цінності майбутнього фахівця. Підготовка майбутнього спеціаліста потребує не лише високих здібностей у свої професійній галузі, а й наявність вихованості та духовних цінностей. Сучасний фахівець повинен не тільки виконувати свої професійні обов'язки, а й бути всебічно та гармонійно розвиненою особистістю, патріотом нашої держави, котрий збереже духовні цінності накопиченні українським народом протягом багатьох століть. ЛІТЕРАТУРА 1. Атрощенко 1. Т. Культура міжнаціонального спілкування в студентському середовищі // Шлях освіти. – 2004. - № 2. – С.31-35. 2. Гессен С. И. Основи педагогики: Введение в прикладную философию / [отв. ред. и сост. П. В. Алексеев]. — М: Школа-пресс, 1995. — 448 с. 3. Драгомирова І. Концептуальні аспекти формування сучасного спеціаліста /Вища школа. – 2002. - № 2-3. – С. 49-52. 4. Чибісова Н. Г. Формування культурної особистості – завдання сучасної освіти / Педагогіка і психологія. – 2002. - № 3 (36). – С. 135-139. 5. Гончаров С.М. Основи педагогічної праці [Електронний ресурс]: навч. посіб. для виклад. вищ. навч. закладів. – Рівне: Рівненський державний технічний університет, 2000. - http://nuwm.rv.ua 6. Проказа А. Т., Гречка Е. А. Духовная культура личности учителя - предпосылки и залог прогрессивного преобразования образования // Ціннісні пріоритети у XXI столітті: Матеріали Міжнародної науково-практичної конференції 11-13 листопада 2003 р., м. Луганськ. - Ч. 1. - С. 126-130. 7. Пархоменко 0. М. До питання оновлення парадигми виховання гуманістично спрямованої особистості підлітка /Педагогіка і психологія. – 2007. - № 1 (54). – С. 28-34. 8. Лустенко І. Школа як духовно-інтелектуальне середовище //Шлях освіти. – 2006. - № 4. – С. 32-34.

## CYBERCRIMES

**Klimov P.,student,**
**Yarmak T.V., PhD, Associate Prof.,**
**Gubareva O.S., PhD, Associate Prof.**
**Kharkiv National Automobile and Highway University**

INTRODUCTION

In the context of global threats, ensuring security in the world requires the coordination and settlement of many political and economic issues. In particular, these are hotbeds of civil, interethnic conflicts and wars, food threats, the negative effects of climate change, environmental pollution, the depletion of natural resources and slowing down their re-renewal, the need to ensure an economical regime with energy carriers, the development of a green economy, the rational use of natural resources and human potential. However, among all the components of security, a new and at the same time complex element of security has appeared - cybersecurity.

The concept of cybersecurity includes many problems of various types, as well as an even greater number of solutions. Cybersecurity is by far the most related to Internet security, including technical issues and vulnerabilities, social and behavioral issues, and criminal activity in cyberspace. This area is considered the most difficult

in terms of cybersecurity in the world. Cybersecurity is a branch of security that studies the processes of formation, operation and evolution of cyber objects in order to identify sources of cyber danger that can damage them, among the strategic problems in many countries of the world. This article is aimed at finding a more optimal model of the state cybersecurity policy, which should be based on strengthening the security and reliability of information systems, the Internet.

MAIN CONTENT

Every year, the damage to large organizations, companies, individuals and business people from cyberattacks and attacks by intruders is growing. According to Gartner's forecasts, the annual cost of corporations and companies around the world to improve the security of the information technology system is 76-77 billion US dollars. In general, the growth of cyber risks in 2021 cost the global economy more than $500 billion, of which $110 billion fell to the United States. The risks Associate with cyber espionage and crimes in the field of Internet activities continue to pose an increasing threat to business. Half of the cost of cyber risk prevention was borne by the economies of the United States, China, Germany and Japan, amounting to more than $200 billion.

