Министерство энергетики Российской Федерации

(Минэнерго России)

ПРИКАЗ

2 августа 2019 г. № 819

Москва

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

В соответствии с частью 5 статьи 19 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (Собрание законодательства Российской Федерации, 2006, № 31 (ч. I), ст. 3451; 2009, № 48, ст. 5716, № 52 (ч. I), ст. 6439; 2010, № 27, ст. 3407, № 31, ст. 4173, ст. 4196, № 49, ст. 6409, № 52 (ч. I), ст. 6974; 2011, № 23, ст. 3263, № 31, ст. 4701; 2013, № 14, ст. 1651, № 30 (ч. I), ст. 4038, № 51, ст. 6683; 2014, № 23, ст. 2927, № 30 (ч. I), ст. 4217, ст. 4243; 2016, № 27 (ч. I), ст. 4164; 2017, № 9, ст. 1276, № 27, ст. 3945, № 31 (ч. I), ст. 4772; 2018, № 1 (ч. I), ст. 82) 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 при осуществлении Минэнерго России функций, определенных законодательством Российской Федерации (далее – информационные системы), по перечню согласно приложению.

2. Организациям, подведомственным Минэнерго России, определять угрозы безопасности персональных данных при их обработке в информационных системах исходя из перечня, указанного в пункте 1 настоящего приказа, с учетом структурно-функциональных характеристик информационных систем.

Министр А.В. Новак

Департамент проектного управления и обеспечения деятельности Министерства
Смирнов И.В.
(495) 631-83-13

Приложение
к приказу Минэнерго России
от «02» 09 2019 № 819

ПЕРЕЧЕНЬ
угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении Минэнерго России функций, определенных законодательством Российской Федерации

1. Угрозы безопасности персональных данных (далее – угрозы), защищаемых без использования средств криптографической защиты информации (далее – СКЗИ):

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

1.2. угрозы несанкционированного доступа (воздействия) к отчуждаемым носителям персональных данных;

1.3. угрозы воздействия вредоносного кода и (или) вредоносной программы, внешних по отношению к системам обработки персональных данных (далее – СОПД);

1.4. угрозы несанкционированного доступа (воздействия) к персональным данным лицами, обладающими полномочиями в СОПД, в том числе в ходе создания, эксплуатации, технического обслуживания и (или) ремонта, модернизации, снятия с эксплуатации СОПД;

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

1.6. 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;

1.7. 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;

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

1.9. 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;

1.10. угрозы, связанные с возможностью использования новых информационных технологий.

2. 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:

2.1. угрозы проведения атаки при нахождении вне контролируемой зоны;

2.2. угрозы проведения атаки путем внесения 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;

2.3. угрозы проведения атак на этапе эксплуатации СКЗИ на:

2.3.1. ключевую, аутентифицирующую и парольную информацию СКЗИ;

2.3.2. программные компоненты СКЗИ;

2.3.3. аппаратные компоненты СКЗИ;

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

2.3.5. аппаратные компоненты СФ;

2.3.6. данные, передаваемые по каналам связи;

2.4. угрозы 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 информационных системах, в которых используются СКЗИ:

2.4.1. сведений о протоколе взаимодействии СОПД и СКЗИ;

2.4.2. содержания находящейся в свободном доступе документации на аппаратные и программные компоненты СКЗИ и СФ;

2.4.3. общих сведений о защищаемой информации, используемой в процессе эксплуатации СКЗИ;

2.4.4. сведений о каналах связи, по которым передаются защищаемые СКЗИ персональные данные;

2.4.5. сведений, получаемых в результате анализа любых сигналов от аппаратных компонентов СКЗИ и СФ;

2.5. угрозы применения специально разработанных аппаратных средств и программного обеспечения;

2.6. угрозы проведения атаки при нахождении в пределах контролируемой зоны;

2.7. угрозы проведения атак на этапе эксплуатации СКЗИ на:

2.7.1. документацию на СКЗИ и компоненты СФ;

2.7.2. помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем, на которых реализованы СКЗИ и СФ;

2.8. угрозы получения в рамках предоставленных полномочий, а также в результате наблюдений:

2.8.1. сведений о физических мерах защиты объектов, в которых размещены ресурсы СОПД;

2.8.2. сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы СОПД;

2.8.3. сведений о мерах по разграничению доступа в помещения, в которых находятся средства вычислительной техники, на которых реализованы СКЗИ и СФ;

2.9. угрозы физического доступа к средствам вычислительной техники, на которых реализованы СКЗИ.