МИНИСТЕРСТВО ЗДРАВООХРАНЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
(МИНЗДРАВ РОССИИ)

ПРИКАЗ

3 июля 2023 г. № 340н

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Москва
Регистрационный № 74650
от "07" августа 2023 г.

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 здравоохранения Российской Федерации

В соответствии с частью 5 статьи 19 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», пунктом 1 Положения о Министерстве здравоохранения Российской Федерации, утвержденного постановлением Правительства Российской Федерации от 19 июня 2012 г. № 608, 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, эксплуатируемых в сферах деятельности, нормативно-правовое регулирование которых осуществляется Министерством здравоохранения Российской Федерации, согласно приложению к настоящему приказу.

Министр М.А. Мурашко

Приложение
к приказу Министерства здравоохранения
Российской Федерации
от «3» июля 2023 г. № 340н

Угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в сферах деятельности, нормативно-правовое регулирование которых осуществляется Министерством здравоохранения Российской Федерации

1. Угрозами безопасности персональных данных, актуальными при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в сферах деятельности, нормативно-правовое регулирование которых осуществляется Министерством здравоохранения Российской Федерации, 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.

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, обладающими пользовательскими правами доступа к государственным информационным системам, автоматизированным и информационным системам (далее – информационные системы), 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 сетевого взаимодействия и каналов передачи данных, в том числе с использованием протоколов межсетевого взаимодействия;

в обеспечении защиты вычислительных сетей информационных систем;

вызванных несоблюдением требований по эксплуатации средств защиты информации;

8) использованием новых информационных технологий.

3. Для 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 актуальными являются угрозы:

1) создания способов, подготовки и проведения атак без привлечения специалистов в области разработки и анализа СКЗИ;

2) создания способов, подготовки и проведения атак на различных этапах жизненного цикла СКЗИ;

3) проведения атак нарушителями, находящимися вне пространства, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств (далее - контролируемая зона);

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

направленных на 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;

направленных на внесение несанкционированных изменений в документацию на СКЗИ и компоненты СФ;

5) проведения на этапе эксплуатации СКЗИ атак на:

персональные данные;

ключевую, аутентифицирующую и парольную информацию СКЗИ;

программные компоненты СКЗИ;

аппаратные компоненты СКЗИ;

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

аппаратные компоненты СФ;

данные, передаваемые по каналам связи;

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) 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 информационной системе, в которой используется СКЗИ, такой как:

общие сведения об информационных системах, в которых используются СКЗИ (назначение, состав, оператор, объекты, в которых размещены ресурсы информационной системы);

сведения об информационных технологиях, базах данных, АС, ПО, используемых в информационных системах 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;

содержание конструкторской документации на СКЗИ;

содержание документации на аппаратные и программные компоненты СКЗИ и СФ;

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

сведения о каналах связи, по которым передаются защищаемые СКЗИ персональные данные (далее - КС);

все возможные данные, передаваемые в открытом виде по КС, не защищенным от несанкционированного доступа к информации организационными и техническими мерами;

сведения обо всех проявляющихся в КС, не защищенных от несанкционированного доступа к информации организационными и техническими мерами, нарушениях правил эксплуатации СКЗИ и СФ;

сведения обо всех проявляющихся в КС, не защищенных от несанкционированного доступа к информации организационными и техническими мерами, неисправностях и сбоях аппаратных компонентов СКЗИ и СФ;

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

7) применения:

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

специально разработанных АС и ПО;

8) использования на этапе эксплуатации в качестве среды переноса действий, осуществляемых при подготовке и (или) проведении атаки:

КС, не защищенных от несанкционированного доступа к информации организационными и техническими мерами;

каналов распространения сигналов, сопровождающих функционирование СКЗИ и СФ;

9) проведения на этапе эксплуатации атаки из информационно-телекоммуникационных сетей, доступ к которым не ограничен определенным кругом лиц, в том числе из информационно-телекоммуникационной сети «Интернет», если информационные системы, в которых используются СКЗИ, имеют выход в эти сети;

10) использования 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) проведения атак при нахождении в пределах контролируемой зоны;

12) получения на этапе эксплуатации СКЗИ несанкционированного доступа к следующим объектам:

документация на СКЗИ и компоненты СФ;

помещения, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ, 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) получения в рамках предоставленных полномочий, а также в результате наблюдений следующей информации:

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

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

сведений о мерах по разграничению доступа в помещения, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ, в которых находятся СВТ, на которых реализованы СКЗИ и СФ;

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

15) получения несанкционированного физического доступа к СВТ, на которых реализованы СКЗИ и СФ;

16) связанные с возможностью располагать аппаратными компонентами СКЗИ и СФ, ограниченные мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.