Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в сферах деятельности, нормативно-правовое регулирование которых осуществляется Федеральным архивным агентством

В соответствии с частью 5 статьи 19 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и пунктом 1 Положения о Федеральном архивном агентстве, утвержденного Указом Президента Российской Федерации от 22 июня 2016 г. № 293, **п р и к а з ы в а ю**:

определить угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в сферах деятельности, нормативно-правовое регулирование которых осуществляется Федеральным архивным агентством, согласно приложению к настоящему приказу.

Руководитель А.Н. Артизов

Приложение
к приказу Федерального архивного агентства
от «____» _____ 20___ г. №_____

Угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в сферах деятельности, нормативно-правовое регулирование которых осуществляется Федеральным архивным агентством

1. Угрозами безопасности персональных данных, актуальными при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в сферах деятельности, нормативно-правовое регулирование которых осуществляется Федеральным архивным агентством (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. 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 доступа к государственным информационным системам, автоматизированным и информационным системам (далее - информационные системы), в ходе создания, ввода в эксплуатацию, эксплуатации, технического обслуживания и (или) ремонта, модернизации, вывода из эксплуатации информационных систем и дальнейшего хранения содержащейся в их базах данных информации;

3) угрозы воздействия вредоносного кода и (или) вредоносной программы;

4) угрозы использования социального и психологического воздействия на лиц, обладающих правами доступа к информационным системам, правами доступа к администрированию программных, программно-аппаратных средств, средств защиты информации, входящих в состав информационных систем;

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

6) угрозы несанкционированного доступа к персональным данным лицами, не обладающими правами доступа к информационным системам, правами доступа администрирования программных, программно-аппаратных средств,

средств защиты информации, входящих в состав информационных систем, с использованием уязвимостей:

в организации защиты персональных данных;

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

в обеспечении защиты вычислительных сетей информационных систем, вызванных несоблюдением требований по эксплуатации средств защиты информации;

7) угрозы, связанные с возможностью использования новых информационных технологий (технологии виртуализации, беспроводные технологии, облачные технологии, технологии удаленного доступа).

3. Для 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 актуальными являются угрозы:

1) проведения атак нарушителями, находящимися вне пространства, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств (далее – контролируемая зона);

2) проведения на этапах разработки (модернизации), производства, хранения, транспортировки СКЗИ и этапе ввода в эксплуатацию СКЗИ (пусконаладочные работы) атаки путем внесения несанкционированных изменений в СКЗИ, документацию на СКЗИ и (или) в компоненты аппаратных и программных средств, совместно с которыми штатно функционируют СКЗИ и которые в совокупности представляют среду функционирования СКЗИ, которые способны повлиять на выполнение предъявляемых к СКЗИ требований, в том числе с использованием вредоносных программ;

3) проведения атак на этапе эксплуатации СКЗИ на:

персональные данные;

ключевую, аутентифицирующую и парольную информацию СКЗИ;

программные компоненты СКЗИ;

аппаратные компоненты СКЗИ;

программные компоненты среды функционирования СКЗИ, включая базовую систему ввода (вывода);

аппаратные компоненты среды функционирования СКЗИ;

данные, передаваемые по каналам связи;

4) 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:

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

сведений об информационных технологиях, базах данных, аппаратных средствах, программном обеспечении, используемых в информационных

системах совместно с СКЗИ, за исключением сведений, содержащихся только в конструкторских документах на информационные технологии, базы данных, аппаратные средства, программное обеспечение, используемые в информационных системах совместно с СКЗИ;

содержания конструкторской документации на СКЗИ;

содержания документации на аппаратные и программные компоненты СКЗИ и среду функционирования СКЗИ;

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

сведений о каналах связи, по которым передаются персональные данные, защищаемые с использованием СКЗИ;

сведений, получаемых в результате анализа сигналов от аппаратных компонентов СКЗИ и среды функционирования СКЗИ;

5) применения специально разработанных аппаратных средств и программного обеспечения;

6) 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 среды функционирования СКЗИ;

7) проведения атаки при нахождении в пределах контролируемой зоны;

8) проведения атак на этапе эксплуатации СКЗИ и несанкционированный доступ к следующим объектам:

документаций на СКЗИ и компоненты среды функционирования СКЗИ;

помещениям, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем, на которых реализованы СКЗИ и среда функционирования СКЗИ;

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

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

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

сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы;

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

10) получения несанкционированного физического доступа к средствам вычислительной техники, на которых реализованы СКЗИ и среда функционирования СКЗИ;

11) связанные с наличием у нарушителя аппаратных компонентов СКЗИ и среды функционирования СКЗИ, реализованных в информационных системах, в которых используются СКЗИ.