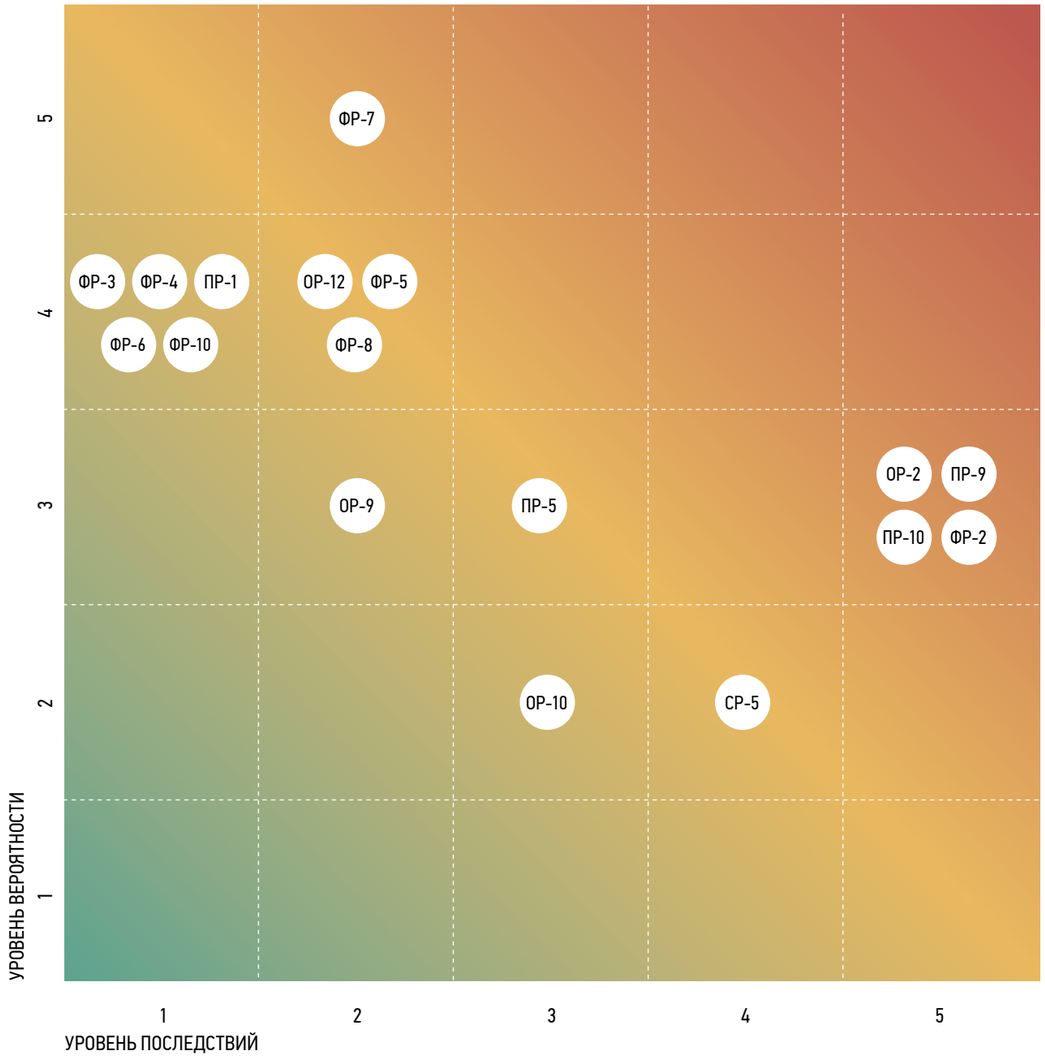
Карта ключевых рисков Общества



РЕАЛИЗАЦИЯ КЛЮЧЕВЫХ РИСКОВ

Информация о реализации критических и значимых рисков рассматривается органами управления Общества в рамках Отчета об организации, функционировании и эффективности системы управления рисками и внутреннего контроля Компании за 2024 г. (СУРиВК).

ИНФОРМАЦИЯ О РИСКАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И КИБЕРУГРОЗ

В условиях повышенного уровня киберугроз в Обществе идентифицированы следующие риски информационной безопасности:

- риск нарушения и/или прекращения функционирования объектов информационной инфраструктуры и телекоммуникационных систем объектов электросетевого комплекса, основным внешним фактором для которого являются кибератаки. Данный риск оценен как значимый ввиду высокого уровня последствий реализации риска, связанного с отключением потребителей электроэнергии, причинением материального ущерба и репутационными рисками Общества;
- риск неправомерного доступа к конфиденциальной информации. Данный риск оценен как значимый и характеризуется средним уровнем последствий реализации риска в виде утечки информации, составляющей коммерческую тайну, или персональных данных.

С целью снижения (минимизации) вышеуказанных рисков в Обществе ведется работа:

- по установке на объектах электроэнергетики инженерных средств охраны, систем видеонаблюдения, систем контроля удаленного доступа, охранной сигнализации;
- организации и контролю исполнения физической охраны наиболее важных объектов электросетевого комплекса Общества;
- реконструкции инженерно-технических средств охраны на объектах электросетевого комплекса в соответствии с Инвестиционной программой Общества;
- обеспечению включения требований по информационной безопасности в технические задания на создание объектов информационной инфраструктуры и телекоммуникационных систем объектов электросетевого комплекса, а также контролю последующей реализации объектов в соответствии с техническим заданием;
- осуществлению контроля на постоянной основе за действиями работников Общества посредством систем информационной безопасности;
- мониторингу и анализу внешних событий информационной безопасности;
- применению сертифицированных средств защиты информации.