JOURNAL OF INTELLECTUAL PROPERTY AND HUMAN RIGHTS

Volume: 4 Issue: 1 | Jan–2025 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

Investigation and Prevention of Cybercrime

Davronov Atobek Ravshanovich, PhD
A professor at the Department of Criminal Procedural Law at Tashkent State University of Law

Annotation: The article provides a comprehensive analysis of the transformation of criminal activities in the context of the rapid development of information technologies and the digitalization of society. Special attention is given to studying new forms and methods of committing crimes using modern digital tools. The authors thoroughly examine the pressing issue of integrating advanced information technologies into law enforcement activities to enhance the effectiveness of crime detection and investigation.

Key words: Economy, personal data, criminology, investigations, personal data, digital information, cybercrime.

In the context of the rapid development of the digital economy in recent years, extensive and multifaceted activities are being carried out to ensure the comprehensive security of participants in criminal proceedings.

This process encompasses a wide range of measures, including the development of secure platforms, the implementation of advanced authentication systems, and the creation of robust mechanisms for protecting personal data.

Parallel to the development of protective mechanisms, there is an acute need to improve methods for identifying and investigating cybercrimes in the Republic of Uzbekistan.

Modern realities necessitate the creation and implementation of innovative digital tools and methodologies tailored to the specifics of crimes in the information space. The establishment of effective protocols for handling digital evidence, including its collection, storage, analysis, and presentation in court, has become particularly significant.

The successful counteraction of cybercrime is also closely tied to the development of the human resources potential of law enforcement agencies.

This includes the creation of specialized educational programs aimed at training experts in digital forensics who can effectively apply modern technologies in combating crime.

In accordance with Presidential Decree No. PP-229, "On Measures to Organize Scientific Research Activities in the Field of Digital Forensics," dated June 21, 2024, the Research Institute of Digital Forensics was established. According to this Decree, additional tasks have been assigned to the Law Enforcement Academy, including:

Conducting innovative research in the field of digital forensics, analyzing, and applying big data ("Big Data"), artificial intelligence, and other advanced technologies in practice;

Providing practical assistance to law enforcement agencies in digital forensics during operational and investigative activities, preliminary inquiries, and investigative actions to identify, seize, store, and analyze digital traces of crimes;

Introducing modern technologies and tools for digital examination;

Volume: 4 Issue: 1 | Jan–2025 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

Implementing advanced technologies and methods for searching, collecting, and analyzing digital data, as well as detecting crimes committed using crypto-assets, "cloud technologies," and other methods within criminal investigations;

Participating in the development of international scientific and technical cooperation and implementing scientific, technical, and innovative projects in combating cybercrime in collaboration with foreign partners;

Preparing qualified personnel with knowledge and skills in combating cybercrime and using modern technologies;

Developing and improving methods for conducting forensic examinations in digital forensics;

Identifying existing problems in the practice of solving and investigating crimes committed using digital technologies and developing proposals for their resolution.

This comprehensive approach highlights the commitment to strengthening digital forensic capabilities and enhancing the effectiveness of combating cybercrime in Uzbekistan.[1]

Special attention should be given to developing an interdisciplinary approach that combines the achievements of information technology, forensic science, law, and related fields.

Such integration will enable the creation of an effective system to counter modern digital threats and ensure the reliable protection of the interests of citizens and organizations in the digital space.

Building a comprehensive security system in the digital environment requires coordinated efforts from the government, law enforcement agencies, the scientific community, and businesses.

These efforts must focus on creating effective mechanisms for the prevention, detection, and investigation of crimes in the field of information and communication technologies.

According to M.V. Saveliev, the widespread use of modern technical means and global informatization has led to a shift from traditional forms of crime—such as theft, robbery, murder, and fraud—to qualitatively different types of crime. This shift is reflected in changes in the structure of recorded offenses.

Currently, a significant number of crimes that were previously committed "traditionally" are now carried out remotely. Today, law enforcement officers are no longer surprised by cases of theft, fraud, drug trafficking, or lewd acts against minors committed remotely through the global network.

These trends highlight the urgent need for innovative strategies and tools to address the challenges posed by cybercrime and protect society in the evolving digital landscape.[2]

The emerging trend of crime transformation raises questions about the digital solutions that the law enforcement system can employ to counter modern criminal activities.

