

**ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ПОСТАНОВЛЕНИЕ**

от \_\_\_\_\_ 201\_ г.

№ \_\_\_\_\_

г. Москва

**О требованиях к защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных**

В соответствии со статьей 19 Федерального закона «О персональных данных» Правительство Российской Федерации **постановляет:**

1. Утвердить прилагаемые Требования к защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных.

2. Признать утратившим силу постановление Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» (Собрание законодательства Российской Федерации, 2007, № 48, ст. 6001).

Председатель Правительства  
Российской Федерации

В. Путин

Утверждено  
Постановлением Правительства  
Российской Федерации  
от \_\_\_\_\_ 201\_ г. № \_\_\_\_

**ТРЕБОВАНИЯ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ  
ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ  
ПЕРСОНАЛЬНЫХ ДАННЫХ, ИСПОЛНЕНИЕ КОТОРЫХ  
ОБЕСПЕЧИВАЕТ УСТАНОВЛЕННЫЕ УРОВНИ ЗАЩИЩЕННОСТИ  
ПЕРСОНАЛЬНЫХ ДАННЫХ**

1. Настоящий документ устанавливает требования к защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных (далее – Требования).

2. Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия в отношении персональных данных при их обработке в информационной системе.

Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные и технические меры, а также использование средств защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии. Указанные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

Для обеспечения безопасности персональных данных при их обработке в информационных системах осуществляется защита речевой информации и информации, обрабатываемой техническими средствами, а также информации, представленной в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, магнитно-оптической и иной основе.

3. Работы по созданию (модернизации) системы защиты персональных данных являются неотъемлемой частью работ по созданию информационной системы, ее эксплуатации или модернизации.

4. Средства защиты информации, применяемые в информационных системах, в установленном порядке проходят процедуру оценки соответствия.

5. К средствам защиты информации, предназначенным для обеспечения безопасности персональных данных при их обработке в информационных системах, прилагаются правила пользования этими средствами, согласованные с Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации в пределах их полномочий.

Изменение условий применения средств защиты информации, предусмотренных указанными правилами, возможно только с письменного разрешения указанных федеральных органов исполнительной власти в пределах их полномочий.

6. Средства защиты информации, предназначенные для обеспечения безопасности персональных данных при их обработке в информационных системах, подлежат учету с использованием индексов или условных наименований и регистрационных номеров. Перечень индексов, условных наименований и регистрационных номеров определяется Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации в пределах их полномочий.

7. Особенности разработки, производства, реализации и эксплуатации шифровальных (криптографических) средств и предоставления услуг по шифрованию персональных данных при их обработке в информационных системах устанавливаются Федеральной службой безопасности Российской Федерации.

8. Размещение информационных систем, специальное оборудование и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

9. Безопасность персональных данных при их обработке в информационной системе обеспечивает оператор или лицо, осуществляющее

обработку персональных данных по поручению оператора (далее – уполномоченное лицо). Существенным условием договора между оператором и уполномоченным лицом является обязанность уполномоченного лица обеспечить безопасность персональных данных при их обработке в информационной системе.

10. Для разработки и осуществления мероприятий по обеспечению безопасности персональных данных при их обработке в информационной системе оператором или уполномоченным лицом может назначаться структурное подразделение или должностное лицо (работник), ответственные за обеспечение безопасности персональных данных.

11. Лица, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим персональным данным на основании списка, утвержденного оператором или уполномоченным лицом.

12. Запросы пользователей информационной системы на получение персональных данных, включая лиц, указанных в пункте 11 настоящих Требований, а также факты предоставления персональных данных по этим запросам регистрируются автоматизированными средствами информационной системы в электронном журнале обращений, защищенном от несанкционированного доступа к его содержанию. Содержание электронного журнала обращений периодически проверяется соответствующими должностными лицами (работниками) оператора или уполномоченного лица.

13. Операторами организуется и проводится периодический контроль (оценка) выполнения настоящих Требований.

Контроль (оценка) проводится операторами самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации.

Сроки периодического контроля (оценки) выполнения Требований определяются оператором. Контроль (оценка) выполнения Требований осуществляется не реже одного раза в два года.