МИНИСТЕРСТВО ЭКОНОМИЧЕСКОГО РАЗВИТИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
(МИНЭКОНОМРАЗВИТИЯ РОССИИ)

ПРИКАЗ

13 ноября 2023 г. | Москва | № 785

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 77323
от "22" февраля 2024 г.

Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении Министерством экономического развития Российской Федерации функций, определенных законодательством Российской Федерации

В соответствии с частью 5 статьи 19 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и пунктом 1 Положения о Министерстве экономического развития Российской Федерации, утвержденного постановлением Правительства Российской Федерации от 5 июня 2008 г. № 437, 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 при осуществлении Министерством экономического развития Российской Федерации функций, определенных законодательством Российской Федерации, согласно приложению к настоящему приказу.

Министр М.Г. Решетников

Приложение
к приказу Минэкономразвития России
от «13» 11. 2023 г. № 785

Угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении Министерством экономического развития Российской Федерации функций, определенных законодательством Российской Федерации

1. К угрозам безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении Министерством экономического развития Российской Федерации функций, определенных законодательством Российской Федерации, относятся:

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. 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 доступа к государственным информационным системам, автоматизированным и информационным системам (далее – информационные системы), в ходе создания, ввода в эксплуатацию, эксплуатации, технического обслуживания и (или) ремонта, модернизации,

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 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 лиц, не обладающих полномочиями в информационных системах, с использованием уязвимостей:

в организации защиты персональных данных;

в системном и прикладном программном обеспечении информационных систем;

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;

7) 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) создание способов, подготовку и проведение атак без привлечения специалистов в области разработки и анализа СКЗИ;

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

3) проведение атак нарушителями, находящимися вне пространства, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных, технических и иных материальных средств;

4) проведение на этапах разработки (модернизации), производства, хранения, транспортировки СКЗИ и этапе ввода в эксплуатацию СКЗИ (пусконаладочные работы) следующих 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 технические и организационно-распорядительные документы на СКЗИ и компоненты СФ;

5) проведение атак на этапе эксплуатации СКЗИ на:

персональные данные;

ключевую, аутентифицирующую и парольную информацию СКЗИ;

программные компоненты СКЗИ;

аппаратные компоненты СКЗИ;

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

аппаратные компоненты СФ;

данные, передаваемые по каналам связи;

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

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

сведения об информационных технологиях, базах данных, автоматизированных системах (далее - АС), программном обеспечении (далее - 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;

содержание конструкторской документации на СКЗИ;

содержание находящейся в свободном доступе 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 – каналы связи);

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

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

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

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

7) применение:

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) 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:

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

каналов распространения сигналов, сопровождающих функционирование СКЗИ и СФ;

9) проведение на этапе эксплуатации атак 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;

11) проведение атак при нахождении в пределах контролируемой зоны;

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

документация на СКЗИ и компоненты СФ;

помещения, 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:

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

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

сведения 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) получение несанкционированного физического доступа 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.