The example provided highlights the outdated nature of the existing methodology for investigating remote crimes. In practice, law enforcement agencies have proven ill-prepared to counteract crimes in the field of information technologies, particularly due to their extraterritorial nature. This shortcoming is largely due to the continued reliance on traditional contact methods for collecting and documenting information.

[1] Постановление Президента Республики Узбекистан «О мерах по организации научно-исследовательской деятельности в сфере цифровой криминалистики» № ПП-229 от 21.06.2024 г.
[2] Савельева М.В. Технологизация криминалистики / М.В. Савельева, А.Б. Смушкин // Вестник Саратовской государственной юридической академии. - 2017. - № 5 (118). - С. 254-257.

Volume: 4 Issue: 1 | Jan–2025 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

In the first 11 months of 2023, approximately 5,500 cybercrimes were recorded in Uzbekistan, 70% of which were related to fraud and theft from bank cards.

These statistics emphasize the urgent need for modernizing investigative practices and integrating advanced digital tools to effectively combat cybercrimes. Developing specialized skills and leveraging innovative technologies will be crucial to addressing the challenges posed by crimes in the digital space.[3] This report highlights the outdated methods of investigating cybercrimes and underscores the urgent need for new approaches to handle these types of offenses.

It is important to recall a crime from a decade ago, when the Target data breach became one of the largest in history. Target was forced to pay $18.5 million in compensation after hackers stole 40 million credit and debit card records. Like many unprecedented security breaches, the Target data leak came with both warnings and lessons that remain relevant today.

During the Target breach, cybercriminals managed to steal 40 million credit and debit card records as well as 70 million customer records. This occurred during the 2013 holiday season. Although it was not the largest security breach in history, it was among the most significant. Given the backdrop of numerous other high-profile data breaches, customers were particularly wary.

The Target data breach highlights a critical issue that arises after such incidents.

It is not merely about the security breach itself or the settlement costs; the real challenge lies in the loss of customer trust. Customers no longer felt secure, and this erosion of confidence had far-reaching implications for the company’s reputation and operations.

This case underscores the pressing need for innovative methods and tools in cybercrime investigation, emphasizing the importance of staying ahead of evolving threats to maintain public trust and security in the digital age.[4]

Following the data breach, customers were concerned that their information might be leaked, leading to hesitation in purchasing from Target.

Similar incidents have occurred with other high-profile data breach victims, such as Sony PlayStation. Like many breaches, the attack targeted Target but did not go directly through its systems. Instead, the breach began with a third-party vendor. Third parties are often compromised because they typically lack robust security measures.

Another notable case occurred three years ago, in May 2021, when the Colonial Pipeline became the victim of a ransom ware attack.

The ransomware infected some of the pipeline's digital systems, shutting it down for several days. The shutdown affected consumers and airlines along the East Coast of the United States. The breach was deemed a national security threat, as the pipeline transports oil from refineries to industrial markets. This led President Joe Biden to declare a state of emergency.

The attack began when a hacker group identified as DarkSide gained access to Colonial Pipeline's network. The attackers stole 100 gigabytes of data within two hours. After stealing the data, they infected Colonial Pipeline's IT network with ransom ware, which affected numerous computer systems, including billing and accounting.

These cases underscore the critical need for enhanced security protocols, particularly when dealing with third-party vendors and critical infrastructure. They also highlight the growing sophistication of

[3] Мирзиёев Шавкат Миромонович «Кардинг в Узбекистане составил 70% киберпреступлений» https://www.spot.uz/ru/2023/12/21/cyber-security/ последний вход 17.10.2024г.
[4] «Картоха» с русскими корнями. https://www.gazeta.ru/tech/2014/01/17_a_5854701.shtml.

Volume: 4 Issue: 1 | Jan–2025 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

cybercriminals and the far-reaching consequences of ransomware attacks, from financial losses to national security risks. Addressing these challenges requires robust cybersecurity frameworks, continuous monitoring, and proactive measures to prevent such incidents.[5]

Colonial Pipeline shut down its pipeline to prevent the ransomware from spreading further.

To investigate the attack, the company enlisted the cybersecurity firm Mandiant. Additionally, the FBI, the Cybersecurity and Infrastructure Security Agency (CISA), the U.S. Department of Energy, and the Department of Homeland Security were notified of the incident.