The most notable cybercrimes are data theft and privacy violations. Massive theft of intellectual property, cyber extortion and sabotage of high technologies are also gaining momentum. Among the main reasons for hacking and external interference in the ICT system, Internet networks and other networks are weak security systems, the lack of data exchange on cyberattacks on government agencies and individual business entities, individuals and legal entities, the lack of detailed research and the development of adequate countermeasures, organized exchange of information and system of consultations, etc.

In addition, many government organizations and subjects of market relations, merchants and business people attach little importance to the problems and serious organization of measures to improve a reliable cybersecurity system, and in many cases do not even take elementary steps for this, and do not carry out the necessary work on one or another elements of cybersecurity, to improve the efficiency and rationality of the protective mechanisms of cyberspace, the stability and reliability of the Internet network.

Most researchers note that modern technological advances have caused a significant expansion of cyberspace, which has led to a change in the way individuals, companies and government organizations interact, conduct business and collaborate. At the same time, the existence of a serious dependence of society on various digital infrastructures, including the Internet, makes this infrastructure a strategic national asset that must be protected to ensure the well-being and security of the nation.

Under these conditions, a detailed consideration and identification of the main factors and causes that encourage hacker attacks is required in order to develop new, more effective and most practical mechanisms in the fight against hackers and intruders, pests of the cyberspace environment and infrastructure. Moreover, in the context of globalization and the rapid expansion of the geography of hacker attacks,

criminal acts of cybercriminals and intruders, it is necessary to coordinate and mobilize mental, intellectual, scientific, and human resources against the fight against cybercrime around the world.All these elements, mechanisms and components must be efficient and adequate to the daily problems generated in cyberspace.

Moreover, there is a need to improve the mechanisms and rules of a multilateral international document that plays a significant role in coordinating the efforts of the world community on cybersecurity issues - the European Convention on Cybercrime, adopted by the Council of Europe on November 23, 2001 in Budapest, which contains a classification of computer crimes, recommendations to legislative and executive power of states to combat cybercrime.

It should also be mentioned that this convention was signed by 39 countries of the European Union, as well as the USA, Canada, Japan and South Africa. The Convention entered into force on July 1, 2004 and is so far the only binding international mechanism in the field of cybersecurity, and is a set of basic principles for any country to organize and strengthen the protection of cyberspace, form and develop national legislation and state policy to combat cybercrime and ensuring cybersecurity in the country.

The elements and components of cybersecurity in the world are said to be constantly growing, their sphere of influence is expanding. Therefore, a deep study of the constituent elements and, in general, the essence of the theoretical aspects of cybersecurity in the world and the emerging new elements in cyberspace is necessary in order to understand and determine the likelihood of cyber threats and the actions of cyber intruders, hackers and other cybercriminals.

In order to ensure the overall cybersecurity in the world and strengthen the protection of cyberspace, it is most necessary to ensure the protection of the data transmission channel and the security of Internet packet resources, the strength of telecommunications infrastructures and the improvement of telecommunications networks, the global space of the Internet, the security of servers and computers of end users from hackers and attackers, the development of anti-virus components, improving the efficiency of Internet applications, protecting the data of participants in cyberspace and basic services, the identity of citizens, protecting state and national, regional and international interests.

The problems of cybersecurity and its essence are characterized ambiguously, and B. Gerald rightly notes that not only problems related to cyberspace are more characteristic of cybersecurity, but at the same time there are technical, legal, state, cultural and economic problems. In practice, "cybersecurity" acts as a cleaner of elements of disruption, undermining, kidnapping, sabotage, terrorism and other criminal acts in the field of cyberspace. The given scale of the damage and loss caused on a global scale, cybersecurity in cyberspace is a major issue worldwide.

