Philosophy, Economics and Law Review

Vol. 4. No. 2. 2024
Received: 01.08.2024
Revised: 19.11.2024
Accepted: 25.12.2024

Journal homepage: https://phelr.com.ua/en

UDC 004.77; 342.7; 343.9

DOI: 10.31733/2786-491X-2024-2-62

The impact of cybersecurity and crime on national security

Liudmyla Rybalchenko*

PhD in Economics, Associate Professor
University of Customs and Finance
49044, 2/4 Volodymyr Vernadsky Str., Dnipro, Ukraine
https://orcid.org/0000-0003-0413-8296

Serghei Ohrimenco

Doctor of Economics, Professor
Moldova Economics Academy
MD 2005, 61 Banulescu-Bodoni Str., Chisinau, Moldova
https://orcid.org/0000-0002-6734-4321

Abstract. The rapid daily growth of cybercrime makes research on this topic extremely relevant. It poses a serious threat to digital infrastructure, citizens' rights and state stability, requiring the development of effective approaches to ensuring national security. The purpose of the article was to study the current state of crime in countries around the world and the impact of various cyber threats on the national security system. The research used the methods of analysis, synthesis, evaluative and situational, comparative, graphical and generalisation. The article showed that the analysis of crime data enables the government and law enforcement agencies to develop effective strategies to combat crime, helps to better understand the problem of crime and take measures to protect the rights and freedoms of every citizen and the security of the entire state. Cybersecurity is a significant priority for Ukraine' s national security system. Reliable protection of the national cybersecurity system and counteraction to any cyber threats must be ensured on an ongoing basis and using the practical experience of other leading countries in this crucial issue. The state of crime has a significant impact on the threat to Ukraine's national security and is one of the factors that negatively affects the efficiency of public authorities, the stability of the country's development and the law and order system, and the protection of citizens' rights and. The practical significance of the results obtained is that they contribute to the development of research on the level of crime and cybercrime to ensure an effective level of protection against threats to national and global security, which will be effective only under the conditions of international cooperation of states in the field of combating cybercrime. The findings of the research can be used by the Cyber Police Department and law enforcement officials to prevent crime and implement effective solutions to reduce cybersecurity in Ukraine

Keywords: state security; economic development; fraud; personal data; crime prevention

Introduction

The country's modern information space is constantly under the influence of various risks, among which cybercrime occupies a special place. Cybersecurity is one of the key factors of information security, which is aimed at ensuring the protection of information, confidentiality, integrity and availability of data in the digital environment. However, cybercrime significantly affects the effectiveness of the implementation of the basic principles of cybersecurity. Such principles of cybersecurity are confidentiality, integrity and availability, which are significantly affected by criminal acts.

There has been a significant increase in cyberattacks aimed at state critical infrastructure, the media, and attacks on information networks, which negatively

Suggested Citation:
Rybalchenko, L., & Ohrimenco, S. (2024). The impact of cybersecurity and crime on national security. *Philosophy, Economics and Law Review*, 4(2), 62-72. doi: 10.31733/2786-491X-2024-2-62.

*Corresponding author

affects the level of national security of Ukraine. The analysis of the scientific literature shows that there are still many unresolved issues on this topic that require scientific research. In 2024, the implementation of malware in emails increased by 349% compared to the previous year worldwide (Department of Cyber Police..., 2024). At the same time, the number of detections of malicious and phishing URLs decreased by 27 % compared to last year. Access to cloud applications posed the greatest risk, as the Attack Surface Risk Management (ASRM) Trend recorded almost 83 billion access attempts (Dovhan *et al*., 2024).

It is noted by A.N. Poliakov (2021) that Ukraine's international cooperation in the field of cybersecurity is aimed at strengthening the protection of cyberspace. Cyberespionage and cyberterrorism in the economic sphere of the state are no less dangerous, as they are aimed at undermining economic relations and provoking social discontent. Thus, the priority task of forming a modern and effective system of countering cyber threats in the country is a guarantee of ensuring an integral component of Ukraine's national security – information security at the proper level (Kolosovskyi, 2023). The North Atlantic Treaty Organisation (NATO) plays a key role in ensuring cybersecurity as a component of national security, and partnership with it is a priority for Ukraine in its foreign policy activities (Gorlynskyi & Gorlynskyi, 2019).

During the war in Ukraine, fundamentally new cyber threats have emerged that are aimed at national and international security and are divided into external, targeted and internal cyber threats (Kuzmenko *et al*., 2022). Due to the growth of cyber risks and cyber threats, it is considered necessary to monitor the current state of cybersecurity in Ukraine and analyse measures to protect computer and telecommunications networks from cyber attacks (Vyshnivskyi & Pampukha, 2022). The impact of major cyber threats on information systems highlights the necessity of ensuring reliable and effective financial and economic security in the face of cyber risks (Trzonkowski & Khalina, 2023). To develop an effective cybersecurity counteraction mechanism, international cooperation with leading global countries is proposed to adopt international legal norms that will enhance Ukraine's cybersecurity legislation (Geer *et al*., 2020; Nikonenko & Khalina, 2024).

Criminal acts such as identity theft and information leakage significantly undermine the principle of confidentiality (Sverdlyk, 2022). Attacks such as phishing or malicious exploitation of software vulnerabilities lead to unauthorised access to sensitive information, which is a violation of this principle. Attacks on databases with personal information of users pose a threat to its confidentiality, as the information obtained can be used for criminal activities with the possibility of obtaining material savings. Crime is spreading significantly in cyberspace and significantly affects the integrity of data by modifying or damaging it. In the banking and financial sectors, criminals can change personal data contained in public documents, which is a significant risk. Attacks involving the use of malware and program errors aimed at compromising data integrity can change information without the user's knowledge. Attacks can also be aimed at disrupting the availability of information resources, which is a type of criminal activity. As a result of such attacks, users lose access to the necessary resources. In addition, criminals may use ransomware to block access to systems and servers in order to obtain a monetary reward.

