https://www.researchgate.net/publication/291154413 (last visited Oct. 27, 2020).

2. The Internet Organised Crime Threat Assessment (IOCTA) 2016. URL: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016 (last visited Oct. 27, 2020).

Савчук А., курсант Національної академії внутрішніх справ
Консультант з мови: ***Лопутько О.***

MODERN MECHANISMS FOR ENSURING INFORMATION SECURITY (FOREIGN EXPERIENCE)

There is a widespread belief among the scientific community that the United States is a leader in information security.

The United States is an example of an established democracy in which a high level of cooperation between civil society and government is an integral attribute of socio-political relations. As already mentioned, the trend of involving non-governmental institutions in management and organizational processes is also present in the information security sector. It can be stated that such steps are one of the defining directions of the US government's security policy. Regulations governing information security in the United States include the National Security Act, the Information Security Management Act, and the Cybersecurity Research and Development Act, and the Freedom of Information Act. Analysing the US legislation in the field of information security, it can be stated that special emphasis is placed on the involvement of non-governmental actors and cooperation with civil society institutions. At the same time, American lawmakers pay special attention to the use of advisory bodies [1].

In general, the main US programs and strategic documents on information security, as well as regulations are characterized by one unifying factor: they all argue that the state in modern conditions is not able to withstand all types of threats in the information sphere, and therefore needs cooperation. both at the international level (with other states) and at the non-state level (with civil society institutions). In particular, one of the main normative documents in this area, the Federal Law on Information Security Management, provides for the functioning of the Advisory Council on Information Security and Confidentiality advisory board) at the National Security Agency (§ 304). The above-mentioned normative document envisages the involvement of representatives of the public sector (representatives of non-governmental organizations, research institutes, universities, "think tanks", etc.) in the work of the advisory council. The main purpose of the council is public control over the work, establishing effective interaction of these bodies with the public sector [2].

In particular, in the framework of the "International Cyberspace Strategy", which was adopted by the Decree of the President of the United

States, much attention is paid to the problems of respect for fundamental civil rights and freedoms. This is, first of all, the section "Internet freedom: support for fundamental freedoms and confidentiality", which indicates the main activities of the United States [3, p. 185].

Today, the US government promotes the active use of information technology and digital communications to maintain a solid foundation for cooperation, exchange of views and information, review of the electoral process, the fight against corruption and the promotion of civic principles of democracy. As part of this policy, the US government is guided by the goals of providing a favourable environment for the development of constitutional rights and real opportunities for the use of information technology by non-governmental organizations, human rights defenders and journalists. Cooperation with the public sector, in general, and individual organizations in order to increase the level of resilience of society to modern information risks [3, p. 185].

In the United States, government agencies and non-government actors are equally interested in cooperation, which in fact encourages two groups of actors to form the necessary platform. At the present stage, the United States is characterized by a well-developed network of non-governmental organizations based on effective protection against modern information threats. One of the leading American organizations in the information security sector is the International Consortium for Information Systems Security Certification (ISC), which is a non-profit association whose activities are aimed at achieving the highest possible security in cyberspace. It should be noted that in its work the organization covers not only the United States but also countries in Europe and Asia. ISC consists of specialists in the field of cybersecurity, infrastructure security, software. The organization's activities to ensure a high level of information security in the United States concern not only the support of the private but also the public apparatus. These areas of ISC's work are largely based on the information security certification program (namely the data protection and infrastructure segment) of a particular institution/structure/organization [4].

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 centre promotes careers in this field by providing scholarships to women, 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 become a source of personnel for the state [4].

A similar field of activity is implemented by the Information Systems Security Association (ISSA), which is a non-profit international organization and unites specialists in the field of information security. The

main tools of the organization are holding scientific conferences, educational forums, 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 non-governmental actors, but also on ensuring broad membership of non-governmental 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. An important element in this aspect is the think tanks.

Список використаних джерел

1. Законодавство та стратегії у сфері кібербезпеки країн європейського союзу США, Канади та інших: інформаційна довідка, підготовлена Європейським інформаційно-дослідницьким центром на запит народного депутата України. Європейський інформаційно-дослідницький центр. URL: http://euinfocenter.rada.gov.ua/uploads/documents/28982.pdf (дата звернення: 19.10.2020).

2. The Federal Information Security Management Act. The National Institute of Standards and Technology. URL: http://csrc.nist.gov/drivers/documents/FISMA-final.pdf (дата звернення: 19.10.2020).

3. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва: монографія. К.: НІСД, 2014. 328 с.

4. About Information Security Education & Certification Leader. URL: https://www.isc2.org/aboutus/default.aspx (дата звернення: 19.10.2020).

5. About Centre for Strategic and International Studies. URL: https://www.csis.org/about-us (дата звернення: 19.10.2020).

Саліонова О., курсант Національної академії внутрішніх справ

Консультант з мови: *Хоменко О.*

CRIME PREVENTION IN DENMARK

Denmark is a Nordic country in Northern Europe, which shares waters with other Scandinavian countries and a land border with the European continent. This geographical location is attractive to international organized crime groups wishing to smuggle illicit produce into Europe or across Scandinavia [3, p.1].

The majority of serious organized crime affecting Denmark relates to information technology and cybercrime, drug trafficking, property crime and terrorism.