Kim V. S., Bokhan Ya. A. Transformatsyia strategii «myagkoi sily» KNR v sovremennykh usloviiakh [Transformation of the strategy of "soft power" of the PRC in modern conditions] [Electronic resource] // Politicheskie nauki. Vostokovedenie. – 2012. – No. 12. – P.18. – Retrieved from: https://cyberleninka.ru/article/n/transformatsiya-strategii-myagkoy-sily-knr-v-sovremennyh-usloviyah. [in Russian]

6. Times Higher Education Official Site [Electronic resource] // World University Rankings 2016-2017. – Retrieved from: https://www.timeshighereducation.com/search?e=404&search=world%20university%20rankings%202017%20worldranking#!/page/1/length/25/sort_by/rank/sort_order/asc/cols/stats.

7. Asia Society Celebrates 10th Anniversary of Asia 21 [Electronic resource] // Asia Society. – Retrieved from: http://asiasociety.org/asia21-young-leaders/asia-21-summit.

Oleksandra Nizitska
Vasyl’ Stus Donetsk National University
Vinnytsia
Research Supervisor: I.H. Lebid, PhD in History, Senior Lecturer
Language Advisor: V.I.Kalinichenko, PhD in Philology, Ass. Prof.

RUSSIA'S POLICY ON CYBERSPACE

Introduction. Russia's aggression against Ukraine in the framework of the hybrid warfare in the East of Ukraine, as well as Russia's actual attempts to dismantle the current international security system, due to this confrontation, causes increased attention to all elements of the security policy of Russia by other actors. Russia's policy is considered to be no exception in the plane of national and international cyberspace and their attempts to use it for their own benefit, thus forming a closed informational model of society and trying to impose the same model throughout the world.

Cybersecurity policy in Russia has several peculiarities that make up both the advantages and disadvantages of this policy. This approach, especially its foreign policy dimension, is based on the information security concept. It covers a wide range of content issues, including advocacy and psychological operations through information networks.

Objective of the paper is to discuss the issues related to the cybersecurity policy in the Russian Federation.

Results of the research. In fact, the term “cybersecurity” does not exist in Russian legislation or in any accepted doctrine. The Russian government first used this term in the draft document “The Concept of the Strategy of Cybersecurity in Russia,” which was adopted in January 2014. The key difference between Russian and Western approaches to cybersecurity and cyberspace is understanding of Russia's

Internet content as a total threat [1]. In the Russian list of problematic issues this is expressed as "the threat of using content for inflation in the social and humanitarian field." In contrast, the Western consensus recognizes the threat from hostile codes, but in general destroys the problem of hostile content. According to Russia's Communications Minister Igor Shchegolev, "for the time being, in the West not everybody always understands what rules we are following" [2]. This remains true despite the fact that Russia for over a decade has been attempting to gather international support for these rules in a variety of international fora including the United Nations and others [1].

In its policy in relation to the future of cyberspace, the Russian Federation makes a significant emphasis not so much on the technical content but on the content component itself. By forming, apparently, a closed information system in their country, the Russian leadership is trying to establish a priority control over internal information flows. In those aspects of its own policy in the field of information security, which requires only government actions to solve certain tasks (increased responsibility for publishing in the Internet, global monitoring of the national segment of the Network, the ability to turn off sites located in the Russian segment of the Internet, etc.) has reached quite significant results. Actually the current Russian information model may be viewed as a propaganda model for the past 10 years, in addition, the destruction of the opposing media can be clearly observed [3]. Since 2012 political analysts have been discussing the issues related to the transition from soft (indirect) methods of control over inform space to much more rigid (direct). And most of them are aimed at strengthening the state control over the Internet.

At the same time, one can not claim that the Russian Federation does not care about the issues of cybersecurity. In 2014 at the background of strengthening Western sanctions against Russia for its aggression against Ukraine, the Russian Federation held multiple events that can be called "cyber educational operations". Moreover, in 2014 they announced about the creation of information operations in the structure of the Ministry of Defense of the Russian Federation. Their main task is to protect Russian military systems of control and communication from cyberterrorism and to provide reliable information protection. It is assumed that these troops will include parts in military districts and in the fleets equipped with highly skilled specialists: mathematicians, programmers, engineers, cryptographers, communications, officers of the electronic counteraction, interpreters and others.

Conclusion. Taking into consideration the above-mentioned facts, it should be mentioned that the Russian Federation remains a very influential player in the global cyberspace, which Western officials and experts regularly pay attention to. Mostly Russia's danger in cyberspace is based on two main factors. Firstly, we may observe here the experience of two well-known cyber attacks – namely, in Estonia in 2007 and in Georgia in 2008. Secondly, let us mention here a high activity of Russian hackers in their capacity of cybercriminals aiming at personal enrichment. Based largely on this, Western experts indicate that cyber threats from Russia may be substantial [4]. In addition, Russia is often referred to as one of those five countries (along with the United States, China, Great Britain and France) that have the highest potential of cybersecurity and cybercrime in the world.

References:

1. Giles K. Russia’s Public Stance on Cyberspace Issues / K. Giles // Conflict Studies Research Centre Oxford, UK. – 2012. – Retrieved from: https://ccdcoe.org/publications/2012proceedings/2_1_Giles_RussiasPublicStanceOnCyberInformationWarfare.pdf

1. Щеголев: цензуры Интернета в России не допустят // Интерфакс. – 2012. – Режим доступу: http://www.interfax.ru/russia/226823.

Shchegolev: tsenzury Interneta v Rossii ne dopustyat [Schegolev: Internet censorship in Russia will not allow] // Interfax. – 2012. – Retrieved from: http://www.interfax.ru/print.asp?sec=1448&id=226823 [in Russian]

2. Дугин А. Good bye, golden boy. Первые мысли об уходе Суркова / А. Дугин. – 2011. – Режим доступу: http://evrazia.org/article/1876.

Dugin A. Good bye, golden boy. Pervyie mysli ob uhode Surkova [Good bye, golden boy. The first thoughts about Surkov’s resignation] / A. Dugin. – 2011. – Retrieved from: http://evrazia.org/article/1876 [in Russian]

Cîrlig C. Cyber Defence In The EU: Preparing For Cyber Warfare? / C. Cîrlig // European Parliamentary Research Service Blog. – 2014. – Retrieved from: https://epthinktank.eu/2014/10/31/cyber-defence-in-the-eu-preparing-for-cyber-warfare/

Bohdana Sas
Vasil’ Stus Donetsk National University
Vinnytsia
Research Supervisor: O.P. Pismenna, PhD in Law, Ass.Prof.
Language Advisor: N.Yu. Ishchuk, PhD in Pedagogy, Ass.Prof.

THE IMPACT OF ROMAN LAW ON THE UKRAINIAN COMMON LAW

Introduction. Roman law is of particular importance in the history of the development of legal systems worldwide. From a historical point of view, earlier Roman law was in force in a number of countries rather than in Italy only. Studying Romal law allows us to understand the origin and essence of the majority of legal bases and institutions of Ukraine.

Review of recent publications. The issue of the impact of Roman private law on the Ukrainian legislation has been covered in publications of such scientists as Ye. O. Kharytonov, O. I. Kharytonova, P. P. Muzychenko, Ye. M. Orach, O. A. Pidopryhora, B.Yo. Tyshchyk, P.P. Zakharchenko and others.

Objectives of the paper. The study is aiming at the determining the impact of Roman private law on the development of the Ukrainian common law.

Results of research. It is a well-known fact that the reception of Roman law began in XI–XII centuries and spread almost over the whole contemporary Europe. In continental Europe, the basis for the reception (in the field of economics) was the