Scientific Journal "Newsletter on the results of scholarly work in sociology, criminology, philosophy and political science" | www.sci-result.de
ISSN (Print) 2699-9382 | ISSN (Online) 2699-9005
Volume 1, Issue 2, 48-57, Published: May 13, 2020
DOI: https://doi.org/10.61439/ZTUH3582

Cybercrime as the Newest Phenomenon of Information and Communication Society and the Means of Its Prevention

Dr. Valentyna Voronkova
Zaporizhzhia National University
Email: valentinavoronkova236@gmail.com
ORCID: https://orcid.org/0000-0002-0719-1546

Dr. Vitalina Nikitenko
Zaporizhzhia National University
Email: vitalina2006@ukr.net
ORCID: https://orcid.org/0000-0001-9588-7836

Dr. Nataliia Kapitaneko
Zaporizhzhia National University
Email: kapitanenko.np@gmail.com
ORCID: https://orcid.org/0000-0002-1475-5784

Dr. Regina Andriukaitiene
Marijampole University of Applied Sciences
Email: regina.andriukaitiene@gmail.com
ORCID: https://orcid.org/0000-0002-0691-7333

Dr. Roman Oleksenko
Dmytro Motornyi Tavria state agrotechnological University
Email: roman.xdsl@ukr.net
ORCID: https://orcid.org/0000-0002-2171-514X

Abstract

The purpose of the research is to analyze cybercrime as the most recent phenomenon of the information society, induced by the technological breakthrough of the Fourth Industrial Revolution, which brought risks and challenges to all mankind. Objective of the study is the theoretical analysis of a rather complex and dangerous phenomenon of cybercrime, the occurrence of which is caused by a dynamic process of criminal use of disruptive technologies in selfish purposes of criminals for the enrichment and unlawful use. Cybercriminals are regularly updating techniques and tools to apply the latest technology to their illegal activities. Today, criminals are developing their clandestine mobile radio telecommunications systems in all countries and are demon-

strating the highest level of technical expertise to improve them and in doing so outperform the defenders of law and order. Nowadays cybercriminals are practicing hacking into hundreds of millions of dollars' worth of accounts, and they are far ahead of the curve. Thus, today we must realize the threatening scale of both organized cybercrime and terrorist organizations, to which governments have fallen out of favor as they turn on the people. The control of cybercrime in the information space acts as an object of research. The subject of the study includes ways to overcome the challenges and threats spread in cyberspace.

Keywords
cybercrime, information technology, information space, complex systems, risks and threats

Introduction

The significance of this research topic is rooted in our existence within an interconnected world, where individuals are inherently linked or exposed to vulnerability due to the pervasive presence of cybercrime in the information landscape. Cybercriminals have developed an extensive arsenal of methods and tactics for financial gain, often targeting digital data under their control. This situation poses a pervasive threat to the integrity of information, particularly as it accumulates during the "big data revolution" (Drewer & Miladinova, 2017; see also Antonescu & Birău, 2015; Brewster et al., 2015; Eddolls, 2016).

The ubiquity of vulnerable computer systems underscores that the imminent technological peril can no longer be disregarded. It is crucial to recognize that the issue lies not in the inherent malevolence of technology itself, but rather in the imperative to comprehend its vulnerabilities. Consequently, a broad spectrum of critical information infrastructures, which sustain the functioning of society, faces imminent threats (Rodofile et al., 2019; see also Alcaide & Llave, 2020; Maglaras et al., 2018; Mansfield-Devine, 2017; Onyeji et al., 2014). Moreover, the risks associated with artificial intelligence and synthetic biology compound the challenge.

It is indisputable that scientific and technological advancements, including breakthrough technologies, offer tremendous benefits to humanity. However, to thrive securely in this era, we must confront the technological risks that invariably accompany progress. This underscores the pressing need to safeguard cyberspace, which holds greater relevance than ever in the context of modern civilization's evolution (Andriukaitiene et al., 2017).

