Изменения
в Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования, утвержденные приказом ФСТЭК России от 21 декабря 2017 г. № 235, внесенные приказом ФСТЭК России от 27 марта 2019 г. № 64

Действующая редакция	Редакция с изменениями, вступающими в силу с 25 июня 2019 г. (за исключением п. 12, изменения в который вступают силу с 1 января 2012 г.)
3. Создание и функционирование систем безопасности должно быть направлено на обеспечение устойчивого функционирования значимых объектов критической информационной инфраструктуры при проведении в отношении них компьютерных атак. Системы безопасности создаются в отношении всех значимых объектов критической информационной инфраструктуры субъектов критической информационной инфраструктуры. По решению субъекта критической информационной инфраструктуры для одного или группы значимых объектов критической информационной инфраструктуры могут создаваться отдельные системы безопасности.	3. Создание и функционирование систем безопасности должно быть направлено на обеспечение устойчивого функционирования значимых объектов критической информационной инфраструктуры при проведении в отношении них компьютерных атак. Системы безопасности создаются в отношении всех значимых объектов критической информационной инфраструктуры субъекта критической информационной инфраструктуры, эксплуатируемых в обособленных подразделениях (филиалах, представительствах) субъекта критической информационной инфраструктуры. По решению субъекта критической информационной инфраструктуры для одного или группы значимых объектов критической информационной инфраструктуры могут создаваться отдельные системы безопасности.
9. Руководитель субъекта критической информационной инфраструктуры определяет состав и структуру системы безопасности, а также функции ее участников при обеспечении безопасности значимых объектов критической информационной инфраструктуры в зависимости от количества значимых объектов критической информационной инфраструктуры, а также особенностей деятельности субъекта критической информационной инфраструктуры.	9. Руководитель субъекта критической информационной инфраструктуры определяет состав и структуру системы безопасности, а также функции ее участников при обеспечении безопасности значимых объектов критической информационной инфраструктуры в зависимости от количества значимых объектов критической информационной инфраструктуры, а также особенностей деятельности субъекта критической информационной инфраструктуры. 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.
	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 дочерни 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.
12. Работники структурного подразделения по безопасности, специалисты по безопасности должны обладать знаниями и навыками, необходимыми для обеспечения безопасности значимых объектов критической информационной инфраструктуры в соответствии с настоящими Требованиями и требованиями по безопасности.	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 на менее 3 лет; наличие у штатных работников 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 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».
23. Субъектом критической информационной инфраструктуры в рамках функционирования системы безопасности должны быть утверждены организационно-распорядительные документы по безопасности значимых объектов, определяющие порядок и правила функционирования системы безопасности значимых объектов, а также порядок и правила обеспечения безопасности значимых объектов критической информационной инфраструктуры. Организационно-распорядительные документы по безопасности значимых объектов являются частью документов по вопросам обеспечения информационной безопасности (защиты информации) субъекта критической информационной инфраструктуры. При этом положения, определяющие порядок и правила обеспечения безопасности значимых объектов критической информационной инфраструктуры, могут быть включены в общие документы по вопросам обеспечения информационной безопасности (защиты информации), а также могут являться частью документов по вопросам функционирования значимого объекта критической информационной инфраструктуры.	23. Субъектом критической информационной инфраструктуры в рамках функционирования системы безопасности должны быть утверждены организационно-распорядительные документы по безопасности значимых объектов, в том числе значимых объектов, которые эксплуатируются в подразделениях (филиалах, представительствах) субъекта критической информационной инфраструктуры, определяющие порядок и правила функционирования системы безопасности значимых объектов, а также порядок и правила обеспечения безопасности значимых объектов критической информационной инфраструктуры. 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. Организационно-распорядительные документы по безопасности значимых объектов являются частью документов по вопросам обеспечения информационной безопасности (защиты информации) субъекта критической информационной инфраструктуры. При этом положения, определяющие порядок и правила обеспечения безопасности значимых объектов критической информационной инфраструктуры, могут быть включены в общие документы по вопросам обеспечения информационной безопасности (защиты информации), а также могут являться частью документов по вопросам функционирования значимого объекта критической информационной инфраструктуры.
