МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 87202
от "24" июня 2026 г.

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)

П Р И К А З

«27» февраля 2026 г. Москва № 60

О внесении изменений в Порядок организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну, утвержденный приказом ФСТЭК России от 29 апреля 2021 г. № 77

В соответствии с подпунктом 13.3 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085, **П Р И К А З Ы В А Ю:**

1. Внести изменения в Порядок организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну, утвержденный приказом ФСТЭК России от 29 апреля 2021 г. № 77 (зарегистрирован Минюстом России 10 августа 2021 г., регистрационный № 64589), согласно приложению к настоящему приказу.

2. Установить, что настоящий приказ вступает в силу с 1 сентября 2026 г.

ДИРЕКТОР ФЕДЕРАЛЬНОЙ СЛУЖБЫ
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

В.СЕЛИН

ПРИЛОЖЕНИЕ
к приказу ФСТЭК России
от 11 февраля 2026 г. № 60

ИЗМЕНЕНИЯ,

которые вносятся в Порядок организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну, утвержденный приказом ФСТЭК России от 29 апреля 2021 г. № 77

1. Абзац первый сноски 1 к пункту 1 изложить в следующей редакции:

«[1] Требования о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, утвержденные приказом ФСТЭК России от 11 апреля 2025 г. № 117 (зарегистрирован Минюстом России 16 июня 2025 г., регистрационный № 82619).».

2. Пункт 3 изложить в следующей редакции:

«3. Настоящий Порядок распространяется на аттестацию на соответствие требованиям по защите информации (далее — аттестация) и проведение периодического контроля уровня защиты информации (далее — периодический контроль) следующих объектов информатизации[2]:

государственных и муниципальных информационных систем, в том числе государственных, муниципальных информационных систем персональных данных;

информационных систем управления производством, используемых организациями оборонно-промышленного комплекса, в том числе автоматизированных систем станков с числовым программным управлением;

помещений, предназначенных для ведения конфиденциальных переговоров (далее – защищаемые помещения)[3].

Настоящий Порядок применяется также для аттестации следующих объектов информатизации, для которых их владельцами установлено требование по проведению оценки соответствия систем защиты информации этих объектов требованиям по защите информации в форме аттестации:

информационных систем государственных органов, государственных унитарных предприятий, государственных учреждений (за исключением государственных информационных систем);

значимых объектов критической информационной инфраструктуры Российской Федерации;

информационных систем персональных данных (за исключением государственных, муниципальных информационных систем персональных данных);

автоматизированных систем управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды.».

3. Сноску 2 к абзацу первому пункта 3 изложить в следующей редакции:

«[2] Пункт 3.1 национального стандарта Российской Федерации ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения», утвержденного и введенного в действие приказом Ростехрегулирования от 27 декабря 2006 г. № 374-ст (Москва: Стандартинформ, 2007).».

4. Сноску 3 к абзацу четвертому пункта 3 изложить в следующей редакции:

«[3] Подпункт «г» пункта 4 Положения о лицензировании деятельности по технической защите конфиденциальной информации, утвержденного постановлением Правительства Российской Федерации от 3 февраля 2012 г. № 79.».

5. Абзац первый пункта 6 изложить в следующей редакции:

«6. По решению руководителя федерального органа государственной власти, органа государственной власти субъекта Российской Федерации, органа местного самоуправления аттестация, а также проведение периодического контроля принадлежащих этому органу объектов информатизации проводятся в соответствии с настоящим Порядком структурным подразделением (работниками) этого органа, ответственными за защиту информации, после информирования ФСТЭК России о принятом решении и при наличии необходимых для проведения работ по аттестации:».

6. Пункт 7 изложить в следующей редакции:

«7. Для проведения аттестационных испытаний, а также периодического контроля на аттестованных объектах информатизации органом по аттестации из числа своих работников назначается аттестационная комиссия в составе руководителя комиссии и не менее двух экспертов, обладающих знаниями и навыками в области технической защиты конфиденциальной информации и аттестации объектов информатизации (далее — эксперты органа по аттестации).».

7. Подпункт «б» пункта 16 изложить в следующей редакции:

«б) при проведении работ, предусмотренных подпунктом «и» пункта 15

настоящего Порядка, — тестирование объекта информатизации путем проверки реализованных мер по защите информационной системы (функциональное тестирование), автоматизированное и (или) ручное выявление уязвимостей объекта информатизации с последующей экспертной оценкой возможности их использования нарушителем для нарушения безопасности информации и (или) нарушения функционирования информационной системы (далее — анализ уязвимостей), а также тестирование объекта информатизации путем моделирования реализации актуальных угроз с целью оценки возможностей несанкционированного доступа к ней (воздействий на нее) или повышения привилегий при реализованных мероприятиях и мерах по защите информационной системы и содержащейся в ней информации (далее — тестирование на проникновение) проводятся в соответствии с методическими документами, утвержденными ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085;».

