Росжелдор: защита данных — приоритетная задача

Roszheldor: data protection is a priority

Сегодня без доступа к интересующей информации в любое время и в любом месте существование человека стало невозможным. При этом средства связи и коммуникации, а также все точки доступа потенциально уязвимы. Для защиты данных от утечки или хищения есть отрасль знания — информационная безопасность.

Информационная безопасность охватывает инструменты и процессы, которые организации применяют в качестве защиты информации.

Средства, обеспечивающие информационную безопасность, постоянно развиваются. Основные ее принципы — конфиденциальность, целостность, доступность, защита информации и информационной инфраструктуры от случайных или преднамеренных воздействий, предотвращение несанкционированного доступа, вирусных атак, утечек данных, блокирование работы критической информационной инфраструктуры объектов промышленности страны. Она включает в себя технические, организационные и правовые меры, содержащие широкий спектр вопросов, начиная от защиты сетей и инфраструктуры до тестирования и аудита.

Информационная безопасность — сфера, охватывающая множество областей, таких как физическая безопасность, безопасность конечных точек, шифрование данных, сетевая безопасность. Также требуется постоянное соблюдение мер информационной безопасности, которое защищает ее от таких угроз, как несанкционированный доступ к данным, фишинг и мошенничество, уязвимость в программном обеспечении, потеря данных из-за сбоев систем.

Указ Президента РФ от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» направлен на повышение устойчивости и безопасности информационных ресурсов страны.

Руководители федеральных органов исполнительной власти и других организаций обязаны обеспечить информационную безопасность своих структур. На руководителей органов и организаций возложена персональная ответственность за ее обеспечение.

С 1 января 2025 г. запрещается использовать средства защиты информации, произведенные в недружественных странах, а также пользоваться сервисами (работами, услугами) по обеспечению информационной безопасности, предоставляемыми (выполняемыми, оказываемыми) этими организациями.

Федеральное агентство железнодорожного транспорта (Росжелдор) находится под прямым действием Указа № 250. В связи с этим Росжелдор постоянно работает над решением вопросов обеспечения эффективных мер информационной безопасности своих ресурсов, защищая их от физического искажения или уничтожения; возможности несанкционированной (случайной или злоумыш-

ленной) модификации; несанкционированного (случайного и преднамеренного) получения информации лицами, для которых она не предназначена.

Защита персональных данных в государственных информационных системах Росжелдора выполняется с помощью организационных, технических мероприятий, плана контрольных мероприятий.

Государственные информационные системы Росжелдора аттестованы по требованиям информационной безопасности и соответствуют установленным стандартам для защиты данных и информационных ресурсов.

Приказом Федерального агентства железнодорожного транспорта от 22.07.2021 № 344 утверждены документы по информационной безопасности Росжелдора:

- концепция информационной безопасности центрального аппарата;
- политика информационной безопасности локальной вычислительной сети;
- политика использования сети интернет и электронной почты;
- регламент реагирования на инциденты информационной безопасности;
- регламент предоставления прав доступа к информации ограниченного доступа;
- порядок резервирования и восстановления работоспособности технических средств;
- инструкции по организации антивирусной и парольной защиты;
- инструкции администратора государственных информационных систем и администратора информационной безопасности;
- инструкция по учету и хранению машинных носителей конфиденциальной информации.

В конце декабря 2024 г. завершился тендер на оказание услуг по осуществлению мероприятий по обеспечению информационной безопасности Росжелдора.

В рамках технического сопровождения системы защиты информации Агентства исполнитель оказывает услуги органа криптографической защиты информации; администрирования средств защиты информации; проводит мероприятия, направленные на обеспечение безопасности информации, обрабатываемой Росжелдором.

Санкции повлияли на российский рынок информационной безопасности.

За 2024 г. количество кибератак на российские компании выросло в 2,5 раза, большинство из них приходится на организации отраслей критической информационной инфраструктуры страны. Это следствие кибервойны со стороны недружественных стран, в данных условиях важно осуществлять переход на отечественные средства защиты информации, чтобы эффективно отражать подобные атаки.

Одним из первых документов, описывающих национальные интересы в информационной сфере, стала Доктрина информационной безопасности РФ, утвержденная Указом Президента РФ от 05.12.2016 № 646.

Активные меры по импортозамещению компании стали применять с выходом Указа Президента РФ от 30.03.2022 № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации».

Информационная безопасность в России в условиях санкций продолжает развитие. Уход западных компаний дал возможность отечественным производителям программно-аппаратных комплексов развивать свои средства защиты, занимать новые ниши. Росжелдор успешно применяет новейшие решения в области информационной безопасности для решения вопросов сохранности данных и бесперебойной работы критической информационной инфраструктуры Агентства.

Заместитель руководителя
Федерального агентства
железнодорожного транспорта
Александр Олегович Иванов