Отже, робимо висновки, що створена в Україні система фінансового моніторингу функціонує з метою реалізації головного завдання – ефективного застосування механізмів і інструментів протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення. Банк, що високо оцінює свою репутацію, повинен працювати відповідно до кращих міжнародних стандартів, завжди дотримуватися законів, тому що, як показує світова практика, банки, причетні до сумнівних видів діяльності та легалізації злочинних доходів, зіткнулися з проблемою не тільки фінансових втрат, але і з відкликанням банківської ліцензії та ліквідацією.

Література

1. Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення: Закон України від 14 жовт. 2014 р. № 1702-VII. *Відомості Верховної Ради України*. 2014. № 50-51. Ст. 2057.

2. Дмитров С.О., Діденко С.В., Медвідь Т.А. Фінансовий моніторинг у банку: навч. посіб. Черкаси: Вид. Чабаненко Ю.А. 2014. 266 с.

3. Колодізєв О.М., Плєскун І.В. Фінансовий моніторинг у банках України: сутність і визначення проблем реалізації в сучасних умовах розвитку економіки. 2017. URL: htpp file:///E:/%D0%B1%D0%B4%D0%B6%D0% BE%D0% BB% D0% B8/Uproz_2017_3-4_6.pdf (дата звернення: 12.04.2020).

UDC 340:004.056:477 (043.2)

Dudnik V.K., Student,
National Aviation University, Kyiv, Ukraine
Scientific Advisor: Myronets O.M., PhD in Law

CYBER SECURITY AS AN INTEGRATED PART OF UKRAINE'S NATIONAL SECURITY

In the process of high technology development, a fundamentally new environment has emerged that is cyberspace, which is formed from the social, technical, telecommunication, information, networking components.

Cyberspace simultaneously acts as a subject and an object of influence. Contemporary successful geopolitics is impossible without sustainable domination in cyberspace. The cyber struggle has become a strategic management direction. It is conducted without international legal restrictions in space and time and is highly effective in achieving a military-political goal. The decisive factor in achieving success in the global confrontation is the information and technological disorganization of the systems of state and military governance and the informational and psychological demoralization of

the population of the countries, first of all, the composition of their armed forces. Cyberspace has become an integral part of the informational space and the fifth area of armed struggle. The armed struggle itself, thanks to an informational factor, has acquired a high degree of controllability [2, p. 174-175].

In accordance with the Decree of the President of Ukraine of May 1, 2014 No. 449/2014 "On measures to improve the formation and implementation of state policy in the field of informational security of Ukraine", with the aim of improving the legal support and the prevention and neutralization of potential and real threats to national security in the informational field, emphasized the need to accelerate the development of the Cyber Security Strategy of Ukraine, the provisions of which should determine organizational and informational measures and explanatory measures on comprehensive coverage of measures for the implementation of state policy in the field of informational security; introduction of enhanced control over the observance of the legislation on informational-psychological and cyber security, creation of a new version of the Informational Security Doctrine of Ukraine. These legal documents have been developed, but the measures of state policy in the field of cyber security are not clearly defined, there is no mechanism for implementation of the provisions themselves, one can notice the lack of interagency coordination on issues of cybersecurity of the state [3, p. 112].

Ya. Volkov rightly points out that "the national security system itself now becomes the object of geopolitical theory. This nature of the relationship between geopolitics and security theory is due, on the one hand, to a broad-based understanding of security as a system that provides not only the protection of the state against threats but also its stable development in economic, political, social and humanitarian spaces. On the other hand, the outlook on geopolitics and, above all, on the role of physical and geographical space in the development of states has changed. The concept of economic, political, information, civilization spaces has emerged, and the nature of the confrontation of states and their allies in the international arena is being re-examined". I. Kefeli notes, in particular, that it is now possible to state "the establishment of interdisciplinary links between cybernetics and the theory of information (in their modern sense) and geopolitics in the field of knowledge, called informational (virtual) geopolitics. The study of the latter in geostrategy takes the form of an informational-psychological war" [1, p. 45].

Analyzing the current state of cybersecurity, it can be noted that the component of the problem of cyber volunteers are not normalized in the Ukrainian legislation and practice mechanisms of relations between the state (state bodies) and the environment of IT professionals (often referred to as "hackers").

It is impossible to solve the problems of the strategic importance of the cyber security sphere without a clear understanding of the condition in which

the conditional “domestic cyber security sector” is located. The principal review should clearly and explicitly point out systemic problems and possible ways of solving them, at times of duplication of functions by agencies involved in informational (cyber) security or at functions not specific to certain agencies, as well as to elements of the cyber security sphere that have been neglected of this security sector.

In addition to the problems of a purely normative-legal direction, it is necessary to state the lack of interagency coordination on the issues of cybersecurity of the state. Currently, Ukraine lacks national interagency coordination structures capable of coordinating and coordinating the activities of various law enforcement agencies in the investigation of cyberspace crime and the creation of an effective system for the protection of domestic cyberspace (including in the military sphere). At the same time, coordination on cybersecurity needs to be achieved at two levels – strategic and operational. Strategic coordination is obviously the area of responsibility of the National Security and Defense Council, and operational – a specially authorized structure (perhaps newly created specifically for these purposes).

Literature

1. Дубов Д. Геополітичне суперництво у кіберпросторі як чинник впливу на національну безпеку України: Основи нац. безпеки держави (політ. науки): Київ, 2016. 434 с.

2. Ліпкан В., Діордіца І. Національна система кібербезпеки як складова частина системи забезпечення національної безпеки України. *Підприємництво, господарство і право*. 2017. С. 174-180.

3. Лук’янчук Р.В. Державна політика у сфері забезпечення кібернетичної безпеки в умовах проведення антитерористичної операції. *Вісник Національної академії державного управління при Президентові України*. 2015. С. 110-116.

УДК 342.951:351.713 (043.2)

Дьякова Ю. В., студентка,
Національний авіаційний університет, м. Київ, Україна
Науковий керівник: Кунєв Ю. Д., д.ю.н., професор

АДМІНІСТРАТИВНО-ПРАВОВЕ РЕГУЛЮВАННЯ ДІЯЛЬНОСТІ ЗАСОБІВ МАСОВОЇ ІНФОРМАЦІЇ В УКРАЇНІ

Засоби масової інформації називають ще «четвертою владою», тому що вони мають змогу впливати на свідомість людей за допомогою пропаганди, використання прихованої реклами та інших засобів впливу на маси, а значить і впливати на політику в державі. Крім того, ЗМІ виступають інструментом в інформаційній війні,яка ведеться між державами, тому завданням кожної країни стає посилення контролю за