

UNITED NATIONS
ESCAP
Economic and Social Commission for Asia and the Pacific



Expert Group Meeting on Transport Connectivity and Logistics: Emerging opportunities and challenges for enhancing rail connectivity along the Trans-Asian Railway network

29-30 April 2024, Bangkok

CYBERSECURITY



- Our information infrastructure utilizes various components to ensure network security and functionality. Our routers are protected by several security mechanisms, including password protection, access restriction based on IP addresses, and the use of SSH protocol for remote access. This allows us to effectively control access to network resources and protect the network from unauthorized intrusions.

- Our servers are constantly updated with antivirus software to detect and prevent malicious programs, as well as to protect the data stored on the servers. This is important for ensuring the reliability and integrity of our information system.

- We also use a firewall to protect our network and Internet access. The firewall controls data flows between internal and external networks, preventing unauthorized access and ensuring secure communication with the outside world.

- Our computers are also equipped with antivirus software to protect against malicious programs and other security threats. We place great importance on the security of our information infrastructure and regularly update and configure all our security mechanisms to ensure their effective operation.

Actions Planned to Strengthen Cybersecurity

- **Security Audit**: Conducting regular security audits to identify vulnerabilities in infrastructure and applications.



Employee Training:

- Training employees to comply with security policies, recognize phishing attacks, and other types of social engineering.



Monitoring and Analytics:

- Implementing monitoring and analytics systems for early detection of abnormal behavior and potential cyberattacks.



Penetration Testing:



- Regular penetration testing to verify the effectiveness of protective measures and identify potential weaknesses.

Railway cybersecurity is a critical area, especially with the increasing automation and digitization in the railway industry. It is important to understand that there are a variety of aspects that can be vulnerable to cyberattacks, including network infrastructure, train management systems, information systems, etc.

Cybersecurity issues in the railway industry in Tajikistan, as in many other countries, are becoming increasingly relevant in the context of digitization and automation. Railways play an important role in the economic development and social stability of the country, and their security should be a high priority.

Strengthening cybersecurity in the railway industry in Tajikistan requires a comprehensive approach that includes technical, organizational, and international aspects.



Thank you for your attention.