МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ВЕТЕРИНАРНОМУ И ФИТОСАНИТАРНОМУ НАДЗОРУ (Россельхознадзор)

П Р И К А З

от 4 марта 2026 года **№** 256

Москва

Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных Федеральной службы по ветеринарному и фитосанитарному надзору, эксплуатируемых при осуществлении Федеральной службой по ветеринарному и фитосанитарному надзору функций, определенных законодательством Российской Федерации

В соответствии с частью 5 статьи 19 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и пунктом 1 Положения о Федеральной службе по ветеринарному и фитосанитарному надзору, утвержденного постановлением Правительства Российской Федерации от 30 июня 2004 г. № 327, 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 Федеральной службы по ветеринарному и фитосанитарному надзору, эксплуатируемых при осуществлении Федеральной службой по ветеринарному и фитосанитарному надзору функций, определенных законодательством Российской Федерации, согласно приложению к настоящему приказу.

Руководитель С.А. Данкверт

Приложение
к приказу Федеральной службы по ветеринарному и фитосанитарному надзору
от 04.03.2026 г. № 256

Угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных Федеральной службы по ветеринарному и фитосанитарному надзору, эксплуатируемых при осуществлении Федеральной службой по ветеринарному и фитосанитарному надзору функций, определенных законодательством Российской Федерации

1. Угрозами безопасности персональных данных, актуальными при обработке персональных данных в информационных системах персональных данных Федеральной службы по ветеринарному и фитосанитарному надзору, эксплуатируемых при осуществлении Федеральной службой по ветеринарному и фитосанитарному надзору функций, определенных законодательством Российской Федерации (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[1].

2. Для персональных данных, защищаемых без использования СКЗИ, актуальными являются угрозы, связанные с:

1) особенностями функционирования технических, программно-технических и программных средств, обеспечивающих хранение, обработку и передачу информации;

2) несанкционированным доступом к персональным данным лицами,

[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 июля 2014 г. № 378 (зарегистрирован Минюстом России 18 августа 2014 г., регистрационный № 33620).

обладающими пользовательскими правами доступа к информационным системам, правами доступа к администрированию программных, программно-аппаратных средств, средств защиты информации, входящих в состав информационных систем, в ходе создания, эксплуатации, технического обслуживания и (или) ремонта, модернизации, вывода из эксплуатации информационных систем;

3) воздействием вредоносного кода, вредоносной программы;

4) использованием 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) несанкционированным доступом к отчуждаемым носителям персональных данных, включая переносные персональные компьютеры пользователей информационных систем;

6) воздействием на отчуждаемые носители персональных данных, включая переносные персональные компьютеры пользователей информационных систем;

7) несанкционированным доступом к персональным данным лицами, не обладающими правами доступа к информационным системам, правами доступа к администрированию программных, программно-аппаратных средств, средств защиты информации, входящих в состав информационных систем, с использованием уязвимостей:

в организации защиты персональных данных;

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

8) использованием 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:

1) угрозы проведения атак нарушителями, находящимися 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, 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) угрозы 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) 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:

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) угрозы применения специально разработанных аппаратных средств и программного обеспечения;

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 среды функционирования СКЗИ;

7) угрозы проведения атаки при нахождении в пределах контролируемой зоны;

8) угрозы проведения атак на этапе эксплуатации СКЗИ на:

документацию на СКЗИ и компоненты среды функционирования СКЗИ;

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 среда функционирования СКЗИ;

9) угрозы 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 разграничению доступа в помещения, в которых находятся средства вычислительной техники, на которых реализованы СКЗИ и среда функционирования СКЗИ;

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

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