Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, являющихся подсистемами федеральной государственной информационной системы "Автоматизированная информационная система Федеральной службы судебных приставов", и информационных системах персональных данных, не являющихся подсистемами федеральной государственной информационной системы "Автоматизированная информационная система Федеральной службы судебных приставов"

Приказ · № 264 · от 21.11.2019 · Министерство юстиции · Действует без изменений

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

МОСКВА

---

21 ноября 2019 г. № 264

Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, являющихся подсистемами федеральной государственной информационной системы "Автоматизированная информационная система Федеральной службы судебных приставов", и информационных системах персональных данных, не являющихся подсистемами федеральной государственной информационной системы "Автоматизированная информационная система Федеральной службы судебных приставов"

Зарегистрирован Минюстом России 9 декабря 2019 г.
Регистрационный № 56737

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; 2018, № 1 (ч. 1), ст. 82) и Указом Президента Российской Федерации от 13.10.2004 № 1313 "Вопросы Министерства юстиции Российской Федерации" (Собрание законодательства Российской Федерации, 2004, № 42, ст. 4108; 2018, № 44, ст. 6713) приказываю:

1. Определить угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, являющихся подсистемами федеральной государственной информационной системы "Автоматизированная информационная система Федеральной службы судебных приставов", и информационных системах персональных данных, не являющихся подсистемами федеральной государственной информационной системы "Автоматизированная информационная система Федеральной службы судебных приставов", эксплуатируемых при осуществлении Федеральной службой судебных приставов функций, определенных Указом Президента Российской федерации от 13.10.2004 № 1316 "Вопросы Федеральной службы судебных приставов" (далее - Угрозы, информационные системы соответственно), согласно приложению.

2. Федеральной службе судебных приставов (Д.В.Аристов) при определении угроз безопасности персональных данных при их обработке в информационных системах руководствоваться Угрозами с учетом структурно-функциональных характеристик информационных систем.

3. Признать утратившим силу приказ Минюста России от 09.08.2017 № 142 "Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, являющихся подсистемами федеральной государственной информационной системы "Автоматизированная информационная система Федеральной службы судебных приставов", и информационных системах персональных данных, не являющихся подсистемами федеральной государственной информационной системы "Автоматизированная информационная система Федеральной службы судебных приставов", эксплуатируемых при осуществлении Федеральной службой судебных приставов функций по обеспечению установленного порядка деятельности судов, исполнению судебных актов, актов других органов и должностных лиц" (зарегистрирован Минюстом России 15.08.2017, регистрационный № 47782).
4. Контроль за исполнением настоящего приказа возложить на статс-секретаря - заместителя Министра В.В.Федорова.

Министр А.В.Коновалов

ПРИЛОЖЕНИЕ
к приказу Министерства юстиции
Российской Федерации
от 21 ноября 2019 г. № 264

Угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, являющихся подсистемами федеральной государственной информационной системы "Автоматизированная информационная система Федеральной службы судебных приставов", и информационных системах персональных данных, не являющихся подсистемами федеральной государственной информационной системы "Автоматизированная информационная система Федеральной службы судебных приставов", эксплуатируемых при осуществлении Федеральной службой судебных приставов функций, определенных Указом Президента Российской Федерации от 13.10.2004 № 1316 "Вопросы Федеральной службы судебных приставов"

1. Угрозами безопасности персональных данных, актуальными при обработке персональных данных в информационных системах персональных данных, являющихся подсистемами федеральной государственной информационной системы "Автоматизированная информационная система Федеральной службы судебных приставов", и информационных системах персональных данных, не являющихся подсистемами федеральной государственной информационной системы "Автоматизированная информационная система Федеральной службы судебных приставов" 1 , эксплуатируемых при осуществлении Федеральной службой судебных приставов функций, определенных Указом Президента Российской Федерации от 13.10.2004 № 1316 "Вопросы Федеральной службы судебных приставов" (далее - информационные системы), являются:
угрозы безопасности персональных данных, защищаемых без использования средств криптографической защиты информации (далее - СКЗИ);
угрозы реализации целенаправленных действий с использованием аппаратных и (или) программных средств с целью нарушения безопасности защищаемых с использованием СКЗИ персональных данных или создания условий для этого 2 .

---

1 Перечень информационных систем персональных данных Федеральной службы судебных приставов, утвержденный приказом ФССП России от 17.07.2015 № 354 "Об обработке персональных данных в Федеральной службе судебных приставов" (зарегистрирован Минюстом России 07.08.2015, регистрационный № 38405), с изменениями, внесенными приказами ФССП России от 29.06.2016 №

395 (зарегистрирован Минюстом России 20.07.2016, регистрационный № 42921) и от 07.11.2016 № 589 (зарегистрирован Минюстом России 25.11.2016, регистрационный № 44440).
2 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).

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 лицами, обладающими полномочиями в информационных системах, в том числе в ходе создания, эксплуатации, технического обслуживания и (или) ремонта, модернизации, снятия с эксплуатации информационных систем;
3) угрозы воздействия вредоносного кода, вредоносной программы;
4) угрозы использования социального и психологического воздействия 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 лицами, не обладающими полномочиями в информационных системах, с использованием уязвимостей в организации защиты персональных данных;
7) угрозы несанкционированного доступа (воздействия) к персональным данным лицами, не обладающими полномочиями в информационных системах, с использованием уязвимостей в системном и прикладном программном обеспечении информационных систем;
8) угрозы несанкционированного доступа (воздействия) к персональным данным лицами, не обладающими 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 лицами, не обладающими полномочиями в информационных системах, с использованием уязвимостей в обеспечении защиты вычислительных сетей информационных систем;
10) угрозы несанкционированного доступа (воздействия) к персональным данным лицами, не обладающими полномочиями в информационных системах, с использованием уязвимостей, вызванных несоблюдением требований по эксплуатации средств защиты информации;
11) угрозы, связанные с возможностью использования новых информационных технологий.
3. Угрозы реализации 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 лица вне пространства, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств (далее - контролируемая зона);
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 в совокупности представляющие среду функционирования СКЗИ (далее - СФ), 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);
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 которой используется 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 конструкторских документах на информационные технологии, базы данных, АС, ПО, используемые в информационных системах совместно с СКЗИ;
в) содержания находящихся в свободном доступе документов 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 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 лицом при нахождении в пределах контролируемой зоны;
8) угрозы несанкционированного доступа на этапе эксплуатации СКЗИ на объекты:
а) документов 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.