МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
(МИНЮСТ РОССИИ)

ПРИКАЗ

Москва

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 48666
от "25" октября 2017 г.

23 октября 2017 г. № 208

Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных Министерства юстиции Российской Федерации, эксплуатируемых при осуществлении Министерством юстиции Российской Федерации и его территориальными органами функций, определенных Указом Президента Российской Федерации от 13.10.2004 № 1313 «Вопросы Министерства юстиции Российской Федерации»

В соответствии с частью 5 статьи 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (Собрание законодательства Российской Федерации, 2006, № 31 (ч. 1), ст. 3451; 2009, № 48, ст. 5716, № 52 (ч. 1), ст. 6439; 2010, № 27, ст. 3407, № 31, ст. 4173, ст. 4196, № 49, ст. 6409, № 52 (ч. 1), ст. 6974; 2011, № 23, ст. 3263, № 31, ст. 4701; 2013, № 14, ст. 1651, № 30 (ч. 1), ст. 4038, № 51, ст. 6683; 2014, № 23, ст. 2927, № 30 (ч. 1), ст. 4217, ст. 4243; 2016, № 27 (ч. 1), ст. 4164; 2017, № 9, ст. 1276, № 27, ст. 3945, № 31 (ч. 1), ст. 4772) и Указом Президента Российской Федерации от 13.10.2004 № 1313 «Вопросы Министерства юстиции Российской Федерации» (Собрание законодательства Российской Федерации, 2004, № 42, ст. 4108; 2005, № 44, ст. 4535, № 52 (ч. 3), ст. 5690; 2006, № 12, ст. 1284, № 19, ст. 2070, № 23, ст. 2452, № 38, ст. 3975, № 39, ст. 4039; 2007, № 13, ст. 1530, № 20, ст. 2390; 2008, № 10 (ч. 2), ст. 909, № 29 (ч. 1), ст. 3473, № 43, ст. 4921; 2010, № 4, ст. 368, № 19, ст. 2300; 2011, № 21, ст. 2927, ст. 2930, № 29, ст. 4420; 2012, № 8, ст. 990, № 18, ст. 2166, № 22, ст. 2759, № 38, ст. 5070, № 47, ст. 6459, № 53 (ч. 2), ст. 7866; 2013, № 26, ст. 3314, № 49 (ч. 7), ст. 6396, № 52 (ч. 2), ст. 7137; 2014, № 26 (ч. 2), ст. 3515, № 50, ст. 7054; 2015, № 14, ст. 2108, № 19, ст. 2806, № 37, ст. 5130; 2016, № 1 (ч. 2), ст. 207, ст. 211, № 19, ст. 2672, № 51, ст. 7357; 2017, № 16, ст. 2397, № 17, ст. 2549) п р и к а з ы в а ю:

1. Определить угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных Министерства юстиции Российской Федерации, эксплуатируемых при осуществлении Министерством юстиции Российской Федерации и его территориальными органами функций, определенных Указом Президента Российской Федерации от 13.10.2004 № 1313 «Вопросы Министерства юстиции Российской Федерации» (далее – Угрозы, информационные системы соответственно), согласно приложению.

2. Департаменту организации и контроля (А.В. Чумаков), Департаменту управления делами (С.В. Буйволов), ФБУ НЦПИ при Минюсте России (А.В. Федичев) определять угрозы безопасности персональных данных при их обработке в информационных системах исходя из Угроз с учетом структурно-функциональных характеристик информационных систем.

3. Контроль за исполнением настоящего приказа возложить на первого заместителя Министра О.А. Плохого.

Министр А.В. Коновалов

ПРИЛОЖЕНИЕ
к приказу Министерства юстиции
Российской Федерации
от 23.10.2017 № 208

Угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных Министерства юстиции Российской Федерации, эксплуатируемых при осуществлении Министерством юстиции Российской Федерации и его территориальными органами функций, определенных Указом Президента Российской Федерации от 13.10.2004 № 1313 «Вопросы Министерства юстиции Российской Федерации»

1. Угрозами безопасности персональных данных, актуальными при обработке персональных данных в информационных системах персональных данных Министерства юстиции Российской Федерации, эксплуатируемых при осуществлении Министерством юстиции Российской Федерации и его территориальными органами функций, определенных Указом Президента Российской Федерации от 13.10.2004 № 1313 «Вопросы Министерства юстиции Российской Федерации» (далее – информационные системы), являются:

угрозы безопасности персональных данных, защищаемых без использования средств криптографической защиты информации (далее – СКЗИ);

угрозы целенаправленных действий с использованием аппаратных и (или) программных средств с целью нарушения безопасности защищаемых с использованием СКЗИ персональных данных или создания условий для этого[1].

