функционирования государственной экономики и обеспечения ее дальнейшего развития, что подчеркивает необходимость постоянного совершенствования процедур и механизмов их сбора и распределения.

Литература

1. Таможенный кодекс Евразийского экономического союза по состоянию на 2024 год. – Москва : Эксмо, 2024. – 480 с. – (Законы и кодексы).

2. Богданчук, В. П. Таможенные платежи: состав и место в доходах бюджета Республики Беларусь / В. П. Богданчук // Веснік Беларускага дзяржаўнага эканамічнага ўніверсітэта : навукова-практычны часопіс. – 2014. – № 4. – С. 64.

Modern customs and cybersecurity: securing digital infrastructures

Denisevich V. I., Yurchuk A. A., std. of II c. of School of Business of BSU, Scientific supervisor, Elovaya E. M., MA of Economics, Senior Lecturer

Advancing technologies and digitalization are transforming customs operations, improving efficiency, risk management, and transparency in global trade. Tools like automation, AI, and blockchain enhance processes but also bring new cybersecurity risks, such as cyberattacks that threaten trade security. Cybersecurity in customs involves protecting digital systems, networks, and data from threats like ransomware, phishing, data breaches, supply chain attacks, malware, and Denial-of-Service (DoS) attacks, all of which can disrupt operations and compromise data integrity.

Cyberattacks on customs systems have become more advanced and frequent. For example, in August 2024, Sable International, a UK-based firm, was attacked by a ransomware group, leading to data breaches and the shutdown of its servers. In another case, Orion, a Luxembourg-based carbon supplier, lost $60 million in a data breach caused by a Business Email Compromise (BEC) scheme. The FBI has identified BEC as one of the most damaging types of cybercrime, with losses totaling billions of dollars annually.

The global cost of cybercrime is expected to reach $23.84 trillion by 2027, underscoring the critical need for strong cybersecurity measures in customs systems. Digitalization, such as electronic customs declarations and automated systems, has streamlined operations and improved efficiency in countries like the U.S., where automated export systems are being implemented. However, digitalization also requires skilled staff, necessitating training in information technology and cybersecurity for customs personnel.

To safeguard customs data, several strategies should be implemented. These include encryption, multi-factor authentication (MFA), and the use of Public Key

Infrastructure (PKI) to secure data exchanges. Regular security audits can help identify vulnerabilities, while incident response and recovery plans ensure customs can quickly address cyberattacks and minimize disruptions. Collaboration with law enforcement and conducting training drills further strengthens cybersecurity efforts.

In conclusion, cybersecurity in customs is a strategic priority as digital systems become vital to global trade. For trade-dependent countries like Belarus, implementing robust measures such as encryption, real-time monitoring, and staff training is essential to safeguard customs data, support economic growth, and ensure national security.

Literature

1. LinkedIn: Cybersecurity in Modern Infrastructure: Guarding the Digital Fortresses of Tomorrow [Electronic resource]. – Mode of access: https://www.linkedin.com/pulse/cybersecurity-modern-infrastructure-guarding-digital-fortresses-goly-w8yme. – Date of access: 12.11.2024.

2. Nembrini [Electronic resource]: Introduction to Cybersecurity: Safeguarding Your Digital World. – Mode of access: https://www.nembrini.com/outlook/introduction-to-cybersecurity-safeguarding-your-digital-world/. – Date of access: 12.11.2024.

3. Statista [Electronic resource]: Cybercrime Expected To Skyrocket in Coming Years. – Mode of access: https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/. – Date of access: 12.11.2024.

4. Intelligent CIO [Electronic resource]: The role of cybersecurity in securing critical infrastructure. – Mode of access: https://www.intelligentcio.com/eu/2024/04/22/the-role-of-cybersecurity-in-securing-critical-infrastructure/. – Date of access: 12.11.2024.

5. United Nations Office for Disarmament Affairs [Electronic resource]: Protecting the cybersecurity of critical infrastructures and their supply chains. – Mode of access: https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/ICC-2024_Protecting-the-cybersecurity-of-critical-infrastructures-and-their-supply-chains.pdf. – Date of access: 12.11.2024.

6. Cyber Management Alliance [Electronic resource]: August 2024: Biggest Cyber Attacks, Data Breaches, Ransomware Attacks. – Mode of access: https://www.cm-alliance.com/cybersecurity-blog/august-2024-biggest-cyber-attacks-data-breaches-ransomware-attacks#DataBreach. – Date of access: 12.11.2024.