Theft of credentials and their use by criminals leads to a breach of the authentication principle. It is unauthorised access to user accounts, the use of stolen passwords and biometric data that is becoming the most common phenomenon among cybercriminals. The article was devoted to the numerous problems of crime prevention that have reached a new level, and the threats facing society have been rethought.

Materials and methods

The methodology of the study was based on the use of such methods of analysis as the evaluative and situational method, which analysed crime statistics in different countries of the world obtained from open sources and identifies the highest and lowest indicators; the graphical method was important for visualising the results of the study of crime rates in countries of the world and for better perception of information presented in the form of graphs and tables; the method of generalisation was used to formulate conclusions, fulfil the task and achieve the goal in this work.

The article analysed national and international cybersecurity legislation, its effectiveness and application. Particular attention was paid to the global crime trends in countries and the consequences that occur and affect the country's security. Crime indices in the countries of the world and the factors that affected their growth were presented. The European Union Directive on Network and Information Security (NIS2) and the operation of the domain name system DNS (The European Union Directive on Network..., 2022), the Convention on Cybercrime (2005), which is the first international treaty aimed at combating Internet crime and cybercrime are being studied. As part of the research methodology, an analysis was conducted of Ukraine's legislative acts in the field of cybersecurity, including the Law of Ukraine No. 2163-VIII (2017), which established the legal framework for the functioning of the state cybersecurity system and defines its fundamental principles. Additional regulatory act was also reviewed, such as the Decree of the President of Ukraine No. 447/2021 (2021). This analysis enabled an evaluation of Ukraine's regulatory framework in the cybersecurity domain and its alignment with international standards.

The study used widely recognised ratings, in particular: Global Cybersecurity Index (GCI), Global Cybersecurity Outlook, Cyber Europe, U.S. Cyber Command, National Cyber Security Index (NCSI), Crime and Safety Indexes from Numbeo, The National Cyber League and others. First, the above rankings were analysed, and then graphs were created for better data visualisation. The authors also searched for and analysed previous studies on the topic. The conclusions and prospects for further research were drawn.

Results and Discussion

Issues related to international cooperation in the field of cybersecurity and countering cybercrime have been studied by scholars V. Bykov *et al*. (2019) and V. Savchenko & O. Maklyuk (2024). Author A. Poliakov (2021) in his work, studied the issues of cybersecurity protection and cooperation between Ukraine and NATO (2021). The study of important mechanisms for ensuring cybersecurity was considered by scientists O. Khalina & Y. Sydorenko (2023), as well as V. Emelianov & H. Bondar (2019). With the development of information technologies, it is necessary to create a reliable international cybersecurity system that will become an effective and efficient legal mechanism in the fight against cybercrime. It is proposed to involve international cooperation in cyber defence, which will allow the ratification of international treaties and regulations in the field of cybersecurity into the national legislation of Ukraine (Zhyla, 2023). Other authors have studied issues related to financial and economic security in the field of cybersecurity (Trzonkowski *et al*., 2023).

Ukraine, along with European countries, is implementing a number of laws that regulate cybercrime in the country. One of these documents is the European Union Directive on Network and Information Security (NIS2), which aims to establish security requirements in the digital ecosystem and create cybersecurity measures (The European Union Directive on Network…, 2022). The Convention on Cybercrime, which is the first international treaty to combat cybercrime, stipulates the importance of cooperation between states and private enterprises in the use and development of information technology to combat cybercrime (Convention on Cybercrime, 2005). The Law of Ukraine No. 2163-VIII (2017) establishes that all essential conditions, directions, and principles of state policy in cybersecurity are implemented in cyberspace to safeguard the vital interests of individuals, citizens, society, and the state, as well as the national interests of Ukraine. Ensuring cybersecurity is a priority in the national security system of Ukraine. This priority will be implemented by strengthening the capabilities of the national cybersecurity system to counter cyber threats in the modern security environment (Decree of the President of Ukraine No. 447/2021, 2021).

An analysis of the published scientific works of these experts showed that ensuring cybersecurity for Ukraine is an important and priority area of international activity that will strengthen the state of cybersecurity in Ukraine country (Cybersecurity: Global trends..., 2011; Kuzmenko *et al*., 2022). Scientists have confirmed that the development of partnerships in the field of cybersecurity, the development of joint measures, legislation and mechanisms of international cooperation will become a priority in protecting the information cyberspace of Ukraine and all countries of the world. According to Ukraine's cyber police, since 2018, the attackers have targeted the world's most powerful companies in France, Norway, Germany, the Netherlands, Canada and the United States. The offenders used self-developed malware, including several ransomware viruses, to carry out the hacking attacks. The Joint Investigation Team (JIT) was set up, which included colleagues from Europol (the EU law enforcement agency for combating international organised crime) and Eurojust (the agency that coordinates the EU judiciary).

The attackers hacked into user accounts using information from open sources and social engineering techniques. The hackers used the accounts to spread malicious software code, access servers and steal information from them. During the investigation, it was established that over several years of criminal activity, the criminals encrypted more than 1, 000 servers of global enterprises and caused losses of more than UAH 3 billion in national currency. Subsequently, the police, together with their foreign colleagues, found crypto assets worth more than UAH 24 million in equivalent, apartments, houses, nine luxury cars and 24 land plots with a total area of almost 12 hectares belonging to members of the hacker group. At the request of the investigation, the court seised the relevant property (Department of Cyber Police…, 2024).