Research Objectives:

- Examining the complexities associated with digital risk management within the backdrop of the coronavirus crisis.
- Assessing the vulnerabilities and opportunities linked to the misuse of digital identities.
- Illustrating the growth of transnational organized cybercrime as a formidable enterprise.
- Unveiling the conducive factors fostering the expansion of organized cybercrime and strategies for its containment.

Research Methodology

The systemic method and approach entail viewing cybercrime phenomena and processes as interconnected and holistic entities, guided by a procedural-genesis multisystem perspective. This approach considers these phenomena as integral components, with their unity established through the analysis of functions, mechanisms, interconnections, and processes that merge into a cohesive cyberspace system, contingent upon specific tasks, objectives, and programs. In this framework, every element within the cybercrime subsystem can be categorized as an individual constituent of the overarching system, characterized by its multifaceted processes and interrelationships that manifest within the broader and interconnected world.

The method of analysis and synthesis is explicated as an elementary constituent parts or components of the general system, united as a result of analyzing elements, subjects, objects of cybercrime, which occur in the actual information environment in the conditions of globalization

(Voronkova, 2010). In the process of analyzing the topic under study, we managed to obtain reliable knowledge about the processes of the investigated reality, relying on analytical and synthetic methods and techniques. Analytics has helped to bring all the disparate facts, inferences and arguments into a system to obtain knowledge that is true and reliable. The method of comparison played a great role, providing an opportunity to cognise the object of study from those dispositions which enabled it to be distinguish it from other objects or subjects, to show similarities with related objects and models, to discourse and summarisetheir essence and direction, to determine the properties and characteristics of the object under study information society. Thanks to the methods and approaches that have been used, it has been possible to to formulate scientific and conceptual knowledge of the battle against cybercrime in the information space, embedded in them epistemological scientific knowledge and relations between the object-subjects of the investigated sphere. As pointed out by Oleg Maltsev (2018), the scientific possibility of a scientist lies in the fact that they take responsibility for the investigation of an abstract category (phenomenon, problem, etc.) and, stage by stage, transform it into an applied category.

Conducting cybersecurity research demands a systematic and methodical approach to analyze and safeguard information systems. The fundamental steps and principles of cybersecurity research methodology include:

- Defining the Object of Study: Clearly specifying the information systems or networks under examination, encompassing network infrastructures, applications, databases, and other relevant elements.
- Formulation of Goals and Objectives: Clearly defining the study's goals, such as identifying vulnerabilities, assessing protection levels, analyzing current cyber threats, etc. This involves formulating specific objectives to be achieved in the research process.
- Selection of Research Methods: Choose research methods aligned with the defined objectives. This could involve employing techniques such as vulnerability scanning, log analysis, penetration testing, statistical data analysis, and other relevant approaches.
- Information Collection and Analysis: Gather data through activities like network traffic analysis, log examination, configuration auditing, code analysis, etc. Analyze the collected information to identify potential threats and vulnerabilities.
- Risk and Threat Assessment: Evaluate the identified risks and threats to the information system. This encompasses analyzing the likelihood of incidents, assessing potential consequences, and gauging the system's vulnerability.
- Development of Security Enhancement Recommendations: Derive security enhancement recommendations from the study's findings. This could involve suggesting the adoption of new technologies, software upgrades, staff training, and other relevant measures.
- Report Creation: Generate a comprehensive report detailing the study's outcomes, encompassing identified vulnerabilities, recommended security enhancements, and an overall analysis of the cybersecurity landscape.
- Implementation of Solutions: Upon approval of the recommendations, execute the proposed security enhancement solutions to fortify the cybersecurity framework.
- Monitoring and Adaptation: Implement a security monitoring system to monitor shifts in threat levels and evaluate the efficacy of implemented measures. Adjust the security strategy to align with evolving requirements and emerging threats.
- Training and Awareness: Provide training for personnel and enhance awareness of cybersecurity threats to mitigate the risk of human error.

A flexible and responsive cybersecurity research methodology is essential given the dynamic nature of cyber threats. Regular security audits and updates to the methodology to align with emerging trends and threats are crucial elements of an effective approach to cybersecurity research.

