ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ФИНАНСОВОМУ МОНИТОРИНГУ
(РОСФИНМОНИТОРИНГ)

ПРИКАЗ

06.02.2019 № 30

Москва

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 55945
от "06" сентября 2019 г.

Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных государственной информационной системы «Единая информационная система Федеральной службы по финансовому мониторингу», эксплуатируемых при осуществлении Федеральной службой по финансовому мониторингу и ее территориальными органами функций, определенных Указом Президента Российской Федерации от 13 июня 2012 г. № 808 «Вопросы Федеральной службы по финансовому мониторингу»

В соответствии с частью 5 статьи 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, 4196, № 49, ст. 6409, № 52, ст. 6974; 2011, № 23, ст. 3263, № 31, ст. 4701; 2013, № 14, ст. 1651, № 30, ст. 4038, № 51, ст. 6683; 2014, № 23, ст. 2927, № 30, ст. 4217, 4243; 2016, № 27, ст. 4164; 2017, № 9, ст. 1276, № 27, ст. 3945 № 31, ст. 4772, 2018, № 1, ст.82) и Указом Президента Российской Федерации от 13 июня 2012 г. № 808 «Вопросы Федеральной службы по финансовому мониторингу» (Собрание

законодательства Российской Федерации, 2012, № 25, ст. 3314, № 45, ст. 6211; 2013, № 52 , ст. 7137; 2015, № 4, ст. 641; 2016, № 11, ст. 1522) приказываю:

определить угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных государственной информационной системы «Единая информационная система Федеральной службы по финансовому мониторингу», эксплуатируемых при осуществлении Федеральной службой по финансовому мониторингу и ее территориальными органами функций, определенных Указом Президента Российской Федерации от 13 июня 2012 г. № 808 «Вопросы Федеральной службы по финансовому мониторингу», согласно приложению.

Директор Ю.А. Чиханчин

Приложение
к приказу Федеральной службы
по финансовому мониторингу
от 06.02.2018 г. № 30

Угрозы
безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных государственной информационной системы «Единая информационная система Федеральной службы по финансовому мониторингу», эксплуатируемых при осуществлении Федеральной службой по финансовому мониторингу и ее территориальными органами функций, определенных Указом Президента Российской Федерации от 13 июня 2012 г. № 808 «Вопросы Федеральной службы по финансовому мониторингу»

1. Угрозами безопасности персональных данных, актуальными при обработке персональных данных в информационных системах персональных данных, являющихся подсистемами государственной информационной системы «Единая информационная система Федеральной службы по финансовому мониторингу»[1], эксплуатируемых при осуществлении Федеральной службой по финансовому мониторингу и ее территориальными органами функций по противодействию легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения, а также функции национального центра по оценке угроз национальной безопасности, возникающих в результате совершения операций (сделок) с денежными средствами или иным имуществом, и по выработке мер противодействия этим угрозам (далее – информационные системы) являются:

[1] Государственная информационная система «Единая информационная система Федеральной службы по финансовому мониторингу» создана на основании пункта 18 Положения о Федеральной службе по финансовому мониторингу, утвержденного Указом Президента Российской Федерации от 13 июня 2012 г. № 808 «Вопросы Федеральной службы по финансовому мониторингу».

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].

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;

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

5) угрозы несанкционированного доступа (воздействия) к персональным данным лиц, не обладающих полномочиями в информационных системах, с использованием уязвимостей в обеспечении защиты сетевого взаимодействия

---

[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).

и каналов передачи данных, в том числе с использованием протоколов межсетевого взаимодействия;

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

7) 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 лицами, обладающими административными полномочиями в информационных системах;

8) 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 (далее – атака) включают:

1) угрозы проведения атаки 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 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);

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 конструкторской документации и эксплуатационных документов на аппаратные и программные компоненты СКЗИ и СФ, включающих сведения о составе, характеристиках, устройстве, условиях и правилах эксплуатации конкретных технических средств и систем обработки и защиты информации;

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 доступных для перехвата 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) эксплуатационную и техническую документацию на СКЗИ и компоненты СФ;

б) помещения, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ, и 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 и СФ.