МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 44796
от "20" декабря 2016.

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО НАДЗОРУ В СФЕРЕ ЗАЩИТЫ ПРАВ ПОТРЕБИТЕЛЕЙ И БЛАГОПОЛУЧИЯ ЧЕЛОВЕКА (РОСПОТРЕБНАДЗОР)

П Р И К А З

28.11.2016 № 1172

Москва

О внесении изменений в Положение об обработке и защите персональных данных в Роспотребнадзоре, утвержденное приказом Роспотребнадзора от 23.12.2013 № 964

Руководствуясь статьями 18.1 и 19 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3451; 2009, № 48, ст. 5716, № 52, ст. 6439; 2010, № 27, ст. 3407, № 31, ст. 4173, № 31, ст. 4196, № 49, ст. 6409; 2011, № 23, ст. 3263, № 31, ст. 4701; 2013, № 14, ст. 1651, № 30, ст. 4038, № 51, ст. 6683; 2014, № 23, ст. 2927, № 30, ст. 4217, № 30, ст. 4243), Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденными приказом ФСТЭК России от 11 февраля 2013 г. № 17 (зарегистрирован Минюстом России 31.05.2013, регистрационный номер 28608), Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденными приказом ФСТЭК России от 18 февраля 2013 г. № 21 (зарегистрирован Минюстом России 14.05.2013, регистрационный номер 28375),

п р и к а з ы в а ю:

1. Внести изменения в Положение об обработке и защите персональных данных в Роспотребнадзоре, утвержденное приказом Роспотребнадзора от 23.12.2013 № 964 (зарегистрирован в Минюсте России 25.04.2014, регистрационный номер 32122), согласно приложению.

2. Контроль за исполнением настоящего приказа возложить на заместителя руководителя Роспотребнадзора Б.П. Кузькина.

Руководитель А.Ю. Попова

Управление делами
Управление делами Козлова Л. И

Приложение

УТВЕРЖДЕНЫ
приказом Роспотребнадзора
от 28.11.2016 № 1172

Изменения
в Положение об обработке и защите персональных данных в Роспотребнадзоре, утвержденное приказом Роспотребнадзора от 23.12.2013 № 964

1. В главе VII «Порядок обработки персональных данных субъектов персональных данных в информационных системах»:

1.1. Пункт 7.1. изложить в следующей редакции:

«7.1. Обработка персональных данных в информационных системах осуществляется после реализации организационных и технических мер по обеспечению безопасности персональных данных, определенных с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

Обеспечение безопасности при обработке персональных данных, содержащихся в информационных системах органов и подведомственных организаций осуществляется в соответствии с постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»[1], Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденными приказом ФСТЭК России от 11 февраля 2013 г. № 17[2], Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденными приказом ФСТЭК России от 18 февраля 2013 г. № 21[3].»;

1.2. Дополнить пунктами 7.5.-7.9. следующего содержания:

«7.5. Меры по обеспечению безопасности персональных данных принимаются для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

7.6. В состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом

---

[1] Собрание законодательства Российской Федерации, 2012, № 45, ст. 6257

[2] Зарегистрирован Минюстом России 31.05.2013, регистрационный номер 28608

[3] Зарегистрирован Минюстом России 14.05.2013, регистрационный номер 28375

актуальных угроз безопасности персональных данных и применяемых информационных технологий, входят:

идентификация и аутентификация субъектов доступа и объектов доступа;

управление доступом субъектов доступа к объектам доступа;

ограничение программной среды;

защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные;

регистрация событий безопасности;

антивирусная защита;

обнаружение (предотвращение) вторжений;

контроль (анализ) защищенности персональных данных;

обеспечение целостности информационной системы и персональных данных;

обеспечение доступности персональных данных;

защита среды виртуализации;

защита технических средств;

защита информационной системы, ее средств, систем связи и передачи данных;

выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных, и реагирование на них;

управление конфигурацией информационной системы и системы защиты персональных данных.

7.7. Согласно пункту 6 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119, 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, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.

Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.

Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных

(недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

Определение типа угроз безопасности персональных данных, актуальных для информационной системы, производится с учетом оценки возможного вреда, проведенной во исполнение пункта 5 части 1 статьи 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»[4].

7.8. В соответствии с пунктом 11 статьи 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» под уровнем защищенности персональных данных понимается комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

При обработке персональных данных в информационных системах устанавливаются 4 уровня защищенности персональных данных.

7.8.1. Необходимость обеспечения 1-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает либо специальные категории персональных данных, либо биометрические персональные данные, либо иные категории персональных данных;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

7.8.2. Необходимость обеспечения 2-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает общедоступные персональные данные;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

в) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает биометрические персональные данные;

г) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

---

[4] Собрание законодательства Российской Федерации, 2006, № 31, ст. 3451; 2009, № 48, ст. 5716, № 52, ст. 6439; 2010, № 27, ст. 3407, № 31, ст. 4173, № 31, ст. 4196, № 49, ст. 6409; 2011, № 23, ст. 3263, № 31, ст. 4701; 2013, № 14, ст. 1651, № 30, ст. 4038, № 51, ст. 6683; 2014, № 23, ст. 2927, № 30, ст. 4217, № 30, ст. 4243

д) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

е) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

7.8.3. Необходимость обеспечения 3-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные сотрудников оператора или общедоступные персональные данные менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

в) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

г) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает биометрические персональные данные;

д) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

7.8.4. Необходимость обеспечения 4-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает общедоступные персональные данные;

б) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

7.9. Состав и содержание мер по обеспечению безопасности персональных данных, необходимых для обеспечения каждого из уровней защищенности персональных данных, приведены в приложении к Составу и содержанию

организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденными приказом ФСТЭК России от 18 февраля 2013 г. № 21[5].»;

2. Дополнить главой XI следующего содержания:

«XI. Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

11.1. Целью осуществления внутреннего контроля соответствия обработки персональных данных в органах и подведомственных организациях требованиям к защите персональных данных (далее – внутренний контроль) является соблюдение в органах и подведомственных организациях законодательства Российской Федерации в области персональных данных, в том числе требований к защите персональных данных.

11.2. Внутренний контроль подразделяется на плановый и внеплановый.

11.3. Внутренний контроль осуществляется лицом, ответственным за организацию обработки персональных данных, либо комиссией, образуемой приказом органа или подведомственной организации, в состав которой входят: лицо, ответственное за организацию обработки персональных данных; лица, уполномоченные на обработку персональных данных.

11.4. Плановый внутренний контроль проводится на основании плана, утвержденного руководителем органа или подведомственной организации.

Периодичность планового внутреннего контроля – не реже одного раза в год.

Срок проведения планового внутреннего контроля составляет не менее 10 рабочих дней.

11.5. Внеплановый внутренний контроль проводится по решению лица, ответственного за организацию обработки персональных данных:

на основании поступившего в орган или подведомственную организацию в письменной форме или в форме электронного документа заявления субъекта персональных данных о нарушении законодательства в области персональных данных, а также устного обращения;

в связи с проведением в органе или подведомственной организации государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных.

Внеплановый внутренний контроль может проводиться на основании решения руководителя органа или подведомственной организации.

11.6. Внеплановый внутренний контроль должен быть завершен не позднее чем через месяц со дня принятия решения о его проведении.

11.7. Результаты внутреннего контроля оформляются в виде справки.

---

[5] Зарегистрирован Минюстом России 14.05.2013, регистрационный номер 28375

11.8. При выявлении в ходе внутреннего контроля нарушений в справке отражается перечень мероприятий по устранению выявленных нарушений и сроки их устранения.

11.9. О результатах внутреннего контроля и мерах, необходимых для устранения выявленных нарушений, руководителю органа или подведомственной организации докладывает лицо, ответственное за организацию обработки персональных данных.

11.10. В отношении персональных данных, ставших известными лицу, ответственному за организацию обработки персональных данных, или членам комиссии в ходе проведения внутреннего контроля, соблюдается конфиденциальность и обеспечивается безопасность при их обработке.».