МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 54443
от "18" апреля 2019 г.

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)

П Р И К А З

«16» марта 2019 г. Москва № 60

О внесении изменений в Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. № 239

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 по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. № 239 (зарегистрирован Министерством юстиции Российской Федерации 26 марта 2018 г., регистрационный № 50524) (с изменениями, внесёнными приказом Федеральной службы по техническому и экспортному контролю от 9 августа 2018 г. № 138 (зарегистрирован Министерством юстиции Российской Федерации 5 сентября 2018 г., регистрационный № 52071), следующие изменения:

1) в пункте 10:

gost.e-ecolog.ru

в подпункте «д» слова «организационные и технические меры, применяемые» заменить словами «требования к организационным и техническим мерам, применяемым»;

дополнить подпунктом «к» следующего содержания:

«к) требования к составу и содержанию документации, разрабатываемой в ходе создания значимого объекта.»;

2) абзац четырнадцатый пункта 11.1 после слов «последствия от» дополнить словами «реализации (возникновения)»;

3) в пункте 11.2:

в подпункте «в» слово «обосновываются» заменить словами «определяются и обосновываются»;

абзац двенадцатый дополнить словами «, разрабатываемой в соответствии с техническим заданием на создание значимого объекта и (или) техническим заданием (частным техническим заданием) на создание подсистемы безопасности значимого объекта»;

после абзаца двенадцатого дополнить абзацем следующего содержания:

«В процессе проектирования значимого объекта его категория значимости может быть уточнена.»;

4) пункт 12.5 дополнить предложением следующего содержания:

«По результатам опытной эксплуатации принимается решение о возможности (или невозможности) проведения приемочных испытаний значимого объекта и его подсистемы безопасности.»;

5) в абзаце одиннадцатом пункта 12.6 слово «действие» заменить словом «эксплуатацию»;

6) в абзаце пятом пункта 12.7 слово «действие» заменить словом «эксплуатацию»;

7) подпункт «в» пункта 14 после слова «уничтожение» дополнить словами «или архивирование»;

8) в пункте 29:

абзац пятый заменить абзацем следующего содержания:

«При этом в значимых объектах 1 категории значимости применяются сертифицированные средства защиты информации, соответствующие 4 или более высокому уровню доверия. В значимых объектах 2 категории значимости применяются сертифицированные средства защиты информации, соответствующие 5 или более высокому уровню доверия. В значимых объектах 3 категории значимости применяются сертифицированные средства защиты информации, соответствующие 6 или более высокому уровню доверия.»;

абзац шестой после слов «Классы защиты» дополнить словами «и уровни

доверия»;

9) дополнить пунктом 29.1 следующего содержания:

«29.1. При проектировании вновь создаваемых или модернизируемых значимых объектов 1 категории значимости в качестве граничных маршрутизаторов, имеющих доступ к информационно-телекоммуникационной сети «Интернет», выбираются маршрутизаторы, сертифицированные на соответствие требованиям по безопасности информации (в части реализованных в них функций безопасности).

В случае отсутствия технической возможности применения в значимых объектах 1 категории значимости граничных маршрутизаторов, сертифицированных на соответствие требованиям по безопасности информации, функции безопасности граничных маршрутизаторов подлежат оценке на соответствие требованиям по безопасности в рамках приемки или испытаний значимых объектов.

Обоснование отсутствия технической возможности приводится в проектной документации на значимые объекты (подсистемы безопасности значимых объектов), разрабатываемой в соответствии с техническим заданием на создание значимых объектов и (или) техническим заданием (частным техническим заданием) на создание подсистемы безопасности значимых объектов.»;

10) пункт 31 дополнить абзацем следующего содержания:

«Входящие в состав значимого объекта 1 категории значимости программные и программно-аппаратные средства, осуществляющие хранение и обработку информации, должны размещаться на территории Российской Федерации (за исключением случаев, когда размещение указанных средств осуществляется в зарубежных обособленных подразделениях субъекта критической информационной инфраструктуры (филиалах, представительствах), а также случаев, установленных законодательством Российской Федерации и (или) международными договорами Российской Федерации).».

