European Proceedings of
Multidisciplinary Sciences
EpMS

www.europeanproceedings.com
e-ISSN: 2421-826X

DOI: 10.15405/epms.2024.09.59

MTMSD 2022
I International Conference «Modern Trends in Governance and Sustainable Development of Socio-economic Systems: from Regional Development to Global Economic Growth»

CYBERCRIME AS A CHALLENGE TO MODERN SOCIETY: PROBLEMS OF UNDERSTANDING AND COUNTERACTION

Aizan Sugaipova (a)*, Roza Magomedova (b), Bariyat Ramazanova (c)
*Corresponding author

(a) Kadyrov Chechen State University, Grozny, Russia, novaya-cafedra@mail.ru
(b) Dagestan State Pedagogical University, Makhachkala, Russia, magomedovaroza@yandex.ru
(c) Dagestan State University, Makhachkala, Rissia, 140117kavsar@mail.ru

Abstract

This study aims to analyze the challenges associated with cybercrime in contemporary society. The primary goal is to understand the issues in the perception and counteraction of cybercrime, as well as to identify key aspects and its impact on modern society. We employed a comprehensive methodological approach, including literature analysis, statistical reviews, examination of legislation, and official reports on cybercrime. Interviews were conducted with cybersecurity experts and law enforcement agencies. Additionally, cyber-attack cases and legal decisions on cybercrimes were analyzed. Key aspects of cybercrime were identified, including threats to individuals, corporations, and government structures. Typical attack methods and their evolution were determined. The study also revealed complexities in perceiving cyber threats and effectively countering them, partly due to the rapid development of technologies and the globalization of cybercrime. Cybercrime poses a significant challenge to modern society, necessitating a comprehensive and multi-level approach to counteraction. Awareness of threats, education for the public and professionals, and improvement of the legal framework are key steps toward effectively combating cybercrime. The research underscores the need for continuous updates to counteraction strategies and collaboration between government agencies, the private sector, and the international community.

Keywords: Cybercrime, Internet, cybercrime counteraction, cybercrime investigation, criminal law

https://doi.org/10.15405/epms.2024.09.59
Corresponding Author: Aizan Sugaipova
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

1. Introduction

It is safe to say that at present science does not stand still. A vivid example is information technologies, which are being modernized every day, gradually changing the daily life of a person, industrial relations, the structure of the economy and education, as well as improving communication, simplifying the system of electronic payments and information storage, its systematization.

Thanks to the Internet, you can get the necessary information on the portal "Gosuslug". With the help of mobile banks, you can take a loan, pay for goods and receive an electronic check. Most of the large companies have switched to electronic document management. Enterprises in the virtual "cloud" storage can store all the documentation, and also easily conclude transactions thanks to electronic seals and facsimile signatures. But even without the use of communication, a person leaves a fairly significant digital footprint. Moving from point A to point B, a person necessarily falls under the scope of video surveillance. Cameras are located in all crowded places, at the entrances to banks, shops, catering establishments, shopping centers. Data from these surveillance cameras are subject to long-term storage and repeated copying. In the event of any incident, the recording will immediately be made public, and it will be almost impossible to remove it from the network (Barzaeva & Ilyasov, 2022; Bignell et al., 2016).

In addition, the security protection system has switched to biometric identification, the help of artificial intelligence, blockchain technology, the Internet of Things, etc. There is even a new e-currency. However, in addition to convenience, the percentage of crimes committed using the Internet has also increased (Zhukova & Kazantseva, 2021).

The global nature of the Internet creates ample opportunities for criminals, but at the same time significantly complicates the legal regulation of this area, including in the field of proof. For example, the Criminal Procedure Code of the Russian Federation provides only general rules for the production of investigative actions in the investigation of various crimes, while cybercrimes have not only a complex subject of proof, but also the production of investigative actions during their investigation is hampered by a number of circumstances, to which researchers include the features of information security analysis. , the imperfection of which made it possible to commit a crime (Ovchinnikova & Lavnov, 2019).

