

ПРИКАЗ

26.12.2024 № 06-02/116/24
г. Хабаровск

Об определении угроз безопасности персональных данных при обработке персональных данных в информационных системах персональных данных

Во исполнение Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных»

ПРИКАЗЫВАЮ:

1. Утвердить прилагаемый Перечень угроз безопасности персональных данных при их обработке в информационных системах персональных данных и методику определения угроз безопасности.
2. Контроль за исполнением приказа оставляю за собой.

Директор
МБУК «Камерный театр «Триада»



Гогольков В.С.

Перечень угроз безопасности персональных данных при их обработке в информационных системах персональных данных и методику определения угроз безопасности

1. Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе персональных данных, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.
2. Угрозами безопасности персональных данных при их обработке в информационных системах персональных данных, являются в том числе:
 - 2.1. угроза несанкционированного доступа к персональным данным лицами, обладающими полномочиями в информационной системе персональных данных, в том числе в ходе создания, эксплуатации, технического обслуживания и (или) ремонта, модернизации, снятия с эксплуатации информационной системы персональных данных;
 - 2.2. угроза воздействия вредоносного кода, внешнего по отношению к информационной системе персональных данных;
 - 2.3. угроза использования методов социального инжиниринга к лицам, обладающим полномочиями в информационной системе персональных данных;
 - 2.4. угроза несанкционированного доступа к отчуждаемым носителям персональных данных;
 - 2.5. угроза утраты (потери) носителей персональных данных, включая переносные персональные компьютеры пользователей информационной системы персональных данных;
 - 2.6. угроза несанкционированного доступа к персональным данным лицами, не обладающими полномочиями в информационной системе персональных данных, с использованием уязвимостей в организации защиты персональных данных;
 - 2.7. угроза несанкционированного доступа к персональным данным лицами, не обладающими полномочиями в информационной системе персональных данных, с использованием уязвимостей в программном обеспечении информационной системы персональных данных;
 - 2.8. угроза несанкционированного доступа к персональным данным лицами, не обладающими полномочиями в информационной системе персональных данных, с использованием уязвимостей в обеспечении защиты сетевого взаимодействия и каналов передачи данных;
 - 2.9. угроза несанкционированного доступа к персональным данным лицами, не обладающими полномочиями в информационной системе персональных данных, с использованием уязвимостей в обеспечении защиты вычислительных сетей информационной системы персональных данных;
 - 2.10. угроза несанкционированного доступа к персональным данным лицами, не обладающими полномочиями в информационной системе персональных данных, с использованием уязвимостей, вызванных несоблюдением требований по эксплуатации средств криптографической защиты информации.
3. Перечень актуальных угроз может быть дополнен на дополнительной оценке существующих актуальных угроз безопасности персональных данных.
4. В ходе оценки угроз безопасности информации должны быть определены негативные последствия, которые могут наступить от реализации (возникновения) угроз безопасности информации.

5. Должностное лицо Оператора, ответственное за организацию обработки персональных данных и обеспечение их безопасности, при необходимости проводит оценку угроз безопасности информации. Результаты оценки угроз безопасности информации отражаются в модели угроз, которая представляет собой описание систем и сетей и актуальных угроз безопасности информации.
6. Оценка угроз безопасности информации включает следующие этапы:
 - 6.1. определение негативных последствий, которые могут наступить от реализации (возникновения) угроз безопасности информации;
 - 6.2. определение возможных объектов воздействия угроз безопасности информации;
 - 6.3. оценку возможности реализации (возникновения) угроз безопасности информации и определение их актуальности.
7. Ответственным лицом за проведение оценки угроз является должностное лицо Оператора, ответственное за организацию обработки персональных данных и обеспечение их безопасности.

Директор
МБУК «Камерный театр «Триада»



Гогольков В.С.