КОМИТЕТ СОЦИАЛЬНОЙ ЗАЩИТЫ НАСЕЛЕНИЯ ВОЛГОГРАДСКОЙ ОБЛАСТИ

ПРИКАЗ

29.09.2020 № 2103

Волгоград

Об определении перечня угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении деятельности комитета социальной защиты населения Волгоградской области

В соответствии с частью 5 статьи 19 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных", п р и к а з ы в а ю:

1. Определить перечень угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении деятельности комитета социальной защиты населения Волгоградской области (далее - перечень), согласно приложению.

2. Отделу информационных технологий определять угрозы безопасности персональных данных при их обработке в информационных системах исходя из перечня с учетом структурно-функциональных характеристик информационных систем.

3. Контроль за исполнением настоящего приказа возложить на заместителя председателя комитета А.Ю. Завражина.

4. Настоящий приказ вступает в силу со дня его подписания и подлежит официальному опубликованию.

Председатель комитета Л.Ю. Заботина

Приложение
к приказу комитета социальной
защиты населения Волгоградской области
от 29.09.2020 № 2103

Перечень угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении деятельности комитета социальной защиты населения Волгоградской области

1. Угрозами безопасности персональных данных, актуальными при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении деятельности комитета социальной защиты населения Волгоградской 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 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 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) внесение несанкционированных изменений в документацию на СКЗИ

и компоненты СФ;

4) проведение на этапе эксплуатации атаки из информационно-телекоммуникационных сетей, доступ к которым не ограничен определенным кругом лиц, если информационные системы, в которых используются СКЗИ, имеют выход в эти сети;

5) 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;

ж) персональные данные;

6) угрозы применения специально разработанных АС и ПО;

7) использование на этапе эксплуатации находящихся за пределами контролируемой зоны АС и ПО из состава средств информационной системы, применяемых на местах эксплуатации СКЗИ.