The social conditionality of crime in the world is explained by the fact that it is created by society and has social consequences. Crime is a special type of social behavior of certain categories of the population that oppose the interests of society and create their own individual manifestations, which thereby cause harm and problems to state institutions, law enforcement agencies, certain categories of the population, disrupting the normal existence of society. Crime is a historical phenomenon and is a threat to the country. Interestingly, the nature of crime can change dramatically with the development of society. Changes in the legislation regulating the level of crime in the country change the types and consequences of crimes.

Ukraine's legal framework for cybersecurity is based on both international commitments and national legislation. The country has adopted several laws regulating cybersecurity, forming its national legal foundation in this area. This framework includes legislation on state secrets, personal data protection, the

Security Service of Ukraine, and information security, among others. The Law of Ukraine No. 2163-VIII (2017) defines the legal and organisational foundations for protecting national interests in cyberspace, as well as the key directions and principles of state cybersecurity policy. According to Article 106 of the Constitution of Ukraine, the President plays a crucial role in ensuring national security, including cybersecurity. Additionally, Ukraine's Cybersecurity Strategy identifies various cyber threats and assigns responsibility for addressing them to the relevant government agencies.

For the first time, the Cybersecurity Strategy of Ukraine developed a system of cybersecurity status identifiers that will identify and indicate the state of threats to the critical infrastructure of state information resources and the compliance of their protection. The Cybersecurity Strategy of Ukraine has developed relevant models of cyber troops and cybersecurity event monitoring and management systems (SIEM) (Order of the Cabinet of Ministers of Ukraine No. 1163-r, 2023). The European Union, the United Nations, the OSCE, Interpol and other international organisations play a special role in creating international efforts and building fruitful cooperation in the fight against cybercrime.

Cybersecurity is a key priority in the EU's long-term budget for 2021-2027. Through the Digital Europe program, the EU aims to support cybersecurity research, innovation, infrastructure development, cyber defense, and the growth of the European cybersecurity industry. Discussions are currently underway on the draft UN Convention against Cybercrime, approved on 8 August 2024, which raises issues of human rights protection, international cooperation, information and communication technology security, and more. The OSCE is actively working to combat cybersecurity threats and challenges, constantly adapting to such threats as terrorism, organised crime, and cybercrime. In accordance with OSCE Resolution 1202, member states invest in defence cyber capabilities, conduct trainings and activities to improve cybersecurity between states, deepen international cooperation, and create conditions for effective response to cybersecurity events and crises. The Department of International Cooperation, which is responsible for the activities of Interpol's National Central Bureau and ensuring compliance with international standards in the field of criminal policing and combating cybercrime, is also working hard to prevent threats and ensure an adequate level of security at the global level.

Ukraine's cooperation with the world's leading countries in the field of cybersecurity is based on cooperation in countering cyber threats and cyber attacks, implementing cybersecurity standards, and exchanging experience in the functioning of national cybersecurity systems. Ukraine has adopted a number of national standards in the field of cybersecurity and information protection, combined with international standards such as Order of the Ukrainian Research and Training Centre for Standardisation Problems No. 210 (2023), biometric information protection, privacy, security and data protection assessment, information technology, risk management, etc. To create a reliable cybersecurity system, Ukraine has fruitful cooperation with the United States, the United Kingdom, Germany, Israel, and France. Ukraine's international cooperation, gaining experience in legal support in the field of cybersecurity, and improving the current legislation are a priority for improving the effectiveness of the national cybersecurity system.

The most advanced cybersecurity system is created in the United States, which has also developed security standards (NIST Cybersecurity Framework) and international standards for information security (DSTU ISO\IEC 27001:2022, 2023). The National Institute of Standards and Technology has developed the PCI DSS and ISO 2700 security standards, which are used worldwide and are effective in detecting and preventing cyber incidents. The NIST cybersecurity system is based on the main approaches to information security (IS). Germany has adopted a significant number of cybersecurity regulations that provide for liability for cybersecurity offences. In France, the basic regulatory act defining strategic directions in the field of security are the White Paper on Defence and National Security, which was implemented in 2013, and the National Digital Security Strategy of 2015. Ukraine has created a standard – the General Data Protection Regulation (GDPR) of the European Union, which regulates the protection of personal data in the territory of member states (Regulation of the European Parliament..., 2016). Within the EU and in countries such as the United Kingdom, Australia and the United States, the ISO/IEC 27001 standard is in place, requiring organisations to establish, implement, maintain and continuously improve an information security management system (European Union Agency..., n.d).

Since January 2024, the European Union has had new cybersecurity regulations in place that define measures to improve the security of institutions, organisations and agencies. They establish internal management rules for cybersecurity risks, management and control for each EU entity, and provide for monitoring of their implementation (Cyber Europe, 2024). The most common types of cybercrime are cyberattacking, which cybercriminals and hackers use to gain access to a computer network to steal or destroy private information. Cybercriminals also often use malicious software, including ransomware, spyware, Trojans, worms and rootkits, phishing, vishing, account attacks, and more. Considering international cooperation to strengthen cybersecurity around the world, the United States has established a partnership with the EU in the field of cybersecurity and cyberspace, developed a joint Cybersecurity Action Plan of the US Department of Homeland Security and the Department of Public Safety Canada, the US-Estonia Partnership for Cybersecurity and Internet Freedom, and more (Statement

of Anthony J. Cotton…, 2024).

One of the key organisations regulating cyberspace in the European Union is the European Network and Information Security Agency (ENISA), founded in 2004. ENISA has enhanced network and information security across the EU and fostered a strong cybersecurity culture. Its efforts have contributed to safeguarding citizens, consumers, businesses, and public organisations throughout the European Union. NATO operates the Cyber Defense Committee, the NATO Cyber Defense Center of Excellence (CCDCOE) and the NATO Cooperative Cyber Defense Center of Excellence (The NATO Cooperative…, n.d). The International Cyber Security Alliance (ICSPA), INTERPOL, and the International Multilateral Partnership Against Cyber Threats (IMPACT) were also established. In the United States of America, the National Security Agency is responsible for cybersecurity (Fedchenko, 2018). States are increasingly paying attention to the development and protection of their own information resources, as well as the ability to influence the information resources of other countries.

