

# Ensuring information security in the railway industry

**ANDREY APOLONIN**
**RUSSIAN RAILWAYS**

# Characteristics of the information infrastructure of Russian Railways

**16**
Railway branches

**18**
Computing centers

**>9,000 km**
Length of infrastructure

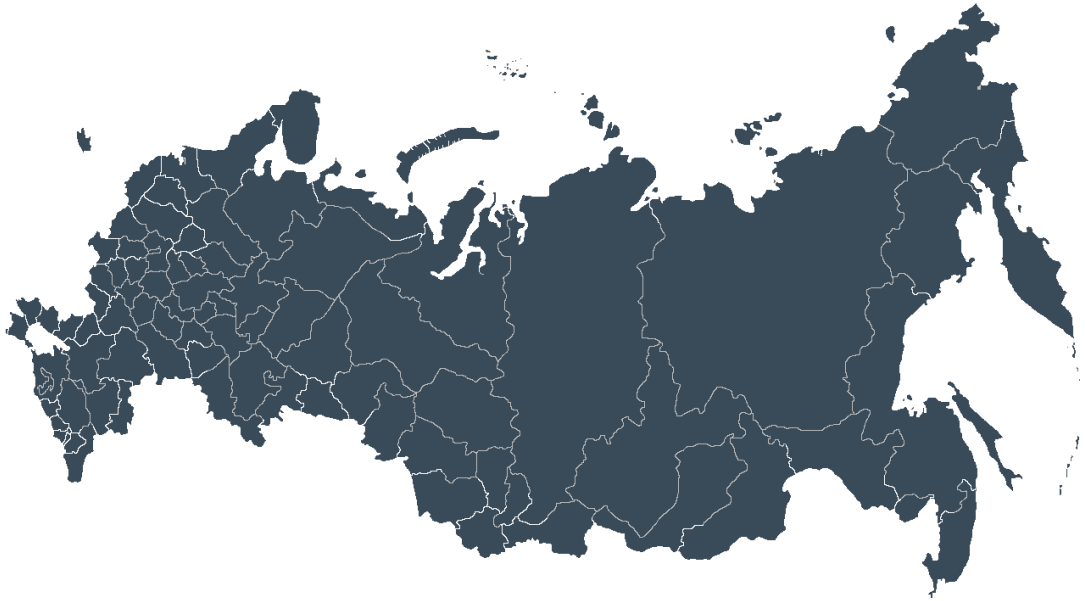
**>30,000**
IT infrastructure nodes

**>1,500**
Systems

**>500,000**
information assets (security event generation points – automated workstations, servers, information protection tools, etc.)

