 billion dollars and imported goods by 990 billion dollars, resulting in a negative trade balance of $ 127.5 billion dollars. In the 2014 calendar year, Japan's GDP was 4.6 trillion dollars, and GDP per capita exceeded 37 thousand US dollars [8].

Traditionally, in Japan informatization of all sectors of the economy is very high. Also, Japan occupies high places in terms of the number of cyber incidents and currently is on the 11th place in the list of countries of the world among sources of cyber attacks and 16 among the recipients of cyber attacks. At the same time, high places in all ratings of hacking activity are occupied by neighboring China and the main ally of Japan – the United States. The main targets of attacks as of 2015 (by industry) are presented in Figure 1.

Since 1999, Japanese legislation passes through a stage of serious change, as a result of which a separate block of information legislation has been formed in the country in a short time. However, despite the urgency of studying the legal regulation of information relations in Japan, as enshrined in the latest legal documents, this has not been fully reflected in Russian scientific and legal literature [10].

As of mid-2013, Japan has 100.7 million Internet users, the penetration of the Internet into households by 2011 was 86% and after that it continued to grow. 99% of Japan's entire business segment (with more than 100 employees) were connected to the Internet. In 2012, Japan ranked second in the world in terms of the number of Internet hosts (website owners or pages on the Internet) in the territory of one state.

The service approach is one of the concepts of all existing methods and standards for organizing the work of IT departments, based on the concept of «quality of service provided» and associated with the concept of «customer-oriented». And since quality is always determined by the client (and not by the service provider), it directly depends not only on the operability of the service itself, but also on how convenient the customer is to the processes of its operation.

Outsourcing of information security is a form of interaction of the customer with the information security market common in Japan (and many other countries). It is characteristic for it to delegate organizations to protect its infrastructure to various contract organizations that have rich experience in providing services of this kind, security certificates, and build or customize the information security system of the customer [2]. In particular, they purchase solutions from vendors, carry out their configuration, installation and debugging, maintenance on the customer's side. For companies that produce solutions, such contractors are authorized dealers on a certain territory and appear as service providers for the solution of a vendor (supplier). Most often in the role of such service providers are local vendor partners – Security-oriented IT companies, people of the local market.

The basic principles of information security outsourcing are set out in the information security management standards, for example, in ISO 27001: 2013; ISO 13335-3; NIST SP800-35 Guide to Information Technology Security Services or Cobit (short for version 4.0 or version 5.0 of Control Objectives for Information and Related Technologies) [9].

A common characteristic feature of the Internet industry in Japan is the voluntary self-regulation of participants. In Japan, there is still no independent commission or government body directly responsible for regulating the Internet. The Ministry of Internal Affairs and Communications of Japan (co-mu-sho), which is responsible for telecommunications, Internet and broadcasting, is allocated the largest range of powers in the regulation of relations on the Internet [7].

The Government and the Ministry of the Interior of Japan adhere to the exemption approach, the minimum of telecommunications restrictions, while law enforcement agencies tend to seek to strengthen formal regulation.

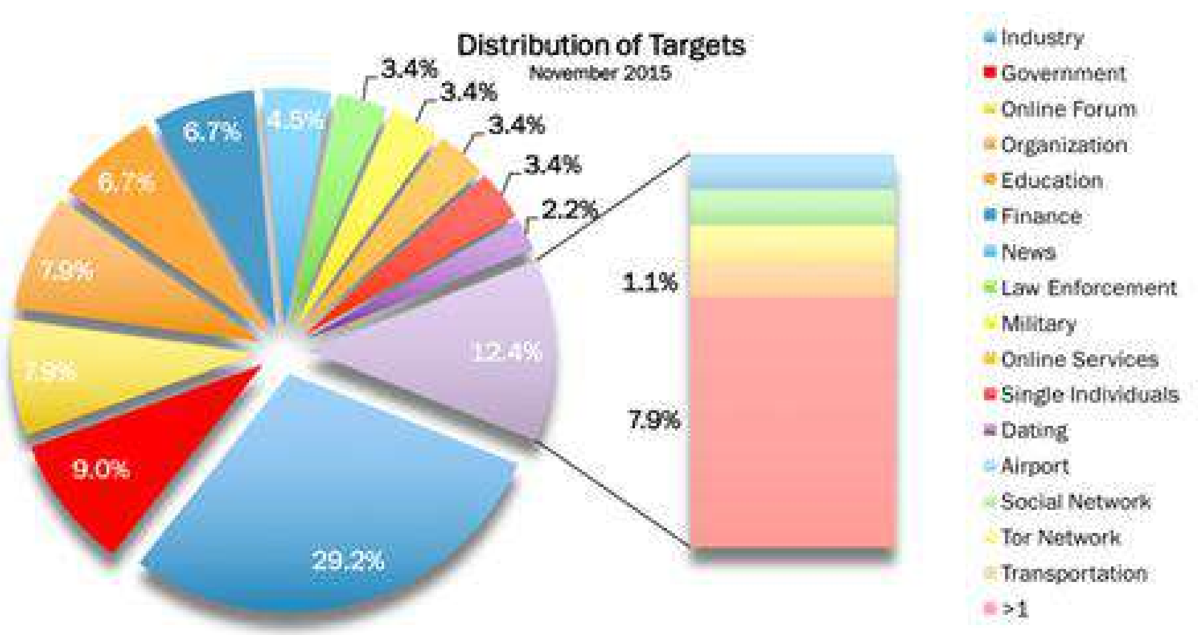

Fig. 1. Main objectives of attacks [4].

To regulate the industry, non-governmental, non-profit organizations, supported by commercial companies, were established: Mobile Content Forum (MCF); Content Evaluation and Monitoring Association; Japan Internet Safety Promotion Association (JISPA); Japan Social Game Association (JASGA) and other similar organizations. Most often they are responsible for determining the unacceptability of content and blocking prohibited content, for example, such as child pornography [1]. The 2001 Liability Limitation Act, which was adopted in 2001, predetermined the format of interaction between participants regarding content on the Internet. According to it, a self-regulatory environment was created that responds to requests from the government for the removal of content that violates copyrights or related rights, copyright and other forms of ownership.

In technical terms, the main organizational features of Japan's information security system: high level of information threats; wide and voluminous market; common information security outsourcing; service approach; high cost of reputational risks; low participation of government regulatory structures in Internet governance; a large proportion of internal traffic, its predominant value over the external; high involvement of criminal structures in information security of the country.

According to the risk of local infection in the world ranking, China is leading with an aggregated threat level of 47%. It is followed by Russia with a share of 42% – both countries belong to a group with a high level of infection. The remaining three are classified as «medium» – the USA shows the lowest risk level of 5 countries, 29%. For Japan, its special formats of information threats are typical [3].

The high cost of reputational risks in the Japanese information security market is connected, on the one hand, with traditionally high reputation risks in this industry, and on the other hand, with the established format of doing business in Japan.

Conclusions.

Therefore, it is proved in the article that Japan is really one of the most informationally developed countries in the world. The constitutional legal doctrine of determining the guarantees of information rights of citizens and the regulation of information relations consists of such sources as the Constitution, international documents, normative legal acts, judicial precedents, interpretations and professional opinions of jurists, as well as traditions and social regulators of society. Information rights of citizens include such rights as the right to access to information and the right to privacy of a person, including the right to protect personal information.

In Japan, there is a system of implicit state censorship, which, on the one hand, promotes compliance with the law and journalistic ethics, and on the other – restricts freedom of information, because the government source of information controls the content of the information it provides to a journalist who is part of the press club.

The problem of cyber security for this state is inextricably linked to its role as a sovereign, independent state. Traditionally, in Japan informatization of all sectors of the economy is very high. Also, it occupies high places in terms of the number of cyber incidents and currently is on the 11th place in the list of countries of the world among sources of cyber attacks and 16 among the recipients of cyber attacks. A common characteristic feature of the Internet industry in Japan is the voluntary self-regulation of participants. There is still no independent commission or government body directly responsible for regulating the Internet.

A high level of information threats in the information security system in Japan is associated with a combination of conditions and factors that create the danger of information security breaches. A threat here means a possible event (impact), a process or phenomenon that can lead to damage to someone's interests.

References:

1. В Японии принята стратегия кибербезопасности [Electronic resource] / 20.06.2013 – Mode of access : http://d-russia.ru/v-yaponii-prinyata-strategiya-kiberbezopasnoti.html.

2. Йоко Нитта О реагировании Японии на киберугрозы [Electronic resource] – Digital.Report. Mode of access : https://digital.report/podhodyi-yaponii-k-kiberbezopasnosti-2/.

3. Отчет по информационной безопасности [Electronic resource] / Полугодовой отчет Cisco за 2014 год. Mode of access : https://tucha.ua/wp-content/uploads/cisco_2014_midyear_security_report.pdf.

4. Atlantic Council [Electronic resource]. – Mode of access : http://www.atlanticcouncil.org/

5. Chris Giles and Kate Allen Financial Times «Southeastern shift: The new leaders of global economic growth» [Electronic resource] / JUNE 4, 2013. Mode of access : https://www.ft.com/content/b0bd38b0-ccfc-11e2-9efe-00144feab7de.

6. Financial Times «Nations are chasing the illusion of sovereignty» [Electronic resource] / 6 July 2013. Mode of access : http://ww w.ft.com/intl /cms/s/0/d1dcdb6a-cddb-11e2-a13e-00144feab7de.html#axzz2WqqIiyJz.

7. Information Security Policies in Japan. [Electronic resource] – Towards a safe and secure network infrastructure. Mode of access : http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/presentation/pdf/070522_1.pdf.

8. Japan and information security [Electronic resource]. – Mode of access : http://www.sciencedirect.com/science/article/pii/S0960259305800576?via%3Dihub.

9. Japan's Information Security Initiatives [Electronic resource] – OECD: better policies for better lives. Mode of access : http://www.oecd.org/japan/japansinformationsecurityinitiatives.htm.

10. National Cyber Security Strategies, Practical Guide on Development and Execution, – European Network and Information Security Agency (ENISA), 2012, 47 p.

Вознюк Є. В. Принципи та особливості системи інформаційної безпеки Японії

Охарактеризовано Японію як одну з інформаційно найрозвинутіших держав світу. Висвітлено сучасні шляхи боротьби уряду зі всіма можливими кібер загрозами національній безпеці держави, а також наголошено на досить детальному документальному забезпечені інформаційного протистояння країни.

Проаналізовано стратегії Японії по кібербезпеці (2013), основні положення стратегії по інформаційній безпеці – можна виділити наступні чотири основні цілі системи інформаційної безпеки: забезпечення вільного та безпечного обміну інформацією; спроба подолати проблему кібербезпеки на більш високому рівні; оптимізація дій реагування, спрямованих на вирішення цієї проблеми; розроблення плану дій та посилення співпраці, заснованої на принципах соціальної відповідальності. Розкрито вплив повної інформатизації на всі сектори економіки.

Наголошено на аутсорсингу інформаційної безпеки, Інтернет індустрії в межах японського суспільства. Розкрито суть «інформаційного суспільства» Японії та його шістдесятирічний річний шлях становлення, «права на доступ до інформації» (згідно з Конституцією), «прихованої державної цензури» – її переваги і недоліки.

Ключові слова: *Японія, система інформаційної безпеки, кібер напади, національна безпека, загрози, кібербезпека.*