К разделу «Управление рисками»

Риски в сфере кибербезопасности

Немаловажное место занимают риски, связанные с информационной безопасностью. В результате реализации угроз безопасности информации возможны нарушение или остановка предоставляемых ИТ-сервисов, технологических и производственных процессов Компании, в том числе утечка информации ограниченного доступа.

Основными факторами рисков, связанных с информационной безопасностью в информационной инфраструктуре ОАО «РЖД», рассматриваются не только действия третьих лиц, направленные на несанкционированный доступ к информации ОАО «РЖД» и его контрагентов, в том числе хакерские и вирусные атаки, но и на внутренние факторы, связанные с действиями работников и инструментарием по анализу и корреляции событий информационной безопасности.

Основными мероприятиями по обеспечению информационной безопасности ОАО «РЖД» являются:

- классификация, категорирование систем ОАО «РЖД», формирование модели угроз безопасности информации, формирование требований по защите информации (на основе классификационных признаков информационных активов, угроз безопасности информации, требований действующего законодательства Российской Федерации в области защиты информации);
- рациональная организация элементов информационной инфраструктуры ОАО «РЖД» с учетом необходимости в обеспечении безопасности информации, проектирование и внедрение в информационную инфраструктуру ОАО «РЖД» систем защиты информации, оценка соответствия систем требованиям безопасности информации;
- подготовка персонала ОАО «РЖД» по вопросам защиты информации;
- поддержание информационной безопасности информационных систем ОАО «РЖД» в процессе эксплуатации, выявление и обработка инцидентов информационной безопасности, проведение служебных расследований по нарушениям требований защиты информации;
- реализация документооборота в ОАО «РЖД» с учетом требований по защите информации;
- совершенствование нормативных документов ОАО «РЖД» в области защиты информации.

Для управления рисками в 2021 году были выполнены следующие мероприятия:

- формирование функциональных требований по созданию Единого центра мониторинга по информационной безопасности ОАО «РЖД»;
- организация выполнения мероприятий по развитию программно-аппаратных комплексов контроля доступа привилегированных и иных пользователей;
- организация выполнения мероприятий по анализу защищенности (тесты на проникновение, контроль защищенности, анализ исходного кода), по реализации требований по безопасности информации при создании и эксплуатации систем ОАО «РЖД»;
- развитие системы управления информационной безопасностью ОАО «РЖД» в части следующих ее элементов: системы антивирусной защиты, миграции программного комплекса по управлению информационной безопасностью систем ОАО «РЖД» на новую платформу, внедрения программного комплекса защиты от целевых атак, системы мониторинга и контроля передачи информации, внедрения программно-аппаратного комплекса системы контроля защищенности.

На 2022 год запланированы следующие мероприятия:

- организация работы по совершенствованию нормативной базы ОАО «РЖД» в части обеспечения информационной безопасности;
- организация работ по развитию системы управления информационной безопасностью ОАО «РЖД», по разработке и внедрению системы управления учетными данными, по тиражированию системы мониторинга и контроля каналов передачи информации, программно-аппаратных комплексов контроля доступа привилегированных и иных пользователей;
- реализация концепции по созданию Единого центра мониторинга по информационной безопасности ОАО «РЖД»;
- организация работ по внедрению контуров безопасности защиты информации типовых центров обработки данных ОАО «РЖД», модернизация централизованного узла доступа к информационным системам ОАО «РЖД»;
- внедрение программно-аппаратного комплекса для защиты от компьютерных атак типа «отказ в обслуживании» «Периметр».