International cooperation focuses on developing effective strategies to combat cyber threats, prevent cybercrime, and restrict the use of cyberspace for illegal activities (Poliakov, 2021). Considering the European Union's experience in enhancing cybersecurity mechanisms across member states, Ukraine should actively engage in these security processes. On one hand, Ukraine's participation aligns with its integration ambitions and contributes to strengthening the country's international reputation. On the other hand, it plays a crucial role in shaping the organisational and legal framework for national cybersecurity (Kyva, 2022). To effectively counter cyber threats, it is essential to establish a robust defense system against both current and potential risks by employing highly skilled professionals and utilising advanced software solutions.

According to research, the largest number of crimes as of the beginning of 2023 was committed in Venezuela, Papua New Guinea, and South Africa. Ukraine ranked 57th in the ranking of 136 countries with 47.42 crimes per 100 thousand inhabitants. The United States ranked 56th with 47.8 crimes per 100 thousand people (The Independent, 2024). When examining the Top 10 countries with the highest crime rates in the world in 2022, it should be noted that Venezuela took the first place. Here, there are 83.76 crimes per 100 thousand people (Table 1).

Comparing the crime index in the world in 2023, the highest level remains in Venezuela, Papua New Guinea, Afghanistan, and other countries, although it has slightly decreased compared to 2022. Syria, Jamaica, and Yemen have the lowest crime rates among the countries in this index (Fig. 1). This situation in the countries indicates a high level of crime, which has a significant impact on the life of the population, its security, development and protection from possible threats. Of particular concern is Venezuela, where murders, torture, violence and disappearances are common, as well as high levels of poverty and unemployment. The countries with the lowest crime index in the world in 2023 include: Andorra, the United Arab Emirates, Qatar, Taiwan, Oman, and others (Fig. 2). These countries have effective law enforcement agencies, strict gun laws, and a high level of economic development and protection of human rights. They are also among the safest countries in the world.

Table 1. Countries with the highest crime rates in the world

№	Country	Number of crimes per 100 thousand people
1	Venezuela	83.76
2	Papua New Guinea	80.79
3	South Africa	76.86
4	Afghanistan	76.31
5	Honduras	74.54
6	Trinidad and Tobago	71.63
7	Guyana	68.74
8	El Salvador	67.79
9	Brazil	67.49
10	Jamaica	67.42
56	United States	47.8
57	Ukraine	47.42

Source: complited by the authors according to The Independent (2024)

The global trend in crime analysis for 2022-2023 is interesting (Fig. 3). The lowest crime rates, according to the 2023 ranking, are in Japan (22.7), China (24.9) and Poland (30.5).

A high level of poverty and unemployment often leads to an increase in a country's crime rate. Converse-

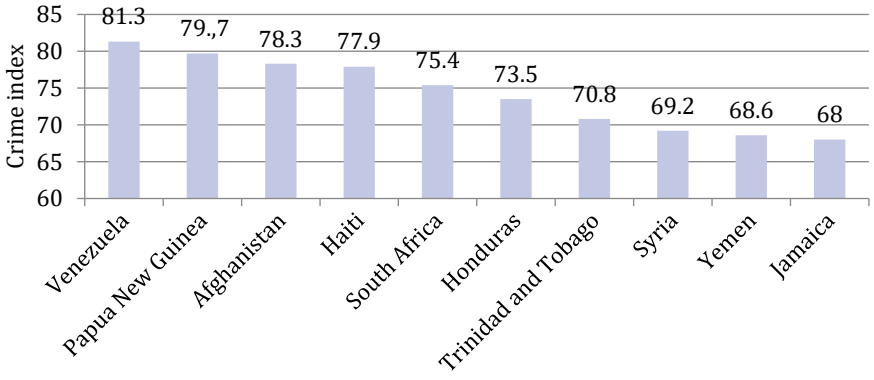

Figure 1. The highest crime index in the world in 2023
Source: complited by the authors according to The Independent (2024)

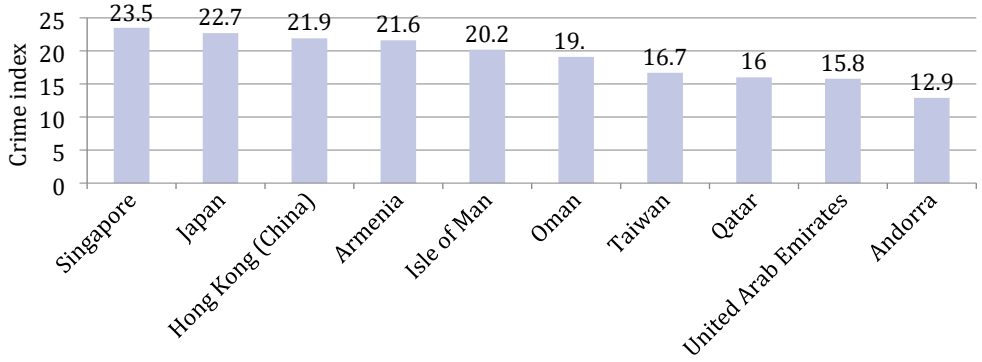

Figure 2. The lowest crime index in the world in 2023
Source: complited by the authors according to Global Cybersecurity Outlook (2024)

