УКАЗ

ГУБЕРНАТОРА ОМСКОЙ ОБЛАСТИ

1 февраля 2017 года № 10

г. Омск

Об отдельных мерах по обеспечению безопасности персональных данных при их обработке

В соответствии с частью 5 статьи 19 Федерального закона «О персональных данных» постановляю:

Утвердить прилагаемый Перечень угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных органов исполнительной власти Омской области, эксплуатируемых при осуществлении соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки.

Губернатор Омской области В.И. Назаров

Приложение
к Указу Губернатора Омской области
от 1 февраля 2017 года № 10

ПЕРЕЧЕНЬ
угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных органов исполнительной власти Омской области, эксплуатируемых при осуществлении соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки

1. Угрозы утечки информации по техническим каналам (в том числе угрозы утечки видовой информации).

2. Угрозы несанкционированного доступа к информации:

1) угрозы доступности и целостности информации из-за сбоев в программном обеспечении, выхода из строя технических средств, на которых размещается информационная система персональных данных (далее – ИСПДн);

2) угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа с применением стандартных функций (уничтожение, копирование, перемещение, форматирование носителей информации и т.п.) операционной системы или какой-либо прикладной программы (например, системы управления базами данных), с применением специально созданных для выполнения несанкционированного доступа программ (программ просмотра и модификации реестра, поиска текстов в текстовых файлах и т.п.);

3) угрозы безопасности персональных данных, реализуемые с использованием протоколов межсетевого взаимодействия:

- угрозы типа «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой ИСПДн из внешних сетей информации, а также передаваемой по локальной сети информации;
- угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений;
- угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях;
- угрозы подмены доверенного объекта;
- угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных как внутри локальной сети, так и во внешних сетях;
- угрозы выявления паролей;
- угрозы типа «Отказ в обслуживании»;
- угрозы удаленного запуска приложений;

4) угрозы несанкционированного доступа к информации при использовании среды виртуализации в ИСПДн;

5) угрозы, связанные с непреднамеренными действиями пользователей и нарушениями безопасности функционирования ИСПДн и системы защиты персональных данных в её составе из-за сбоев в программном обеспечении;

6) угрозы, связанные с преднамеренными действиями внутренних нарушителей.

Примечание. В связи с наличием при обработке персональных данных в ИСПДн органов исполнительной власти Омской области актуальных угроз безопасности, которые могут быть нейтрализованы только с помощью средств криптографической защиты информации, органам исполнительной власти Омской области, являющимся операторами ИСПДн, необходимо руководствоваться при разработке частных моделей угроз безопасности персональных данных для имеющихся ИСПДн положениями Методических рекомендаций по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в ИСПДн, эксплуатируемых при осуществлении соответствующих видов деятельности, утвержденных Федеральной службой безопасности Российской Федерации 31 марта 2015 года № 149/7/2/6-432.