

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

ИНФОРМАЦИОННОЕ СООБЩЕНИЕ

по вопросам обеспечения безопасности информации в ключевых системах информационной инфраструктуры в связи с изданием приказа ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении 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»

от 25 июля 2014 г. № 240/22/2748

Во исполнение поручения Президента Российской Федерации от 13 августа 2013 г. № Пр-1921 и в соответствии с Положением о Федеральной службе по техническому и экспортному контролю, утвержденным Указом Президента Российской Федерации от 16 августа 2004 г. № 1085, Федеральной службой по техническому и экспортному контролю (ФСТЭК России) в пределах своих полномочий утверждены 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 (далее – Требования) (приказ от 14 марта 2014 г. № 31, зарегистрирован Минюстом России 30 июня 2014 г., рег. № 32919).

В связи с изданием указанного нормативного правового акта в адрес ФСТЭК России поступают обращения по вопросам применения методических документов ФСТЭК России по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, а также о разъяснении отдельных положений утвержденных Требований.

Учитывая характер наиболее часто задаваемых вопросов, и в целях разъяснения отдельных положений указанного приказа ФСТЭК России, считаем целесообразным сообщить следующее.

1. По вопросам применения методических документов ФСТЭК России по обеспечению безопасности информации в ключевых системах информационной инфраструктуры в связи с изданием Требований, утвержденных приказом ФСТЭК России от 14 марта 2014 г. № 31.

В настоящее время в области обеспечения безопасности информации в ключевых системах информационной инфраструктуры разработана и утверждена система методических документов, основными из которых являются:

«Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры»;

«Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры»;

«Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры»;

«Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры»;

«Положение о реестре ключевых систем информационной инфраструктуры».

В соответствии с указанными методическими документами к ключевым системам информационной инфраструктуры относятся системы, обеспечивающие управление потенциально опасными производствами или технологическими процессами на объектах, а также обеспечивающие функционирование информационно-опасных объектов, осуществляющих управление (или информационное обеспечение управления) чувствительными (важными) для государства процессами (за исключением процессов на потенциально опасных объектах).

Таким образом, понятие ключевой системы информационной инфраструктуры обобщает в себе множество различных классов информационных, автоматизированных систем и информационно-телекоммуникационных сетей (системы предупреждения и ликвидации чрезвычайных ситуаций, географические и навигационные системы, системы управления водоснабжением, энергоснабжением, транспортом и другие системы и сети).

Автоматизированные системы 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, рассматриваются как один из классов ключевых систем информационной инфраструктуры, обладающий отдельными характерными особенностями.

Учитывая особенности автоматизированных систем управления производственными и технологическими процессами ФСТЭК России издан приказ от 14 марта 2014 г. № 31 «Об утверждении 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».

Автоматизированные системы управления производственными и технологическими процессами подлежат отнесению к соответствующему уровню важности в соответствии с утвержденной системой признаков и включаются в реестр ключевых систем информационной инфраструктуры в порядке, установленном Положением о реестре ключевых систем

информационной инфраструктуры (приказ ФСТЭК России от 4 марта 2009 г. № 74).

Для определения угроз безопасности информации в автоматизированных системах управления производственными и технологическими процессами применяются методические документы ФСТЭК России «Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры» и «Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры».

Вместе с тем, защита автоматизированных систем управления производственными и технологическими процессами, включая формирование требований к защите информации, разработку и внедрение системы защиты, обеспечение защиты информации в ходе эксплуатации автоматизированной системы и вывода из эксплуатации, должна обеспечиваться в соответствии с Требованиями, утвержденными приказом ФСТЭК России от 14 марта 2014 г. № 31.

Методические документы ФСТЭК России «Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры» и «Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры» могут применяться при защите автоматизированных систем управления производственными и технологическими процессами в качестве дополнительного методического материала, в части не противоречащей Требованиям, утвержденным приказом ФСТЭК России от 14 марта 2014 г. № 31.

2. По вопросам вступления в силу Требований, утвержденных приказом ФСТЭК России от 14 марта 2014 г. № 31, а также необходимости модернизации систем защиты автоматизированных систем управления производственными и технологическими процессами, введенных в эксплуатацию до вступления в силу указанных Требований.