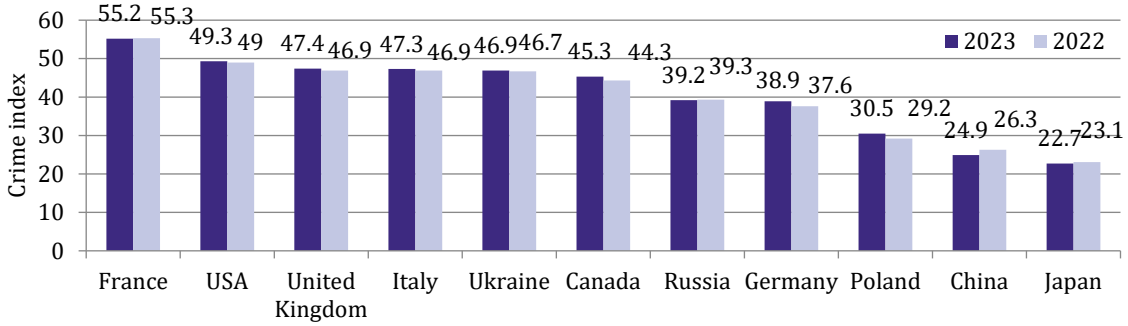

Figure 3. Comparison of crime rates in countries around the world in 2022-2023
Source: complited by the authors according to Global Cybersecurity Outlook (2024)

ly, strict law enforcement and severe penalties tend to reduce criminal activity. There is a strong correlation between age and crime, with most offenses, particularly violent ones, being committed by individuals between the ages of 20 and 30. In the United States, the overall crime rate is 47.70. While violent crime has declined significantly over the past 25 years, its prevalence varies greatly across states. Alaska, New Mexico, and Tennessee have notably higher violent crime rates compared to Maine, New Hampshire, and Vermont. Globally, the lowest crime rates are observed in Switzerland, Denmark, Norway, Japan, and New Zealand. These countries have highly effective law enforcement, and Denmark, Norway, and Japan enforce some of the world's strictest gun control laws. A 2023 study by the Institute for Economics and Peace identified the safest countries in the world, ranking Iceland, Denmark, Ireland, New Zealand, Austria, Singapore, Portugal, Slovenia, Japan, and Switzerland among the top.

Finland is ranked 13th in this ranking, but it is one of the best, happiest and safest places to visit in 2023. Finland also has a low crime and violence rate, the lowest mortality rate, and a reduced risk of natural disasters among the Scandinavian countries, making it the

best place to travel. In addition, Finland is the country with the highest level of joy and happiness in the world. The indicators used to measure this indicator are: gross domestic product per capita, level of freedom, healthy life expectancy, social support, generosity, and corruption. Ukraine was ranked 157th out of 163 in this rating, down 14 positions. The Democratic Republic of Congo is ranked 159th, South Sudan 160th, Syria 161st, Yemen 162nd, and Afghanistan 163rd. The most dangerous countries to visit in 2024 are South Sudan, Afghanistan, Syria, Libya, and Somalia. These countries include Ukraine (The Independent, 2024).

According to Eurostat, the crime rate in Ukraine is generally higher than in most European countries. The most common crimes in Ukraine are theft, fraud, bribery, and hooliganism. The murder rate in Ukraine is also higher than in most European countries. The factors that influence the crime rate include low economic development, social inequality, ineffective law enforcement and lack of trust in the government. The study of crime in some European cities in 2023, conducted by Numbeo (Numbeo..., 2023). The most dangerous cities in Europe were Bradford (UK), Marseille (France), Catania (Italy), Nantes (France), Birmingham (UK), and others (Fig. 4). The Swiss city of Bern was recognised as the safest city in Europe, followed by Munich (Germany) and The Hague (Netherlands), which took third place, tied with another city in Switzerland – Zurich (Numbeo..., 2023). This ranking includes 127 of the most dangerous and safest cities in Europe as of 2023.

In 2023, the efficiency of solving serious and especially serious crimes by police increased (The National

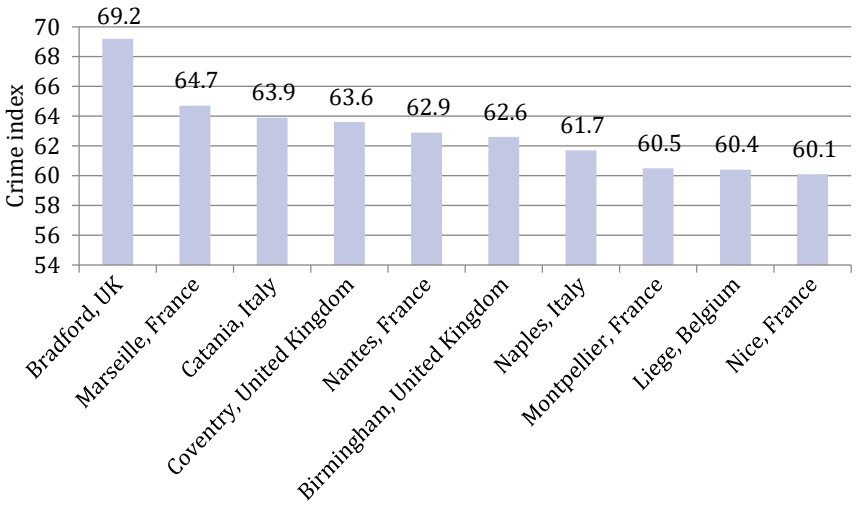

Figure 4. Crime index in European cities in 2023
Source: complited by the authors according to Numbeo... (2023)

Police of Ukraine, 2023). The list of the most dangerous cities in Ukraine in 2023 includes: Dnipro (17th), Odesa (20th), Kharkiv (35th), Kyiv (45th), and Lviv (67th).

The following indicators were taken into account and included in this rating:

- general perception of the crime rate;
- responses from residents and visitors to the city regarding the feeling of safety while walking during the day and at night
- concerns about specific crimes;
- assessment of the scale of property crimes and assessment of the perception of violent crimes, including assaults, murders, sexual crimes, etc.

