ІНФОРМАЦІЙНА БЕЗПЕКА ЯК СКЛАДОВА НАЦІОНАЛЬНОЇ БЕЗПЕКИ

УДК 343.37/53
DOI: 10.31733/15-03-2024/2/295-297

Volodymyr KRASNOPOLSKY
Professor of the Department of Ukrainian Studies and Foreign Languages,
Dr of Pedagogucal Sciences, Prof.

Maksym MARCHENKO
Cadet of the SEI of Law and Training Specialists for Criminal Police Units
of Dnipropetrovsk State University
of Internal Affairs

CYBERCRIME INVESTIGATION: NAVIGATING THE DIGITAL FRONTIER

Modern society, intertwined with a vast amount of information and technological innovations, has become a target of systematic cyber attacks and cybercrime. A thorough investigation of these crimes necessitates the adaptation of law enforcement agencies to the digital environment and the utilization of advanced methodologies and technologies. Cybercrime, as a contemporary phenomenon, is characterized by a diverse range of manifestations. This section examines key terms and concepts associated with cybercrime to refine their meanings and understanding. Primarily, «cybercrime» is defined as any criminal activity that utilizes technological means or Internet networks to commit offences. This encompasses a wide spectrum of actions, such as hacking attacks, theft of personal information, and the dissemination of malicious software, among others. Additionally, the classification of cybercrimes, such as phishing, DDoS attacks, ransomware, data abuse, and others, is explored. This expands the comprehension of the diversity of cybercriminal actions and lays the groundwork for further investigation analysis.

Digital investigation in the context of cybercrime emerges as a pivotal element in combating this phenomenon. Defining methodologies and approaches to digital investigation, their development, and enhancement are mandatory steps in implementing effective investigative strategies. Some methodologies and approaches:

Digital Trace Analysis: In the realm of cybercrime, the analysis of digital traces becomes a crucial stage in investigations. For instance, in the case of cyber attacks on corporate networks, digital investigation experts can analyze event logs, network traffic, and virus artefacts to identify attack methods and identify perpetrators.

Electronic Evidence Repository: The application of an electronic evidence repository allows the collection, storage, and analysis of digital data that can serve as evidence in cybercrime cases. An example is the use of hash functions to verify the integrity of data stored in the evidence repository.

It is noteworthy that the effective implementation of these methods requires continuous updating of personnel skills and the improvement of existing technologies, as cybercriminals are constantly evolving their methods. Moreover, digital technologies applied in investigations must account for the rapid and constant changes in cyberspace to be effective and adaptive. Law enforcement agencies must enhance their technical skills and methods to meet the challenges of the digital era. In the context of ongoing technological advancements and increased online interactions, global cybercrime has become more complex and perilous. One of the current threats is the rise in state-sponsored or cyber espionage-initiated cyber attacks. For instance, attacks on critical infrastructure leading to disruptions in energy networks or transportation systems underscore the importance of global cooperation and the protection of critical assets. The growing activity of cybercriminal groups and the use of ransomware pose a serious threat to businesses and

citizens. For example, the REvil group demonstrated high organization and the ability to execute effective attacks, demanding significant ransom amounts in cryptocurrencies [1].

The contemporary law enforcement environment faces a multitude of challenges in combating cybercrime that warrant careful consideration and analysis. The rapid evolution of cybercrime makes it difficult for law enforcement to keep pace with the new techniques and methods employed by cybercriminals. The global nature of cyber attacks underscores the importance of collaboration between countries and organizations to effectively respond to threats. Additionally, cybercriminals utilize technologies to safeguard their anonymity, complicating the task of law enforcement in detecting and apprehending offenders. Measures to enhance anonymity in cryptocurrencies and the use of anonymizers further complicate investigations.

In a modern world where cybercrime is becoming increasingly sophisticated, the use of technological innovations in the field of cyber investigations becomes exceptionally crucial. Artificial intelligence (AI) emerges as a key tool for analyzing large volumes of data and identifying patterns, crucial in the realm of cyber investigations. The application of machine learning algorithms and neural networks allows for the automation of anomaly detection and the identification of potential threats. The National Police Agency of Japan has implemented an artificial intelligence system for analyzing large volumes of cyber-related data [2]. The system automatically detects discrepancies and anomalies, streamlining the work of investigators and aiding in timely responses to cyber threats.

Blockchain technologies prove to be highly effective tools in enhancing the security and integrity of electronic evidence repositories. Blockchain systems provide a reliable registration of events and enable the creation of traces that cannot be altered or deleted. Airbus Corporation utilizes blockchain for protection against cyber attacks [3]. Each access to digital data is recorded in the blockchain, allowing for the timely detection of breaches and prevention of unauthorized access. The development of quantum computing promises to fundamentally change the paradigm of cyber investigations. Quantum computers can quickly solve tasks that are too complex for classical computers, thereby increasing the efficiency of investigations. As part of the Sycamore project, Google uses quantum computing to create algorithms aimed at solving cybersecurity challenges [4]. This opens up new possibilities for rapid analysis of cryptographic algorithms and the detection of vulnerabilities.

Considering global trends and technological innovations in the field of cybercrime, it is particularly important to examine the national context and challenges that Ukraine faces in combating this issue. Ukraine, like many other countries, is a constant target of cyber threats. Specifically, the conflict in the country's east and the geopolitical situation contribute to the intensification of cyber attacks targeting critical infrastructure and government agencies. In response, Ukraine is actively enhancing its cybersecurity measures, including strengthening the protection of critical assets and increasing cybersecurity in state institutions.