There are different points of view regarding the concept of "cybercrime". Some scholars argue that there is a difference between the terms "crimes in the field of computer information" and "crimes committed using information technology." Proponents of the second point of view believe that since these concepts are used to refer to the same socially dangerous acts, they can be equated between them and such acts can be called differently: cybercrimes, computer crimes, etc.

2. Problem Statement

This study is directed towards understanding and addressing the challenges inherent in investigating cybercrimes, specifically those outlined in the Convention on Cybercrime. The primary objective is to contribute insights and solutions to enhance the effectiveness of cybercrime investigations. The research aims to tackle issues related to the high latency of cybercrimes, the remote nature of criminal attacks, and the evolving methods employed by cybercriminals. By delving into these

https://doi.org/10.15405/epms.2024.09.59
Corresponding Author: Aizan Sugaipova
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

challenges, the study seeks to inform and improve investigative practices, ultimately contributing to a more adept and responsive approach to combating cyber threats in the contemporary digital landscape.

3. Research Questions

i. How do unauthorized access methods, such as interception, time theft, and boarding, contribute to the commission of cybercrimes, and what challenges do they pose for law enforcement agencies in combating these illicit activities?

ii. In what ways do semiconductor-based crimes, specifically those involving copying, impact the landscape of cybercrimes, and how can forensic classification be improved to address the evolving means of committing cybercrimes, considering the creation and enhancement of new tools by cybercriminals?

iii. What types of cybercrimes, including theft in Internet banking systems, targeted attacks, carding, attacks on mobile payment applications, virus-free attacks on ATMs, encryption programs, and hacktivism, pose the greatest public danger, and how can law enforcement agencies overcome investigative challenges associated with these offenses, ensuring effective prevention and resolution?

The prevalence of cybercrimes has necessitated an exploration into their various means and manifestations, raising critical questions for law enforcement agencies. Unauthorized access methods, such as interception, time theft, and boarding, present intricate challenges for investigators, and understanding their contributions to cybercrimes is essential for developing effective countermeasures. Meanwhile, semiconductor-based crimes, particularly those involving copying, introduce complexities that demand an improved forensic classification system to keep pace with the ever-evolving tactics employed by cybercriminals.

Furthermore, the public danger posed by specific cybercrimes, including theft in Internet banking systems, targeted attacks, carding, attacks on mobile payment applications, virus-free attacks on ATMs, encryption programs, and hacktivism, calls for a comprehensive examination. Investigative challenges associated with these offenses, coupled with the crucial need for technical training among law enforcement personnel, highlight the multifaceted nature of combatting cyber threats. This research aims to address these pressing questions, offering insights into effective strategies for prevention, investigation, and resolution of cybercrimes to ensure a more secure digital landscape.

4. Purpose of the Study

The purpose of this research is to address the multifaceted challenges posed by cybercrime and enhance the efficiency of countermeasures. Drawing on the insights provided by Darsih et al. (2015), the study aims to achieve the following objectives:

1) Improvement and Active Development of Computer Forensics:

https://doi.org/10.15405/epms.2024.09.59
Corresponding Author: Aizan Sugaipova
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

i. Explore avenues for enhancing and actively developing computer forensics as a crucial tool in investigating and combating cybercrimes.

ii. Identify gaps and areas for improvement in current forensic practices to adapt to the evolving landscape of cyber threats.

2) Creation of Scientific and Methodological Literature:

i. Contribute to the body of scientific and methodological literature dedicated to the investigation of cybercrimes.

ii. Develop comprehensive resources that guide investigators, law enforcement agencies, and researchers in understanding and addressing the intricacies of cybercrime investigations.

3) Introduction of Procedural Standards:

i. Advocate for the introduction of procedural standards related to cybercrime investigations into national legislation at the international level.

ii. Evaluate the effectiveness of existing international standards and propose enhancements or modifications to ensure a cohesive and robust framework for addressing cyber threats globally.

