КОПИЯ

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 46487
от "25" апреля 2017 г.

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)

П Р И К А З

«23» марта 2017 г. Москва № 49

О внесении изменений в Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 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 Федеральной службы по техническому и экспортному контролю от 14 марта 2014 г. № 31

Внести в Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 (зарегистрирован Министерством юстиции Российской Федерации 14 мая 2013 г., регистрационный № 28375), 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 Федеральной службы по техническому и экспортному контролю от 14 марта 2014 г. № 31 (зарегистрирован Министерством юстиции Российской Федерации 30 июня 2014 г., регистрационный № 32919), изменения согласно приложению к настоящему приказу.

ДИРЕКТОР ФЕДЕРАЛЬНОЙ СЛУЖБЫ
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

В.СЕЛИН

Приложение
к приказу ФСТЭК России
от «23» марта 2017 г. № 49

**Изменения, которые вносятся
в Состав и содержание организационных и технических мер
по обеспечению безопасности персональных данных при их обработке
в информационных системах персональных данных, утвержденные
приказом Федеральной службы по техническому и экспортному
контролю от 18 февраля 2013 г. № 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 Федеральной службы
по техническому и экспортному контролю от 14 марта 2014 г. № 31**

1. Пункт 12 Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных приказом Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 (зарегистрирован Министерством юстиции Российской Федерации 14 мая 2013 г., регистрационный № 28375), изложить в следующей редакции:

«12. Технические меры защиты персональных данных реализуются посредством применения средств защиты информации, в том числе программных (программно-аппаратных) средств, в которых они реализованы, имеющих необходимые функции безопасности.

При использовании в информационных системах сертифицированных по требованиям безопасности информации средств защиты информации:

в информационных системах 1 уровня защищенности персональных данных применяются средства защиты информации не ниже 4 класса, а также средства вычислительной техники не ниже 5 класса;

в информационных системах 2 уровня защищенности персональных данных применяются средства защиты информации не ниже 5 класса, а также средства вычислительной техники не ниже 5 класса;

в информационных системах 3 уровня защищенности персональных данных применяются средства защиты информации не ниже 6 класса, а также средства вычислительной техники не ниже 5 класса;

в информационных системах 4 уровня защищенности персональных данных применяются средства защиты информации не ниже 6 класса, а также средства вычислительной техники не ниже 6 класса.

Классы защиты определяются в соответствии с нормативными правовыми актами, изданными в соответствии с подпунктом 13.1 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085.

При использовании в информационных системах средств защиты информации, сертифицированных по требованиям безопасности информации, указанные средства должны быть сертифицированы на соответствие обязательным требованиям по безопасности информации, установленным нормативными правовыми актами, или требованиям, указанным в технических условиях (заданиях по безопасности).

Функции безопасности средств защиты информации должны обеспечивать выполнение мер по обеспечению безопасности персональных данных, содержащихся в настоящем документе.

Для обеспечения 1 и 2 уровней защищенности персональных данных, а также для обеспечения 3 уровня защищенности персональных данных в информационных системах, для которых к актуальным отнесены угрозы 2-го типа, применяются сертифицированные средства защиты информации, программное обеспечение которых прошло проверку не ниже чем по 4 уровню контроля отсутствия недекларированных возможностей.».

2. Пункт 24 Требований 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, утвержденных приказом Федеральной службы по техническому и экспортному контролю от 14 марта 2014 г. № 31 (зарегистрирован Министерством юстиции Российской Федерации 30 июня 2014 г., регистрационный № 32919), изложить в следующей редакции:

«24. Технические меры защиты информации реализуются посредством применения средств защиты информации, в том числе программных (программно-аппаратных) средств, в которых они реализованы, имеющих необходимые функции безопасности. В качестве средств защиты информации в первую очередь подлежат рассмотрению механизмы защиты (параметры настройки) штатного программного обеспечения автоматизированной системы управления при их наличии.

В случае использования в автоматизированных системах управления сертифицированных по требованиям безопасности информации средств защиты информации применяются:

в автоматизированных системах управления 1 класса защищенности применяются средства защиты информации не ниже 4 класса, а также средства вычислительной техники не ниже 5 класса;

в автоматизированных системах управления 2 класса защищенности применяются средства защиты информации не ниже 5 класса, а также средства вычислительной техники не ниже 5 класса;

в автоматизированных системах управления 3 класса защищенности применяются средства защиты информации не ниже 6 класса, а также средства вычислительной техники не ниже 5 класса.

Классы защиты определяются в соответствии с нормативными правовыми актами, изданными в соответствии с подпунктом 13.1 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085.

В случае использования в автоматизированных системах управления средств защиты информации, сертифицированных по требованиям безопасности информации, указанные средства должны быть сертифицированы на соответствие обязательным требованиям по безопасности информации, установленным нормативными правовыми актами, или требованиям, указанным в технических условиях (заданиях по безопасности).

Функции безопасности средств защиты информации должны обеспечивать выполнение настоящих Требований.

В автоматизированных системах управления 1 и 2 классов защищенности применяются сертифицированные средства защиты информации, программное обеспечение которых прошло проверку не ниже чем по 4 уровню контроля отсутствия недекларированных возможностей.

Заказчиком (оператором) в зависимости от потенциала нарушителя может быть принято решение о повышении уровня контроля отсутствия недекларированных возможностей средств защиты информации.».