3.6.Оценка выполнения Оператором обязанностей, установленных законодательством Российской Федерации в области персональных данных, а в случае выявления несоответствий – выработка рекомендаций по их устранению.
3.7.Организация подготовки и направления в уполномоченный орган по защите прав субъектов персональных данных Уведомления об обработке персональных данных, а в случае изменения сведений, содержащихся в Реестре операторов, осуществляющих обработку персональных данных, направление сведений о таких изменениях.
3.8.В случае выявления неправомерных действий с персональными данными, Комиссия направляет уведомление об устранении нарушений.
3.9.Анализ и оценка соответствия Требованиям законодательства типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных, а в случае выявления несоответствий – выработка рекомендаций по их устранению.
3.10.Анализ и оценка соответствия договорной базы Оператора Требованиям законодательства, а в случае выявления несоответствий – внесение соответствующих изменений и дополнений.
3.11.Контроль выполнения Требований законодательства, в части касающейся согласия субъектов персональных данных на обработку их персональных данных.
3.12.Общий контроль соблюдения Оператором требований по обеспечению безопасности персональных данных и соблюдения Требований законодательства.
3.13.Организация работ и сбор необходимых документов при прохождении федерального государственного контроля (надзора) за соответствием обработки персональных данных Требованиями законодательства.
3.14.Ведение журнала по учету проверок в соответствии с Требованиями законодательства.
3.15.Организация работ по разработке моделей угроз безопасности персональных данных при их обработке в информационных системах персональных данных Оператора, в том числе:
3.15.1.оценка полноты и правильности определения угроз безопасности;
3.15.2.плановый и внеплановый пересмотр.
3.16.Организация работ по созданию системы защиты персональных данных (комплекса организационно-технических мер), обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего уровня защищенности информационных систем персональных данных.
3.17.Проверка готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации.
Обучение лиц, применяющих средства защиты информации, правилам работы с ними.
3.18.Организация учета применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных.
3.19.Контроль выполнения мероприятий по защите персональных данных, реализуемых в рамках подсистем защиты с учетом уровня защищенности информационной системы персональных данных (не реже 1 раза в 3 года):
3.19.1.идентификация и аутентификация субъектов доступа и объектов доступа;
3.192.управление доступом субъектов доступа к объектам доступа;
3.19.3.ограничение программной среды;
3.19.4.защита машинных носителей информации, на которых хранятся и (или)
3.19.5.обрабатываются персональные данные (далее - машинные носители персональных данных);
3.19.6.регистрация событий безопасности;
3.19.7.антивирусная защита;
3.19.8.обнаружение (предотвращение) вторжений;
3.19.9.контроль (анализ) защищенности персональных данных;
3.19.10.обеспечение целостности информационной системы и персональных данных;
3.19.11.обеспечение доступности персональных данных;
3.19.12.защита среды виртуализации;
3.19.13.защита технических средств;
3.19.14.защита информационной системы, ее средств, систем связи и передачи данных;