11) в приложении к указанным Требованиям:

строку первую раздела I изложить в следующей редакции:

«	ИАФ.0	Регламентация правил и процедур идентификации и аутентификации	+	+	+	»;

в разделе II:

строку первую изложить в следующей редакции:

«	УПД.0	Регламентация правил и процедур управления доступом	+	+	+	»;

строку третью изложить в следующей редакции:

«	УПД.2	Реализация модели управления доступом	+	+	+	»;

строку девятую изложить в следующей редакции:

«	УПД.8	Оповещение пользователя при успешном входе о предыдущем доступе к информационной (автоматизированной) системе				»;

строку первую раздела III изложить в следующей редакции:

«	ОПС.0	Регламентация правил и процедур ограничения программной среды		+	+	»;

в разделе IV:

строку первую изложить в следующей редакции:

«	ЗНИ.0	Регламентация правил и процедур защиты машинных носителей информации	+	+	+	»;

строки шестую - восьмую изложить в следующей редакции:

	ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на съемные машинные носители информации	+	+	+	
«	ЗНИ.6	Контроль ввода (вывода) информации на съемные машинные носители информации			+	»;
	ЗНИ.7	Контроль подключения съемных машинных носителей информации	+	+	+	

в разделе V:

строку первую изложить в следующей редакции:

«	АУД.0	Регламентация правил и процедур аудита безопасности	+	+	+	»;

строку десятую изложить в следующей редакции:

«	АУД.9	Анализ действий отдельных пользователей			+	»;

строку двенадцатую изложить в следующей редакции:

«	АУД.11	Проведение внешних аудитов			»;

строку первую раздела VI изложить в следующей редакции:

«	АВЗ.0	Регламентация правил и процедур антивирусной защиты	+	+	+	»;

строку первую раздела VII изложить в следующей редакции:

«	СОВ.0	Регламентация правил и процедур предотвращения вторжений (компьютерных атак)		+	+	»;

строку первую раздела VIII изложить в следующей редакции:

«	ОЦЛ.0	Регламентация правил и процедур обеспечения целостности	+	+	+	»;

строку первую раздела IX изложить в следующей редакции:

«	ОДТ.0	Регламентация правил и процедур обеспечения доступности	+	+	+	»;

строку первую раздела X изложить в следующей редакции:

«	ЗТС.0	Регламентация правил и процедур защиты технических средств и систем	+	+	+	»;

в разделе XI:

строку первую изложить в следующей редакции:

«	ЗИС.0	Регламентация правил и процедур защиты информационной (автоматизированной) системы и ее компонентов	+	+	+	»;

строку седьмую изложить в следующей редакции:

«	ЗИС.6	Управление сетевыми потоками	+	+	+	»;

строки двадцать четвертую - двадцать шестую изложить в следующей редакции:

«	ЗИС.23	Контроль использования мобильного кода				
	ЗИС.24	Контроль передачи речевой информации				»;
	ЗИС.25	Контроль передачи видеоинформации				

строки двадцать девятую и тридцатую изложить в следующей редакции:

«	ЗИС.28	Исключение возможности отрицания отправки информации				
	ЗИС.29	Исключение возможности отрицания получения информации				»;

строку тридцать вторую изложить в следующей редакции:

«	ЗИС.31	Защита от скрытых каналов передачи информации				»;

строку тридцать шестую изложить в следующей редакции:

«	ЗИС.35	Управление сетевыми соединениями	+	+	+	»;

в разделе XII:

строку первую изложить в следующей редакции:

«	ИНЦ.0	Регламентация правил и процедур реагирования на компьютерные инциденты	+	+	+	»;

строку седьмую изложить в следующей редакции:

«	ИНЦ.6	Хранение и защита информации о компьютерных инцидентах	+	+	+	»;

строку первую раздела XIII изложить в следующей редакции:

«	УКФ.0	Регламентация правил и процедур управления конфигурацией информационной (автоматизированной) системы	+	+	+	»;

строку первую раздела XIV изложить в следующей редакции:

«	ОПО.0	Регламентация правил и процедур управления обновлениями программного обеспечения	+	+	+	»;

строку первую раздела XV изложить в следующей редакции:

«	ПЛН.0	Регламентация правил и процедур планирования мероприятий по обеспечению защиты информации	+	+	+	»;

строку первую раздела XVI изложить в следующей редакции:

«	ДНС.0	Регламентация правил и процедур обеспечения действий в нештатных ситуациях	+	+	+	»;

строку первую раздела XVII изложить в следующей редакции:

«	ИПО.0	Регламентация правил и процедур информирования и обучения персонала	+	+	+	».

2. Установить, что изменения, предусмотренные подпунктом 9 пункта 1 настоящего приказа, вступают в силу с 1 января 2020 г.

ДИРЕКТОР ФЕДЕРАЛЬНОЙ СЛУЖБЫ
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ



В.СЕЛИН

gost.e-ecolog.ru