DOI: 10.52363/passa-2024.2-2
UDC: 355/359.07; 342.08

Filonov M. - Postgraduate student of the Classic Private University, Zaporizhzhia
ORCID: 0009-0001-3958-5822

THEORETICAL FOUNDATIONS OF PUBLIC MANAGEMENT OF INFORMATION SECURITY AT THE REGIONAL LEVEL

The theoretical foundations of public information security management at the regional level are determined. The role of new technologies in ensuring the development of the public information security management system in the region is investigated. It is emphasized that the impact of new technologies on the information security sector should be predicted and regulated taking into account the scale of cyberattacks. Public information security management measures at the regional level are substantiated.

Keywords: public administration, information security sector, digitalization technologies, cyberattacks, authorities.

Formulation of the problem. Information flows and processes carried out in a certain region are the information space or environment of the region. The information space of a region is formed by a set of information resources of a certain region, and access to these resources may be limited for certain individuals, legal entities, organizations, for a circle of people, for the media, etc. Regional information resources can be developed by both individuals and legal entities, using any technical or software means. In this regard, there is a need to study the state of use of information resources in the region and the formation of state policy in this area.

Analysis of recent research and publications. Publications of such scientists as Ya. Bazylyuk, A. Hrytsenko, M. Denysenko, S. Dombrovska, A. Karsrud, R. Klyut, P. Kolisnichenko, S. Lekar, V. Orlyk, G. Pocheptsov, and others are devoted to consideration of the peculiarities of the formation and implementation of state policy in the sphere of information security.

However, many issues related to the possibilities of implementing in Ukraine the existing best world experience in the formation and implementation of state policy in the field of ensuring national security remain insufficiently researched, and these aspects are related to the use of digital technologies.

Setting objectives. The purpose of the article is to define the theoretical foundations of public management of information security at the regional level.

Presenting main material. Information security is generally defined as methods of preventing unauthorized access, hacking, disclosure, leakage, modification or deletion of data in the information space. But if we consider the information security of a region, then this is the ability of government bodies to prevent negative impacts in the information environment of a particular region.

Negative impacts may include: loss of access, loss of connection with the service provider, change or modification of data, replacement and falsification of information, distribution of malicious software, creation of fictitious information, destruction or restriction of access to data, disabling important components of Internet resources, introduction of malicious code,

restriction of access to resources, etc. Considering that currently the main method of disseminating information is Internet technologies, it is easy to guess that this segment is most susceptible to attacks from intruders.

According to Positive Technologies, the number of cyberattacks has increased by 17% compared to last year, and the main actions of hackers are the theft of personal data and attacks on government agencies [1; 2; 6].

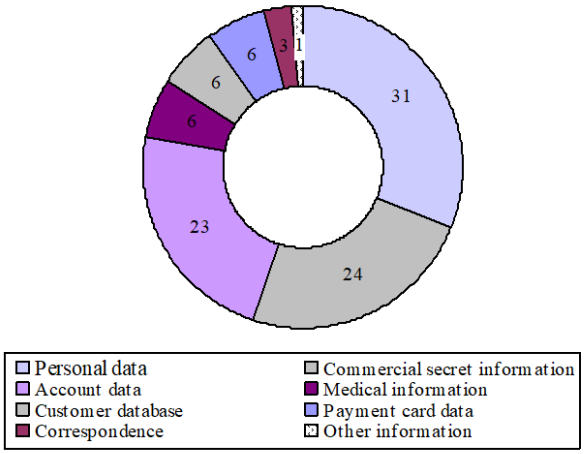

Fig. 1. Types of stolen data
Source: compiled based on [1; 2]

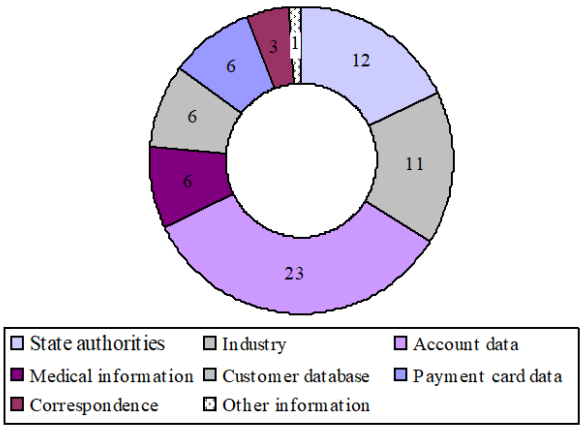

Fig. 2. Categories of victims
Source: compiled based on [1;2]

To carry out attacks, hackers usually use malware, as well as social engineering methods, in which they trick the victim into performing the required actions by means of psychological influence, after which they gain access to data or accounts. In addition to cyber attacks, there are other information security threats in the information spaces of regions, for example, the growth of "information contacts". This phenomenon contributes to a decrease in security and leakage of personal information, increases the risks of unauthorized access threats, and reduces protection from viruses and spam.

In addition to the above, one of the main threats is falsification of information. This is distorted, false, counterfeit and incomplete information in the information space of the region. Falsified fragments of information, as a rule, are pre-planned emissions to manipulate public opinion or a certain subject, but accidents that contribute to the spread of false information in the information space are also possible. The dissemination of fictitious information can be both within the region and beyond its borders. Mass media are often used to publish such information, such as: printed publications, Internet resources, mailings (electronic and physical). Falsified information can also be disseminated through oral speech, but the effectiveness of this method is determined by a number of factors, for example, it may depend on the significance and relevance of the information for legal entities or individuals, the level of trust, education, etc. Often, false information is disseminated on the eve of any election campaigns to influence public opinion.

