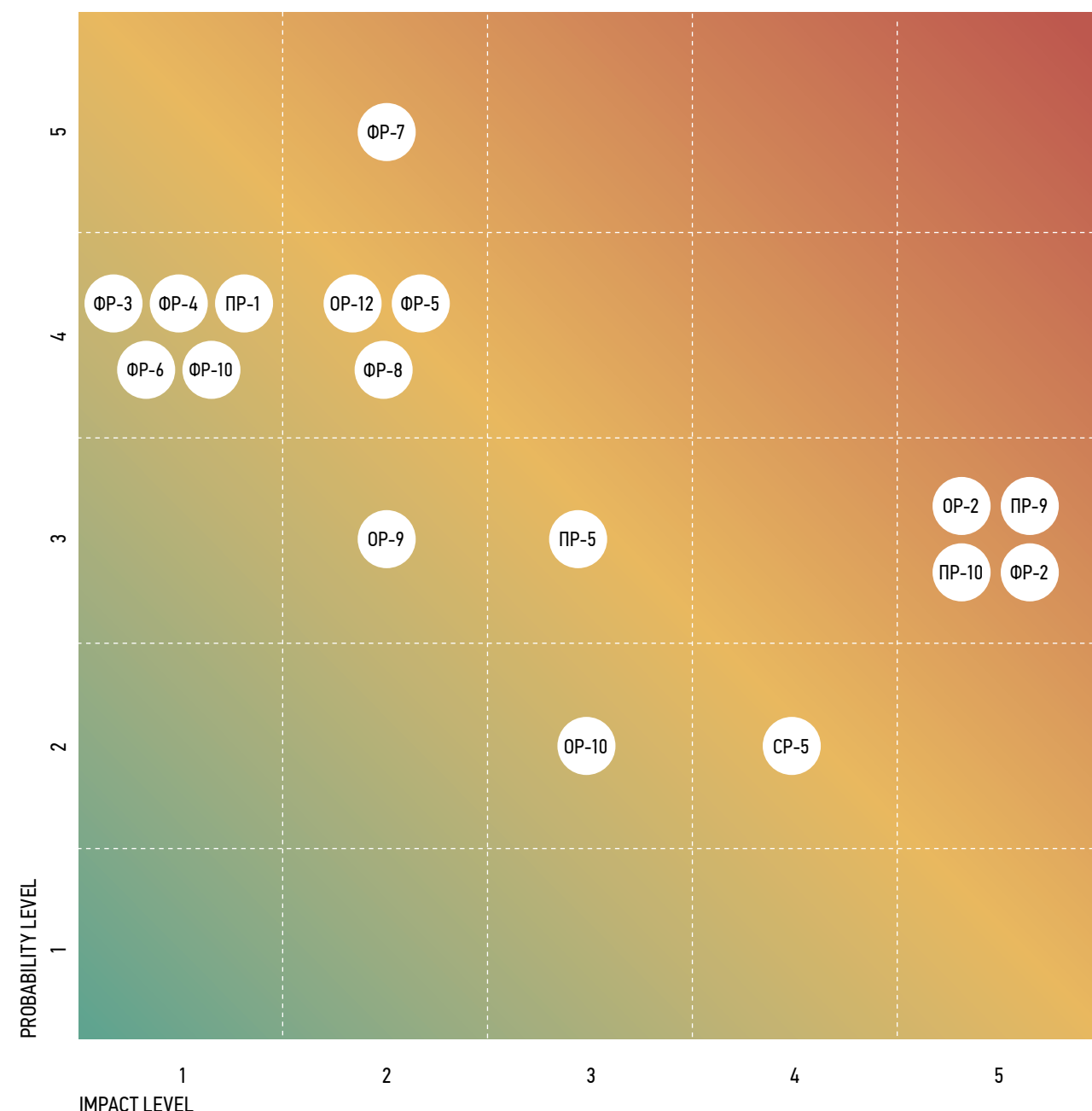


Map of key risks of the Company



## REALISATION OF KEY RISKS

Information on the realisation of critical and significant risks is reviewed by the Company's management bodies as part of the Report on the Organisation, Functioning and Effectiveness of the Company's Risk Management and Internal Control System (RM&ICS) for 2024.

# INFORMATION ON INFORMATION SECURITY RISKS AND CYBER THREATS

Due to a rise in cyber threats at the Company, the following information security risks were identified:

- Disruption and/or shutdown of the information infrastructure and telecommunication systems of power grid facilities caused by cyberattacks. This risk is assessed as significant due to the high level of consequences associated with disconnection of electricity consumers, material damage and reputational risks of the Company.
- Unauthorised access to confidential information. This risk is assessed as significant and characterised by a medium level of consequences in the form of leakage of information constituting a trade secret or personal data.

In order to reduce (minimise) the above risks, the Company takes the following measures:

- Installation of technical security equipment, video surveillance systems, access control system and security alarm system
- Organisation and control over the physical security of the Company's most important power grid facilities
- Renovation of security equipment at the power grid facilities as set forth in the Company's Investment Programme
- Inclusion of information security requirements in terms of reference for information infrastructure facilities and telecommunication systems of power grid facilities, control over the subsequent construction of facilities in compliance with the terms of reference
- Ongoing monitoring of the actions of the Company's employees through information security systems
- Monitoring and analysis of external information security events
- Use of certified information security means