2. Угрозы безопасности персональных данных, защищаемых без использования СКЗИ, включают:

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

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

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

---

[1] Состав и содержание 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, утвержденные приказом ФСБ России от 10.07.2014 № 378 (зарегистрирован Минюстом России 18.08.2014, регистрационный № 33620).

4) угрозы использования методов социального инжиниринга к лицам, обладающим полномочиями в информационных системах;

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

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 системном и прикладном 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, в том числе с использованием протоколов межсетевого взаимодействия;

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, связанные с возможностью использования новых информационных технологий (технологии виртуализации, беспроводные технологии, облачные технологии, технологии удаленного доступа и иные новые технологии).

3. Угрозы целенаправленных действий с использованием аппаратных и (или) программных средств с целью нарушения безопасности защищаемых с использованием СКЗИ персональных данных или создания условий для этого включают:

1) угрозы проведения атаки при нахождении вне контролируемой зоны;

2) угрозы проведения на этапах разработки (модернизации), производства, хранения, транспортировки СКЗИ и этапе ввода в эксплуатацию СКЗИ (пусконаладочные работы) атаки путем внесения несанкционированных изменений в СКЗИ и (или) в компоненты аппаратных и программных средств, совместно с которыми штатно функционируют СКЗИ и которые в совокупности представляют среду функционирования СКЗИ (далее – СФ), а также которые способны повлиять

на выполнение предъявляемых к СКЗИ требований, в том числе с использованием вредоносных программ;

3) угрозы проведения атак на этапе эксплуатации СКЗИ на:

а) ключевую, аутентифицирующую и парольную информацию СКЗИ;

б) программные компоненты СКЗИ;

в) аппаратные компоненты СКЗИ;

г) программные компоненты СФ, включая базовую систему ввода (вывода) (BIOS);

д) аппаратные компоненты СФ;

е) данные, передаваемые по каналам связи;

4) угрозы получения из находящихся в свободном доступе источников (включая информационно-телекоммуникационные сети, доступ к которым не ограничен определенным кругом лиц, в том числе информационно-телекоммуникационную сеть «Интернет») информации об информационных системах, в которых используются СКЗИ:

а) общих сведений об информационных системах, в которых используются СКЗИ (назначение, состав, оператор, объекты, в которых размещены ресурсы информационных систем);

б) сведений об информационных технологиях, базах данных, аппаратных средствах (далее – АС), программном обеспечении (далее – ПО), используемых в информационных системах совместно с СКЗИ, за исключением сведений, содержащихся только в конструкторской документации на информационные технологии, базы данных, АС, ПО, используемые в информационных системах совместно с СКЗИ;

в) содержания находящейся в свободном доступе документации на аппаратные и программные компоненты СКЗИ и СФ;

г) общих сведений о защищаемой информации, используемой в процессе эксплуатации СКЗИ;

д) сведений о каналах связи, по которым передаются защищаемые СКЗИ персональные данные;

е) сведений, получаемых в результате анализа любых сигналов от аппаратных компонентов СКЗИ и СФ;

5) угрозы применения специально разработанных АС и ПО;

6) угрозы использования на этапе эксплуатации в качестве среды переноса от субъекта к объекту (от объекта к субъекту) атаки действий, осуществляемых при подготовке и (или) проведении атаки каналов распространения сигналов, сопровождающих функционирование СКЗИ и СФ;

7) угрозы проведения атаки при нахождении в пределах контролируемой зоны;

8) угрозы проведения атак на этапе эксплуатации СКЗИ на:

а) документацию на СКЗИ и компоненты СФ;

б) помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем, на которых реализованы СКЗИ и СФ;

9) угрозы получения в рамках предоставленных полномочий, а также в результате наблюдений:

а) сведений о физических мерах защиты объектов, в которых размещены ресурсы информационных систем;

б) сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационных систем;

в) сведений о мерах по разграничению доступа в помещения, в которых находятся средства вычислительной техники, на которых реализованы СКЗИ и СФ;

10) угрозы физического доступа к средствам вычислительной техники, на которых реализованы СКЗИ.