Results

1. Challenges of Digital Risk Management in the Context of the Coronavirus Crisis

As the analysis shows, the COVID-19 pandemic has, on the one hand, dramatically acceler-

ated the digital transformation globally, by some estimates by five years or even more. On the other hand, it has led to a similarly rapid increase in digital risks. Companies are now more susceptible to online threats due to increased contact, resulting in more issues, which include data privacy, public health. Due to increasing attacks by hackers, people's fears and anxieties are increasing, involving people in phishing operations, downloading malware through deception. More worrying in the midst of a pandemic are threats of cyber-attacks on hospitals with ransom demands and theft of intellectual property from vaccine manufacturers. None of this is new: awareness of cyber risks increased before the pandemic. Geopolitical tensions and new opportunities for cyberattacks have triggered new agendas by states, non-state actors, blurring the distinction between spies and malicious hackers. The World Economic Forum recognised this threat as early as 2019, placing cybersecurity among the most dangerous risks of our time next to climate change. However, the scale and landscape of threats are changing rapidly. For countries looking to reap the benefits of digital transformation, cybercrime is just one of many digital risks. The role of technology in spreading disinformation is no longer a matter of explanation, and not just in the United States. Experts fear that so-called "deepfakes" (an image synthesis technique based on artificial intelligence) can inflame political tensions by spreading disinformation that is difficult to refute (Newitz, 2019). Artificial intelligence fear is increasing as a result of accelerated automation of some professions, strengthening of gender and racial bias, and the so-called "black box" problem - when artificial intelligence makes decisions that even its creators cannot explain (Goodman, 2016).

The transition to a hyperconnected world offers billions of citizens a unique opportunity to gain improved access to education, healthcare, labor market and financial services. In the current decade, we will witness an acceleration of digitalisation, an increase in the challenges associated with it, and an ever-changing digital risk landscape (Broadhead, 2018; Tsakalidis et al., 2019). The question is: will governments be able to become more agile and able to adopt more comprehensive approaches to risk management and digital strategy quickly to reap the benefits of this acceleration while limiting risks?

2. Risks and Potential of Digital Identity Abuse

To those countries seeking to capitalize on the benefits of digital transformation, cybercrime is only one of many digital risks (Nikitenko et al., 2019). The technologies involved are already quite mature. For example, security and encryption algorithms such as two-factor authentication and asymmetric encryption improve data integrity and privacy.

Artificial intelligence, machine learning and biometric sensors integrated into mobile devices are significantly reducing fraud. They can also improve technology by scanning fingerprints, face or voice. In addition, recently developed specialized open source software, solutions based on an open application programming interface (API) solutions and international standards are reducing the cost of national digital identity programmes. Technology providers are already ahead of the curve, and the next generation of identity solutions is just around the corner. Some countries, including Estonia, are beginning to test blockchain-based identity cards. This potentially breakthrough technology could transfer control and ownership of data from governments to citizens while preserving the prerogative of governments to issue and validate ID cards and related services. However, the risks and potential for digital identity abuse remain real and require careful and ongoing attention from policy makers and regulators (Goode, 2019; Olivero et al., 2020). While the pandemic has undoubtedly made the benefits of digital identities clear, it has also highlighted the dangers of digital identity and it has also highlighted the dangers that threaten privacy when combined with other technologies such as tracking applications. No matter what technologies are used, successful digital identity systems must be secure, inclusive, and mutually compatible in order to have a transformative impact on billions of people (Oleksenko, 2019).

3. Development of Transnational Organized Cybercrime as a Huge Business

Transnational organized crime is now a huge business that earns $2 trillion dollars a year: the money comes from drug trafficking, intellectual property theft, trafficking in human beings, child pornography, identity theft, human and contraband goods, gaining access to

private email accounts (Boddy, 2018), including Gmail, access to the password system, which allowed users to log in to a number of services Google and successfully hack into databases around the world.