8. Дополнить пунктами 16^1 — 16^3 следующего содержания:

«16^1. Тестирование на проникновение проводится в отношении государственных информационных систем, иных информационных систем государственных органов, государственных унитарных предприятий, государственных учреждений 1, 2 классов защищенности, которые имеют подключение к информационно-телекоммуникационной сети «Интернет» и (или) взаимодействуют с иными информационными системами, в том числе с информационными системами подрядных организаций (за исключением случаев, когда такое взаимодействие реализовано с использованием сети шифрованной связи или виртуальных частных сетей с применением сертифицированных шифровальных (криптографических) средств защиты информации).

16^2. В случае если объект информатизации создается на базе информационно-телекоммуникационной инфраструктуры в соответствии с абзацем третьим пункта 3 Положения об учете ИТ-активов, используемых для осуществления деятельности по цифровой трансформации системы государственного (муниципального) управления, утвержденного постановлением Правительства Российской Федерации от 1 июля 2024 г. № 900, такая инфраструктура аттестуется на соответствие требованиям по защите информации по классу защищенности не ниже класса защищенности объекта информатизации.

16^3. В состав аттестованного объекта информатизации допускается

включать сегменты, аналогичные в части состава программных, программно-аппаратных средств и их конфигураций сегментам, входящим в состав аттестованного объекта информатизации.

В отношении включаемых в состав аттестованного объекта информатизации сегментов проводятся аттестационные испытания, определенные программой и методиками аттестационных испытаний объекта информатизации.

По результатам проведения аттестационных испытаний принимается решение о включении сегментов в состав аттестованной информационной системы либо о невозможности включения сегментов в состав аттестованной информационной системы.».

9. Пункт 31 изложить в следующей редакции:

«31. Аттестат соответствия выдается на весь срок эксплуатации объекта информатизации.

Владелец аттестованного объекта информатизации обеспечивает поддержку его безопасности в соответствии с аттестатом соответствия путем реализации требований по защите информации в ходе эксплуатации аттестованного объекта информатизации и проведения самостоятельно или с привлечением организации, имеющей лицензию на осуществление деятельности по технической защите конфиденциальной информации (с правом проведения работ и оказания услуг по аттестационным испытаниям и аттестации на соответствие требованиям по защите информации, по контролю защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации), выданную ФСТЭК России в соответствии с Положением о лицензировании деятельности по технической защите конфиденциальной информации, утвержденным постановлением Правительства Российской Федерации от 3 февраля 2012 г. № 79, периодического контроля уровня защищенности информации на аттестованном объекте информатизации, результаты которого оформляются отчетом (протоколами) и включаются в технический паспорт на объект информатизации.».

10. Дополнить пунктами 31^1 и 31^2 следующего содержания:

«31^1. Контроль уровня защищенности информации на аттестованном объекте информатизации проводится следующими методами:

анализ уязвимостей;

тестирование на проникновение.

31^2. По результатам проведения контроля уровня защищенности информации на аттестованном объекте информатизации оформляется отчет (протокол), содержащий сведения о:

а) наименовании объекта информатизации и его назначении, составе программно-технических, программных средств и средств защиты информации;

б) классе защищенности информационной (автоматизированной) системы, категории значимости значимого объекта;

в) фамилии, имени, отчестве (при наличии), должности экспертов, проводивших контроль уровня защищенности информации объекта информатизации;

г) сроке проведения контроля уровня защищенности информации;

д) дате и номере аттестата соответствия объекта информатизации;

е) порядке проведения работ по анализу уязвимостей, их результатах;

ж) порядке проведения работ по тестированию на проникновение, их результатах.

Указанный отчет (протокол) подписывается специалистами, проводившими контроль уровня защищенности информации объекта информатизации, и утверждается руководителем структурного подразделения органа по аттестации или работниками федерального органа государственной власти, органа государственной власти субъекта Российской Федерации, органа местного самоуправления.».