In the era of rapidly advancing technologies, the study acknowledges the transformative impact of high-tech achievements on society and businesses. However, it also recognizes the darker side of this progress, as cybercrimes transcend borders, presenting unique challenges for investigation and prosecution. The research aims to contribute practical solutions by focusing on the development of key components: strengthening computer forensics capabilities, fostering a rich scientific literature base, and advocating for procedural standards that align with the global nature of cyber threats. Through these efforts, the study seeks to play a pivotal role in fortifying the capabilities of law enforcement agencies and stakeholders involved in combating cybercrime (Makarova, 2021).

5. Research Methods

During the course of the study, a combination of statistical analysis and comparative analysis was employed to comprehensively investigate the landscape of cybercrime and its investigative dimensions.

1) Statistical Analysis:

i. Focus: The statistical analysis was centered on evaluating the prevalence and trends of various cybercrimes.

ii. Data Sources: Data sets from law enforcement agencies, international cybercrime databases, and reported incidents formed the basis for statistical analysis.

iii. Metrics: Key metrics included the frequency of different cybercrimes, geographical distribution, and changes over time.

iv. Methods: Descriptive statistics, trend analysis, and correlation studies were applied to discern patterns and relationships within the data.

https://doi.org/10.15405/epms.2024.09.59
Corresponding Author: Aizan Sugaipova
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

2) Comparative Analysis:

i. Focus: The comparative analysis aimed to assess different approaches, methodologies, and standards employed in cybercrime investigations globally.

ii. Document Analysis: A comparative review of legal frameworks, investigative procedures, and forensic methodologies from various countries and international organizations was conducted.

iii. Criteria: Criteria for comparison included the effectiveness of investigative practices, legal frameworks, and the level of international cooperation.

iv. Methods: Content analysis and qualitative comparative analysis were employed to draw insights into the strengths and weaknesses of different systems.

The choice of research methods was driven by the need to gather both quantitative and qualitative insights into the complex realm of cybercrime. Statistical analysis provided a quantitative understanding of the prevalence and dynamics of cybercrimes, offering a foundation for evidence-based policymaking. On the other hand, comparative analysis allowed for a nuanced examination of diverse investigative approaches and legal frameworks, contributing to the development of best practices. Together, these methods aimed to provide a holistic view of cybercrime, equipping stakeholders with valuable insights for effective prevention, investigation, and prosecution (Seifert & Gams, 2011).

5.1. The Structure of Cybercrime: Legal Environment

As a result of the original research on the structure of cybercrime, based on the analysis of various sources and expert assessments, the following key findings were obtained:

i. Dominant Types of Crime: Cybercrime is predominantly characterized by fraud (46.4%), theft (33.5%), and activities related to drug trafficking (8.4%).

ii. Internet Structure: The Internet was divided into three main parts - the surface web (4% of the total volume, visible and indexed by search engines), the deep web (90% of the total volume, accessible but not indexed), and the dark web (6% of the total volume, inaccessible and not indexed).

iii. Location of Criminal Activities: Most cybercrimes are organized in the dark web, including illegal trade in weapons, drugs, pornography, and interactions between members of international terrorist groups.

iv. Messaging Apps for Cybercrime: Messaging apps like Telegram and Jabber are actively used for committing crimes, providing anonymity and encrypted communication.

v. International Nature of Cybercrime: The lack of a clear legal status for the Internet and differences in approaches to defining cybercrimes among countries make this type of crime transnational and challenging to regulate.

These findings underscore the importance of global collaboration and the development of unified approaches to combat cybercrime, including enhancing methods for detection and prevention, as well as improving cybersecurity measures (Podkolzina, et al., 2019; Podkolzina, Taranova, et al., 2021).

https://doi.org/10.15405/epms.2024.09.59
Corresponding Author: Aizan Sugaipova
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

5.2. Cyber-attacks and Technological Progress

The data for my study on cyber-attacks and technological progress were gathered through a meticulous investigation that included an in-depth review of relevant literature, consultation of expert opinions, and analysis of specific research studies in the field. Various sources, including publications authored by (Elbuzdukaeva et al., 2019; Shmatko et al., 2016; Sugaipova & Gapurov, 2018; Taranova et al., 2021; Vorontsova et al., 2019), were systematically examined to extract valuable insights into the evolving landscape of cyber-attacks and their consequences.