The company has repeatedly been in the crosshairs of dodgy hacking firms, with hackers back in 2010 stealing the text of a password management system programme that allowed users to log into different Google apps at the same time. The theft caused panic among senior executives at Google, a company that prides itself on the security of its users and their personal data and has built a reputation for ensuring that safety. The agency has a policy of buying information about vulnerabilities and paying the highest price for it, as well as conducting offensive cyber operations that could defeat them. The cyber army is being pushed by large-scale espionage operations targeting defence companies. In general, according to experts, organised crime, which forms modern corporate structures, creates from 15 to 20% of global GDP (Glenny, 2012). Local criminal networks and groups, quickly gather and adjust to exploit any illegal opportunities and channels for their illicit activities, well structured and self-regulating, create clearing houses (intermediaries, financial institutions offering a variety of settlement services), guarantee illegal products or stolen information. Criminal corporations have online tutorials on all critical issues and skills, from problems with overcoming firewalls to cloning credit cards. Criminals have access to online courses created by corporations where they learn how to run companies from phishing, spread spam, and use blanks to create malware, learning the craft of digital crime and cyber fraud. The cyber underground world has created a kind of "Wikipedia" with detailed links categorising how to hack all available devices, software and operating systems. Cybercriminals are much more powerful and forward-thinking, more successful and technologically prepared criminal teams that provide themselves with high profits at relatively low risk. Judicial investigations of cybercrime are extremely rare because convictions account for less than a thousandth of a per cent of all criminal sentences.Cybercriminals continue to carry out aggressive cyber operations aimed at stealing information, with hacker counterattacks being most active in the banking sector (Punchenko & Punchenko, 2019).

4. Conditions For The Development Of Organised Cybercrime And Ways To Stop It

So-called criminal enterprises create their own structures, always using their own jurisdiction of offshore zones or countries with weak state governance and unstable political regimes, which are ready to turn a blind eye to the illegal activities of criminal structures for a certain fee (Harris, 2015). Within these criminal syndicates, labour and supply management departments, department heads, external consultants and execution teams are formed. Hackers are improving and demonstrating their skills in hacking into technology, while continuing their constant search for new technologies, and cybercrime is on the rise while companies lack the technical resources to protect themselves. There is a market for cyber hackers who develop and sell spyware (software) and hacking tools as much as U.S. government developments. The spyware of cyber underground members can monitor a computer, copy files and record every word, technological innovation is emerging from the underground world and thriving, and collective criminal intelligence is steadily taking over from anti-virus companies. Software losses. Today, when we are confronted with the facts of the poor state of the world's software, programmers say that there is no perfect software, as it will be broken no matter what it is (Schwab, 2017). Users seek powerful, multifunctional software, making security a priority and a key component of reliable computing. This problem is growing as more and more devices begin to communicate with each other and software errors, security flaws are all cumulative in the context of the global information network. For this reason, 75% of computer systems can be hacked in a matter of minutes (Cherep & Lubenets, 2010). Given that software drives the global economy and all critical infrastructures, from electricity to telephone networks, governments have no time to waste. Governments should help companies realize that, taking a long-term view, it is in their interest to create more secure and stable software necessary for a general technological future and refusing to do this will have dire consequences for them.