В соответствии с пунктом 12 Указа Президента Российской Федерации от 23 мая 1996 г. № 763 «О порядке опубликования и вступления в силу актов Президента Российской Федерации, Правительства Российской Федерации и нормативных правовых актов федеральных органов исполнительной власти», нормативные правовые акты федеральных органов исполнительной власти вступают в силу одновременно на всей территории Российской Федерации по истечении десяти дней после их официального опубликования, если самими актами не установлен другой порядок вступления в силу.

Таким образом, Требования, утвержденные приказом ФСТЭК России от 14 марта 2014 г. № 31, вступают в силу через 10 дней после их официального опубликования.

Исходя из общих принципов норм права по действию во времени, изданные в установленном порядке нормативные правовые акты не имеют обратной силы и применяются к отношениям, возникшим после вступления актов в силу (если иное не установлено федеральными законами).

Учитывая изложенное, системы защиты автоматизированных систем управления производственными и технологическими процессами, введенные в эксплуатацию до вступления в силу Требований, утвержденных приказом ФСТЭК России от 14 марта 2014 г. № 31, могут эксплуатироваться без доработки их системы защиты. В случае принятия решения владельцем автоматизированной системы управления производственными и технологическими процессами о ее плановой модернизации, такие мероприятия проводятся с учетом указанных Требований.

Вместе с тем ФСТЭК России рекомендует владельцам автоматизированных систем управления производственными и технологическими процессами спланировать (в случае технической возможности) поэтапное приведение своих систем управления в соответствие с Требованиями, утвержденными приказом ФСТЭК России от 14 марта 2014 г. № 31.

3. По вопросам применения в автоматизированных системах управления производственными и технологическими процессами средств защиты информации.

В соответствии с пунктом 11 Требований, утвержденных приказом ФСТЭК России от 14 марта 2014 г. № 31, в автоматизированных системах управления производственными и технологическими процессами применяются средства защиты информации, прошедшие оценку соответствия в соответствии с законодательством Российской Федерации о техническом регулировании.

При этом формы оценки соответствия средств защиты информации установлены частью 3 статьи 7 Федерального закона от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании» (испытания, подтверждение соответствия (обязательная сертификация, добровольная сертификация, декларирование соответствия), приемка и ввод в эксплуатацию, иные формы).

В соответствии с пунктом 13 Требований, утвержденных приказом ФСТЭК России от 14 марта 2014 г. № 31, требования к защите информации в автоматизированной системе управления производственными и технологическими процессами устанавливаются заказчиком и включаются в техническое задание на создание (модернизацию) автоматизированной системы управления и (или) техническое задание (частное техническое задание) на создание системы защиты автоматизированной системы управления.

Таким образом, в автоматизированной системе управления применяются средства защиты информации, прошедшие оценку соответствия в форме, установленной заказчиком в техническом задании в соответствии с Федеральным законом «О техническом регулировании».

При этом пунктом 24 Требований, утвержденных приказом ФСТЭК России от 14 марта 2014 г. № 31, установлены классы средств защиты информации, применяемые в автоматизированной системе управления производственными и технологическими процессами, в случае если заказчиком принято решение об использовании средств защиты информации, прошедших оценку соответствия в форме обязательной сертификации.

4. По вопросам аттестации автоматизированных систем управления производственными и технологическими процессами на соответствие требованиям по защите информации.

Требований, утвержденных приказом ФСТЭК России от 14 марта 2014 г. № 31, не содержат положений, устанавливающих обязательную аттестацию автоматизированных систем управления производственными и технологическими процессами.

В то же время оценка соответствия системы защиты автоматизированной системы управления производственными и технологическими процессам должна проводиться в ходе приемочных испытаний этой автоматизированной системы. При этом порядок проведения приемочных испытаний автоматизированной системы управления производственными и технологическими процессам определяется национальными стандартами и стандартами организации (пункт 15.8 Требований).

Таким образом, решение об аттестации автоматизированной системы управления производственными и технологическими процессами может быть принято заказчиком самостоятельно. В этом случае аттестация на соответствие требованиям защиты информации проводится в соответствии с национальными стандартами и методическим документами ФСТЭК России.

Заместитель директора
ФСТЭК России

А.Куц