Effective, practical measures are required in many areas of the information environment of the cybersecurity system, and to increase its resilience. Specialists of the Austrian Center for Cyber Security note that it is necessary to take into account all the problems and issues of tension in the relationship between privacy and national security, protecting people, including the state itself from cyberattacks,

threats of cyber wars and cyber terrorism, closely monitoring cyber espionage in order to suppress it, ensuring effective practical measures to prevent it in cyberspace, compliance with ethics, norms and international law.

Cybersecurity problems are problems on a global scale and at the same time a new direction for researchers, so the unexplored elements of the cybersecurity sphere need more detailed consideration in order to improve the counteraction to the activities of hackers and intruders. Thus, A. Kohen came to the conclusion that it is necessary to shift the focus to the crimes of hackers and cyberattacks, which are most of all Associate with massive information or electronic resources of companies and governments of the countries of the world. The time has come to sharpen our focus on the priorities and ensure the security of information arrays, and in general to develop new strategies for the security of cyberspace.Indeed, many believe that the new and more complex international threats of cyber hackers and attackers need to build a strong and systematic cyber defense architecture in order to ensure full and effective cyber security in the world. It is required to maximize the security of the entire digital infrastructure, develop the offensive or defensive potential of the information communications system, but, as noted, these measures do not guarantee the complete elimination of cyberattacks and the onset of intruders, that is, cybersecurity problems are not guaranteed.

Cyberattacks are a means of fighting against the state, which may or may not catch their opponents by surprise, since cyberattacks are not accompanied by excessive human costs, but at the same time destroy communications and the economy. In fact, the nature of cyberattacks and cyber wars taking place in the world practically for the state and for individual subjects do not differ much, and acting, hackers strictly adhere to the surprise of the attack, destruction, damage and loss to the potential victim. The safety of important information of business processes, their transfer is considered; the fact is that hackers and other interested parties easily gain access to competitors' business systems, seize important data on valuable business components, use them to destroy a competitor's business, damage its activities, carry out other malicious actions, infect systems with viruses, steal funds, distribute compromising materials, etc.

Every year, 40% of the basic data of business processes are stolen, and in these processes the role of hackers who hacked the electronic machine and other means of cyberspace is especially noted, and the so-called smart programmers and other specialists cannot seriously change this situation yet.Cyberspace is in dire need of mitigating the effects of systemic threats and intentional agents that stem from the inherent unpredictability of computers and the information system, which themselves create unintended, in other words, potentially or actually dangerous situations for the physical and human environment in which they are embedded. That is, the cyber threat comes from software, and cannot be corrected with the help of digital technology, improving its fundamentals and programming. Therefore, researchers rightly point to the need to develop and implement a more advanced concept of computer security in the field of cyberspace, awareness of the relevance in the broad

sense of the problem of cybersecurity and the development of cyberspace security strategies, scientists-researchers L. Hansen and N. Helen point out.

The problem of in-depth study of the nature and essence of the elements and conceptual foundations of cybersecurity, its effectiveness necessitates the development of a unified, integrated approach to the formation of effective cybersecurity systems and mechanisms, the development and implementation of rational measures for the functioning of cyberspace, ensuring its protection from possible cybercrimes, reliable mechanisms and services for countering cyberattacks, ensuring the use of intelligent methods to improve the cybersecurity system, preventing the ingress of virus elements, timely detection and neutralization of attacks and intrusions, etc.Researchers note that cybersecurity no longer covers only information as an object of protection, not only technical means that determine the possibility of information functioning, but the protection of the ways of functioning of a new entity - cyberspace. The activity of people, which is carried out with the help of information disseminated through the technical infrastructure of information and communication technologies, is protected.

Cybersecurity, as it were, ensures the security of cyberspace by maintaining the confidentiality, integrity and availability of information in it, where there is network security, uninterrupted and secure transmission of Internet resources, and other backbone components. With the effectiveness of the cybersecurity system, the possibility of cybercriminals to penetrate them into cyberspace is minimized. The formation of elements of cybercrime in cyberspace determines a clearer mechanism and means for their neutralization and elimination in order to reduce losses and damage.