It is more difficult to combat counterfeiting in the Internet space, since sites can be hosted on foreign servers, and the contact details of the owners are carefully hidden. In addition, the dissemination of false information is much easier, compared to printed publications, and anyone can access them with the right link to the resource. According to statistic information, the number of letters sent via e-mail is growing annually, for example: in 2018, 281 billion letters were sent, and according to analytics, this number may grow to 347 billion by 2023 [3; 4].

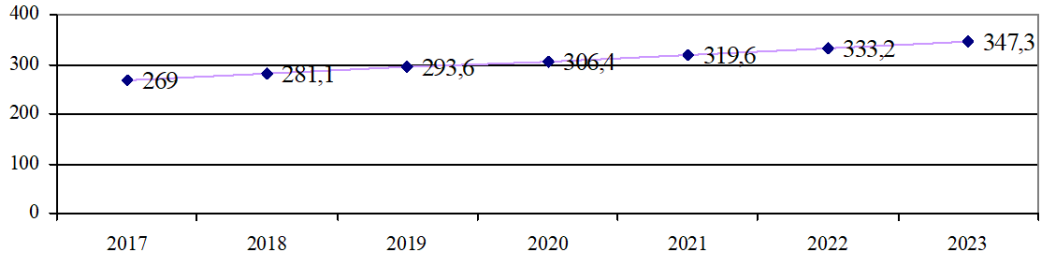

Fig. 3. Number of letters sent by e-mail
Source: compiled based on [3; 4]

If we consider the falsification carried out with the help of mailings, e-mails, then in most cases it is blocked with the mark "spam". Modern services for receiving e-mails are quite developed, and this problem is thus solved. To maintain the information security of the region, it is necessary to involve various government agencies, organizations and individuals, regional educational institutions.

1. These are universities and students in the field of "Information Technology". Since the specialized specialty of this category of students is mainly related to work in the field of information technology, laying the foundations for ensuring information security for the region is important. To improve the level of education in this area, it is necessary to improve the qualifications of teachers, update technical equipment, provide a high-quality Internet connection and provide access to regional Internet resources.

2. Internet providers. To ensure information security, Internet providers need to improve the quality of services, ensure control of incoming and outgoing traffic, update spam databases and databases of prohibited Internet sites, and also install current software on the equipment.

3. Mass media: physical and electronic.

4. Regional Internet portals. Monitor content and advertising posted on websites, use antivirus software, ensure high-quality user-server connection, warn users about possible phishing attacks and ensure the security of user data.

5. Persons responsible for ensuring information security at enterprises. System administrators must properly perform their duties and protect the organizations' data from hacker attacks [1; 2].

Conclusions. To ensure information security of the regions, it is first necessary to raise the level of information culture of society. Currently, most people have personal computers at home, and often they are used not only by adults, but also by children, therefore work in the field of increasing knowledge of computer use, studying information threats and methods of combating them is necessary both at the regional and federal levels. Thus, information security at the regional level is complex, and the fight against threats in the information space is complicated by the existence of interrelations between attackers. To analyze security threats, an assessment of information crimes is carried out, and at the regional level, this is much easier to do. One of the main dangers of information security is the falsification of information, then cyber threats, which mainly consist of attacks on government agencies to steal personal data and accounts. All structures should be involved in the fight against information crimes and improving information security: government agencies, enterprises, law enforcement agencies, as well as individuals and legal entities.

References:

1. Pocheptsov G. Toxic infospace. How to maintain clarity of thinking and freedom of action. Kharkiv: Vivat, 2022. 384 p.
2. Dombrovska S.M., Pomaza-Ponomarenko A.L., Kryukov O.I., Poroka S.G. Information threats and communication infrastructure in the government sector: monograph. 2024. Kharkiv: NUTSZU. 244 p. URL: http://repositsc.nuczu.edu.ua/handle/123456789/19990.
3. Electronic mail. URL: https://uk.wikipedia.org/wiki/%D0%95%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B0_%D0%BF%D0%BE%D1%88%D1%82%D0%B0#:~:text=2018%20%D1%80%D0%BE%D0%BA%D1%83%20%D1%89 %D0%BE%D0%B4%D0%BD%D1%8F%20%D0%B2%20%D1%81%D0%B5%D1%80%D0%B5%D0%B4%D0%BD%D1%8C%D0%BE%D0%BC% D1%83,%D1%80%D1%96 %D0%B2%D0%BD%D1%96%20347%20%D0%BC%D0%BB%D1%80%D0%B4%20%D0%BD%D0%B0%20%D0%B4%D0%B5%D0%BD%D1%8C.
4. "Did They Open My Email?" All You Wanted to Know About Email Tracking. URL: https://web.archive.org/web/20200629123723/https://www.getmailbird.com/email-tracking/.
5. Information Economy Report: Digitalization, Trade and Development, (United Conference on Trade and Development, 2017), https://unctad.org/en/PublicationsLibrary/ier2017_en.pdf.
6. Twilio Study Shows Consumers Aren't Paying Attention to Brands' Social Media or Mobile Apps — They Prefer Email or Text Instead. URL: https://web.archive.org/web/20200630100359/https://www.twilio.com/press/releases/twilio-study-shows-consumers-arent-paying-attention-to-brands-social-media-or-mobile-apps-they-prefer-email-or-text-instead/.