S. Dyomina
С.А. Демина
БрГУ им. А.С. Пушкина (Брест)
Научный руководитель И.В. Повх

CYBERSECURITY IN MODERN SOCIETY: PERSONAL DATA PROTECTION

Кибербезопасность в современном обществе: защита персональных данных

Cybersecurity in today's society is becoming one of the most important areas affecting both individuals and organizations. With the growth of digitalization and the increase in the amount of data we generate and store, the threat of hacking and leakage of personal data is becoming more and more urgent. Cybersecurity is a vast and dynamic field that encompasses the protection of computer systems, networks, and data from cyber threats. With increasing reliance on technology and the internet, cybersecurity is becoming critical to protect personal and corporate information. The purpose of our research is to outline the main principles and methods of personal data protection as well as measures taken to enhance digital security.

Over the past few years, the introduction of modern technologies into human life has turned out to be rapid and colossal in its consequences. Risk to industrial communication networks, especially those that support critical infrastructures (local, regional, or national), has been steadily increasing in recent years, so there has been an increase in research in the field of cybersecurity.

Personal data protection is a set of measures aimed at ensuring the confidentiality, integrity and availability of personal information. In the context of digitalization and an increase in the volume of data being processed, the protection of personal data (name and surname, e-mail address, phone numbers, date of birth, identification numbers (e.g., passport or social security number), biometric data, financial information) is becoming especially relevant. Different countries have their own laws and regulations regarding the protection of personal data. For example, GDPR (General Data Protection Regulation) in the European Union is one of the strictest data protection laws that regulates the processing of personal data of EU citizens, Law on the Protection of Personal Data in Russia (152-FZ) regulates the processing of personal data in Russia, while CCPA (California Consumer Privacy Act) in the United States provides California residents with certain rights regarding their personal data.

Basic principles of personal data protection include the consent of the data subject, collecting the data for specific, legitimate purposes without further processing that is incompatible with these purposes, collecting only the data necessary for the purposes of processing, accuracy and relevance of personal data must be accurate and updated if necessary, retention and storage of the data for only as long as required for the purposes of processing, and applying adequate security measures to protect data from unauthorized

access, leakage, or destruction. The most common methods of personal data protection are as follows: encryption; anonymization and pseudonymization, removing identifying information from data sets to minimize risks; access control, restricting access to data to authorized users only; conducting regular security audits and testing to identify vulnerabilities; and raising employee awareness of the importance of protecting personal data and possible threats. Compliance with cybersecurity and personal data protection regulations and standards helps organizations not only avoid legal consequences, but also increase customer trust.

Ultimately, cybersecurity is not a one-time task, but an ongoing process that requires attention and adaptation to new threats. Protecting personal data is an important part of this process, as the leakage or compromise of such data can lead to serious consequences for individuals and organizations. A comprehensive approach based on technology, training, and compliance is key to effective protection in the face of an ever-changing cyber threat.

Y. Darakhovich
Я.Д. Дорохович
БГЭУ (Минск)
Научный руководитель О.П. Гуминская

ARTIFICIAL INTELLIGENCE IN ECONOMIC DATA ANALYSIS

Искусственный интеллект в анализе данных в экономике

Artificial intelligence (AI) has transformed economic data analysis by enabling the processing of large datasets and providing insights previously unattainable. As of 2023, the global AI market in economics and finance was valued at USD 63 billion and is expected to reach USD 123 billion by 2030, with a 15 % compound annual growth rate (CAGR) [1]. The focus on the U.S. economy in this study arises from its significant global economic impact and the vast amount of data available, which allows for a more comprehensive and reliable analysis using AI models. The primary objective is to evaluate how AI-driven methodologies, specifically in economic forecasting, demand prediction, credit scoring, and fraud detection, can enhance accuracy and efficiency in economic and financial analysis. By leveraging AI, this study aims to showcase improvements in these areas and highlight AI's potential for driving more effective economic policy and business decision-making.

AI is enhancing macroeconomic forecasting by allowing for more precise predictions of key indicators like GDP, inflation, and unemployment. Unlike traditional econometric models that rely on historical data, AI-driven time-series models can adjust to current economic conditions, improving adaptability in volatile markets. Machine learning