з здійсненням кібератак з боку російської федерації, проведенням деструктивної зовнішньої і внутрішньої пропаганди, намагання суб'єктів розвідувально-підривної діяльності отримати доступ до відомостей, що становлять державну таємницю та службову інформацію, а також іншої інформації з обмеженим доступом та інше.

## Список використаних джерел:

1. Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року "Про Стратегію забезпечення державної безпеки". Президент України. Указ. 16 лютого 2022 року № 56/2022. URL: https://zakon.rada.gov.ua/laws/show/56/2022#n5 (дата звернення: 20.09.2023).
2. Діяльність вітчизняних підприємств під час війни в Україні: дослідження реального стану та потреб (липень 2022). К. : Центр ресурсоефективного та чистого виробництва, 2022. 23 с. URL: http://www.recpc.org/wp-content/uploads/2022/11/National_businesses_ during-war_2022. pdf (дата звернення: 20.09.2023).
3. Іванов С. Вплив збройного конфлікту (війни, бойових дій) на вартість підприємства : монографія. Дніпропетровськ : Маков., 2015. 179 с.

DOI https://doi.org/10.36059/978-966-397-355-5-50

**Sardarian K. H.,**
*Candidate of Philological Sciences, Associate Professor,*
*Visiting researcher at the Department of Literary Studies*
*Uppsala University, Sweden*

**Sardarian D. A.,**
*Student*
*Kyiv University of Law of the National Academy of Sciences of Ukraine*
*Kyiv, Ukraine*

# THREATS TO INFORMATION SECURITY IN WARTIME

Currently, ensuring information security is especially important. Hybrid methods of conducting modern wars are aimed at creating information chaos on enemy territory. For this purpose, the targeted work of the media and hacker attacks on especially important security systems of the enemy state are used. Therefore, today information warfare or cyberwar is a real threat.

Information has value, namely the degree of protection against criminal attempts and attacks is highly valued. Since information security is a guarantee of the security of the state itself. Protecting information resources in the modern world is a priority task for cybersecurity specialists.

There are two types of sources of information threats: internal and external. Internal sources of information threats create tension in the socio-political life of the country and destabilize the situation. Destabilization is created artificially. This provokes conflicts within society. Chaos and unrest are provoked by specially targeted information influence. Such actions are serious threats. Therefore, today it is especially important to provide preventive psychological support to the population.

Falsification of facts and the introduction of false information are used by opponents to increase social tension and incite conflicts within society and are also a threat to information security.

In addition, technical components should be mentioned among the threats to information security. These are information systems and management systems.

Technical threats can be of a different nature, including: intentional damage to information systems, theft of information, and negligence of employees in their duties. To minimize these above-mentioned risks, protection measures should be strictly followed: train personnel and bear responsibility, comply with requirements related to data protection, and also increase the reliability and security of control systems.

External information threats are diverse. Information and psychological measures are often used. The real threat is the use of information attacks. Cybersecurity experts name a large number of types of psychological weapons. It is known that the strategic enemy has specially trained departments for targeted information and psychological influence. To counter propaganda, not only journalists, but also the population must be prepared and media literate in order to distinguish and identify threats of psychological influence.

We will mention social networks as a separate point, which are a serious problem for the security of the country, society and the individual. Often on social networks, media literate people share strategically important information. By doing this they cause irreparable damage. There are many examples of this. Therefore, preventive work with the population should be carried out more often with an explanation not to transmit or publish photos and information about important strategic points of the infrastructure.

For example, sending messages to mobile numbers of Ukrainian operators is very useful in this sense. Text of the message: “The Security Service of Ukraine informs! Strictly follow safety precautions when announcing the “Air Raid” signal. Do not take photographs, shoot videos or publish the movement of military equipment of the Ukrainian Military

Forces and their locations! Report discovered explosive devices, abandoned military equipment..." [personal archive].

Illiterate use, disclosure, publication of such information on social networks (we often see this) to attract attention to one's own person can cost the lives of civilians, and important infrastructure facilities also suffer. It is important to note that after several precedents of similar publications by fellow citizens who unknowingly, due to information illiteracy, caused harm, the services engaged in educational work and notified fellow citizens of responsibility. As a result, the number of thoughtless publications has decreased significantly.

Also, a threat to information security is posed by internal enemies who specialize in collecting information for the enemy side. For example, already this month the Security Service of Ukraine discovered the attackers and prevented their crime. The attackers photographed strategically important infrastructure facilities in Kyiv and planned to transfer information to the enemy. The so-called "home" videos of numerous bloggers also pose a threat to information security. In addition, media funds work with journalists on countering disinformation.

On March 26, 2022, President of Ukraine Vladimir Zelensky signed a law establishing criminal liability for unauthorized dissemination of information about the movement or location of the Armed Forces of Ukraine. The law also focuses the attention of the media on their obligation to comply with the requirements of the new law.

The law amends the Criminal and Criminal Procedure Code of Ukraine to ensure counteraction to the unauthorized dissemination of information about the direction, movement of international military assistance to Ukraine, movement, movement or deployment of the Military Forces of Ukraine or other military formations, committed under conditions of martial law or a state of emergency.

According to the new law, it is prohibited to publish videos and photos with the following content:

- trajectory and location of missile impact;
- names of streets, transport stops, shops, factories, etc.;
- relocation of Ukrainian military and military facilities;
- work of Ukrainian air defense;
- location of shelling or projectile impact;
- address, visual reference information or battle coordinates;
- license plate numbers of cars and armored vehicles;
- names of victims or dead (except for official data).

Violation of these requirements is subject to criminal liability – imprisonment from 3 to 12 years.

If information about the direction of movement or movement of weapons and ammunition on the territory of Ukraine was not publicly available by the Ministry of Defense, or in official sources of the relevant structures of partner countries, reporting by individuals about their location or movement will be punishable by imprisonment from 3 to 5 years.

For the dissemination of information about the movement and location of the Military Forces of Ukraine, if it is possible to identify them on the ground, punishment is provided in the form of imprisonment from 5 to 8 years.

The greatest punishment is provided for the publication of such information for selfish reasons or by prior conspiracy or for the purpose of providing such information to an aggressor country – imprisonment for a term of 8 to 12 years [2].

Preventing threats to information security is not only the task of the state, but also the task of representatives of civil society as a whole and each individual.

## Bibliography:

1. Конфіденційна інформація. URL: https://wiki.legalaid.gov.ua/index.php/%D0%9A%D0%BE%D0%BD%D1%84%D1%96%D0%B4%D0%B5%D0%BD%D1%86%D1%96%D0%B9%D0%BD%D0%B0_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%8F

2. Набув чинності закон про відповідальність за розголошення інформації, що може зашкодити країні під час війни. URL: https://www.nrada.gov.ua/nabuv-chynnosti-zakon-pro-vidpovidalnist-za-rozgoloshennya-informatsiyi-shho-mozhe-zashkodyty-krayini-pid-chas-vijny/

3. Національна рада проведе круглий стіл для медіа щодо запобігання проявам мови ворожнечі й дискримінації осіб за різними ознаками. URL: https://webportal.nrada.gov.ua/