КОМИТЕТ СТРОИТЕЛЬСТВА
ВОЛГОГРАДСКОЙ ОБЛАСТИ
(ОБЛСТРОЙ)

ПРИКАЗ

15.07.2022 № 1618-ОД

Волгоград

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

В соответствии с частью 5 статьи 19 Федерального закона от 27.07.2006 № 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 строительства Волгоградской области (далее - Перечень), согласно приложению.

2. Ответственному за обеспечение безопасности персональных данных и защиту информации, не содержащей сведения, составляющие государственную тайну, в информационных системах комитета строительства Волгоградской области определять угрозы безопасности персональных данных при их обработке в информационных системах исходя из Перечня с учетом структурно-функциональных характеристик информационных систем.

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

Председатель комитета Е.Е.Панкин

КОМИТЕТ СТРОИТЕЛЬСТВА ВОЛГОГРАДСКОЙ ОБЛАСТИ
Отдел организационного обеспечения и документооборота

Приложение к приказу
комитета строительства
Волгоградской области
от 15.07.2022 № 1618-ОД

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

1. Угрозами безопасности персональных данных, актуальными при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении деятельности комитета строительства 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:

угрозы, связанные с особенностями функционирования технических, программно-технических и программных средств, обеспечивающих хранение, обработку и передачу информации;

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;

угрозы воздействия вредоносного кода и (или) вредоносной программы, внешних по отношению к информационным системам;

угрозы использования методов социального инжиниринга к лицам, обладающим полномочиями в информационных системах;

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

угрозы несанкционированного доступа (воздействия) к персональным данным лиц, не обладающих полномочиями в информационных системах, с использованием уязвимостей в организации защиты персональных данных;

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;

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;

угрозы несанкционированного доступа (воздействия) к персональным данным лиц, не обладающих полномочиями в информационных системах, с использованием уязвимостей в обеспечении защиты вычислительных сетей информационных систем;

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;

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:

угрозы проведения атаки при нахождении вне контролируемой зоны;

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;

внесение несанкционированных изменений в документацию на СКЗИ и компоненты СФ;

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;

угрозы проведения атак на этапе эксплуатации СКЗИ на:

ключевую, аутентифицирующую и парольную информацию СКЗИ;

программные компоненты СКЗИ;

аппаратные компоненты СКЗИ;

программные компоненты СФ, включая базовую систему ввода (вывода) (BIOS);

аппаратные компоненты СФ;

данные, передаваемые по каналам связи;

персональные данные;

угрозы применения специально разработанных автоматизированных средств и программного обеспечения (далее – АС и ПО);

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