5. Legal Framework for Cyber Security in Ukraine

The establishment of market relations in Ukraine, informatisation and intellectualisation of production, the growing level of competition between economic agents, which is not always of a bona fide nature, contribute to the growing importance of information in all spheres of society. The process of expanded production of information resources, their use and protection, starting from the middle of the twentieth century, ensured the transition to the information society, where human efforts are increasingly less focused on the production of material values, and at the same time communications and information processing become relevant. In the conditions of modernisation of information relations, constant expansion of possibilities of using the information space of the Internet, development of competitive economic activity, the problem of protection of information about production, technologies, management, financial and other activities in the sphere of economic activity, as well as the security of society and the state as a whole, is as acute as ever. It is relevant to adopt the Law of Ukraine "On the Basic Principles of Cybersecurity of Ukraine" dated 5 October 2017, which defines the legal and organizational basis for ensuring the protection of vital interests of a person and a citizen, society and the state, national interests of Ukraine in cyberspace (On The Basic Principles of Cybersecurity of Ukraine, 2017). The legal basis for ensuring cyber security of Ukraine consists of the Constitution of Ukraine, the laws of Ukraine regarding the foundations of national security, the foundations of domestic and foreign policy, electronic communications, protection of state information resources and information, the requirement to protect which is established by law. The legal basis for cyber security in Ukraine consists of the laws of Ukraine, the Convention on Cybercrime, other international treaties agreed to be mandatory by the Verkhovna Rada of Ukraine, decrees of the President of Ukraine, acts of the Cabinet of Ministers of Ukraine, and other legal and regulatory acts adopted in pursuance of the laws of Ukraine. For example, the EU Convention on Cybercrime (ETS No. 185 dated 23 November 2001 No. 994_575, ratified by the Verkhovna Rada of Ukraine on 7 September 2005) recognises that EU countries are concerned that computer networks and electronic information can be used to commit criminal offenses and therefore believe that a joint criminal policy aimed at protecting society from cybercrime by creating appropriate legislation and strengthening international cooperation is a priority. Cyber espionage, as defined by the Law of Ukraine - is espionage carried out in cyberspace (virtual space), which provides opportunities for communications and/or the realization of social relations, formed as a result of the functioning of compatible (connected) communication systems and the provision of electronic communications using the Internet and/or other global data transmission networks or its use. Accordingly, cyber defense is supposed to be used against cyber attacks, which is a set of organisational, legal, engineering and technical measures, as well as cryptographic and technical information protection measures aimed at preventing cyber incidents, detecting and protecting against cyber attacks, eliminating their consequences, restoring the permanence and reliability of the functioning of communication and technological systems (Lee, 2019).

Discussion

Cybersecurity stands as a crucial advancement in the information and communication society, gaining significance amid rapid technological development and the widespread use of the Internet and digital systems. It involves safeguarding computer systems, networks, data, and information from a range of threats, including hacker attacks, viruses, malware, phishing, cyber espionage, and more.

Key facets of cybersecurity and strategies for prevention encompass:

1. Promoting Awareness: It is essential for users and organizations to enhance their understanding of diverse threats and protective measures. This involves educating employees on security issues and adhering to fundamental precautions.

2. Anti-virus Software and Firewalls: Utilizing anti-virus software and firewalls plays a crucial role in identifying and preventing malware and unauthorized connections.
3. Authentication and Access Control: Numerous attacks result from insufficient authentication and access control. Implementing robust passwords, two-factor authentication, and effective access rights management can substantially diminish vulnerability.
4. Frequent Updates and Patches: Consistent updates to operating systems and application software play a vital role in addressing known vulnerabilities.
5. Incident Monitoring and Detection: The presence of effective incident monitoring and detection systems is crucial for preventing and responding to potential cyber attacks.

Cybersecurity is a crucial innovation in the information and communication society, gaining increased relevance with technological advancements and the proliferation of the internet. It encompasses various aspects of safeguarding information, systems, and data from cyber threats. It is essential to recognize that cyber threats encompass a range of issues such as cybercrime, hacker attacks, viruses, phishing, cyber espionage, and more. Numerous methods and approaches exist to ensure cybersecurity:

1. Education and Training: Establishing a cybersecurity culture commences with education. Individuals need awareness about fundamental principles of internet safety and the ability to recognize and thwart cyber threats. Education should cover both foundational and advanced cybersecurity techniques.
2. Network Defense: A robust cybersecurity foundation relies on effective network defense. This involves employing anti-virus software, firewalls, intrusion detection systems (IDS), DDoS attack defense systems, and data encryption. Consistent updating and vigilant system monitoring are also imperative.
3. Legal and Regulatory Compliance: Adhering to cybersecurity legislation and regulations relevant to your organization is crucial. This encompasses safeguarding personal data, fulfilling incident notification obligations, and more.
4. Access Control: Restricting access to information and resources to the essential minimum contributes to lowering the risk of data breaches and unauthorized access.
5. Regular Data Backups: Consistently backing up crucial data facilitates information recovery in the event of an attack or incident.
6. Monitoring and Incident Detection: The establishment of monitoring and incident detection systems aids in recognizing unusual activities and promptly responding to them.
7. Adherence to Best Practices: Abide by cybersecurity recommendations and guidance from organizations specializing in the field. Regularly update your systems and processes in accordance with current standards.
8. Incident Preparedness: Creating and testing an incident response plan is crucial for enabling your organization to respond swiftly and effectively to cyber attacks.
9. Collaboration and Information Sharing: Establishing collaboration with other organizations and law enforcement to exchange information on cyber threats and incidents is vital.