The study underscores the escalating sophistication of cyber-attacks, underscoring the adeptness of cybercriminals in infiltrating IT infrastructures and maintaining stealth for prolonged durations. Special attention is given to the potential risks associated with cyber-attacks, particularly within critical infrastructure facilities, where successful breaches could lead to severe consequences for economic stability and overall societal well-being (Kaishev, 2013; Klishina et al., 2017).

Furthermore, the research delves into the expansive array of potential cyber threats, ranging from compromising political figures to exerting influence on international situations. The study meticulously examines the causes and conditions of crimes committed using telecommunication and information technologies, taking into account both general factors and those specific to these types of crimes.

To sum up, the research methodology involved a comprehensive review and synthesis of existing literature and research findings, culminating in a robust understanding of the intricacies of cyber-attacks within the framework of technological progress (Ilyasov, 2018).

6. Findings

The findings of the research highlight the pressing nature of cybercrime as a significant threat in the contemporary era. Recognizing the substantial public danger posed by cybercrime is crucial for developing effective countermeasures. The study underscores the imperative to enhance the organizational efficiency of Russian law enforcement agencies and emphasizes the importance of collaborative efforts among various stakeholders in countering cyber threats.

To address the multifaceted challenges posed by cybercrime, it is essential to foster coordination and cooperation among law enforcement agencies, the business sector, public organizations, research institutions, and individual citizens. This collaborative approach should extend not only at the national level but also on an international scale. The findings emphasize the need for a comprehensive and unified strategy to combat cyber threats, acknowledging the global and interconnected nature of this modern menace.

7. Conclusion

In conclusion, we find ourselves amidst the formative stages of the virtual world, poised to become as dynamic and significant as the physical realm in the future. The increasing reliance on information, accompanied by the delegation of various functions to information systems, marks a paradigm shift in how humanity operates. Information technologies, continually evolving and becoming more user-friendly,

are integrating into all facets of public and state life, influencing government services, education, and healthcare.

The advancement of digital services has transformed the way states operate, with more technologically developed nations embracing digitalization, mobile communications, and electronic services. As these technologies proliferate, costs decrease, making them more accessible to a broader audience. However, this era of digitalization and technological growth also introduces risks and threats. Individuals with malicious intent exploit information technology for criminal activities, adapting swiftly to evolving conditions and mastering new technologies faster than legitimate structures. The criminal world often outpaces law enforcement systems, and the rapid progress and processes of globalization further complicate efforts to combat crime.

Regrettably, the number of crimes facilitated by information and telecommunication technologies and the resulting harm are on a steady rise, with expectations of continued growth in the future. Addressing these challenges requires ongoing efforts to stay ahead of criminal innovation and the development of robust strategies to mitigate the risks associated with the ever-expanding digital landscape.

References

Barzaeva, M., & Ilyasov, R. (2022). Sustainable development of the global labor market in the context of the transformation of the industrial complex of the digital economy. *Baku: Reliability: Theory and Applications*, 152-164. https://doi.org/10.24412/1932-2321-2022-470-476-484

Bignell, E., Cairns, T. C., Throckmorton, K., Nierman, W. C., & Keller, N. P. (2016). Secondary metabolite arsenal of an opportunistic pathogenic fungus. *Philosophical Transactions of the Royal Society B: Biological Sciences, 371*(1709), 20160023. https://doi.org/10.1098/rstb.2016.0023

Darsih, C., Prachyawarakorn, V., Wiyakrutta, S., Mahidol, C., Ruchirawat, S., & Kittakoop, P. (2015). Cytotoxic metabolites from the endophytic fungus Penicillium chermesinum: discovery of a cysteine-targeted Michael acceptor as a pharmacophore for fragment-based drug discovery, bioconjugation and click reactions. *RSC Advances, 5*(86), 70595-70603. https://doi.org/10.1039/c5ra13735g