Colonial Pipeline paid the DarkSide hackers to obtain a decryption key, allowing the company's IT personnel to regain control of their systems.

In Uzbekistan, the scale of cyberattacks has also been alarming.

In 2023, over 11.02 million cyberattacks were targeted at web resources in the country. Analyzing the geographic origins of these attacks, the majority were launched from IP addresses in the Netherlands (759,500), the United States (696,600), Russia (100,000), Germany (58,000), India (53,000), and China (51,000).

This ongoing "war" against hackers in Uzbekistan has been waged for several years.

These figures emphasize the persistent nature of cyber threats and the urgent need to bolster cybersecurity measures. The lessons learned from global incidents like the Colonial Pipeline ransomware attack demonstrate the importance of proactive defenses, incident response planning, and international cooperation to counteract such threats effectively.[6]

Many researchers have explored issues related to the necessity of implementing remote practices in crime detection and investigation.

The possibilities of conducting various investigative actions remotely have been analyzed extensively. For instance, P.G. Smagin, as an argument in favor of such methodologies, cites the positive experience of remote investigative actions practiced by investigative agencies in foreign countries.

This perspective highlights the potential benefits of integrating remote technologies into investigative procedures, including enhanced efficiency, reduced time and resource consumption, and increased accessibility to critical information across jurisdictions. Adopting these methodologies could significantly improve the effectiveness of law enforcement operations, especially in addressing cybercrimes and other offenses involving digital technologies.[7] E.G. Kravets emphasizes that the use of information and communication technologies in conducting investigative actions requires specialized facilities equipped for remote sessions.

The connection to a remote location and the implementation of technical measures are carried out by personnel from information support units who have undergone specialized training in organizing videoconferencing sessions.

This approach underlines the importance of technical preparedness and specialized training for law enforcement personnel to ensure the effective and secure use of remote technologies during

[5] Темные хроники: к чему привела атака на Colonial Pipeline. https://ics-cert.kaspersky.ru/publications/reports/2021/05/21/darkchronicles-the-consequences-of-the-colonial-pipeline-attack/. Дата обращения: 14.11.2024г.

[6] "O'zbekiston Respublikasi kiberxavfsizligi - 2023 yil hisoboti" https://csec.uz/uz/news/maqolalar/o-zbekiston-respublikasi-kiberxavfsizligi-2023-yil-hisoboti/.

[7] Смагин П.Г. К вопросу о возможности дистанционного производства следственных действий / П.Г. Смагин // Уголовно-процессуальные и криминалистические проблемы борьбы с преступностью : Всероссийская науч. -практ. конф., Орел, 29 мая 2015 г. - Орел, 2015. - С. 309-314.

Volume: 4 Issue: 1 | Jan–2025 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

investigative procedures. Properly equipped facilities and skilled staff can significantly enhance the quality and efficiency of remote investigative actions, while also maintaining the integrity and admissibility of collected evidence.[8]

Comprehensive analysis of existing issues allows us to formulate several key areas that require priority attention and development in our country.

1. Technological Development of Cybercrime Investigation Systems

The technological advancement of cybercrime investigation systems is of paramount importance. Active implementation of modern technologies, such as artificial intelligence (AI) and machine learning (ML), is necessary to automate the analysis of digital traces and identify hidden links between various cyber incidents. Developing and introducing specialized software tailored to the specific tasks of digital forensics is crucial. Establishing unified cybercrime databases will enable more effective trend analysis and detection in this field.

2. Human Resource Development

Particular attention should be paid to staffing the departments within each governmental structure. This includes creating a comprehensive system for training specialists, combining foundational education with regular advanced training. Internship programs in leading international cybersecurity centers are essential to adopt best practices and modern investigation methodologies for emerging crimes.

3. Organizational Measures

Organizational efforts should focus on establishing specialized cybercrime units in each administrative region of the country. Ensuring clear coordination between various law enforcement agencies and creating mechanisms for the rapid exchange of information is critical. Forming interagency working groups will help consolidate efforts across different organizations in combating cybercrime.