**>1 million**
security events

**>1 billion**
Passengers per year



# 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

НКЦКИ

ФСТЭК

МИНИСТЕРСТВО ТРАНСПОРТА РФ

Минцифры России

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

People



## ISMS

Information Security Management System

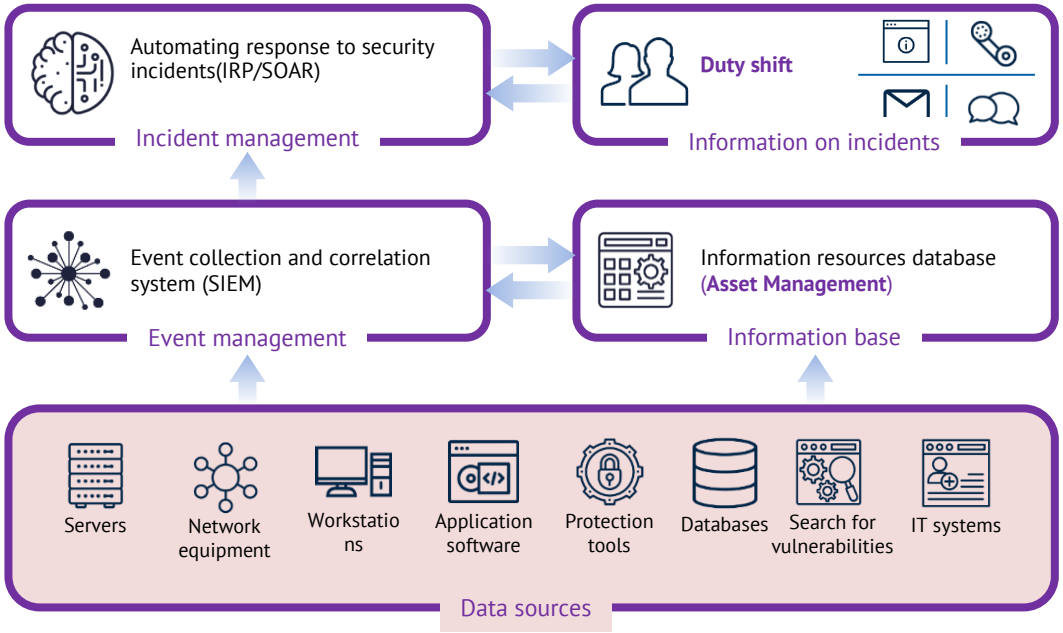


IS processes

- 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

Protection tools

# Security Operation Centre (SOC)




2023

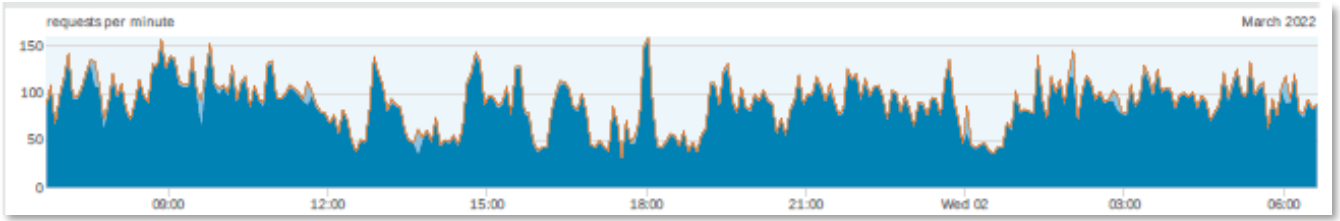
- > 4,800,000 computer attacks
- > 3,400,000 malicious mailings
- > 600,000 attempted malware infections