Analysing the number of car thefts by region in 2019-2023, it should be noted that the highest level occurred in 2022, where the number of car thefts amounted to 12448 (Fig. 5). Dnipropetrovska oblast was among the three leaders of the anti-rating for car theft (Dnipro is operational, 2023). 1278 car thefts were recorded in Ukraine in 2023. This is almost 90% less than in 2022, when a record number of car thefts were recorded – 12,448 cars. For comparison, in 2021, this figure was 1148 stolen cars.

Half of the car thefts in 2023 were in the three frontline regions. For the second year in a row, Donetsk

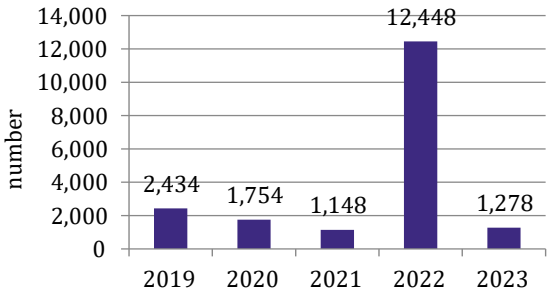

Figure 5. Number of stolen carsin 2019-2023 in Ukraine
Source: complited by the authors according to Dnipro is operational (2023)

region is the leader with 375 thefts, followed by Kherson region with 178 vehicles. Dnipropetrovs'k region rounds out the bottom three with 168 car thefts.

The most frequently stolen vehicles were cars (59%), trucks (15%), and scooters (less than 1%). The most popular car among car thieves was VAZ – 206 cars (16%) of the total, GAZ – 60 (4.7%), Volkswagen – 46 (3.6%), Renault – 42 (3.3%) and Hyundai – 30 (2.3%). In 2023, the most frequently stolen models were: VAZ 2107, 21063, 2121, 2106, and Daewoo Lanos (Dnipro is operational, 2023).

It should be noted that Italy is recognised as one of the countries in Europe with the highest number of pickpockets, whose victims are tourists. Some experts inform tourists on how to protect themselves from pickpockets in crowded tourist cities such as Rome, Milan, Naples, and other cities when visiting major attractions. Italy topped the anti-rating for several popular tourist attractions that have become real magnets for pickpockets – the Colosseum, Trevi Fountain and Pantheon in the capital Rome. The Duomo di Milano in Milan and the Galleria dell'Uffizi in Florence are also popular targets for pickpockets. France ranked second on the list with all five major attractions, including the Eiffel Tower in Paris. It is followed by the Netherlands and Germany.

The top 10 countries in Europe with the highest number of pickpocketing incidents in 2023 are as follows: Italy, France, the Netherlands, Germany, Greece, Spain, Portugal, Turkey, Ireland, and Poland. The most common crimes in Germany are theft and fraud, in France there are theft and robbery, and in Poland there are theft and fraud. Theft can occur anywhere, and tourist hotspots provide an ideal opportunity for criminals to target travelers' wallets and bags. While visitors are distracted by popular attractions, pickpockets take advantage of the dense crowds to commit their crimes. Another crime indicator is corruption. In 2023, Ukraine ranked 104th out of 180 on the Corruption Perceptions Index. This means that Ukraine received 36 out of 100, compared to 2022, which is an increase of three points. To compare Ukraine with other European countries, it should be noted that Ukraine is one of the most corrupt countries (Fig. 6). There are many unresolved issues that need to be addressed.

Thus, the crime rate in Ukraine is higher than in majority of European countries. The structure of crime

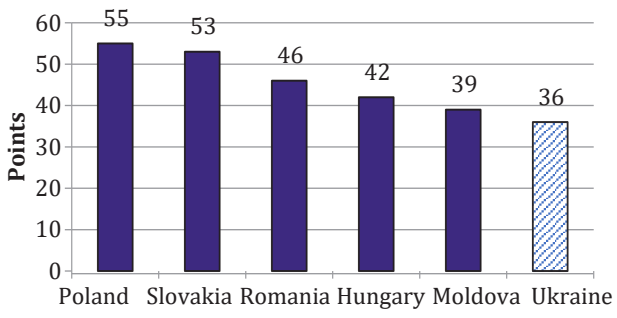

Figure 6. Level of corruption in European countries and Ukraine in 2023 (points)
Source: complited by the authors according to Numbeo… (2023)

in Ukraine is similar to that of other Eastern European countries. The crime rate in Ukraine is influenced by various factors, such as the level of economic development, the level of social inequality, the effectiveness of law enforcement and the level of trust in the government. When examining the ITU Global Cybersecurity Index (2024) among European countries, it should be noted that in 2023, Belgium topped the ranking with a score of 95 points, ranking 1st in the ranking. Lithuania is in second place (94 points), and Estonia is in third place (93.5 points). They are followed by: Czech Republic (90 points), Germany (85.9 points, 5th place), Romania (89 points), Greece (88.5 points), Portugal (88.3 points), United Kingdom (89.1 points), Spain ranked 10th (88.5 points), Poland 11th (88.2 points). Ukraine was ranked 24th (76 points) among 176 countries. After Ukraine became a candidate for EU membership in 2023, the issue of harmonising personal data legislation with European Directives became even more urgent. When processing personal data for law enforcement purposes, there should be a requirement to clearly differentiate and store information on different categories of individuals - suspects, convicts, victims, and other participants in criminal proceedings - in separate databases, as well as to strengthen liability for violations or unauthorised disclosure.

