УДК 35.077.3

INFORMATION SECURITY RISK ANALYSIS IN INTEGRATING NATIONAL DATA IN INDONESIA: COMPARING WITH GOSUSLUGI SERVICES IN RUSSIA

Algar K. Dawam (ITMO), **Muhammad A. Rizki** (ITMO)

Scientific supervisor – Muhammad A. Rizki (ITMO)

Introduction. Information security in public services is a crucial issue in the digital era, especially in the management of national data that includes personal information of the population [1]. Indonesia faces great challenges in integrating national data due to the administrative system that is still scattered across various government agencies and public service facilities.

As a country that has advanced in the field of information security, Russia has implemented Gosuslugi, an integrated digital public service platform and as primary e-government portal with a high security system [2]. With this approach, population data is stored in one centrally managed system, enabling more efficient and secure data utilization. This study aims to analyze the challenges Indonesia faces in integrating national data and compare it with Russia's success in implementing a structured system such as Gosuslugi.

Main part. One of the main challenges in national data integration in Indonesia is the fragmentation of data storage systems across different government agencies and public services. These data silos cause inefficiencies in coordination and increase the risk of leakage due to the lack of unified security standards. In addition, uneven digital infrastructure and weak personal data protection regulations are major obstacles in building a secure and integrated administrative system. Underinvestment in cybersecurity technology also exacerbates the situation, leaving many institutions vulnerable to increasingly complex cyber threats.

In 2024, Indonesia experienced several major cyberattacks targeting government institutions and public services. The types of cybercrime that often occur in Indonesia include malware, phishing, DDoS, cyberstalking, fake identity, cyberbullying, and others [3]. One of the most significant cases is the attack on the national data center which resulted in service disruptions in various agencies. In addition, the attack on the Directorate General of Taxes resulted in data leaks of millions of individuals, including information on high-ranking state officials. Another incident involved the election commission's system, which suffered a DDoS attack during the election. This series of incidents shows that there are security gaps in Indonesia's digital administration system that must be fixed immediately. Cyberattacks can create vulnerabilities in critical infrastructure such as financial, health, and energy systems [4].

In comparison, Russia through Gosuslugi has successfully created an integrated public service system with high security. Citizen data is stored in one central system with strict access control, high-level encryption, and multi-factor authentication [2]. This approach enables efficiency in administration while ensuring maximum protection of citizens' personal data. Gosuslugi's success shows that secure national data integration can be achieved through careful planning, strict regulation, and investment in information security technology.

Conclusion. Based on the analysis conducted, it can be concluded that Indonesia faces major challenges in national data integration due to fragmented systems, weak data protection regulations, and lack of investment in cybersecurity. The cyberattacks that occurred in 2024 further emphasized the need for reform in national data management. In Russia, Gosuslugi has proven that a structured administrative system can improve the efficiency of public services while ensuring information security. Indonesia can learn from this model by strengthening data protection regulations, improving digital infrastructure, and implementing an integrated system to minimise the risk of personal information leakage.

List of references:

1. Alfi, M., Yundari, N.P., Tsaqif, A. Analisis Risiko Keamanan Siber dalam Transformasi Digital Pelayanan Publik di Indonesia (Cybersecurity Risk Analysis in the Digital Transformation of Public Services in Indonesia). Journal of Resilience Strategic Studies, 2023.
2. Gorelova, Y.S. E-government in Russia: Practices and Developments. MGIMO Journal of Society and The State, 2019.
3. Hapsari, R.D., Pambayun, K.G. Ancaman Cybercrime di Indonesia: Sebuah Tinjauan Pustaka Sistematis (Cybercrime Threats in Indonesia: Literatur Review). Journal of National Security, 2022.
4. Wati, D.S., Nurhaliza, S., Sari, M.W., Amallia, R. Dampak Cyber Crime Terhadap Keamanan Nasional dan Strategi Penanggulangannya: Ditinjau Dari Penegakan Hukum (The Impact of Cybercrime on National Security and Mitigation Strategies). Journal Bevinding, 2024.