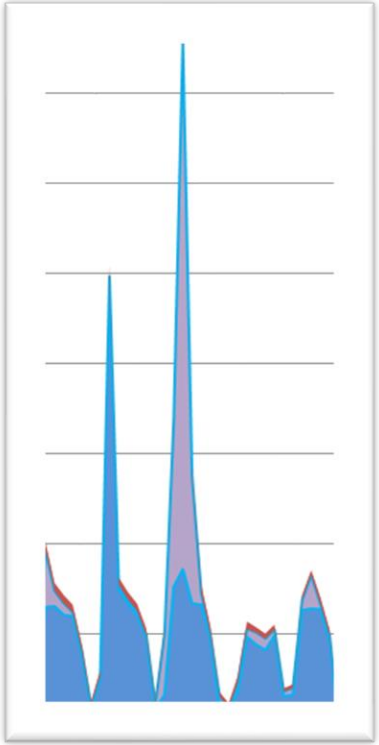
# Change of attack vector

Prolonged and intense unaddressed attacks

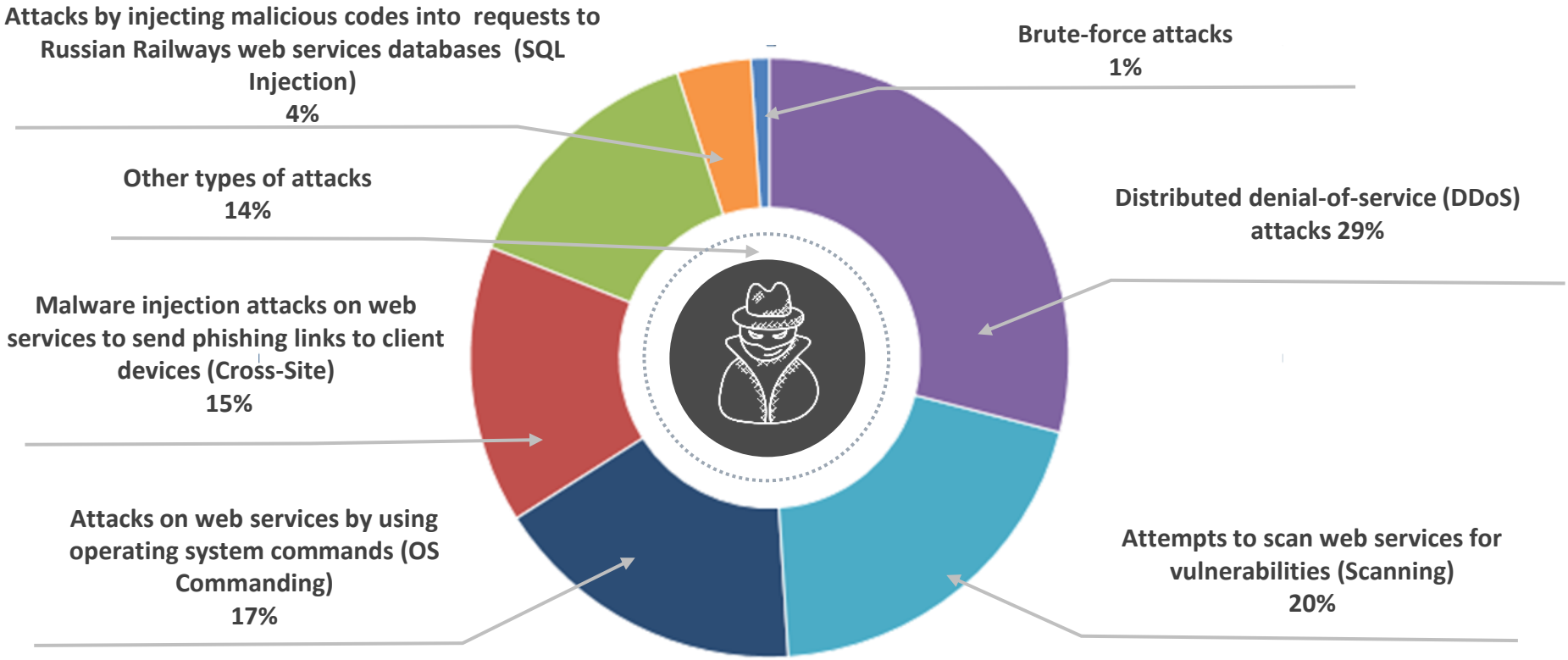
Short, intensive attacks masking another type of attack: vulnerability exploitation, malicious software

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

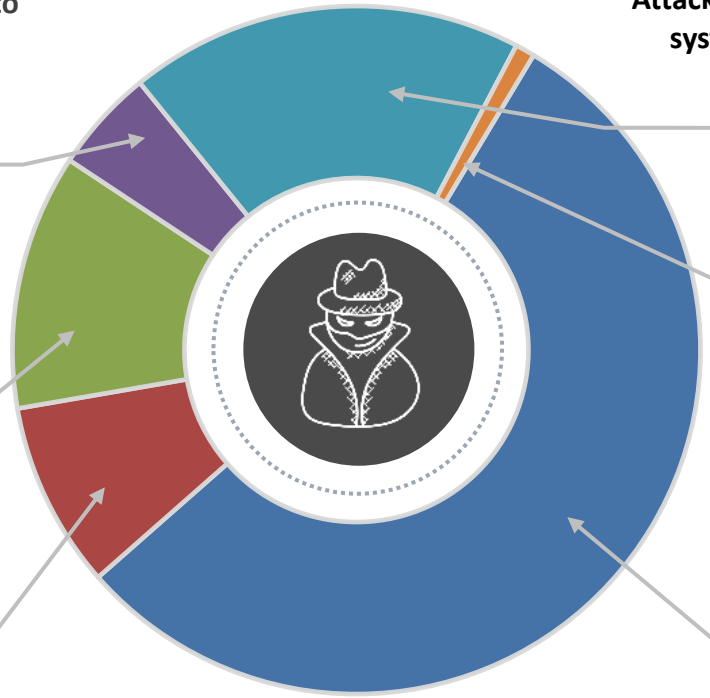


# Types of computer attacks (2022)



# Types of computer attacks (2023)



-10%

Attacks by injecting malicious codes into web services to send phishing links to client devices (Cross-Site)
5%

+8%

Attacks by injecting malicious codes into requests to web services databases of Russian Railways (SQL Injection)
12%

-11%

Attempts to scan web services for vulnerabilities (Scanning)
9%

Attacks on web services by using operating system commands (OS Commanding)
18%

+1%

Other types of attacks 1%

Distributed denial-of-service (DDoS) attacks (DDoS)
55%

+26%

**Thank you!**

Andrey Apolonin
Russian Railways