***В. С. Греков, студ.; рук. А. Г. Уймин, ст.преподаватель***

***(РГУ нефти и газа им. И.М.Губкина, Москва)***

**INNOVATIONS IN CYBERPOLYGONS: ADVANTAGES AND CHALLENGES OF USING RUSSIAN SOFTWARE**

Греков В.С., Уймин А.Г.

Cyberpolygons, platforms designed to simulate cyberattacks, play a pivotal role in developing and testing defensive strategies against a range of threats in cyberspace [1]. With the progression of cutting-edge technologies like artificial intelligence, machine learning, and automation, the sophistication and capabilities of cyberpolygons have markedly improved. The assimilation of Russian-made software within these frameworks has bolstered their security and dependability. Such an amalgamation aids in the expansion of the domestic industry by nurturing the Russian market and supporting local software developers [2]. Additionally, it ensures adherence to national standards and laws, an essential element in the realm of cybersecurity.

However, integrating Russian software into cyberpolygons presents certain challenges. Limited functionality and compatibility issues may arise when this software is paired with international systems. Additionally, there is a notable lack of resources and expertise necessary for sustaining high-level software development and operation. There is also an inherent risk of lagging behind in international standards of innovation and technology. One particularly notable issue is the management of intense network traffic [3].

In conclusion, finding a balance between the use of Russian and open-source software in cyberpolygons is crucial. While Russian software offers numerous benefits in terms of security, reliability, and adherence to local standards, maintaining the competitiveness and innovative edge of cyberpolygons requires the consideration and integration of international best practices and technologies. The advancement of Russian software in the field of cybersecurity necessitates collaborative efforts among specialists, government entities, and academic institutions to overcome existing limitations and sustain its innovative capacity.

**Литература**

1. **Ciuperca E., Stanciu A., Cîrnu C.** Postmodern education and technological development. Cyber range as a tool for developing cyber security skills //INTED2021 Proceedings. – IATED, 2021. – С. 8241-8246.
2. **Miloslavskaya N., Tolstoy A.** Cyber polygon site project in the framework of the MEPhI network security intelligence center //Brain-Inspired Cognitive Architectures for Artificial Intelligence: BICA\* AI 2020: Proceedings of the 11th Annual Meeting of the BICA Society 11. – Springer International Publishing, 2021. – С. 295-308.
3. **Uymin A.** Application of machine learning in the classification of traffic in telecommunication networks: working with network modeling systems //E3S Web of Conferences. – EDP Sciences, 2023. – Т. 402. – С. 03001.