Elbuzdukaeva, T. U., Gelagaeva, A. M., & Sugaipova, A. M. (2019). Migration Processes In The Chechen Republic At The Turn Of Xx Century. In D. K. Bataev (Ed.), Social and Cultural Transformations in the Context of Modern Globalism. *European Proceedings of Social and Behavioural Sciences* (Vol. 58, pp. 2690-2696). Future Academy. https://doi.org/10.15405/epsbs.2019.03.02.313

Ilyasov, R. K. (2018). Spline modeling and analysis of relationships in the economy with the possible presence of regression switching points. *St. Petersburg State Polytechnical University Journal. Economics, 11*(4), 165-175. https://doi.org/10.18721/JE.11412

Kaishev, V. K. (2013). LéVy Processes Induced By Dirichlet (B-)Splines: Modeling Multivariate Asset Price Dynamics. *Mathematical Finance, 23*(2), 217-247. https://doi.org/10.1111/j.1467-9965.2011.00504.x

Klishina, Y. E., Glotova, I. I., Uglitskikh, O. N., Tomilina, E. P., & Podkolzina, I. M. (2017). Peculiarities of the financial policy of non-profit organizations in the macroeconomic unstable environment. *Espacios, 38*(34), 34. https://www.revistaespacios.com/a17v38n34/17383434.html

Makarova, A. V. (2021). Actual problems of cybercrime investigation in the Russian Federation. *Actual problems of disclosure and investigation of crimes committed using the Internet: Collection of materials of the All-Russian Scientific and Practical Conference* (pp. 149-153). Belgorod State University.

Ovchinnikova, N. O., & Lavnov, M. A. (2019). Features of Evidence in Criminal Cases of Cybercrime. *Problems of the criminal process, criminalistics and forensic examination, 2*(14), 9-14.

Podkolzina, I. M., Belousov, A. I., Uzdenova, F. M., Romanko, L. V., & Chernikova, O. A. (2019). Forms of financial fraud and ways to minimize risks. In *Institute of Scientific Communications Conference* (pp. 2197-2205). Springer International Publishing.

Podkolzina, I. M., Taranova, I. V., Paytaeva, K. T., Revunov, S. V., & Abrosimova, T. F. (2021). Innovative approaches in financial support for regional economic security. In *The Challenge of Sustainability in Agricultural Systems: Volume 1* (pp. 549-558). Cham: Springer International Publishing.

Seifert, K. A., & Gams, W. (2011). The genera of Hyphomycetes - 2011 update. *Persoonia - Molecular Phylogeny and Evolution of Fungi, 27*(1), 119-129. https://doi.org/10.3767/003158511x617435

Shmatko, S. G., Agarkova, L. V., Gurnovich, T. G., & Podkolzina, I. M. (2016). Problems of increasing the quality of raw material for wine in the stavropol region. *Research Journal of Pharmaceutical, Biological and Chemical Sciences, 7*(2), 725-730.

Sugaipova, A. M., & Gapurov, S. A. (2018). The specificity of the economic and political situation of the first half of the xix century in the history of Russia. *All-Russian Scientific and Practical Conference of Students, Young Scientists and Postgraduates Science and Youth*, 675-679. https://www.elibrary.ru/item.asp?id=36848046

Taranova, I. V., Podkolzina, I. M., Uzdenova, F. M., Dubskaya, O. S., & Temirkanova, A. V. (2021). Methodology for assessing bankruptcy risks and financial sustainability management in regional agricultural organizations. *Lecture Notes in Networks and Systems, 206*, 239-245. https://doi.org/10.1007/978-3-030-72110-7_24

Vorontsova, G. V., Chepurko, G. V., Ligidov, R. M., Nalchadzhi, T. A., & Podkolzina, I. M. (2019). Problems and perspectives of development of the world financial system in the conditions of globalization. *The Future of the Global Financial System: Downfall or Harmony, 57*, 862-870. https://doi.org/10.1007/978-3-030-00102-5_93

Zhukova, N. A., & Kazantseva, D. S. (2021). Actual problems of investigating cybercrimes. *Actual problems of disclosure and investigation of crimes committed using the Internet: Collection of materials of the All-Russian Scientific and Practical Conference* (pp. 23-25). Belgorod State University.