Conclusions

Thus, effective work to reduce crime requires cooperation between law enforcement agencies, courts and correctional institutions, which must work together to prevent, investigate, punish and rehabilitate crimes. It should also be noted that in order to ensure reliable protection of Ukraine's information space, it is necessary to increase the state's capacity in the security and defense sector to create reliable and strengthen existing measures to avoid possible threats and negative information influences by conducting awareness-raising activities among citizens on cyber hygiene in the information space, protecting personal data from cyber attacks, and effectively responding to internal and external threats to protect the national security of the state. Conducting cybersecurity monitoring with the involvement of international experience and training of highly qualified cybersecurity specialists will help reduce the level of cyber threats to citizens and increase the country's cyber resilience.

It should be emphasised that an effective level of protection of the information space from cyber threats requires the training of highly qualified cybersecurity specialists among managers and employees of enterprises and institutions. This is the only way to ensure that businesses are prepared to meet new challenges and threats arising in the digital environment. Prospects for further research include the analysis of criminal activity related to economic fraud, the use of artificial intelligence technologies to strengthen cyber defence systems, and the deepening of international partnerships with NATO, the European Union, Inter-

pol, the OSCE and other organisations to develop and implement new strategies for protecting national and international cybersecurity systems.

Acknowledgements
None.

Conflict of interest
None.

References
[1] Bykov, V., Burov, O., & Dementievska, N. (2019). Cyber security in a digital educational environment. *Information Technologies and Teaching Aids*, 70(2), 313-331.
[2] Convention on Cybercrime. (2005, September). Retrieved from https://zakon.rada.gov.ua/laws/show/994_575#Text.
[3] Cyber Europe. (2024). Retrieved from https://ec.europa.eu/jrc/en.
[4] Cybersecurity: Global trends and challenges for Ukraine. (2011). Retrieved from https://niss.gov.ua/doslidzhennya/nacionalna-bezpeka/kiberbezpeka-svitovi-tendencii-ta-vikliki-dlya-ukraini-analitichna.
[5] Decree of the President of Ukraine No. 447/2021 "On the Cybersecurity Strategy of Ukraine". (2021, May). Retrieved from https://ips.ligazakon.net/document/view/u447_21?an=27&ed= 2021_08_26.
[6] Department of Cyber Police of the National Police of Ukraine. (2024). Retrieved from https://cyberpolice.gov.ua/.
[7] Directive of the European Parliament and of the Council No. 2022/2555 "On Network and Information Security (NIS2) and the operation of the domain name system DNS". (2022, December). Retrieved from https://www.nis-2-directive.com/.
[8] Dnipro is Operational. (2023). Retrieved from https://dnepr.express/ua.
[9] Dovhan, O., Lytvynova, L., & Dorohykh, S. (2024). *Cybersecurity in the information society: Information and analytical digest*. Kyiv: State Scientific Institution "Institute of Information, Security and Law of the National Academy of Sciences of Ukraine"; Vernadsky National Library of Ukraine.
[10] DSTU ISO\IEC 27001:2022. (2023). *Information security, cybersecurity and personal data protection. Information security management system. Requirements*. Retrieved from https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=104398.
[11] Emelianov, V.M., & Bondar, H.L. (2019). Cybersecurity as a component of national security and cyber defence of critical infrastructure of Ukraine. *Public Administration and Regional Development*, 5, 493-523.
[12] European Union Agency for Network and Information Security. (n.d). Retrieved from https://www.enisa.europa.eu/.
[13] Fedchenko, D.I. (2018). Cybersecurity system: Problems of formation and effective activity. *Young Scientist*, 5(57), 653-658.
[14] Geer, D., Jardine, E., & Leverett, E. (2020). On market concentration and cybersecurity risk. *Journal of Cyber Policy*, 5(1), 1-21. doi: 10.1080/23738871.2020.1728355.
[15] Global Cybersecurity Index. (2024). Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf.
[16] Global Cybersecurity Outlook. (2024). Retrieved from https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf.
[17] Gorlynskyi, V.V., & Gorlynskyi, B.V. (2019). Cybersecurity as a component of information security of Ukraine. *Information Technology and Security*, 7(2), 136-148.
[18] Kharytonenko, I.O. (2020). The phenomenon of cybercrime in modern criminological theory. *Journal of Kyiv University of Law*, 4, 401-406. doi: 10.36695/2219-5521.4.2020.72.
[19] Kolosovskyi, E. (2023). The current state of cybersecurity of Ukraine in the conditions of wartime. *Legal Scientific Electronic Journal*, 12, 402-405. doi: 10.32782/2524-0374/2023-12/100.
[20] Kuzmenko, O., Maklyuk, O., & Chernysheva, O. (2022). Cybersecurity of business during the war. *Economy and Society*, 44. doi: 10.32782/2524-0072/2022-44-21.
[21] Kyva, V. (2022). Analysis of factors influencing the cybersecurity of a higher military educational institution. *Cybersecurity Education Science Technique*, 3(15), 53-70. doi: 10.28925/2663-4023.2022.15.5370.
[22] Law of Ukraine No. 2163-VIII "On the Basic Principles of Ensuring Cybersecurity of Ukraine". (2017, October). Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19#top.
[23] Nikonenko, U., & Khalina, O. (2024). Organisational and legal mechanism for ensuring cybersecurity of socio-economic systems in the face of modern challenges. *Economic Scope*, 190, 108-113. doi: 10.32782/2224-6282/190-20.
[24] Numbeo. Europe: Crime index by city. (2023). Retrieved from https://www.numbeo.com/crime/region_rankings.jsp?title=2023-mid&region=150.

