

Перечень основных изменений

1. Постановлением Правительства РФ от 11.05.2017 № 555 установлено, что при реализации органами исполнительной власти мероприятий по созданию, развитию, вводу в эксплуатацию, эксплуатации и выводу из эксплуатации систем и дальнейшему хранению информации должны выполняться:

- требования о защите информации, содержащейся в системах, устанавливаемые ФСБ России и ФСТЭК России, в пределах их полномочий;
- требования к организации и мерам защиты информации, содержащейся в системе;
- техническое задание на создание системы и модель угроз безопасности информации утверждаются должностным лицом органа исполнительной власти, на которое возложены соответствующие полномочия;
- модель угроз безопасности информации и (или) техническое задание на создание системы согласовываются с ФСБ России и ФСТЭК России, в пределах их полномочий в части, касающейся выполнения установленных требований о защите информации;
- ввод системы в эксплуатацию не допускается в следующих случаях:
 - невыполнение требований о защите информации, включая отсутствие действующего аттестата соответствия требованиям безопасности информации;
 - отсутствие в реестре территориального размещения объектов контроля сведений о размещении технических средств информационной системы на территории Российской Федерации;
 - невыполнение вышеуказанных требований, выявленных в ходе осуществления контроля в соответствии с Правилами осуществления контроля за соблюдением требований к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации.

2. Приказом ФСТЭК России от 15.02.2017 № 27 внесены изменения в Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденные приказом ФСТЭК России от 11.02.2013 № 17:

- изменено количество классов защищенности информационной системы (вместо четырех классов стало три класса);
- в качестве исходных данных для определения угроз безопасности информации должен использоваться банк данных угроз безопасности информации (bdu.fstec.ru);
- добавлены положения в требования к системе защиты информации информационной системы включаемые в техническое задание на создание

информационной системы и (или) техническое задание (частное техническое задание) на создание системы защиты информации информационной системы;

- уточнен результат анализа уязвимостей в информационной системе;
- дополнены методы проверок (испытаний) при проведении аттестационных испытаний;
- увеличен срок проведения повторной аттестация информационной системы с трех лет до пяти лет;
- при создании, функционировании информационной системы на базе центра обработки данных, он должен быть аттестован по классу защищенности не ниже класса защищенности информационной системы, при аттестации информационной системы должны использоваться результаты аттестации центра обработки данных;
- изменены организационные меры и средства защиты информации, применяемые в информационной системе в связи с изменением количества классов защищенности;
- изменен состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы в связи с изменением количества классов защищенности.

3. Приказом ФСТЭК России от 23.03.2017 № 49 внесены изменения в Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденные приказом ФСТЭК России от 18.02.2013 № 21, и в Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, утвержденные приказом ФСТЭК России от 14.03.2014 № 31:

- изменены классы применяемых сертифицированных по требованиям безопасности информации средств защиты информации в зависимости от уровня защищенности персональных данных и классов автоматизированных систем управления.

Эксплуатация ГИС не допускается в случаях, указанных в части 7 статьи 14 Федерального закона "Об информации, информационных технологиях и о защите информации", а также в пункте 15 настоящего документа. (п. 19 (1) введен Постановлением Правительства РФ от 11.05.2017 № 555, вступает в силу с 01.01.2019).