ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)

П Р И К А З

« 27 » марта 2019 г. Москва № 64

О внесении изменений в Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 21 декабря 2017 г. № 235

В соответствии с пунктом 4 части 3 статьи 6 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (Собрание законодательства Российской Федерации, 2017, № 31, ст. 4736) **П Р И К А З Ы В А Ю:**

1. Внести в Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 21 декабря 2017 г. № 235 (зарегистрирован Министерством юстиции Российской Федерации 22 февраля 2018 г., регистрационный № 50118), следующие изменения:

1) предложение первое абзаца второго пункта 3 изложить в следующей редакции:

«Системы безопасности создаются в отношении всех значимых объектов критической информационной инфраструктуры субъекта критической информационной инфраструктуры с учетом значимых объектов критической информационной инфраструктуры, эксплуатируемых в обособленных подразделениях (филиалах, представительствах) субъекта критической информационной инфраструктуры.»;

2) пункт 9 дополнить абзацем следующего содержания:

«Создаваемая система безопасности должна включать силы обеспечения безопасности значимых объектов критической

информационной инфраструктуры обособленных подразделений (филиалов, представительств) субъектов критической информационной инфраструктуры, в которых эксплуатируются значимые объекты критической информационной инфраструктуры.»;

3) дополнить пунктами 10.1 и 10.2 следующего содержания:

«10.1. По решению руководителя субъекта критической информационной инфраструктуры (уполномоченного лица) в обособленных подразделениях (филиалах, представительствах) субъекта критической информационной инфраструктуры, в которых эксплуатируются значимые объекты критической информационной инфраструктуры, создаются (определяются) структурные подразделения по безопасности или назначаются специалисты по безопасности.

Координацию и контроль выполнения функций структурными подразделениями по безопасности, специалистами по безопасности обособленных подразделений (филиалов, представительств) осуществляют структурные подразделения по безопасности, специалисты по безопасности субъекта критической информационной инфраструктуры.

Порядок взаимодействия структурных подразделений по безопасности, специалистов по безопасности субъекта критической информационной инфраструктуры и структурных подразделений по безопасности, специалистов по безопасности обособленных подразделений (филиалов, представительств) определяется организационно-распорядительными документами субъекта критической информационной инфраструктуры.

10.2. В случае если субъект критической информационной инфраструктуры является хозяйственным обществом (товариществом), имеющим дочерние общества, также являющиеся субъектами критической информационной инфраструктуры, или некоммерческой организацией, участвующей в организациях, являющихся субъектами критической информационной инфраструктуры, в которых некоммерческая организация имеет возможность определять принимаемые этими организациями решения, то структурные подразделения по безопасности, специалисты по безопасности основного хозяйственного общества (товарищества), некоммерческой организации должны осуществлять координацию структурных подразделений по безопасности, специалистов по безопасности дочерних обществ, организаций, в которых участвует некоммерческая организация.»;

4) пункт 12 изложить в следующей редакции:

«12. Работники структурного подразделения по безопасности, специалисты по безопасности должны соответствовать следующим требованиям:

наличие у руководителя структурного подразделения по безопасности высшего профессионального образования по направлению подготовки (специальности) в области информационной безопасности или иного высшего профессионального образования и документа, подтверждающего прохождение обучения по программе профессиональной переподготовки по

направлению «Информационная безопасность» (со сроком обучения не менее 360 часов), наличие стажа работы в сфере информационной безопасности не менее 3 лет;

наличие у штатных работников структурного подразделения по безопасности, штатных специалистов по безопасности высшего профессионального образования по направлению подготовки (специальности) в области информационной безопасности или иного высшего профессионального образования и документа, подтверждающего прохождение обучения по программе повышения квалификации по направлению «Информационная безопасность» (со сроком обучения не менее 72 часов);

прохождение не реже одного раза в 5 лет обучения по программам повышения квалификации по направлению «Информационная безопасность».»;

5) в пункте 23:

абзац первый после слов «документы по безопасности значимых объектов,» дополнить словами «в том числе значимых объектов, которые эксплуатируются в подразделениях (филиалах, представительствах) субъекта критической информационной инфраструктуры,»;

после абзаца первого дополнить абзацами следующего содержания:

«В случае если субъект критической информационной инфраструктуры является дочерним обществом хозяйственного общества (товарищества), являющегося субъектом критической информационной инфраструктуры, организационно-распорядительные документы дочернего общества должны разрабатываться с учетом положений организационно-распорядительных документов основного хозяйственного общества (товарищества) и не противоречить им.

В случае если субъект критической информационной инфраструктуры является организацией, в которой участвует являющаяся субъектом критической информационной инфраструктуры некоммерческая организация, имеющая возможность определять принимаемые организацией решения, организационно-распорядительные документы организации должны разрабатываться с учетом положений организационно-распорядительных документов некоммерческой организации и не противоречить им.»;

6) пункт 29 дополнить абзацем следующего содержания:

«В план мероприятий должны включаться мероприятия по обеспечению безопасности значимых объектов критической информационной инфраструктуры, функционирующих в обособленных подразделениях (филиалах, представительствах) субъекта критической информационной инфраструктуры.»;

7) в пункте 36:

в абзаце первом слово «ежегодно» исключить;

после абзаца первого дополнить абзацем следующего содержания:

«Контроль проводится не реже, чем раз в 3 года. Периодичность контроля определяется руководителем субъекта критической информационной инфраструктуры.».

2. Установить, что изменения, предусмотренные подпунктом 4 пункта 1 настоящего приказа, вступают в силу с 1 января 2021 г.

ДИРЕКТОР ФЕДЕРАЛЬНОЙ СЛУЖБЫ
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

В.СЕЛИН