Cybersecurity is a continuous process demanding ongoing attention and effort. In the dynamic threat environment, staying vigilant and adapting to new challenges is of paramount importance.

1. Multi-Factor Authentication: Implementing Multi-Factor Authentication (MFA) or Two-Factor Authentication (2FA) strengthens the security of account and system access by necessitating two or more methods to verify a user's identity.
2. Vulnerability Assessment: Consistently scanning your systems and applications for vulnerabilities can pinpoint potential entry points for attacks, allowing for remediation before attackers can exploit them.
3. Block Unwanted Traffic: Employ tools like Intrusion Detection and Prevention Systems (IDPS) and anti-malware systems to filter out undesired traffic, thereby minimizing the risk of attacks.
4. Data Preservation and Archiving: Proficient data management encompasses safeguarding, long-term storage, and compliant destruction in adherence to regulations and legislation.
5. Auditing and Monitoring: Conducting regular security audits and system monitoring

aids in the identification of unauthorized access and other potential threats.
6. Threat Intelligence Systems: Employing Threat Intelligence systems enables organizations to stay abreast of the latest cyber threats and attacks, facilitating the development of more effective cybersecurity strategies.
7. Social Engineering: Instructing employees to identify social engineering, recognized as one of the most potent attack methods, is crucial in thwarting attacks.
8. Experience Sharing: Collaborating and exchanging information with other organizations and industries contributes to refining methods for safeguarding against and preventing cyber threats.
9. Cybersecurity Monitoring Services: Numerous organizations leverage third-party cybersecurity monitoring services to bolster their capacity for detecting and preventing attacks.
10. Internet of Things (IoT): Emphasizing the security and regular updates of IoT devices is crucial to prevent potential attacks through these devices.
11. Continuous Improvement: The realm of cybersecurity demands continual enhancement and adaptation to address evolving threats and technologies. Organizations should routinely assess and refine their practices and strategies.

With the cyber threat landscape rapidly evolving, the importance of preventing attacks and safeguarding information has never been more critical. Cybersecurity is an ongoing process, requiring sustained attention and efforts. In the face of the ever-changing threat environment, staying vigilant and adapting to new challenges is imperative.

Conclusions

To safeguard the future of technology and address the growing threats it poses to humanity, it is imperative to take proactive measures. This entails enhancing government oversight of the escalating cybercrime activities across networks.

Elevating security standards and ensuring cybersecurity is paramount, irrespective of the sophistication of technology or internet services. The digital underground is agile and prepared to employ innovative tools, with a primary focus on monetary gains through substantial yet precision-targeted thefts that challenge authority and disregard regulations and laws. This encompasses activities such as malware creation, the stimulation of innovation for criminal purposes, exploration of new avenues for cybercrime against businesses, and the development of novel methods for cyber exploitation.

The state must devise a comprehensive set of technical, organizational, and educational recommendations as part of its information policy to mitigate the risks associated with technology. It should determine how to harness various tools to maximize benefits while minimizing adverse consequences. This approach is crucial for successfully navigating the trials of technological progress.

In the context of the modern society and economy, trust in the cyberspace is indispensable. With the surge in threats, including daily data breaches orchestrated by hackers, the state's protective capabilities are stretched thin, while businesses often lack the technical resources to fend off cyberattacks.

