scouts were able to successfully use affordable and simple serial drones, such as DJI or Autel, to determine the positions of the Russian military and direct artillery strikes. Drones helped destroy a significant amount of enemy equipment, personnel and artillery. For example, assistance from the Mavik-3 drone, which has a value of about UAH 100,000, contributed to the destruction of the Ural vehicle, valued at approximately UAH 2 million. [5].

From the analysis presented in this study, it can be concluded that the development and use of unmanned aerial vehicles (UAVs) is becoming a significant factor in the field of law enforcement and defense. According to the stated data, the use of UAVs opens up new opportunities for conducting military operations, in particular for performing tactical tasks and delivering precise strikes on strategic targets. UAV technologies are used for reconnaissance, establishing the coordinates of enemy objects, as well as for directing artillery strikes, which contributes to more effective warfare and reducing risks for personnel.

It also states that scouts and drone operators have learned to successfully use affordable and simple drones to locate enemy positions and deliver strikes.

This allows to destroy enemy equipment and personnel with minimal losses on the part of their own troops. For example, the use of Mavik-3 drones contributed to the destruction of an enemy object, which is worth much more than the drone itself.

This approach to the use of UAV technologies, which is based on their availability and capabilities, allows to increase the effectiveness of combat operations, as well as to reduce risks for one's own personnel. Programs aimed at maximizing the use of reconnaissance and attack UAVs show that developers and the military are rapidly adapting to new challenges in modern military technology to ensure the safety and effectiveness of military operations.

1. Kalashchenko S. I. Justification of preventive rehabilitation criteria based on assessment of psychophysiological status of cadets of the Academy of the National Guard of Ukraine: dissertation. ... PhD : 14.02.01. Kyiv, 2022. 274 p.

2. Yaroshenko Ya., Gerasimenko V., Blyskun O., Basilo S., Ikayev D. Experience of using unmanned aircraft in the Armenian-Azerbaijani conflict in the fall of 2020. Lessons for Ukraine // Military Historical Bulletin, 2021. No. 2(40). P. 53-71.

3. Rud S. S. Kurbatov A. A. The role and place of UAVs in the conditions of the war with Russia. Actual problems of the theory and practice of service and combat activity of the components of the security and defense sector in modern conditions: materials of the All-Ukraine. science and practice conf. (Kyiv, October 27, 2023), p. 277.

4. Kamikaze with wings and propellers: experts spoke about the role of drones in the fight against the Russian aggressor // FREEDOM, 10/12/2023. URL : https://uatv.ua/uk/kamikadze-z-krylamy-j-gvyntamy-eksperty-rozpovily-pro-rolbezpilotnykiv-u-borotbi-z-rosijskym-agresorom/.

5. Rodak K. This is a real breakthrough, 06/13/2022. URL : https://zaxid.net/statti_tag50974/.

УДК 623.746-519:351.862.4
DOI: 10.31733/15-03-2024/2/351-353

**Кароліна ГОНЧАР**
курсант ННІ права та підготовки
фахівців для підрозділів
Національної поліції
**Ганна ДЕКУСАР**
старший викладач кафедри
українознавства та іноземних мов
Дніпропетровського державного
університету внутрішніх справ

## PRIORITIES FOR ENSURING CYBERSECURITY OF UKRAINE IN THE CONTEXT OF ARMED AGGRESSION

In today's world, which is becoming increasingly digital and dependent on information technology, the role of cybersecurity is extremely important and crucial. It creates the basis for security and resilience in the information space, protecting individuals, companies, government agencies and national interests from potential threats.

Currently, this topic is of particular importance, as Ukraine is in a difficult geopolitical situation where cyberattacks can be used as a tool of hybrid warfare. Significant human, material, and financial resources are involved in the conduct of anti-Ukrainian information influence, which makes it possible to effectively "brainwash" some of our compatriots [1].

Protecting Ukraine from cyberattacks is a complex and multifaceted task that requires cooperation between government agencies, the private sector, and the public. It includes some key strategies that can be used for defense, namely:

1. Establishing a national cybersecurity strategy: the government of Ukraine should develop and implement a national cybersecurity strategy that defines the main areas of activities and resources to protect against cyber threats.

2.Increase investment in cybersecurity: the government should allocate sufficient resources to develop and maintain cybersecurity measures, including infrastructure upgrades, training of personnel, and cyber exercises for the public.

3. Strengthening cybersecurity legislation: it is important to improve legislation governing cybersecurity, including prohibiting cybercrime, defining liability for cyberattacks, and ensuring transparency and accountability in relations between government agencies, the private sector, and the public.

4. Establishment of cybersecurity centers: the government may consider establishing specialized cybersecurity centers that will be responsible for monitoring, analyzing and responding to cyber threats.

5. Increasing education and awareness: it is important to conduct ongoing education and awareness campaigns for the public, businesses and government officials on cybersecurity, including training on the most common cyber threats and how to prevent them.

6. Cooperation with international partners: Ukraine should actively cooperate with international organizations and partners in the field of cybersecurity, exchanging information on cyber threats and best practices.

7. Human resource development in the field of cybersecurity: it is important to develop human resources in the field of cybersecurity, including training of cybersecurity specialists and attracting talented professionals to this field.

