МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 65519
от "21" октября 2021 г.

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ГОСУДАРСТВЕННЫМ РЕЗЕРВАМ (РОСРЕЗЕРВ)

П Р И К А З

13.09.2021 Москва № 201

Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных Федерального агентства по государственным резервам, эксплуатируемых при осуществлении Федеральным агентством по государственным резервам и его территориальными органами функций, определенных постановлением Правительства Российской Федерации от 23.07.2004 № 373 «Вопросы Федерального агентства по государственным резервам»

В целях реализации части 5 статьи 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3451; 2011, № 31, ст. 4701), в соответствии с подпунктом 9.9 пункта 9 Положения о Федеральном агентстве по государственным резервам, утвержденного постановлением Правительства Российской Федерации от 23.07.2004 № 373 (Собрание законодательства Российской Федерации, 2004, № 31, ст. 3263; 2017, № 1, ст. 175), 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 Федерального агентства по государственным резервам, эксплуатируемых при осуществлении Федеральным агентством по государственным резервам и его территориальными органами функций, определенных постановлением Правительства Российской Федерации от 23.07.2004 № 373 «Вопросы Федерального агентства по государственным резервам» (далее – информационные системы), согласно приложению к настоящему приказу.

2. Управлению защиты государственной тайны Федерального агентства по государственным резервам, Административному управлению Федерального агентства по государственным резервам, федеральному государственному казенному учреждению Главный информационно-вычислительный центр Федерального агентства по государственным резервам 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 заместителя руководителя Федерального агентства по государственным резервам, координирующего вопросы обеспечения защиты государственной тайны и режима секретности.

Руководитель Д.Ю. Гогин

Приложение
к приказу Федерального агентства
по государственным резервам
от 13.09.2021 № 201

Угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных Федерального агентства по государственным резервам, эксплуатируемых при осуществлении Федеральным агентством по государственным резервам и его территориальными органами функций, определенных постановлением Правительства Российской Федерации от 23.07.2004 № 373 «Вопросы Федерального агентства по государственным резервам»

1. Угрозами безопасности персональных данных, актуальными при обработке персональных данных в информационных системах персональных данных Федерального агентства по государственным резервам, эксплуатируемых при осуществлении Федеральным агентством по государственным резервам и его территориальными органами функций, определенных постановлением Правительства Российской Федерации от 23.07.2004 № 373 «Вопросы Федерального агентства по государственным резервам» (далее – информационные системы), являются:

1.1. Угрозы безопасности персональных данных, защищаемых без использования средств криптографической защиты информации (далее – СКЗИ).

1.2. 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] 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 Министерством юстиции Российской Федерации 18.08.2014, регистрационный № 33620).

2.1. Угрозы, связанные с особенностями функционирования технических, программно-технических и программных средств, обеспечивающих хранение, обработку и передачу информации.

2.2. Угрозы несанкционированного доступа (воздействия) к персональным данным лицами, обладающими 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.

2.3. Угрозы воздействия вредоносного кода и (или) вредоносной программы, внешних по отношению к информационным системам.

2.4. Угрозы использования методов социального и психологического воздействия к лицам, обладающим полномочиями в информационных системах.

2.5. Угрозы несанкционированного доступа (воздействия) к отчуждаемым носителям персональных данных, включая переносные персональные компьютеры пользователей информационных систем.

2.6. Угрозы несанкционированного доступа (воздействия) к персональным данным лицами, не обладающими полномочиями в информационных системах, с использованием уязвимостей в организации защиты персональных данных.

2.7. 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.

2.8. 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.

2.9. Угрозы несанкционированного доступа (воздействия) к персональным данным лицами, не обладающими полномочиями в информационных системах, с использованием уязвимостей в обеспечении защиты вычислительных сетей информационных систем.

2.10. 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.

2.11. Угрозы, связанные с возможностью использования новых информационных технологий.

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:

3.1. 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).

3.2. Угрозы проведения атаки 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.

3.3. 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.

3.4. 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.

3.5. Угрозы применения специально разработанных АС и ПО.

3.6. 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.

3.7. Угрозы проведения атаки лицом при нахождении в пределах контролируемой зоны.

3.8. Угрозы несанкционированного доступа 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.

3.9. 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;

3.10. Угрозы использования штатных средств информационных систем персональных данных, ограниченных мерами, реализованными в информационной системе, в которой используется СКЗИ.

3.11. Угрозы физического доступа к средствам вычислительной техники, на которых реализованы СКЗИ и СФ.