11. Пункт 32 изложить в следующей редакции:

«32. Отчет (протокол) по результатам проведения контроля уровня защищенности информации на аттестованном объекте информатизации не реже одного раза в три года представляется владельцем объекта информатизации в ФСТЭК России (территориальный орган ФСТЭК России) в течение 5 рабочих дней с даты завершения проведения контроля уровня защищенности информации.

Непредставление отчета (протокола) по результатам проведения контроля уровня защищенности информации в ФСТЭК России (территориальный орган ФСТЭК России) является основанием для приостановления действия аттестата соответствия в соответствии с пунктами 34 — 37 настоящего Порядка.».

12. Пункт 33 изложить в следующей редакции:

«33. В случае развития (модернизации) объекта информатизации, в ходе которого изменены архитектура системы защиты информации объекта информатизации (изменены виды и типы программных, программно-технических средств и средств защиты информации), структура системы защиты информации (изменены состав и места расположения объекта информатизации и его компонентов), исключены программные, программно-технические средства и средства защиты информации, дополнительно включены аналогичные средства или заменены на аналогичные средства, проводятся дополнительные

аттестационные испытания в соответствии с настоящим Порядком. Сведения об изменениях аттестованного объекта информатизации и проведенных при этом аттестационных испытаниях включаются владельцем объекта информатизации в технический паспорт. Действие аттестата соответствия не прекращается.».

13. Дополнить пунктами 33^1 — 33^3 следующего содержания:

«33^1. Дополнительные аттестационные испытания объекта информатизации должны проводиться в отношении компонентов объекта информатизации, измененных в ходе развития (модернизации) объекта информатизации, следующими методами:

функциональное тестирование;

анализ уязвимостей.

33^2. По результатам проведения дополнительных аттестационных испытаний объекта информатизации оформляется отчет (протокол), содержащий сведения о:

а) наименовании объекта информатизации и его назначении, составе программно-технических, программных средств и средств защиты информации;

б) классе защищенности информационной (автоматизированной) системы, категории значимости значимого объекта;

в) фамилии, имени, отчестве (при наличии), должности экспертов, проводивших дополнительные аттестационные испытания объекта информатизации;

г) сроке проведения дополнительных аттестационных испытаний объекта информатизации;

д) дате и номере аттестата соответствия объекта информатизации;

е) порядке проведения работ по функциональному тестированию, их результатах;

ж) порядке проведения работ по анализу уязвимостей, их результатах.

Указанный отчет (протокол) подписывается специалистами, проводившими дополнительные аттестационные испытания объекта информатизации, и утверждается руководителем структурного подразделения органа по аттестации или работниками федерального органа государственной власти, органа государственной власти субъекта Российской Федерации, органа местного самоуправления.

33^3. В случае развития (модернизации) объекта информатизации, приводящего к повышению класса защищенности (уровня защищенности, категории значимости) объекта информатизации, проводится повторная аттестация в соответствии с пунктом 15 настоящего Порядка.».

14. В пункте 34:

подпункт «в» изложить в следующей редакции:

«в) непредставления отчетов (протоколов) по результатам проведения контроля уровня защищенности информации на аттестованном объекте информатизации в соответствии с пунктом 32 настоящего Порядка;»;

в подпункте «г» слово «архитектуры» исключить.

15. Пункт 38 изложить в следующей редакции:

«38. Действие аттестата соответствия возобновляется ФСТЭК России (территориальным органом ФСТЭК России) в случае:

а) устранения несоответствия объекта информатизации требованиям по защите информации и представления владельцем объекта информатизации в ФСТЭК России (территориальный орган ФСТЭК России) материалов, подтверждающих устранение недостатков;

б) представления в ФСТЭК России отчета (протокола) по результатам проведения контроля уровня защищенности информации на аттестованном объекте информатизации в соответствии с пунктом 32 настоящего Порядка;

в) обращения владельца объекта информатизации о возобновлении действия аттестата соответствия на объект информатизации в случае, если решение о приостановлении его действия было принято по обращению владельца объекта информатизации.».

16. Пункт 40 изложить в следующей редакции:

«40. Действие аттестата соответствия прекращается ФСТЭК России (территориальным органом ФСТЭК России) в случае:

а) непредставления владельцем объекта информатизации в установленный в уведомлении о приостановлении действия аттестата соответствия срок материалов, подтверждающих устранение недостатков;

б) непредставления владельцем объекта информатизации в установленный в уведомлении о приостановлении действия аттестата соответствия срок отчета (протокола) по результатам проведения контроля уровня защищенности информации на аттестованном объекте информатизации;

в) обращения владельца объекта информатизации о прекращении действия аттестата соответствия.».