29. В рамках планирования мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры осуществляются разработка и утверждение ежегодного плана мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры (далее - план мероприятий). По решению субъекта критической информационной инфраструктуры план мероприятий может разрабатываться на более длительный срок с учетом имеющихся программ (планов) по модернизации, оснащению значимых объектов критической информационной инфраструктуры. План мероприятий разрабатывается структурным подразделением по безопасности, специалистами по безопасности с участием подразделений (работников), эксплуатирующих значимые объекты критической информационной инфраструктуры, и подразделений (работников), обеспечивающих функционирование значимых объектов критической информационной инфраструктуры.	29. В рамках планирования мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры осуществляются разработка и утверждение ежегодного плана мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры (далее - план мероприятий). По решению субъекта критической информационной инфраструктуры план мероприятий может разрабатываться на более длительный срок с учетом имеющихся программ (планов) по модернизации, оснащению значимых объектов критической информационной инфраструктуры. План мероприятий разрабатывается структурным подразделением по безопасности, специалистами по безопасности с участием подразделений (работников), эксплуатирующих значимые объекты критической информационной инфраструктуры, и подразделений (работников), обеспечивающих функционирование значимых объектов критической информационной инфраструктуры. В план мероприятий должны включаться мероприятия по обеспечению безопасности значимых объектов критической информационной инфраструктуры, функционирующих в обособленных подразделениях (филиалах, представительствах) субъекта критической информационной инфраструктуры.
36. Контроль проводится ежегодно комиссией, назначаемой субъектом критической информационной инфраструктуры. В состав комиссии включаются работники структурного подразделения по безопасности, специалисты по безопасности, работники подразделений, эксплуатирующих значимые объекты критической информационной инфраструктуры, и подразделений, обеспечивающих функционирование значимых объектов критической информационной инфраструктуры. По решению субъекта критической информационной инфраструктуры в состав комиссии могут включаться работники иных подразделений субъекта критической информационной инфраструктуры. Для оценки эффективности принятых организационных и технических мер по обеспечению безопасности значимых объектов критической информационной инфраструктуры могут применяться средства контроля (анализа) защищенности.	36. Контроль проводится ~~ежегодно~~ комиссией, назначаемой субъектом критической информационной инфраструктуры. В состав комиссии включаются работники структурного подразделения по безопасности, специалисты по безопасности, работники подразделений, эксплуатирующих значимые объекты критической информационной инфраструктуры, и подразделений, обеспечивающих функционирование значимых объектов критической информационной инфраструктуры. По решению субъекта критической информационной инфраструктуры в состав комиссии могут включаться работники иных подразделений субъекта критической информационной инфраструктуры. Контроль проводится не реже, чем раз в 3 года. Периодичность контроля определяется руководителем субъекта критической информационной инфраструктуры. Для оценки эффективности принятых организационных и технических мер по обеспечению безопасности значимых объектов критической информационной инфраструктуры могут применяться средства контроля (анализа) защищенности.

Результаты контроля оформляются актом, который подписывается членами комиссии и утверждается руководителем субъекта критической информационной инфраструктуры (уполномоченным лицом). В случае проведения по решению руководителя субъекта критической информационной инфраструктуры внешней оценки (внешнего аудита) состояния безопасности значимых объектов критической информационной инфраструктуры внутренний контроль может не проводиться. Для проведения внешней оценки привлекаются организации, имеющие лицензии на деятельность в области защиты информации (в части услуг по контролю защищенности информации от несанкционированного доступа и ее модификации в средствах и системах информатизации). Замечания, выявленные по результатам внутреннего контроля или внешней оценки (внешнего аудита), подлежат устранению в порядке и сроки, установленные руководителем субъекта критической информационной инфраструктуры (уполномоченным лицом).	Результаты контроля оформляются актом, который подписывается членами комиссии и утверждается руководителем субъекта критической информационной инфраструктуры (уполномоченным лицом). В случае проведения по решению руководителя субъекта критической информационной инфраструктуры внешней оценки (внешнего аудита) состояния безопасности значимых объектов критической информационной инфраструктуры внутренний контроль может не проводиться. Для проведения внешней оценки привлекаются организации, имеющие лицензии на деятельность в области защиты информации (в части услуг по контролю защищенности информации от несанкционированного доступа и ее модификации в средствах и системах информатизации). Замечания, выявленные по результатам внутреннего контроля или внешней оценки (внешнего аудита), подлежат устранению в порядке и сроки, установленные руководителем субъекта критической информационной инфраструктуры (уполномоченным лицом).