EURASIAN JOURNAL OF ACADEMIC RESEARCH
Innovative Academy Research Support Center
UIF = 8.1 | SJIF = 7.899
www.in-academy.uz

CRIMINOLOGICAL ASPECTS OF PERSONAL INFORMATION SECURITY

Iskandarov K.I.
Ministry of Internal Affairs of the Republic of Uzbekistan,
Researcher

https://doi.org/10.5281/zenodo.11001142

ARTICLE INFO
Received: 13th April 2024
Accepted: 19th April 2024
Online: 20th April 2024

KEYWORDS
Security, identity, cybercrime, personal data, privacy, threat to national security.

ABSTRACT
The paper examines the impact of widespread cybercrime, among which a special type is crimes that infringe on personal information security. These types of cybercrimes carry a number of risks and threats that violate personal rights and freedom, destabilize the situation in the country, cause reputational damage, affect the course of elections, etc. The paper provides a comprehensive analysis of the problems associated with ensuring personal information security. In the course of the research, methods of cognition, analysis, synthesis, logic, comparative legal analysis, observation, generalization, system analysis and forecasting were widely used.

With the development of the Internet and information technology, criminals are finding new ways to commit crimes. Cybercrime, such as cyber fraud, cyber espionage and cyberterrorism, is becoming more common. Digital technologies also facilitate communication and coordination between members of criminal groups. In 2022 and 2023, cybercrimes on an astounding scale occurred, costing companies and countries billions of dollars.

Personal information security is the state of protection of personal information and data from unauthorized access, modification, destruction or disclosure. It includes measures and practices aimed at ensuring the confidentiality, integrity and accessibility of information that relates to personal life, identification data, financial means, medical records and other personal data. This also includes protection against cyber threats, malicious software, social engineering and other forms of attacks on personal information and privacy. Ensuring personal information security is becoming increasingly important in today's digital world, where personal data becomes the object of valuable digital assets and is often at risk from cybercriminals and intruders.

Criminological aspects play a key role in the context of information security, as they help to understand the nature, motivation and methods of crimes in the field of information technology.

Threat and vulnerability analysis: Criminological analysis makes it possible to identify potential threats and vulnerabilities in the information infrastructure and behavioral patterns of criminals, which helps to develop effective protection strategies.

Criminal profiling: Understanding the profiles of cybercriminals, their motivations, modes of action and goals helps to build more accurate and effective methods of protection against cyber threats.

Studying trends and statistics: The analysis of statistical data on cybercrimes allows us to identify trends, identify the most common types of attacks and their consequences, which in turn allows us to take appropriate protection measures.

Psychological aspects of criminal behavior: Criminological analysis of the psychological mechanisms of criminal behavior helps to understand how criminals can manipulate and mislead people to gain access to personal information and data.

Development of protection strategies and crime prevention: Based on criminological analysis, protection strategies can be developed and improved, as well as training and education to increase awareness of cyber security and prevent crimes.

Cybercrimes pose a serious threat to personal security, as attacks in the digital sphere can cause significant damage to both financial resources and personal privacy. There are several main aspects that link cybercrime and personal security:

– theft of personal information;
– cyber-blackmail and threats;
– cyberbullying and online violence;
– threat to financial security;
– violation of confidentiality and privacy.

Cybercriminals can hack into accounts, steal personal data such as identification numbers, passwords, financial information and medical records, which can lead to identity theft, financial fraud and other forms of abuse.

Attackers use stolen data for blackmail and threats, for example, to demand a ransom in exchange for not posting compromising information on the network.

Cybercriminals often abuse technology for online violence, including intimidation, discrediting, divulging personal secrets, etc., which creates serious psychological and emotional consequences for victims. They can carry out financial fraud, hack into banking systems, steal financial data and carry out fraudulent transactions in the digital space, which leads to loss of funds and financial instability for those affected. After gaining access to sensitive personal information such as medical records, photographs, correspondence, which violates privacy and leads to potential blackmail or other negative consequences.

Given these threats, it is important to take precautions such as using strong passwords, two-factor authentication, regular software updates, and cybersecurity training to protect your personal information and minimize the risks of cybercrime.

In addition to the mentioned types of cybercrimes that threaten personal information security, there are a number of other types of attacks, including:

– phishing: This method of fraud in which attackers impersonate trusted individuals or organizations by sending fake emails or creating fake websites in order to obtain sensitive information such as passwords, credit card numbers etc.

– Social engineering: The process of manipulating people to reveal confidential information or perform certain actions. For example, attackers can call or send emails posing as bank or technical support staff to gain access to personal information.

ransomware: Cybercriminals send malicious software that blocks access to a computer or encrypts data, and then demands a ransom for unlocking it. The user becomes a hostage of his own data, which can lead to serious losses of information and finances.

– Identity theft: Attackers can often use stolen personal data, such as social security numbers or passport numbers, to create false identification documents or commit fraudulent acts on behalf of the victim.