4. International Cooperation

Given the cross-border nature of cybercrime, international cooperation is vital. Mechanisms for real-time information sharing between law enforcement agencies across countries must be developed. Establishing international investigative teams and standardizing approaches to the collection and analysis of digital evidence are key. Joint exercises and training programs will enhance the effectiveness of international collaboration.

5. Legal and Regulatory Framework

The legal framework must be continually updated to address emerging types of cybercrime and investigative technologies. Clear standards for handling digital evidence and procedures for presenting it in court need to be developed. Harmonizing national legislation with international norms in the fight against cybercrime is also essential.

6. Scientific and Methodological Support

Scientific support for cybercrime investigations should include the development of new methods and algorithms for analyzing digital traces, creating standard methodological guidelines for investigators, and forming knowledge bases on various types of cybercrime. Expanding research in digital forensics and rapidly implementing their results into practice is critical.

[8] Кравец Е.Г. Дистанционные следственные действия сквозь призму применения специальных знаний / Е.Г. Кравец, Н.В. Шувалов // Юридическая наука и правоохранительная практика. - 2017. - № 1 (39). - С. 140-144.

Volume: 4 Issue: 1 | Jan–2025 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

7. Material and Technical Support

Cybercrime units require constant upgrades and modernization of their resources. This includes equipping them with state-of-the-art digital forensic tools, establishing specialized laboratories, and providing mobile units for on-site investigations. Special focus should be given to developing infrastructure for securely storing digital evidence.

8. Collaboration with the Private Sector

Collaboration with private entities is an integral part of effectively combating cybercrime. Mechanisms for public-private partnerships should be established, involving IT experts in investigating complex cybercrimes, organizing joint exercises, and sharing information about current threats and vulnerabilities.

9. Preventive Measures

Preventive measures should include the development of early warning systems for cyber threats, conducting awareness campaigns, and educating the population on cybersecurity measures. An effective incident response system should be created, ensuring coordination among all stakeholders.

10. Analytical Work and Risk Assessment

Analytical efforts must include the adoption of modern data analysis methods, the development of predictive models, and the creation of risk assessment systems. Continuously analyzing trends in cybercrime and adapting investigative methods to new threats are crucial for staying ahead of cybercriminals.

Conclusion

Implementing these proposed measures will significantly enhance the effectiveness of cybercrime investigations and enable an adequate response to contemporary challenges in information security. A comprehensive approach to adopting these measures, with constant adaptation to changing conditions and emerging cyber threats, is essential to ensuring long-term success.

References

1. Мирзиёев Шавкат Миромонович «Кардинг в Узбекистане составил 70% киберпреступлений» https://www.spot.uz/ru/2023/12/21/cyber-security/ последний вход 17.10.2024г.
2. Постановление Президента Республики Узбекистан «О мерах по организации научно-исследовательской деятельности в сфере цифровой криминалистики» № ПП-229 от 21.06.2024 г.
3. Савельева М.В. Технологизация криминалистики / М.В. Савельева, А.Б. Смушкин // Вестник Саратовской государственной юридической академии. - 2017. - № 5 (118). - С. 254-257.
4. «Картоха» с русскими корнями. https://www.gazeta.ru/tech/2014/01/17_a_5854701.shtml.
5. Темные хроники: к чему привела атака на Colonial Pipeline. https://ics-cert.kaspersky.ru/publications/reports/2021/05/21/darkchronicles-the-consequences-of-the-colonial-pipeline-attack/. Дата обращения: 14.11.2024г.
6. "O'zbekiston Respublikasi kiberxavfsizligi - 2023 yil hisoboti" https://csec.uz/uz/news/maqolalar/o-zbekiston-respublikasi-kiberxavfsizligi-2023-yil-hisoboti/.
7. Смагин П.Г. К вопросу о возможности дистанционного производства следственных действий / П.Г. Смагин // Уголовно-процессуальные и криминалистические проблемы

Volume: 4 Issue: 1 | Jan–2025 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

борьбы с преступностью : Всероссийская науч. -практ. конф., Орел, 29 мая 2015 г. - Орел, 2015. - С. 309-314.

8. Кравец Е.Г. Дистанционные следственные действия сквозь призму применения специальных знаний / Е.Г. Кравец, Н.В. Шувалов // Юридическая наука и правоохранительная практика. - 2017. - № 1 (39). - С. 140-144.