Ensuring information security in the railway industry

ANDREY APOLONIN
RUSSIAN RAILWAYS
## Characteristics of the information infrastructure of Russian Railways

<table>
<thead>
<tr>
<th></th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Railway branches</td>
<td>16</td>
</tr>
<tr>
<td>Computing centers</td>
<td>18</td>
</tr>
<tr>
<td>Length of infrastructure</td>
<td>&gt;9,000 km</td>
</tr>
<tr>
<td>IT infrastructure nodes</td>
<td>&gt;30,000</td>
</tr>
<tr>
<td>Systems</td>
<td>&gt;1,500</td>
</tr>
<tr>
<td>Information assets</td>
<td>&gt;500,000</td>
</tr>
<tr>
<td>Security events</td>
<td>&gt;1 million</td>
</tr>
<tr>
<td>Passengers per year</td>
<td>&gt;1 billion</td>
</tr>
</tbody>
</table>
Organisational structure

Chief Information Security Officer (CISO)

Head of Information Security Division

Ensuring the security of critical facilities
Ensuring the security of personal data
Protection of trade secrets
Protection of information from leaks through technical channels

Organising interaction with authorised government agencies and expert organisations

Экспертные организации в сфере обеспечения ИБ
Regulatory documentation on information security

Regulatory and legal basis for the concept of information security

Legal documents
- Federal Laws
- Codes of the Russian Federation
- Decrees and Orders of the President of the Russian Federation
- Resolutions of the Government of the Russian Federation

Organisational and legal documents
- Regulations
- Concept
- Guidelines, instructions
- Orders

Regulatory documents
- GOSTs
- International standards
- Guidance documents
- Special regulatory documents of FSTEC and FSS
Structure of the Information Security Management System of Russian Railways

**ISMS**

Information Security Management System

**People**

**Protection tools**

- Source code analysis
- Vulnerability scanners
- IS event management system
- L3 – L7 firewalls
- Virtual private networks
- EDR\XDR
- Application layer firewalls
- In-depth network packet analysis
- Antivirus defence system
- Intrusion prevention system
- Sandbox
- Access control for privileged users

**IS processes**
Security Operation Centre (SOC)

Automating response to security incidents (IRP/SOAR)

Incident management

Event collection and correlation system (SIEM)

Event management

Information on incidents

Information resources database (Asset Management)

Information base

2023

> 4,800,000 computer attacks

> 3,400,000 malicious mailings

> 600,000 attempted malware infections
Change of attack vector

Prolonged and intense unaddressed attacks

Short, intensive attacks masking another type of attack: vulnerability exploitation, malicious software

Targeted (address-based) attacks on ticketing services, website, rather than across the full range of IP addresses
Types of computer attacks (2022)

- Attempts to scan web services for vulnerabilities (Scanning) 20%
- Distributed denial-of-service (DDoS) attacks 29%
- Attacks on web services by using operating system commands (OS Commanding) 17%
- Malware injection attacks on web services to send phishing links to client devices (Cross-Site) 15%
- Other types of attacks 14%
- Attacks by injecting malicious codes into requests to Russian Railways web services databases (SQL Injection) 4%
- Brute-force attacks 1%
Types of computer attacks (2023)

- Distributed denial-of-service (DDoS) attacks (DDoS): 55%
- Attempts to scan web services for vulnerabilities (Scanning): 9%
- Attacks by injecting malicious codes into web services to send phishing links to client devices (Cross-Site): 5%
- Attacks by injecting malicious codes into requests to web services databases of Russian Railways (SQL Injection): 12%
- Other types of attacks: 1%
- Distributed denial-of-service (DDoS) attacks (DDoS): 55%

Changes from 2022:
- Attempts to scan web services for vulnerabilities (Scanning): -11%
- Attacks by injecting malicious codes into requests to web services databases of Russian Railways (SQL Injection): -10%
- Distributed denial-of-service (DDoS) attacks (DDoS): +26%
- Other types of attacks: +1%
Thank you!

Andrey Apolonin
Russian Railways