FINDINGS

Generalization and disclosure of the generating causes and roots of cybercrime, the actions of hackers and intruders remain one of the most difficult tasks in the field of cybersecurity in the world. It is necessary to accurately and extensively classify the elements of danger in cyberspace, study their characteristics and essence, highlighting the main features of the tactics and actions of hackers and intruders, and develop adequate mechanisms to prevent such criminal acts in cyberspace.

Thus, the results of the study determine the importance of understanding and understanding serious problems, and the issue of ensuring the cybersecurity of the world requires the development and implementation of more efficient mechanisms for the functioning and ensuring the operation of cyberspace, increasing the reliability of the main mechanisms and components of the global Internet and other devices, an integrated and systematic approach to determining the methodological principles and tools for the formation of state policy on cybersecurity in the current conditions, etc.

**Reference**

1. Views on cybersecurity. Internet Security. Geneva, Switzerland. http://www.internetsociety.org.

2. Convention on Cybercrime. Budapest, 23/11/2001. https://www.coe.int.

3. Gerald B.F. The theory the intersectionality can make cyber security collaboration real. USA, 2015. http://www. techcrunch.com.

4. Word Politics, Security and International Law in Cyber Space. Australian Centre for Cyber Security. UNSW, Canberra. http://www.unsw.adfa.edu.au.
5. Cohen A. The Willie Sutton Theory of Cyber Security, 2015. http://www.securityweek.com.
6. Rueter Nicolas. The Cybersecurity Dilemma. Department of political science Duke University, 2011. http://www.dukespace.lib.duke.edu.
7. Salim H. Cyber safety: A systems thinking and systems theory approach to managing cyber security risks. Massachusetts Institute of Technology, 2014.-157 p. http:// www.ic3.mit.edu.
8. Hansen Lene., Nissenbaum Helen. Digital Disaster, Cyber Security and the Copenhagen School. University of Copenhagen, New York University//International Studies

## ГУМАНІЗМ В УМОВАХ СТАЛОГО РОЗВИТКУ

**О. С. Ященко, студентка**
**Ярмак Т.В., к.с.н., доцент**
**Харківський національний автомобільно-дорожній університет**

Поряд із глобалізаційними процесами та інтенсивним розвитком науки і техніки гостро стоять питання екології та моралі. У цьому необхідно вивчити загальні цінності людства на вирішення цих питань. Однією з цих спільних цінностей є принципи гуманізму у традиційних культурних цінностях. Принципи гуманізму засновані на людяності, індикатори розвитку пов'язані з людською діяльністю та головною метою людства є його єдність. Гуманізм включає в себе поняття того, що люди повинні сприймати природу не тільки як місце існування, а як невіддільну частину нас самих, і тому потрібно розглядати світ як єдине ціле.

Вчений Ч.Ган-Улзий писав: “В онтології духовної культури обов'язково має бути поняття цінності як основи розвитку пізнання якості. Інакше висловлюючись, щоб зрозуміти ознаки усвідомлення цінностей, які є сутністю духовної культури, потрібно виробити якісне значення цих цінностей”. Це необхідно для осмислення сталого розвитку як позитивної цінності та в усвідомленні цінностей принципів гуманізму грають дуже значної ролі. Мета принципів гуманізму - створення справедливого суспільства і гуманних відносин між їхніми членами, заснованих на спільній моралі. Тому ми концентруємося нині не на речах, які розуміються під поняттям гуманізму, а в якості цього значення.

“У другій половині XX століття були спроби пошуку нової моделі світопорядку, здатної привести глобальну систему до якісно нового стану. Результатом спільних та цілеспрямованих зусиль світової спільноти, що діяла на підставі мандату ООН, із залученням авторитетних експертів та громадськості різних країн, стала розробка стратегії сталого розвитку (УР), акцент у якій зроблено на пошук принципів устрою суспільства з