ПРАВИТЕЛЬСТВО АМУРСКОЙ ОБЛАСТИ

ПОСТАНОВЛЕНИЕ

25.12.2023 № 1101

г. Благовещенск

Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в аппарате Губернатора области и Правительства области, органах исполнительной власти Амурской области и подведомственных им учреждениях

В соответствии с частью 5 статьи 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» Правительство Амурской области

п о с т а н о в л я е т :

1. Определить угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в аппарате Губернатора области и Правительства области, органах исполнительной власти Амурской области и подведомственных им учреждениях, согласно приложению к настоящему постановлению.

2. Контроль за исполнением настоящего постановления возложить на заместителя председателя Правительства Амурской области Пузанова П.И.

3. Настоящее постановление подлежит официальному опубликованию на «Официальном интернет-портале правовой информации» (www.pravo.gov.ru) и размещению на Портале Правительства Амурской области в информационно-телекоммуникационной сети Интернет (www.amurobl.ru).

Губернатор Амурской области В.А. Орлов

ПРАВИТЕЛЬСТВО АМУРСКОЙ ОБЛАСТИ
АППАРАТ ГУБЕРНАТОРА ОБЛАСТИ И ПРАВИТЕЛЬСТВА ОБЛАСТИ
Отдел регистрации и сопровождения правовых актов

Приложение
к постановлению Правительства
Амурской области
от 25.12.2013 № 1101

Угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в аппарате Губернатора области и Правительства области, органах исполнительной власти Амурской области и подведомственных им учреждениях

Угрозами безопасности персональных данных, актуальных (при наличии соответствующих технологий обработки персональных данных в информационных системах персональных данных) при обработке персональных данных в информационных системах персональных данных (далее – информационные системы), эксплуатируемых в аппарате Губернатора области и Правительства области, органах исполнительной власти Амурской области и подведомственных им учреждениях, являются:

1) угрозы, связанные с особенностями функционирования технических, программно-технических и программных средств, обеспечивающих хранение, обработку и передачу информации;

2) угрозы несанкционированного доступа (воздействия) к отчуждаемым носителям персональных данных, включая переносные персональные компьютеры пользователей информационных систем;

3) угрозы воздействия вредоносного кода и (или) вредоносной программы, внешних по отношению к информационным системам;

4) угрозы несанкционированного доступа (воздействия) к персональным данным лиц, обладающих полномочиями в информационных системах, в том числе в ходе создания, развития, ввода в эксплуатацию, эксплуатации, вывода из эксплуатации информационных систем и дальнейшего хранения содержащейся в их базах данных информации;

5) угрозы использования методов воздействия на лиц, обладающих полномочиями в информационных системах;

6) угрозы несанкционированного доступа (воздействия) к персональным данным лиц, не обладающих полномочиями в информационных системах, с использованием уязвимостей в организации защиты персональных данных;

7) угрозы несанкционированного доступа (воздействия) к персональным данным лиц, не обладающих полномочиями в информационных системах, с использованием уязвимостей в программном обеспечении информационных систем;

8) угрозы несанкционированного доступа (воздействия) к персональным данным лиц, не обладающих полномочиями в информационных системах, с использованием уязвимостей в обеспечении защиты сетевого взаимодействия и каналов передачи данных;

9) угрозы несанкционированного доступа (воздействия) к персональным данным лиц, не обладающих полномочиями в информационных системах, с использованием уязвимостей в обеспечении защиты вычислительных сетей информационных систем;

10) угрозы несанкционированного доступа (воздействия) к персональным данным лиц, не обладающих полномочиями в информационных системах, с использованием уязвимостей, вызванных несоблюдением требований по эксплуатации средств защиты информации;

11) угрозы целенаправленных действий с использованием аппаратных и (или) программных средств с целью нарушения безопасности защищаемых персональных данных с использованием средств криптографической защиты информации или создания условий для этого, определяемые операторами информационных систем в соответствии с составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности, утвержденными приказом Федеральной службы безопасности Российской Федерации от 10.07.2014 № 378;

12) угрозы перехвата передаваемой по каналам связи информации, содержащей персональные данные, или несанкционированного воздействия на эту информацию;

13) угрозы несанкционированного воздействия на персональные данные на носителях информации, доступ к которым не может быть исключен с помощью некриптографических методов и способов.