– money fraud: It includes various types of fraud carried out on the network, such as fake lotteries, investment schemes, pyramids, fake online stores and other schemes aimed at deceiving victims to receive funds.

These types of cybercrimes pose a serious threat to personal information security, and appropriate precautions must be taken to protect against them, including training, the use of antivirus software, regular software updates, and careful handling of personal information in an online environment.

Cybercrimes have serious consequences both for individuals and for society as a whole. Cybercriminals can gain access to sensitive personal information, including financial data, medical records, personal correspondence and other sensitive information (loss of personal information and confidentiality). This can lead to the leakage of private information, which can be used for blackmail, fraud or discredit. Attacks on financial institutions, online stores and individuals can lead to financial losses (financial losses:). Cybercriminals can steal money, carry out fraudulent transactions, block access to bank accounts and demand a ransom for data recovery.

As a result of cybercrimes, personal identification information such as social security numbers, passport numbers and other data can be stolen, which can be used to open fake accounts, obtain loans or commit other fraudulent actions on behalf of the victim (identity theft and fraud). Victims may receive psychological and emotional consequences from this. Victims of cybercrime can experience stress, anxiety, shame, and anxiety due to the violation of their privacy, loss of trust, and financial loss. This can lead to depression, social isolation, and other psychological problems.

One of the main threats from cybercrimes is the threat to national security. Cybercrimes can have global consequences, as they can disrupt critical information infrastructure, including energy supply, transportation, communications, and defense systems. This can lead to serious consequences for national security and the economy.

In general, cybercrimes have a wide range of negative consequences for individuals and society, and effectively combating them requires joint efforts on the part of government organizations, the private sector and society as a whole.

Criminological analysis of cybercrimes reveals a number of features that have an impact on personal security:

– anonymity and remoteness;

– global reach and dissemination;

– technical expertise;
– evolution of methods;
– social engineering.

Cybercrimes are often committed anonymously and remotely, which makes it difficult to detect and stop them. This allows criminals to hide behind virtual barriers, increasing the likelihood of successful crimes and reducing the risk of being caught. These crimes can be committed from anywhere in the world and are directed against victims from different countries. This creates difficulties in interdiction and investigation, as criminals can exploit legal, technological and cultural differences to their advantage. Also, cybercriminals usually have a high level of technical expertise, which allows them to create complex malware, bypass security systems and carry out attacks with maximum efficiency. They are constantly improving their methods and tactics, using the latest technologies and tools to circumvent protective measures and cause damage. This means that cybercrime protection must constantly adapt and evolve.

One of the common methods in cybercrime is social engineering, which aims to manipulate people's psychology and behavior in order to gain access to their personal information or systems. This highlights the importance of education and awareness to protect personal safety.

Based on these characteristics, comprehensive measures must be taken to ensure personal security, including the use of strong passwords, regular software updates, cybersecurity training and prudent online behavior. It is also important to cooperate between law enforcement agencies, the private sector and society to combat cybercrime and increase the level of protection.

Psychological aspects play an important role in ensuring personal information security. There are several key points: the increased threat of cybercrime can cause people to feel vulnerable and fear of losing personal information (feeling vulnerable and fear of threats). It can mainly lead to anxiety, anxiety and a decrease in self-esteem; loss of personal information or attempts to hack accounts can cause people to feel a loss of control over their own digital lives (a sense of loss of control); Concerns about data leakage or cybercrime can lead to distrust of the online environment (lack of trust in the online environment). People may become more cautious in using the Internet and social networks, which in some cases may limit their access to information and resources; psychological methods of attack, such as social engineering, are aimed at manipulating people's feelings and behavior (the influence of social engineering and manipulation). This includes deceiving and convincing people to disclose their personal information or perform actions that may put their information security at risk; to ensure personal information security, it is important to learn how to manage stress and anxiety caused by threats of cybercrime (protection from stress and anxiety).

In general, psychological aspects play a significant role in personal information security, and understanding these aspects allows us to develop effective protection strategies, as well as train people to behave consciously and safely in the digital world.

Criminologists list several options for psychological mechanisms of protection against cyber threats that play an important role in ensuring personal information security:

– the development of healthy skepticism;
– cybersecurity training;
– emotion management;
– development of critical thinking skills;
– careful handling of personal information;
– understanding the basics of cybersecurity;
– development of safe online behavior skills;
– ability to analyze information;
– protection of personal information;
– Raising awareness of rights and legislation.

It is important to be critical of unexpected requests for information or offers, especially if they come from unfamiliar or unknown sources. A healthy skepticism will help you avoid falling under the influence of social engineering and phishing attacks.

Raising awareness about various types of cyber threats and methods of preventing them is an effective way to protect against attacks. Regular trainings and training on cybersecurity issues will help to develop skills in recognizing threats and responding to them correctly.

Understanding your emotional reactions to various online situations and the ability to control them will help you avoid rash actions that can lead to compromising information security. Calmness and reasonableness are important when solving problems in the digital world.