Therefore, it is imperative to bolster state oversight in combating cybercrime, ensuring enhanced security standards, and guaranteeing robust cybersecurity for critical state infrastructure. The state should articulate an effective national security strategy, including the public disclosure of information about hackers and the reinforcement of defensive measures to counter cybercriminal attacks, bolstered by cyber defense forces.

Declaration of Conflicting Interests

The author declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author received no financial support for the research, authorship, and/or publication of this article.

References

Alcaide, J. I., & Llave, R. G. (2020). Critical infrastructures cybersecurity and the maritime sector. Transportation Research Procedia, 45, 547–554. https://doi.org/10.1016/j.trpro.2020.03.058

Andriukaitiene, R., Voronkova, V., Kivlyuk, O., Romanenko, T., & Rizhova, I. (2017). Conceptualization of smart society and smart technologies in the context of the development of modern civilization. In Mokslas Ir praktika: Aktualijos Ir Perspektyvos (pp. 11–12). Lietuvos sporto universitetas.

Antonescu, M., & Birău, R. (2015). Financial and non-financial implications of cybercrimes in emerging countries. Procedia. Economics and Finance, 32, 618–621. https://doi.org/10.1016/s2212-5671(15)01440-9

Boddy, M. (2018). Phishing 2.0: the new evolution in cybercrime. Computer Fraud & Security, 2018(11), 8–10. https://doi.org/10.1016/s1361-3723(18)30108-8

Brewster, B., Kemp, B., Galehbakhtiari, S., & Akhgar, B. (2015). Cybercrime. In Application of Big Data for National Security (pp. 108–127). https://doi.org/10.1016/b978-0-12-801967-2.00008-2

Broadhead, S. (2018). The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments. Computer Law & Security Review, 34(6), 1180–1196. https://doi.org/10.1016/j.clsr.2018.08.005

Cherep, A. V. & Lubenets, I.O. (2010). Konceptualni zasadi ekonomichnoyi bezpeki pidpriyemstv [Conceptual Bases Of Economic Security Enterprises]. Bulletin of Zaporizhzhia National University. Economics, 1(5), 63–66.

Drewer, D., & Miladinova, V. (2017). The BIG DATA Challenge: Impact and opportunity of large quantities of information under the Europol Regulation. Computer Law & Security Review, 33(3), 298–308. https://doi.org/10.1016/j.clsr.2017.03.006

Eddolls, M. (2016). Making cybercrime prevention the highest priority. Network Security, 2016(8), 5–8. https://doi.org/10.1016/s1353-4858(16)30075-7

Glenny, M. (2012). Organized Crime In A Network Society. Journal of International Affairs, 66(1), 145–149. http://www.jstor.org/stable/24388256

Goode, A. (2019). Digital identity: solving the problem of trust. Biometric Technology Today, 2019(10), 5–8. https://doi.org/10.1016/s0969-4765(19)30142-0

Goodman, M. (2016). Future Crimes: Everything Is Connected, Everyone Is Vulnerable and What We Can Do About It. Corgi Books.

Harris, S. (2015). WAR: The Rise of the Military-Internet Complex. Houghton Mifflin Harcourt.

Lee, L. (2019). Cybercrime has evolved: it's time cyber security did too. Computer Fraud & Security, 2019(6), 8–11. https://doi.org/10.1016/s1361-3723(19)30063-6

Maglaras, L. A., Kim, K., Janicke, H., Ferrag, M. A., Rallis, S., Fragkou, P., Maglaras, A., & Cruz, T. (2018). Cyber security of critical infrastructures. ICT Express, 4(1), 42–45. https://doi.org/10.1016/j.icte.2018.02.001

Maltsev, O. V. (2018). Vekovoj obman [The Age-Old Deceiving]. Serednyak T. K. https://books.google.com.ua/books?vid=ISBN6177696635

Newitz, A. (2019). The real fake menace. New Scientist, 244(3256), 24. https://doi.org/10.1016/s0262-4079(19)32160-8