Cyberpolice (the Cyberpolice Department of the National Police of Ukraine) is a territorial body within the National Police of Ukraine. It is part of the criminal police of the National Police and, according to Ukrainian legislation, plays a crucial role in implementing state policies to counter cybercrime. Additionally, it coordinates and conducts operational and investigative activities under the law, specializing in preventing, detecting, stopping, and uncovering criminal offences involving the use of electronic computers, telecommunications, and computer networks and systems. The growth in the quantity and quality of qualified personnel in the field of cybersecurity is one of the key tasks for Ukraine. Ensuring high-quality education in cybersecurity and supporting training programs enable the creation of an effective workforce capable of responding to the growing challenges of cybercrime.

Global trends in cybercrime, as presented in our work, indicate that states and enterprises must enhance their cybersecurity measures, focusing on protecting critical infrastructure and ensuring a high level of cyber defence. Technological innovations in cyber investigations, such as artificial intelligence, blockchain technologies, and quantum computing, open new opportunities for improving the processes of detection and resistance to cyber threats. These technologies not only increase the efficiency of investigations but also make them more adaptive to the rapidly changing cyber landscape. Ukraine, as a subject of global cybersecurity, demonstrates a recognized need to strengthen cybersecurity measures and improve cybercrime investigations. The country successfully develops its cybersecurity infrastructure, actively involving qualified professionals and collaborating both nationally and internationally. By following global trends and integrating new technologies, Ukraine has the opportunity not only to enhance its cyberspace but also to act as a catalyst for global changes in cybersecurity.

1. What is REvil/Sodinokibi Ransomware.LEPIDE. URL : http://surl.li/njaih
2. Cyberdefense report. Japan's National Cybersecurity and Defense Posture URL : http://surl.li/njaiu.
3. Airbus Cybersecurity. URL : https://www.cyber.airbus.com.

УДК 681.5
DOI: 10.31733/15-03-2024/2/297-300

Світлана ЛУЧИК
професор кафедри
протидії кіберзлочинності,
доктор економічних наук, професор

Олександр МОЙКО
курсант спеціальності «Кібербезпека»
Харківського національного
університету внутрішніх справ

МОДЕЛЮВАННЯ КІБЕРАТАК В КІБЕРПРОСТОРІ

Кібератаки – це зловмисні дії в кіберпросторі, що мають на меті порушити функціонування, конфіденційність, цілісність або доступність інформаційних систем, мереж, ресурсів або даних. Кібератаки можуть мати різні мотиви, цілі, методи та наслідки, а також різний рівень складності, масштабу та впливу. Кібератаки можуть бути спрямовані на окремих осіб, організацій, секторів, країн або регіонів.

Протягом останніх років Україна є однією з найбільш атакованих країн у світі в сфері кібербезпеки. З початку війни Україні вдалося відбити понад 5 тис. російських кібератак. За даними Держспецзв'язку, в Україні у 2023 році кількість кібератак зросла, порівняно з 2022 роком, на 15,9% до 2543 інцидентів. За даними урядової команди реагування на комп'ютерні надзвичайні події CERT-UA, 27,8% кібератак було зафіксовано на уряд та урядові організації, 22,1%– на місцеві органи влади, 14,0% – організації у секторі безпеки та оборони, 10,2% – комерційні організації, 7,4% – енергетичний сектор, 6,5% – телеком, 3,0% – освітні установи. 2,6%– транспортну галузь, по 2% – фінансовий сектор та IT-сектор, 1,2% – ЗМІ, менше 1%– медичні установи (рис. 1).

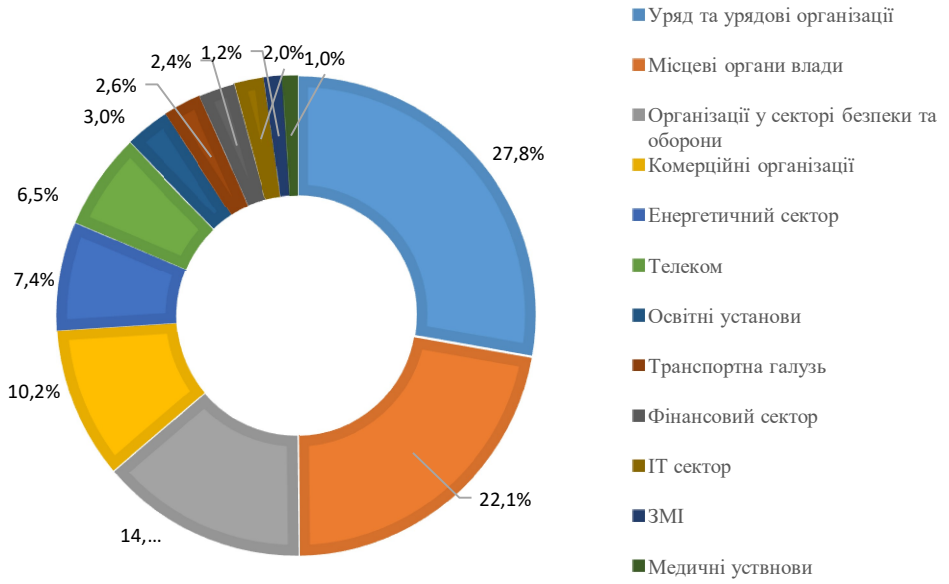

Рис. 1. Кібератаки в Україні, 2023 рік
Джерело: [1]