



**МИНИСТЕРСТВО ТРУДА И СОЦИАЛЬНОЙ ЗАЩИТЫ НАСЕЛЕНИЯ
РЯЗАНСКОЙ ОБЛАСТИ**

ПОСТАНОВЛЕНИЕ

от 19 апреля 2018 года № 19

Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных министерства труда и социальной защиты населения Рязанской области, эксплуатируемых при осуществлении соответствующих видов деятельности министерства труда и социальной защиты населения Рязанской области

В соответствии с частью 5 статьи 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» министерство труда и социальной защиты населения Рязанской области ПОСТАНОВЛЯЕТ:

1. Определить угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных министерства труда и социальной защиты населения Рязанской области, эксплуатируемых при осуществлении соответствующих видов деятельности министерства труда и социальной защиты населения Рязанской области, согласно приложению.

2. Признать утратившими силу постановление министерства труда и занятости населения Рязанской области Рязанской области от 15.07.2013 № 6 «Об определении актуальных угроз безопасности персональных данных в информационных системах персональных данных государственных учреждений службы занятости населения Рязанской области и мер по против».

3. Контроль за исполнением настоящего постановления возложить на начальника управления информационной и аналитической работы министерства труда и социальной защиты населения Рязанской области.

Министр

В.С. Емец

Приложение

к постановлению
министерства труда и социальной
защиты населения Рязанской области
от 19.04.2018 № 19

Угрозы безопасности персональных данных,
актуальные при обработке персональных данных в информационных системах
персональных данных министерства труда и социальной защиты населения
Рязанской области, эксплуатируемых при осуществлении соответствующих
видов деятельности министерства труда и социальной защиты населения
Рязанской области

1. Угрозами безопасности персональных данных, актуальными при обработке персональных данных в информационных системах персональных данных министерства труда и социальной защиты населения Рязанской области, эксплуатируемых при осуществлении министерством труда и социальной защиты населения Рязанской области функций, определенных постановлением Правительства Рязанской области от 11.10.2017 № 243 «Об утверждении Положения о министерстве труда и социальной защиты населения Рязанской области», 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 этого¹.

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;

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 N 33620).

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 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;

б) 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.