

AGRICULTURAL SECTOR AND CYBERSECURITY OF THE DIGITAL ECONOMY: MODERN CHALLENGES

The digitalization of the economy promotes the active implementation of information technologies in various sectors of economic activity, particularly in the agricultural sector. Modern agriculture increasingly uses digital solutions, including precision farming systems, GPS navigation, unmanned aerial vehicles, soil and crop monitoring sensors, automated machinery management systems, and digital platforms for agricultural product trading. These technologies enhance agricultural productivity, optimize resource use, and improve the competitiveness of enterprises.

At the same time, the use of modern agrotechnologies creates new cyber risks. Unmanned aerial vehicles, IoT sensors for monitoring soil and climate conditions, as well as “smart” agricultural machinery connected to the Internet, may be vulnerable to unauthorized access or cyberattacks. Disruptions in these systems may lead to loss of yield data, incorrect machinery control, or failures in technological processes, negatively affecting agricultural efficiency. Thus, the modern agricultural sector is gradually transforming into a complex cyber-physical system combining digital technologies, production processes, and information infrastructure.

One of the most significant consequences of cybercrime is substantial financial losses. According to IBM Global Average Data Breach research, the average cost of a data breach worldwide is steadily increasing: \$3.9 million in 2020, \$4.2 million in 2021, and \$4.4 million in 2022.

Financial losses from cyberattacks may take various forms. These include costs for restoring information systems, upgrading software, and strengthening cybersecurity systems. A notable example is the NotPetya cyberattack in 2017, which caused approximately \$10 billion in global economic damage.

In the context of agricultural digitalization, cyber incidents can also have serious financial consequences for market participants. Agricultural enterprises increasingly use electronic financial systems and online platforms, which increases the risks of financial fraud and theft of commercial information.

Another important consequence is reduced income due to temporary suspension of operations or decreased business activity. For example, in 2013 Target suffered losses of \$162 million due to a credit card data breach, while in 2017 Equifax lost approximately \$1.4 billion.

Cybercrime also causes serious reputational risks. Loss of trust from clients and partners may have long-term economic consequences. According to Ponemon Institute, about 62% of consumers stop cooperating with a company after a data breach. For agricultural enterprises, this may lead to loss of markets and decreased competitiveness.

Cyberattacks on critical infrastructure pose a particular threat. For example, the Colonial Pipeline attack in 2021 caused fuel supply disruptions affecting transportation and production processes. Similar incidents occurred in Ukraine, including a cyberattack on energy infrastructure in 2015 that led to large-scale power outages.

Investments in cybersecurity are therefore essential for the development of the digital economy. The global cybersecurity market is estimated at approximately \$186 billion and is expected to exceed \$271 billion by 2029. In Ukraine, the market reached about \$138 million in 2024.

Thus, ensuring cybersecurity is a key factor for the sustainable development of the agricultural sector. It is necessary to implement modern information protection technologies, develop cyber monitoring systems, increase employee awareness, and improve legal frameworks and

international cooperation in combating cybercrime.

References:

1. Global average total cost of a data breach in 2022 growth up to \$4.4 mn. URL: <https://beinsure.com/news/global-average-data-breach-2022> (accessed: 10.03.2026).
2. History of the NotPetya virus: should we expect similar cyberattacks in the future? URL: <https://www.imena.ua/blog/notpetya-cyberattack> (accessed: 10.03.2026).
3. Statista. URL: <https://www.statista.com/statistics/> (accessed: 10.03.2026).

Prepared by NGO "Institute of Ecological Economics and Digital Agricultural Development"

© 2026 All rights reserved.