[25] Order of the Ukrainian Research and Training Centre for Standardisation Problems No. 210 "On Adoption of National Standards, Amendments to the National Standard and Cancellation of National Standards". (2023, August). Retrieved from https://zakon.rada.gov.ua/rada/show/v0210774-23#Text.
[26] Order of the Cabinet of Ministers of Ukraine No. 1163-r "On Approval of the Action Plan for 2023-2024 for the Implementation of the Cybersecurity Strategy of Ukraine". (2023, December). Retrieved from https://zakon.rada.gov.ua/laws/show/1163-2023-%D1%80#Text.
[27] Poliakov, A.N. (2021). Activation of international cooperation in the field of cybersecurity: Ways to improve in the realities of today. *Information and Law*, 2(37), 129-138. doi: 10.37750/2616-6798.2021.2(37).238348.
[28] Regulation of the European Parliament and of the Council (EU) No. 2016/679 "On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data and Repealing Directive No. 95/46/EC (General Data Protection Regulation)". (2016, April). Retrieved from https://zakon.rada.gov.ua/laws/show/984_008-16#top.
[29] Savchenko, V., & Maklyuk, O. (2024). Cybersecurity as a factor in the efficiency of higher education institutions. *Economy and Society*, 60. doi: 10.32782/2524-0072/2024-60-24.
[30] Sirovatchenko, T.V. (2024). Legal aspects of cybersecurity in Ukraine: Current challenges and prospects. *Scientific Bulletin of Lviv Polytechnic National University: Legal Sciences*, 41, 41-46. doi: 10.23939/law2024.41.314.
[31] Statement of Anthony J. Cotton Commander United States Strategic Command Before the United States Senate Committee on Armed Services. (2024). Retrieved from https://www.stratcom.mil/2024-Posture-Statement/.
[32] Sverdlyk, Z. (2022). Cybersecurity and cyber defence: Issues on the agenda in Ukrainian society. *Ukrainian Journal of Library and Information Science*, 10, 175-188. doi: 10.31866/2616-7654.10.2022.269495.
[33] Tavolzhanskyi, O.V. (2018). Peculiarities of ensuring cybersecurity in the modern world: An overview of the subjects of cybercrime prevention. *Scientific and Information Bulletin of the Ivano-Frankivsk University of Law named after King Danylo Halytskyi: Journal. Series Law*, 6(18), 154-161.
[34] The Independent. (2024). Retrieved from https://www.independent.co.uk/news/uk.
[35] The National Cyber League. (n.d). Retrieved from https://cyberskyline.com/data/power-ranking/fall-2024-central.
[36] The National Police of Ukraine. (2023). *In 2023, the efficiency of solving serious and especially serious crimes by police increased*. Retrieved from https://www.facebook.com/story.php?story_fbid=711882027748497&id=100067801188903.
[37] The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary cyber defence hub. (n.d). Retrieved from https://ccdcoe.org/.
[38] Trzonkowski, K., Khalina, O., Kolisnichenko, P., Rozumovych, N., & Zhyhulin, O. (2023). Information systems for financial and economic security in the face of cyberthreats: Study of characteristics in the context of modern administrative and legal mechanism. *Amazonia Investiga*, 12(69), 315-324. doi: 10.34069/AI/2023.69.09.28.
[39] Vyshnivskyi, V., & Pampukha, A. (2022). Cybersecurity in Ukraine. In *Scientific and practical internet conference* (pp. 31-33). Kyiv: State University of Telecommunications, Educational and Research Institute of Information Protection.
[40] Zhyla, H. (2023). Higher education in times of war: Challenges, problems, prospects for students and researchers. *Youth and the Market*, 2(210), 141-145. doi: 10.24919/2308-4634.2023.276118.

Вплив кібербезпеки та злочинності на національну безпеку

Людмила Рибальченко
Кандидат економічних наук, доцент
Університетеу митної справи та фінансів
49044, вул. В. Вернадського, 2/4, м. Діпро, Україна
https://orcid.org/0000-0003-0413-8296

Сергій Охрименко
Доктор економічних наук, професор
Молдавської економічної академії
MD 2005, вул. Бенулеску-Бодони, 61, м. Кишинів, Молдова
https://orcid.org/0000-0002-6734-4321

Анотація. Стрімке щоденне зростання кіберзлочинності робить дослідження цієї тематики надзвичайно актуальними. Вона становить серйозну загрозу цифровій інфраструктурі, правам громадян та стабільності держави, що вимагає розробки ефективних підходів до забезпечення національної безпеки. Метою статті було дослідження сучасного стану злочинності в країнах світу та впливу різних кіберзагроз на систему національної безпеки. У дослідженні використано методи аналізу, синтезу, оціночно-ситуаційний, порівняльний, графічний та узагальнення. У статті показано, що аналіз даних про злочинність дає можливість уряду та правоохоронним органам розробляти ефективні стратегії боротьби зі злочинністю, допомагає краще зрозуміти проблему злочинності та вжити заходів для захисту прав і свобод кожного громадянина та безпеки всієї держави. Кібербезпека є важливим пріоритетом для системи національної безпеки України. Надійний захист національної системи кібербезпеки та протидія будь-яким кіберзагрозам мають забезпечуватися на постійній основі та з використанням практичного досвіду інших країн-лідерів у цьому надважливому питанні. Стан злочинності має значний вплив на загрози національній безпеці України та є одним із чинників, що негативно впливає на ефективність діяльності органів державної влади, стабільність розвитку країни та системи правопорядку, захист прав і свобод громадян. Практичне значення одержаних результатів полягає в тому, що вони сприяють розвитку досліджень рівня злочинності та кіберзлочинності для забезпечення ефективного рівня захисту від загроз національній та глобальній безпеці, що буде ефективним лише за умови міжнародного співробітництва держав у сфері протидії кіберзлочинності. Результати дослідження можуть бути використані Департаментом кіберполіції та працівниками правоохоронних органів для запобігання злочинності та впровадження ефективних рішень щодо зниження рівня кібербезпеки в Україні

Ключові слова: державна безпека; економічний розвиток; шахрайство; персональні дані; запобігання злочинам