

Lytvynenko Roman, cadet of Kharkiv National University of Internal Affairs

Research Supervisor – **Kuchynskyi Serhii**, senior teacher of Department of tactical and special training Kharkiv National University of Internal Affairs

CYBER PROTECTION OF CRITICAL INFRASTRUCTURE: CHALLENGES FOR LAW ENFORCEMENT AGENCIES IN ARMED CONFLICT

Cyber protection of critical infrastructure facilities in the context of war has become one of the most important tasks for ensuring the security of the entire country. Today, enemy attacks in the digital space are accompanied by phishing, the spread of disinformation, and the risks of leaking official information. Energy networks, transport hubs, communications, water supply systems, and government registers are at risk. Disabling these facilities can completely paralyze the activities of state structures. For law enforcement agencies, this creates serious difficulties, since the usual methods of investigating crimes become little effective against professional hacker groups or foreign agents of the aggressor state.

Modern threat analysis shows that cyberattacks during the war are not aimed at obtaining money, as is the case in ordinary crime, but at large-scale data destruction, stopping industrial equipment and completely blocking communication. The enemy often tries to act with other people's hands, disguising his special services as independent activists or ordinary extortionists in order to hide the direct participation of his state. Because of this, it is extremely difficult for law enforcement officers to prove the involvement of specific persons in the crime. Law enforcement agencies have to work ahead of schedule and constantly learn new tactics and techniques that enemy hackers use to infiltrate closed networks [1].

In order to reduce the risk of cyber attacks and promptly respond to their detection, it is necessary to implement a cyber hygiene policy at enterprises and monitor compliance with its requirements. The policy provides for monitoring of computer networks for vulnerabilities and operational isolation of vulnerabilities, in the event of detection of suspicious activity. When protecting critical infrastructure, there is a factor of leakage or service information or violation of its integrity. SIEM-based database protection involves monitoring databases, monitoring all service file changes, monitoring login and logout attempts, and recording abnormal behavior in the system [7].

Using a DLP system will allow you to focus on monitoring network traffic to protect against powerful DDoS attacks that try to shut down servers [2, 8]. The system provides for full control over the data transmission channel, encryption of traffic and data from unauthorized access, and protection of information devices from third parties [8].

In addition to technical aspects, great attention should be paid to the training of employees, because ordinary phishing (dangerous emails) remains the easiest way for hackers to bypass system protection. The training consists in familiarizing the basic concepts of cyber hygiene, compliance with the basic safety requirements in the digital environment, as well as being supported by checking the level of knowledge of employees. In the event of cyberattacks, the main task of – is to quickly recover from secure backups and simultaneously collect all digital evidence for future lawsuits [3].

Technical analytics and open source intelligence (OSINT) is becoming the main tool for investigating cyber incidents. To establish the type of threat and the source of its origin, experts use such analytical platforms as «VirusTotal» and «Any.Run». Specialized search engines «Shodan» and «Censys» [4] are used to find unsecured servers and identify vulnerabilities in the system. Also, law enforcement officers constantly check possible leaks of official and confidential information about employees and critical enterprises through «Have I Been Pwned» services, and discover hidden channels in the so-called «Dark Web» [5]. The use of the mentioned technical means helps to establish the probability of a threat at the initial stage, when the enemy only analyzes for the presence of weak points, which allows timely use of the model of protection of digital systems.

Reliable protection of the digital space is impossible without close interaction in the middle of the law enforcement structure, as well as proper coordination of mass media. Since most important facilities belong to private or utility companies, law enforcement agencies must quickly transfer technical data about new threats, since the response time for such threats is quite short. Of particular

importance is proper communication with the media in case of emergencies, or when internal threats are identified in the operation of critical infrastructure facilities. The lack of reliable data over long periods of time creates the spread of misinformation as well as distorted information, which the enemy uses to create panic and chaos among the local population. Timely, simple and clear explanations from the official press regarding the nature of the problem and the timing of its elimination help to maintain peace in society, coordinate the further activities of law enforcement agencies, and monitor further developments [6].

Protecting critical infrastructure from cyber threats therefore requires law enforcement to move to a whole new level of technical training. Combining the latest information protection systems and analytical tools provides reliable both external and internal protection of critical infrastructure. Constant training of personnel, enterprises in the basics of digital security and quick exchange of information between the state, interaction with the media allows you to create an effective protection system capable of withstanding any attacks.

References

1. Про основні засади забезпечення кібербезпеки України. Закон України від 19 жовт. 2025 р. № 2163-VIII. *Відомості Верховної Ради України*. 2017. № 45 Ст. 403.
2. Державна служба спеціального зв'язку та захисту інформації України : мет. рек. та ін. щодо підвищення рівня безпеки державних інформаційних ресурсів.
3. Департамент кіберполіції Національної поліції України: практ. Мат. та аналітичні звіти за результатами розслідування комп'ютерних злочинів під час воєнного стану. URL: <https://cyberpolice.gov.ua/news/shhorichnyj-zvit-7096/>
4. 1. LLNL-TR-2011159. Cybersecurity and Infrastructure Security Agency (CISA). Чинний від 18.07.2025. 2025.
5. SANS Institute: нав. посіб. та практ. Ін. з проведення кіберрозвідки на основі відкритих джерел (OSINT).
6. Центр аналізу загроз Microsoft (MSTIC): аналітичні звіти та дослідження щодо тактик і технічних прийомів військових хакерських угруповань. URL: <https://www.microsoft.com/uk-ua/security/security-insider/intelligence-reports/special-report-ukraine>
7. Крижановський В. Г., Сергієнко С. П. Апаратно-програмні засоби захисту інформації у корпораціях : навч.-метод. посіб. Вінниця : ДонНУ імені Василя Стуса, 2019. 36 с.
8. Data Loss Prevention (DLP) – Технологія запобігання витоку конфіденційної інформації. URL: <https://msu.edu.ua/library/wp-content/uploads/2019/02/prykłady-oformlennja-bibliografichnoho-opysu-zhidno-dstu-8302.pdf>

Лігун Андрій Іванович, здобувач кафедри кримінального права НАВС;

Матюшенко Олена Іванівна, професор кафедри кримінального права НАВС, кандидат наук з державного управління, доцент

РОЗМЕЖУВАННЯ КОЛАБОРАЦІЙНОЇ ДІЯЛЬНОСТІ ТА СУМІЖНИХ ДІЯНЬ

Чітке встановлення ознак, які дозволяють розмежувати склад певного кримінального правопорушення та складу суміжних з ним діянь, є необхідною умовою для встановлення правильної правової оцінки фактичних обставин вчиненого суспільно небезпечного діяння. Правильна кваліфікація суспільно небезпечного діяння вимагає встановлення чітких розмежувальних ліній між вчиненим кримінальним правопорушенням і суміжними діяннями. Вважаємо, що розмежування складів кримінальних правопорушень – це юридична діяльність, яка реалізується в ході створення кримінально-правових нормативних приписів, тлумачення норм Кримінального кодексу України (далі – КК), а також у процесі здійснення кримінально-правової кваліфікації та полягає у встановленні місця конкретного складу кримінального правопорушення у системі складів кримінальних правопорушень зі спільними ознаками та системі всіх законодавчих моделей кримінально-каранної поведінки, що впроваджується шляхом порівняння змісту ознак складів правопорушень і полягає у виявленні суті їх зв'язків один з одним.