ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)

П Р И К А З

___ апреля 2026 г. Москва № ____

О внесении изменений в приказы Федеральной службы по техническому и экспортному контролю от 21 декабря 2017 г. № 235 и от 25 декабря 2017 г. № 239

В соответствии с пунктами 3 и 4 части 3 статьи 6 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», абзацем первым пункта 2, а также подпунктами 6^1 и 6^2 пункта 8 Положения о Федеральной службе по экспортному и техническому контролю, утвержденного Указом Президента Российской Федерации № 1085, **П Р И К А З Ы В А Ю**:

1. Утвердить прилагаемые изменения, которые вносятся в приказ Федеральной службы по техническому и экспортному контролю от 21 декабря 2017 г. № 235 (зарегистрирован Минюстом России 22 февраля 2018 г., регистрационный № 50118), с изменениями, внесенными приказами ФСТЭК России от 27 марта 2019 г. № 64 (зарегистрирован Минюстом России 13 июня 2019 г., регистрационный № 54920) и от 20 апреля 2023 г. № 69 (зарегистрирован Минюстом России 23 июня 2023 г., регистрационный № 73969), и в приказ Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. № 239 (зарегистрирован Минюстом России 26 марта 2018 г., регистрационный № 50524), с изменениями, внесенными приказами ФСТЭК России от 9 августа 2018 г. № 138 (зарегистрирован Минюстом России 5 сентября 2018 г., регистрационный № 52071), от 26 марта 2019 г. № 60 (зарегистрирован Минюстом России 18 апреля 2019 г., регистрационный № 54443), от 20 февраля 2020 г. № 35 (зарегистрирован Минюстом России 11 сентября 2020 г., регистрационный № 59793), от 28 августа 2024 г. № 159

(зарегистрирован Минюстом России 24 октября 2020 г., регистрационный № 79900).

2. Настоящий приказ вступает в силу с 1 сентября 2026 г.

ДИРЕКТОР ФЕДЕРАЛЬНОЙ СЛУЖБЫ
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

В.СЕЛИН

Утверждены
приказом ФСТЭК России
от «___» апреля 2026 г. № ____

Изменения,
которые вносятся в приказы Федеральной службы
по техническому и экспортному контролю
от 21 декабря 2017 г. № 235 и от 25 декабря 2017 г. № 239

1. 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, дополнить пунктом 36^1 следующего содержания:

«36^1. В рамках контроля состояния безопасности значимых объектов критической информационной инфраструктуры должен проводиться расчет:

а) показателя, характеризующего текущее состояние обеспечения безопасности значимых объектов критической информационной инфраструктуры от базового уровня угроз безопасности информации (далее — показатель защищенности $К_{зи}$);

б) показателя, определяющего достаточность и эффективность проведенных мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры (далее — показатель уровня зрелости $П_{зи}$).

Для определения значений и расчета показателя защищенности $К_{зи}$ и показателя уровня зрелости $П_{зи}$ должны применяться методические документы, утвержденные ФСТЭК России в соответствии с абзацем вторым пункта 5 и подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085 (далее — методические документы ФСТЭК России).

Расчет и оценка показателя защищенности $К_{зи}$ проводится не реже одного раза в шесть месяцев. Расчет и оценка показателя уровня зрелости $П_{зи}$ проводится не реже одного раза в два года.

О полученных по результатам оценки значениях показателя защищенности $К_{зи}$ и показателя уровня зрелости $П_{зи}$ в случае их несоответствия нормированным значениям, указанным в методических документах ФСТЭК России, в течение 3 календарных дней со дня завершения такой оценки информируется руководитель субъекта критической информационной инфраструктуры для принятия решения о проведении дополнительных мероприятий по

обеспечению безопасности значимых объектов критической информационной инфраструктуры.

Результаты оценки показателя защищенности $К_{зи}$ и показателя уровня зрелости $П_{зи}$ в срок не позднее 5 рабочих дней после дня их расчета направляются субъектом критической информационной инфраструктуры в ФСТЭК России в целях мониторинга текущего состояния обеспечения безопасности значимых объектов критической информационной инфраструктуры и оценки эффективности деятельности по обеспечению безопасности значимых объектов критической информационной инфраструктуры.».

2. В Требованиях по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденных приказом Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. № 239:

а) пункт 31 изложить в следующей редакции:

«31. Применяемые в значимом объекте средства защиты информации должны быть обеспечены технической поддержкой со стороны разработчиков (производителей).

При выборе средств защиты информации должно учитываться возможное наличие ограничений со стороны разработчиков (производителей) или иных лиц на применение этих средств на любом из принадлежащих субъекту критической информационной инфраструктуры значимом объекте критической информационной инфраструктуры.

В случае невозможности обеспечения средств защиты информации технической поддержкой со стороны разработчиков (производителей) субъектом критической информационной инфраструктуры должны быть реализованы организационные и технические меры, обеспечивающие блокирование (нейтрализацию) угроз безопасности информации с необходимым уровнем защищенности значимого объекта в соответствии с настоящими Требованиями.

В значимом объекте не допускаются:

наличие удаленного доступа к программным и программно-аппаратным средствам, в том числе средствам защиты информации, для обновления или управления со стороны лиц, не являющихся работниками субъекта критической информационной инфраструктуры, а также работниками его дочерних и зависимых обществ;

наличие локального бесконтрольного доступа к программным и программно-аппаратным средствам, в том числе средствам защиты информации, для обновления или управления со стороны лиц, не являющихся работниками субъекта критической информационной инфраструктуры, его дочерних и зависимых обществ;

передача информации, в том числе технологической информации, разработчику (производителю) программных и программно-аппаратных средств, в том числе средств защиты информации, или иным лицам без контроля со стороны субъекта критической информационной инфраструктуры.

В случае технической невозможности исключения удаленного доступа к программным и программно-аппаратным средствам, в том числе средствам защиты информации, в значимом объекте принимаются организационные и технические меры по обеспечению безопасности такого доступа, предусматривающие:

определение лиц и устройств, которым разрешен удаленный доступ к программным и программно-аппаратным средствам значимого объекта, предоставление им минимальных полномочий при доступе к этим средствам;

контроль доступа к программным и программно-аппаратным средствам значимого объекта;

защиту информации и данных при их передаче по каналам связи при удаленном доступе к программным и программно-аппаратным средствам значимого объекта;

мониторинг и регистрацию действий лиц, которым разрешен удаленный доступ к программным и программно-аппаратным средствам значимого объекта, а также инициируемых ими процессов, анализ этих действий в целях выявления фактов неправомерных действий;

обеспечение невозможности отказа лиц от выполненных действий при осуществлении удаленного доступа к программным и программно-аппаратным средствам значимого объекта.

В значимом объекте могут приниматься дополнительные организационные и технические меры по обеспечению безопасности удаленного доступа к программным и программно-аппаратным средствам, в том числе средствам защиты информации, направленные на блокирование (нейтрализацию) угроз безопасности информации, приведенных в модели угроз безопасности информации, разрабатываемой в соответствии с пунктом 11.1 настоящих Требований.

Входящие в состав значимого объекта 1 и 2 категорий 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).»;

б) дополнить пунктом 33 следующего содержания:

«33. Меры по обеспечению безопасности значимых, принимаемые в соответствии с настоящими Требованиями, подлежат дополнению организационными и техническими мерами, решение о необходимости осуществления которых принято ФСТЭК России в соответствии с подпунктом «е» пункта 1 Указа Президента Российской Федерации от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации.».

_____