Nikitenko, V., Andriukaitiene, R., & Punchenko, O. (2019). Formation of sustainable digital economical concept: challenges, threats, priorities. Humanities Studies, 1(78), 140–153. http://dx.doi.org/10.26661/hst-2019-1-78-11

Oleksenko, R. (2019). Position and role of modern economic education as the main megatrend of innovative development of Ukraine. Humanities Studies, 2(79), 169–181. https://doi.org/10.26661/hst-2019-2-79-11

Olivero, M. A., Bertolino, A., Mayo, F. J. D., Escalona, M. J., & Matteucci, I. (2020). Digital persona portrayal: Identifying pluridentity vulnerabilities in digital life. Journal of Information Security and Applications, 52, 102492. https://doi.org/10.1016/j.jisa.2020.102492

On the basic principles of cybersecurity of Ukraine: the Law of Ukraine of October 5, 2017 No. 2163-VIII. No. 45. art. 403. (2017) https://zakon.rada.gov.ua/laws/show/2163-19#Text

Onyeji, I., Bazilian, M., & Bronk, C. (2014). Cyber security and critical energy infrastructure. The Electricity Journal, 27(2), 52–60. https://doi.org/10.1016/j.tej.2014.01.011

Punchenko, O., & Punchenko, N. (2019). Basic strategic technology of intellectual duality of humanity in information technology. Humanities Studies, 2(79), 95–114. https://doi.org/10.26661/hst-2019-2-79-07

Rodofile, N. R., Radke, K., & Foo, E. (2019). Extending the cyber-attack landscape for SCADA-based critical infrastructure. International Journal of Critical Infrastructure Protection, 25, 14–35. https://doi.org/10.1016/j.ijcip.2019.01.002

Schwab, K. (2017). The Fourth Industrial Revolution. Penguin UK.

Tsakalidis, G., Vergidis, K., Petridou, S., & Vlachopoulou, M. (2019). A cybercrime incident architecture with adaptive response policy. Computers & Security, 83, 22–37. https://doi.org/10.1016/j.cose.2019.01.011

Voronkova, V. G., & Sosnin, O. V. (2015). Formuvannya informacijnogo suspilstva v ukrayini: viklik chi potreba chasu? [Formation of the information society in Ukraine: challenge or necessity of the time? present need]. Humanities Bulletin of Zaporizhzhe State Engineering Academy, 60, 13–24.

Voronkova, V. H. (2010). Filosofiya globalizaciyi: socioantropologichni, socioekonomichni ta sociokulturni vimiri [The philosophy of globalization: the socioanthropological, socioeconomic and sociocultural dimensions]. DIG Publishing.

Voronkova, V., Kapitanenko, N., & Nikitenko, V. (2019). Legal principles of intellectual property protection in the digital society. ScienceRise: Juridical Science, 4(10), 32–37. http://dx.doi.org/10.15587/2523-4153.2019.188163

Author Biographies

Valentyna Voronkova is a Doctor of Philosophy (D.Sc.), Professor, Academician of the Academy of Higher Education of Ukraine, Head of the Department of Management of Organizations and Project Management, Engineering educational and scientific Institute of Zaporizhzhia National University (Zaporizhzhia , Ukraine).

Vitalina Nikitenko is a PhD in Philosophy, Professor of the Department of Management and Administration, Y. M. Potebnya Engineering Education and Scientific Institute of Zaporizhzhia National University (Zaporizhzhia , Ukraine).

Nataliia Kapitaneko is a PhD in Law, Associate Professor of the Department of Management of Organizations and Project Management, Engineering Educational and Scientific Institute of Zaporizhzhia National University (Zaporizhzhia, Ukraine).

Regina Andriukaitiene is a Doctor PhD of social sciences, Head of the Department of Business and Economics, Associate Professor, Marijampole University of Applied Sciences (Marijampole, Lithuania), lecturer of Lithuanian Sports University (Kaunas, Lithuania).

Roman Oleksenko is a Doctor of Philosophy, Professor, Professor of Department of Management of Public Administration, Dmytro Motornyi Tavria state agrotechnological University (Zaporizhzhia , Ukraine).