**ABSTRACT TITLE**

*Candidate of Military Sciences, Senior Research Fellow  
Name SCIENTIST*

*The Central Research Institute of the Armed Forces of Ukraine, Research Fellow*

*KYIV, UKRAINE, e-mail: test@post.mil.gov.ua*

*Doctor of Technical Sciences, Professor  
Colonel Kyrylo SERVICEMAN*

*The Central Research Institute of the Armed Forces of Ukraine, Chief of Directorate*

*KYIV, UKRAINE, e-mail: test1@post.mil.gov.ua*

**I. Introduction and relevance of the issue**

The history of military conflicts across different eras vividly demonstrates the importance of technological superiority over numerical advantage. The largest military confrontation of the twenty-first century to date – the russian-Ukrainian war – is no exception, where, for the first time in history, unmanned (crewedless) systems, information and psychological, and cyber operations are widely used.The result of employing these innovations helps to understand the critical necessity to improve the forms and methods of conducting military operations and the Ukrainian Armed Forces as a whole. Various information technology elements are already being used in the military, including high-tech systems and equipment samples, yet more practical subsystems of the units functioning remain distant from progressive solutions. The experience of corporate organisations, which achieve leading results through competition, is almost unutilised. As a result, the Ukrainian Defence Forces do not meet modern requirements and are vulnerable to hybrid threats, therefore, the issue of integrating well-known information technologies is highly relevant.

**II. Main ideas**

Due to subjective and objective reasons, the existing cyber defence system in Ukraine at the start of the war was imperfect, both organisationally and technically. Consequently, it had not acquired the necessary capabilities. The process of creating and developing the relevant military organisational structures within the Ukrainian Armed Forces, as well as their staffing, training, and comprehensive support, was also in its infancy. The process of combining the efforts of electronic warfare (EW) and cyber warfare had not been completed. The integration of the cyber defence management system into the state defence management system was not implemented in practice. No less problematic was the issue of the normative definition and inclusion of new forms and methods of military (force) operations into the operational system of the Ukrainian Armed Forces, in and through cyberspace. Unlike in russia, cyber weapons were absent in Ukraine.

**III. Conclusions**

Considering the exhausting and prolonged nature of the armed confrontation in physical spaces, it becomes evident that the development of the Ukrainian Armed Forces' cyber domain capabilities must become a priority of state policy in the military sphere.