In today's military realities, it is difficult and even inappropriate to deny the role of information as a tool of confrontation, in fact, a weapon. Information allows you to win a war without firing a single shot, by creating and fomenting internal contradictions [2]. Therefore, it is appropriate to outline the priorities that Ukraine should set to ensure cybersecurity in the context of armed aggression:

1. Protection of critical infrastructures: the primary task is to protect critical infrastructures, such as energy, transportation, telecommunications and finance, from cyberattacks that could lead to serious consequences for national security and the economy.

As a result of Russia's full-scale invasion of Ukraine in 2022, the number of cyberattacks by Russia doubled, and before the anniversary of the military aggression, it increased sixfold [3]. An example of this is the unpleasant situation that occurred on the morning of December 12 throughout Ukraine, namely, a large-scale failure of the Ukrainian telecommunications company Kyivstar: mobile and Internet communications disappeared, causing significant losses to the company and citizens who were left without communication, which plays an important role in wartime, as fast and reliable communication allows the military, law enforcement agencies and the public to coordinate actions, perform urgent actions and respond to threats.

2.Increase preparedness for cyber attacks: the government of Ukraine should increase preparedness for cyber attacks by developing and implementing cyber defense strategies and technologies, and training personnel to respond to cyber threats.

3.Ensuring information security: it is necessary to ensure the security of information resources and systems of government agencies, military structures and critical infrastructures from cyberattacks and cyberespionage.

4.Strengthening legislation and regulatory measures: the government should consider improving legislation and regulatory measures in the field of cybersecurity, including defining liability for cyberattacks and increasing fines for their commission.

5.International cooperation: Ukraine should actively cooperate with international partners, including NATO, the European Union, and other countries, to share information on cyber threats and respond to them jointly.

6.Raising public awareness: it is important to conduct information campaigns and educational activities for the public on potential cyber threats and methods of preventing them.

7. Developing and implementing cyber defense technologies: it is necessary to actively develop and implement cyber defense technologies, such as systems for detecting and preventing cyber attacks, encrypting data, and identifying anomalous activity.

These priorities and strategies will help Ukraine strengthen its cybersecurity and preserve national security in the face of armed aggression and bring the country closer to victory.

1. Peculiarities of anti-Ukrainian informational (cyber) influence on Ukraine - Oleksandr Vitaliyovych Levchenko, Volodymyr Vasyliovych Okhrimchuk - Protection of information. – 2022. – Vol. 24, No. 4.

URL: https://odnb.odessa.ua/view_post.php?id=4361

2. Koterlin I.B., Actual problems of domestic jurisprudence No. 1.

URL: http://apnl.dnu.in.ua/1_2022/25.pdf

3. Manulov Y.S., Ensuring cyber security of critical infrastructure objects in the conditions of cyber war

УДК 004.738.5:681.5
DOI: 10.31733/15-03-2024/2/353-354

**Марія ЗАВ`ЯЛОВА**
студентка ННІ права
та інноваційної освіти

**Ігор ЧОБОТЬКО**
старший викладач кафедри
фізичного виховання
та тактико-спеціальної підготовки
Дніпропетровського державного
університету внутрішніх справ

## ДИСКУРС ЩОДО РОЗУМІННЯ ОКРЕМИХ АСПЕКТІВ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Сучасний прогрес людства визначається швидким розвитком інформаційних новацій, зокрема комп'ютерних технологій, які є невід'ємною складовою сучасності. Інтернет, безперечно, став неодмінною частиною нашого життя [1]. Однак у кіберпросторі поширені різноманітні загрози, такі як маніпуляції, дезінформація, пропаганда фізичного чи сексуального насилля, поширення заборонених товарів, підбурювання до самогубства та інші. Суспільство усвідомлює потребу у впровадженні передових заходів кібербезпеки, але варто зауважити, що лише свідомість не є достатньою. Кібербезпека постійно обговорюється, оскільки суспільство ще не має достатньої медіаграмотності для повного розуміння загроз. Зростання кількості кримінальних правопорушень у кіберпросторі підкреслює важливість цього питання як на національному, так і на міжнародному рівнях [2].

Будь-який стрімкий розвиток супроводжується як позитивними, так і негативними явищами. Згідно з програмними документами ООН, універсальне підвищення кібербезпеки передбачає врахування різних аспектів, таких як інформованість, відповідальність, етика, демократія, оцінка ризиків, впровадження засобів безпеки та управління ними, а також переоцінка [3]. Націленими напрямами забезпечення безпеки в кіберпросторі є інформаційна безпека, безпека мережі, безпека Інтернету та захист критичних інфраструктур [4].

Одним із недостатньо вивчених аспектів боротьби з цією злочинністю є соціальний план щодо формування глобальної культури кібербезпеки, зокрема в галузі освіти та науки загалом. Комп'ютерна безпека має у своєму складі широкий спектр проблем у сфері телекомунікацій та інформатики, пов'язаних з контролем та оцінкою ризиків, що виникають при використанні комп'ютерів, гаджетів та комп'ютерних мереж [5].

Згідно з Законом України «Про основні засади забезпечення кібербезпеки України», кібербезпека визначається як захист інтересів людини, суспільства та держави в кіберпросторі. Особливу увагу слід звернути на правові, моральні та суспільні аспекти