Critical thinking skills help analyze information, verify the reliability and authenticity of sources, and make informed decisions. This is important to prevent falling under the influence of manipulation and deception.

Striving to minimize the disclosure of personal information on the Internet and the use of strong passwords, two-factor authentication and other security methods will help reduce the risk of getting online.

These psychological protection mechanisms can help strengthen the information security of an individual and make it less vulnerable to cyber threats.

Education plays a key role in improving personal information literacy and protecting it from cyber threats.

Cybersecurity education helps people understand the main threats and methods of protection in the digital world. They learn to recognize typical cyber threats such as phishing, malware, and social engineering, and take appropriate precautions.

Education helps people learn the skills of safe behavior in an online environment, such as creating and using strong passwords, authenticating websites, regularly updating software, and setting up privacy on social networks.

Education promotes the development of critical thinking and the ability to analyze information coming from various sources. This helps people distinguish between reliable and unreliable sources, filter false information, and make informed decisions in an online environment.

Personal information management education helps people understand which data should be protected, which information habits should be avoided, and how to minimize the risk of being exposed to threats such as identity theft and financial fraud.

Cybersecurity education also includes training on digital rights and legislation. People will learn about their online rights, legitimate ways to protect information, and the consequences of violations of cybersecurity legislation.

In general, education plays an important role in improving an individual's information literacy and helps them become more aware, confident and secure in the digital world.

Based on the above, there are the following challenges and prospects in the field of information security in the future:

The development of cybercrime technologies: with the development of technology, cybercriminals are also becoming more sophisticated and skillful in their attacks. The ability to use artificial intelligence, machine learning and other new technologies creates new threats to information security.

The growth of the volume and complexity of data: every year the volume of data on the Internet is growing. This creates challenges in the field of data processing, storage and protection, especially in the context of compliance with confidentiality and personal data protection requirements.

Global cyberattacks and cyberwarfare: cybersecurity threats are becoming more global and organized. Cyber attacks can be carried out by State actors or cybercrime groups in order to destabilize other countries or organizations.

Lack of qualified cybersecurity specialists: the need for qualified cybersecurity specialists is increasing, but the lack of personnel in this area remains one of the main challenges.

The prospects:

The development of security technologies: The emergence of new technologies and methods of protection, such as blockchain, quantum cryptography and biometric authentication, opens up new prospects for improving information security.

Artificial intelligence and machine learning: The use of artificial intelligence and machine learning allows you to automate the processes of threat detection and analysis, which helps you respond faster to potential attacks.

Global cooperation and information exchange: Strengthening international cooperation in the fight against cybercrime and information exchange between States and organizations can help to more effectively prevent cyber attacks and investigate crimes.

Education development and awareness raising: Strengthening cybersecurity education and awareness in society helps to prepare more aware users who are able to independently protect their information and prevent cyber threats.

In general, despite the challenges, the future in the field of information security presents broad prospects due to the development of new technologies, enhanced cooperation and increased awareness in society.

References:

1. УГОЛОВНО-ПРАВОВАЯ ОХРАНА ИНФОРМАЦИОННОЙ .... (n.d.) получен March 18, 2024, от cyberleninka.ru

2. Уголовно-правовая охрана информационной .... (n.d.) получен March 18, 2024, от www.dissercat.com

3. Уголовно-правовая охрана информационной .... (n.d.) получен March 18, 2024, от cyberleninka.ru

4. Уголовно-правовая охрана официального .... (n.d.) получен March 18, 2024, от ifap.ru/pi/07/sr17.doc

5. Уголовно-правовая охрана электронной информации», ... (n.d.) получен March 18, 2024, от www.dissercat.com

6. Информационная безопасность как объект уголовно .... (n.d.) получен March 18, 2024, от cyberleninka.ru

7. Кража персональных данных. (n.d.) получен March 18, 2024, от searchinform.ru

8. Саъдуллаев, Г. (2022). Обеспечение информационной безопасности органами внутренних дел: требование времени. Современные тенденции развития цифровизации в сфере юстиции, 1(1), 193–197. https://doi.org/10.47689/978-9943-7818-1-8-MTDDFJ-2021-pp193-197

9. Саъдуллаев, Г. (2021). Анализ законодательства республики узбекистан и международного законодательства в области обеспечения информационной безопасности личности. Противодействие правонарушениям в сфере цифровых технологий и вопросы организационно-правового обеспечения информационной безопасности, 1(01), 307–309. извлечено от https://inlibrary.uz/index.php/digital_technology_offenses/article/view/7515

10. Анарбоев И. И. АНАЛИЗ ЗАКОНОДАТЕЛЬСТВ ЗАРУБЕЖНЫХ СТРАН ПО ПРОИЗВОДСТВУ ДЕЛ ОБ АДМИНИСТРАТИВНЫХ ПРАВОНАРУШЕНИЯХ //Development of pedagogical technologies in modern sciences. – 2022. – Т. 1. – №. 6. – С. 23-27.