МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 55192
от "10" июля 2019 г.

МИНИСТЕРСТВО СПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ
(МИНСПОРТ РОССИИ)

ПРИКАЗ

«13» марта 20 19 г. № 197

Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных в сфере физической культуры и спорта

В соответствии с частью 5 статьи 19 Федерального закона от 27.06.2006 № 152-ФЗ «О персональных данных» (Собрание законодательства Российской Федерации, 2006, № 31 (ч. 1), ст. 3451; 2011, № 31, ст. 4701), п р и к а з ы в а ю :

1. Определить угрозы безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных в сфере физической культуры и спорта, согласно приложению.

2. Структурному подразделению Министерства спорта Российской Федерации, ответственному за информационную безопасность, обеспечить безопасность персональных данных, при их обработке в информационных системах персональных данных исходя из угроз безопасности персональных данных, с учетом структурно-функциональных характеристик информационных систем персональных данных в сфере физической культуры и спорта.

3. Контроль за исполнением настоящего приказа оставляю за собой.

Министр П.А. Колобков

МИНСПОРТ РОССИИ
Вн. № 197
От 13.03.2019 л.

Приложение
к приказу Минспорта России
от «13» марта 2019 г. № 197

Угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных в сфере физической культуры и спорта

1. К угрозам безопасности персональных данных, актуальным при обработке персональных данных в информационных системах персональных данных в сфере физической культуры и спорта (далее – информационные системы), относятся:

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 лицами, обладающими полномочиями в информационных системах, в том числе в ходе создания, эксплуатации, технического обслуживания и (или) ремонта, модернизации, снятия с эксплуатации информационных систем;

3) угрозы воздействия вредоносного кода, вредоносной программы, внешних по отношению к информационным системам;

4) угрозы использования методов воздействия на лиц, обладающих 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 лицами, не обладающими полномочиями в информационных системах, с использованием уязвимостей в организации защиты персональных данных;

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

8) 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, в том числе с использованием протоколов межсетевого взаимодействия;

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

10) угрозы несанкционированного доступа (воздействия) к персональным данным лицами, не обладающими полномочиями в информационных системах, с использованием уязвимостей, вызванных несоблюдением требований по эксплуатации средств защиты информации;

11) угрозы, связанные с возможностью использования 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) создание способов, подготовка и проведение атак без привлечения специалистов в области разработки и анализа СКЗИ;

2) создание способов, подготовка и проведение атак на различных этапах жизненного цикла СКЗИ;

3) проведение атаки нарушителем, находясь вне пространства, в котором исключено неконтролируемое пребывание сотрудников и посетителей оператора и посторонних транспортных, технических и иных материальных средств (далее – контролируемая зона);

4) проведение на этапах разработки (модернизации), производства, хранения, транспортировки СКЗИ и этапе ввода в эксплуатацию СКЗИ (пусконаладочные работы) следующих атак:

а) внесение несанкционированных изменений в СКЗИ и (или) в компоненты аппаратных и программных средств, совместно с которыми штатно функционируют СКЗИ и в совокупности представляющие среду функционирования СКЗИ (далее – СФ), которые способны повлиять на выполнение предъявляемых к СКЗИ требований, в том числе с использованием вредоносных программ;

б) внесение несанкционированных изменений в технические и организационно-распорядительные документы на СКЗИ и компоненты СФ;

5) проведение атак на этапе эксплуатации СКЗИ на:

а) персональные данные;

б) ключевую, аутентифицирующую и парольную информацию СКЗИ;

в) программные компоненты СКЗИ;

г) аппаратные компоненты СКЗИ;

д) программные компоненты СФ, включая программное обеспечение базовых систем ввода (вывода);

е) аппаратные компоненты СФ;

ж) данные, передаваемые по каналам связи;

з) иные объекты, которые установлены при формировании совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак с учетом применяемых в информационной системе информационных технологий, аппаратных средств (далее – АС)

и программного обеспечения (далее – ПО);

6) получение 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») следующей информации об информационной системе, в которой используется СКЗИ:

а) общие сведения об информационной системе, в которой используется СКЗИ (назначение, состав, оператор, объекты, в которых размещены ресурсы информационной системы);

б) сведения об информационных технологиях, базах данных, АС, ПО, используемых в информационной системе совместно с СКЗИ, за исключением сведений, содержащихся только в конструкторской документации на информационные технологии, базы данных, АС, ПО, используемые в информационной системе совместно с СКЗИ;

в) содержание конструкторской документации на СКЗИ;

г) содержание находящейся в свободном доступе документации на аппаратные и программные компоненты СКЗИ и СФ;

д) общие сведения о защищаемой информации, используемой в процессе эксплуатации СКЗИ;

е) сведения о каналах связи, по которым передаются защищаемые СКЗИ персональные данные (далее – канал связи);

ж) данные, передаваемые в открытом виде по каналам связи, не защищенным от несанкционированного доступа к информации организационными и техническими мерами;

з) сведения о нарушениях правил эксплуатации СКЗИ и СФ в каналах связи, не защищенных от несанкционированного доступа к информации организационными и техническими мерами,;

и) сведения о неисправностях и сбоях аппаратных компонентов СКЗИ и СФ, проявляющихся в каналах связи, не защищенных от несанкционированного доступа к информации организационными и техническими мерами;

к) сведения, получаемые в результате анализа сигналов от аппаратных компонентов СКЗИ и СФ;

7) применение:

а) находящихся в свободном доступе или используемых за пределами контролируемой зоны АС и ПО, включая аппаратные и программные компоненты СКЗИ и СФ;

б) специально разработанных АС и ПО;

8) использование на этапе эксплуатации в качестве среды переноса от субъекта к объекту (от объекта к субъекту) атаки действий, осуществляемых при подготовке и (или) проведении атаки:

а) каналов связи, не защищенных от несанкционированного доступа к информации организационными и техническими мерами;

б) каналов распространения сигналов, сопровождающих функционирование СКЗИ и СФ;

9) 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;

10) использование на этапе эксплуатации находящихся за пределами контролируемой зоны АС и ПО из состава средств информационной системы, применяемых на местах эксплуатации СКЗИ (далее – штатные средства);

11) проведение атаки при нахождении в пределах контролируемой зоны;

12) на этапе эксплуатации СКЗИ возможное уничтожение и несанкционированный доступ к:

а) документации на СКЗИ и компоненты СФ;

б) помещениям, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем (далее – СВТ), на которых реализованы СКЗИ и СФ;

13) получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации:

а) сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы;

б) сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы;

в) сведений о мерах по разграничению доступа в помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ;

14) использование штатных средств, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий;

15) физический доступ к СВТ, на которых реализованы СКЗИ и СФ;

16) наличие у нарушителя аппаратных компонентов СКЗИ и СФ, реализованных в информационной системе, в которой используется СКЗИ.