Государственная регистрация
от 30.09.2025 ГР/692/2025

МИНИСТЕРСТВО ЦИФРОВЫХ ТЕХНОЛОГИЙ И СВЯЗИ КАЛИНИНГРАДСКОЙ ОБЛАСТИ

П Р И К А З

29 сентября 2025 г. № 203
Калининград

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 Министерством цифровых технологий и связи Калининградской области

В соответствии с частью 5 статьи 19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» и пунктом 1 положения о Министерстве цифровых технологий и связи Калининградской области, утвержденного постановлением Правительства Калининградской области от 25 декабря 2018 года № 799, **п р и к а з ы в а ю**:

1. Определить угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в сферах деятельности, нормативно-правовое регулирование которых осуществляется Министерством цифровых технологий и связи Калининградской области, согласно приложению к настоящему приказу.

2. Приказ подлежит государственной регистрации.

3. Приказ вступает в силу со дня его официального опубликования.

Исполняющая обязанности
министра А.Н. Голубых

ПРИЛОЖЕНИЕ
к приказу Министерства цифровых технологий и связи Калининградской области
от 19 09 2025 года № 203

УГРОЗЫ
безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в сферах деятельности, нормативно-правовое регулирование которых осуществляется Министерством цифровых технологий и связи Калининградской области

Угрозами безопасности персональных данных, актуальными при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в сферах деятельности, нормативно-правовое регулирование которых осуществляется Министерством цифровых технологий и связи Калининградской области (далее – информационные системы), являются:

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

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

угрозы несанкционированного доступа (воздействия) к персональным данным лицами, обладающими полномочиями в информационных системах, включая пользователей информационных систем, 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 использования методов воздействия на лиц, обладающих полномочиями в информационных системах;

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

угрозы несанкционированного доступа (воздействия) к персональным данным лицами, не обладающими полномочиями в информационных системах, с использованием уязвимостей в программном обеспечении информационных систем;

угрозы несанкционированного доступа (воздействия) к персональным данным лицами, не обладающими полномочиями в информационных системах, с использованием уязвимостей в обеспечении защиты сетевого взаимодействия и каналов передачи данных;

угрозы целенаправленных действий с использованием аппаратных

и (или) программных средств с целью нарушения безопасности защищаемых с использованием средств криптографической защиты информации персональных данных или создания условий для этого, определяемые операторами информационных систем в соответствии с Составом и содержанием 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, утвержденным приказом Федеральной службы безопасности Российской Федерации от 10 июля 2014 года № 378;

угрозы, связанные с возможностями источников атак самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны;

угрозы физического доступа к средствам вычислительной техники, на которых реализованы средства криптографической защиты информации и среда их функционирования;

угрозы из банка данных угроз безопасности информации Федеральной службы по техническому и экспортному контролю:

УБИ.008. Угроза восстановления и/или повторного использования аутентификационной информации;

УБИ.051. Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания;

УБИ.063. Угроза некорректного использования функционала программного обеспечения;

УБИ.088. Угроза несанкционированного копирования защищаемой информации;

УБИ.091. Угроза несанкционированного удаления защищаемой информации;

УБИ.127. Угроза подмены действия пользователя путем обмана;

УБИ.150. Угроза сбоя процесса обновления BIOS;

УБИ.175. Угроза «фишинга»;

УБИ.176. Угроза нарушения технологического/производственного процесса из-за временных задержек, вносимых средством защиты;

УБИ.179. Угроза несанкционированной модификации защищаемой информации;

УБИ.182. Угроза физического устаревания аппаратных компонентов;

УБИ.201. Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере;

УБИ.205. Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты.