ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК РОССИИ)

П Р И К А З

«19» апреля 2021 г. **г. Москва** **№ 77**

Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну

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 (Собрание законодательства Российской Федерации, 2004, № 34, ст. 3541; 2020, № 35, ст. 5554), **П Р И К А З Ы В А Ю:**

1. Утвердить прилагаемый Порядок организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну.

2. Установить, что настоящий приказ вступает в силу с 1 сентября 2021 г.

ДИРЕКТОР ФЕДЕРАЛЬНОЙ СЛУЖБЫ
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

В.СЕЛИН

УТВЕРЖДЕН
приказом ФСТЭК России
от « 29 » апреля 2021 г. № 77

Порядок организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну

I. Общие положения

1. Настоящий Порядок определяет состав и содержание работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну (далее – требования по защите информации)[1], а также требования к форме и содержанию разрабатываемых при организации и проведении таких работ документов.

---

1 Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом ФСТЭК России от 11 февраля 2013 г. № 17 (зарегистрирован Минюстом России 31 мая 2013 г., регистрационный № 28608), с изменениями, внесенными приказом ФСТЭК России от 15 февраля 2017 г. № 27 (зарегистрирован Минюстом России 14 марта 2017 г., регистрационный № 45933), приказом ФСТЭК России от 28 мая 2019 г. № 106 (зарегистрирован Минюстом России 13 сентября 2019 г., регистрационный № 55924), приказом ФСТЭК России от 27 апреля 2020 г. № 61 (зарегистрирован Минюстом России 12 мая 2020 г., регистрационный № 58322).

Требования к обеспечению защиты информации, содержащейся в информационных системах управления производством, используемых предприятиями оборонно-промышленного комплекса, утвержденные приказом ФСТЭК России от 28 февраля 2017 г. № 31 (зарегистрирован Минюстом России 18 мая 2017 г., регистрационный № 46769), с изменениями, внесенными приказом ФСТЭК России от 14 января 2019 г. № 5 (зарегистрирован Минюстом России 27 февраля 2019 г., регистрационный № 53916), приказом ФСТЭК России от 28 октября 2020 г. № 122 (зарегистрирован Минюстом России 25 марта 2021 г., регистрационный № 62868).

Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденные приказом ФСТЭК России от 25 декабря 2017 г. № 239 (зарегистрирован Минюстом России 26 марта 2018 г., регистрационный № 50524), с изменениями, внесенными приказом ФСТЭК России от 9 августа 2018 г. № 138 (зарегистрирован Минюстом России 5 сентября 2018 г., регистрационный № 52071), приказом ФСТЭК России от 26 марта 2019 г. № 60 (зарегистрирован Минюстом России 18 апреля 2019 г., регистрационный № 54443), приказом ФСТЭК России от 20 февраля 2020 г. № 35 (зарегистрирован Минюстом России 11 сентября 2020 г., регистрационный № 59793).

Требования к обеспечению защиты информации в автоматизированных системах управления производственными процессами на критически важных объектах, потенциально опасных объектах, а также объекта, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, утвержденные приказом ФСТЭК России от 14 марта 2013 г. № 31 (зарегистрирован Минюстом России 30 июня 2014 г., регистрационный № 46769), с изменениями, внесенными приказом ФСТЭК России от 23 марта 2017 г. № 49 (зарегистрирован Минюстом России 25 апреля 2017 г., регистрационный № 46487), приказом ФСТЭК России от 9 августа 2018 г. № 138 (зарегистрирован Минюстом России 5 сентября 2018 г., регистрационный № 52071).

Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденные приказом ФСТЭК России от 18 февраля 2013 г. № 21 (зарегистрирован Минюстом России 14 мая 2013 г., регистрационный № 28375), с изменениями, внесенными приказом ФСТЭК России от 23 марта 2017 г. № 49 (зарегистрирован Минюстом России 25 апреля 2017 г., регистрационный № 46487), приказом ФСТЭК России от 14 мая 2020 г. № 68 (зарегистрирован Минюстом России 8 июля 2020 г., регистрационный № 58877).

Положение по защите информации при использовании оборудования с числовым программным управлением, предназначенного для обработки информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, утвержденные приказом ФСТЭК России от 29 мая 2009 г. № 191 (зарегистрирован Минюстом России 6 июля 2009 г., регистрационный № 14230).

2. Аттестация объектов информатизации осуществляется федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, органами местного самоуправления, организациями, которым на праве собственности или ином законном основании принадлежат объекты информатизации, а также лицами, заключившими контракт на создание объектов информатизации, или лицами, осуществляющими эксплуатацию объектов информатизации (далее – владельцы объектов информатизации).

3. Настоящий Порядок распространяется на аттестацию на соответствие требованиям по защите информации (далее – аттестация) 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:

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.

4. Аттестация объекта информатизации проводится на этапе его создания или развития (модернизации) и предусматривает проведение комплекса организационных и технических мероприятий и работ (аттестационных испытаний), в результате которых подтверждается соответствие объекта информатизации требованиям по защите информации в условиях его эксплуатации. Допускается проведение аттестации объекта информатизации на этапе его эксплуатации в случае, если владельцем объекта принято решение об

---

[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).

3 Положение о лицензировании деятельности по технической защите конфиденциальной информации, утвержденное постановлением Правительства Российской Федерации от 3 февраля 2012 г. № 79 (Собрание законодательства Российской Федерации, 2012, № 7, ст. 863; 2020, № 49, ст. 7943).

обработке защищаемой информации после ввода в эксплуатацию объекта информатизации.

II. Организация работ по аттестации объектов информатизации

5. Для проведения аттестационных испытаний владелец объекта информатизации привлекает организацию, имеющую 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), 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 (далее – орган по аттестации).

6. По решению руководителя федерального органа государственной власти, органа государственной власти субъекта Российской Федерации, органа местного самоуправления аттестация принадлежащих этому органу объектов информатизации проводится 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:

а) средств, предназначенных для контроля эффективности защиты информации от несанкционированного доступа (для аттестации информационных, автоматизированных систем управления, информационно-телекоммуникационных сетей (далее – информационные (автоматизированные) системы), а также контрольно-измерительного, производственного и испытательного оборудования (для аттестации защищаемых помещений);

б) нормативных правовых актов и методических документов ФСТЭК России по вопросам технической защиты конфиденциальной информации, разработанных и утвержденных 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 (Собрание законодательства Российской Федерации, 2004, № 34, ст. 3541; 2020, № 35, ст. 5554), национальных стандартов в области технической защиты информации;

в) работников, обладающих знаниями и навыками в области технической защиты конфиденциальной информации и аттестации объектов информатизации.

7. Для проведения аттестационных испытаний 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).

8. При назначении экспертов органа по аттестации должна быть обеспечена их независимость от владельца объекта информатизации с целью исключения возможности влияния владельца аттестуемого объекта информатизации на

результаты аттестационных испытаний, проведенных экспертами органа по аттестации.

Назначение экспертов органов по аттестации из числа работников, участвующих в разработке и (или) внедрении системы защиты информации объекта информатизации, не допускается.

Эксперты органа по аттестации проводят анализ документов, представляемых владельцем объекта информатизации в соответствии с пунктом 11 настоящего Порядка, и аттестационные испытания объекта информатизации в соответствии с требованиями по технической защите информации.

Выводы экспертов органа по аттестации по результатам проведенных аттестационных испытаний не должны противоречить требованиями по технической защите информации.

9. Срок проведения работ по аттестации объекта информатизации устанавливается владельцем объекта информатизации по согласованию с органом по аттестации, но не может превышать четырех месяцев.

10. Информация об объекте информатизации, полученная органом по аттестации в ходе аттестации объекта информатизации, подлежит защите в соответствии с частью 4 статьи 16 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3448, 2014, № 30, ст. 4243).

III. Проведение работ по аттестации объектов информатизации

11. Для проведения работ по аттестации владелец объекта информатизации представляет в орган по аттестации следующие документы или их копии:

а) технический паспорт на объект информатизации по форме согласно приложениям № 1, 2 к настоящему Порядку;

б) акт классификации информационной (автоматизированной) системы по форме согласно приложению № 3 к настоящему Порядку, акт категорирования значимого объекта критической информационной инфраструктуры Российской Федерации (далее – акт категорирования значимого объекта);

в) модель угроз безопасности информации (в случае ее разработки в соответствии с требованиями по защите информации);

г) техническое задание на создание (развитие, модернизацию) объекта информатизации и (или) частное техническое задание на создание (развитие, модернизацию) системы защиты информации объекта информатизации (для объекта информатизации, входящего в состав объекта капитального строительства, задание на проектирование (реконструкцию) объекта капитального строительства) (в случае их разработки в ходе создания объекта информатизации);

д) проектную документацию на систему защиты информации объекта информатизации (в случае ее разработки в ходе создания объекта информатизации);

е) эксплуатационную документацию на систему защиты информации объекта информатизации и применяемые средства защиты информации;

ж) организационно-распорядительные документы по защите информации владельца объекта информатизации, регламентирующие защиту информации в ходе эксплуатации объекта информатизации, в том числе план мероприятий по защите информации на объекте информатизации, документы по порядку оценки угроз безопасности информации, управлению (администрированию) системой защиты информации, управлению конфигурацией объекта информатизации, реагированию на инциденты безопасности, информированию и обучению персонала, контролю за обеспечением уровня защищенности информации (далее – документы по защите информации владельца объекта информатизации);

з) документы, содержащие результаты анализа уязвимостей объекта информатизации и приемочных испытаний системы защиты информации объекта информатизации (в случае проведения анализа и испытаний в ходе создания объекта информатизации).

По решению владельца объекта информатизации указанные в настоящем пункте документы (их копии) представляются в орган по аттестации в виде электронных документов.

12. На основе анализа документов, предусмотренных пунктом 11 настоящего Порядка, и предварительного ознакомления с объектом информатизации в условиях его эксплуатации орган по аттестации разрабатывает программу и методики аттестационных испытаний.

13. Программа и методики аттестационных испытаний объекта информатизации состоят из следующих разделов:

а) общие положения;

б) программа аттестационных испытаний объекта информатизации;

в) методики аттестационных испытаний объекта информатизации.

13.1. Раздел, касающийся общих положений, должен включать следующие сведения:

а) наименование и краткое описание архитектуры объекта информатизации, класс защищенности информационной (автоматизированной) системы, категорию значимого объекта;

б) фамилии, имена, отчества (при наличии), должности экспертов органа по аттестации, назначенных для проведения аттестации объекта информатизации;

в) наименование и реквизиты документов ФСТЭК России, устанавливающих требования по защите информации, на соответствие которым проводится аттестация объекта информатизации;

г) угрозы безопасности информации, актуальные для объекта информатизации, или сведения о модели угроз безопасности информации в случае ее разработки в соответствии с требованиями по защите информации.

13.2. Раздел, касающийся программы аттестационных испытаний объекта информатизации, должен включать перечень работ по аттестации объекта информатизации, в том числе работы по обследованию объекта информатизации в условиях его эксплуатации, проведению аттестационных испытаний в соответствии с разрабатываемыми методиками испытаний, оформлению результатов аттестационных испытаний, а также общий срок проведения аттестации объекта информатизации и сроки выполнения каждой работы по

аттестации объекта информатизации, фамилию и инициалы эксперта органа по аттестации, ответственного за проведение каждой работы.

13.3. Раздел, касающийся методик аттестационных испытаний объекта информатизации, должен включать для каждого аттестационного испытания порядок, условия, исходные данные и методы испытаний, применяемые при проведении испытаний средства контроля эффективности защиты информации от несанкционированного доступа, а также контрольно-измерительное и испытательное оборудование.

14. Программа и методики аттестационных испытаний объекта информатизации согласовываются органом по аттестации с владельцем объекта информатизации и утверждаются руководителем органа по аттестации до начала аттестационных испытаний.

В ходе аттестационных испытаний объекта информатизации орган по аттестации может вносить изменения в программу и методики аттестационных испытаний объекта информатизации по согласованию с владельцем объекта информатизации.

15. Аттестационные испытания включают следующие мероприятия и работы:

а) оценку соответствия технического паспорта объекта информатизации, акта классификации информационной (автоматизированной) системы, акта категорирования значимого объекта, состава и содержания эксплуатационной документации на систему защиты информации объекта информатизации и документов по защите информации владельца объекта информатизации требованиям по защите информации и настоящему Порядку;

б) проверку наличия и согласования с ФСТЭК России в соответствии с пунктом 3 Требований к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации, утвержденных постановлением Правительства Российской Федерации от 6 июля 2015 г. № 676 (Собрание законодательства Российской Федерации, 2015, № 28, ст. 4241; 2020, № 42, ст. 6615; 2021, № 23, ст. 4079), модели угроз безопасности информации, технического задания на создание (развитие, модернизацию) объекта информатизации (только для государственных информационных систем);

в) обследование объекта информатизации на предмет оценки соответствия объекта информатизации и условий его эксплуатации требованиям по защите информации, а также документам, предусмотренным пунктом 11 настоящего Порядка;

г) проверку наличия документов, содержащих результаты анализа уязвимостей, проведенного на этапах предварительных или приемочных испытаний системы защиты информации объекта информатизации;

д) проверку наличия сведений о средствах защиты информации, установленных на объекте информатизации, в реестре сертифицированных средств защиты информации, ведение которого осуществляет ФСТЭК России в соответствии с Положением о системе сертификации средств защиты информации, утвержденным приказом ФСТЭК России от 3 апреля 2018 г.

№ 55 (зарегистрирован Минюстом России 11 мая 2018 г., регистрационный № 51063) (в случае наличия требования об обязательном применении сертифицированных средств защиты информации), или документов, подтверждающих проведение оценки соответствия средств защиты информации требованиям по безопасности информации в формах, отличных от сертификации;

е) проверку наличия у владельца объекта информатизации работников, ответственных за обеспечение защиты информации в ходе эксплуатации объекта информатизации, в том числе за проведение оценки угроз безопасности информации, управление (администрирование) системой защиты информации (администраторов безопасности), управление конфигурацией объекта информатизации, реагирование на инциденты, информирование и обучение персонала, контроль за обеспечением уровня защиты информации, а также проверку достаточности установленных для них обязанностей в соответствии с требованиями по защите информации;

ж) оценку уровня знаний и умений работников владельца объекта информатизации, ответственных за обеспечение защиты информации, в соответствии с установленными для них обязанностями в эксплуатационной документации и документах по защите информации владельца объекта информатизации;

з) оценку соответствия принятых на объекте информатизации организационных мер требованиям по защите информации и их достаточности для защиты от актуальных для объекта информатизации угроз безопасности информации;

и) оценку соответствия принятых на объекте информатизации технических мер по защите информации от несанкционированного доступа (воздействия на информацию) требованиям по защите информации и их достаточности для защиты от актуальных для объекта информатизации угроз безопасности информации;

к) оценку эффективности защиты (защищенности) информации от утечки по техническим каналам (только для защищаемых помещений).

16. При проведении аттестационных испытаний органом по аттестации проводятся:

а) при проведении мероприятий и работ, предусмотренных подпунктами «а» – «з» пункта 15 настоящего Порядка, – оценка соответствия системы защиты информации объекта информатизации требованиям по защите информации на основе анализа экспертами органа по аттестации документов, предусмотренных пунктом 15 настоящего Порядка;

б) при проведении работ, предусмотренных подпунктом «и» пункта 15 настоящего Порядка, – испытания системы защиты информации путем осуществления тестирования ее функций безопасности (функциональное тестирование), анализ уязвимостей с использованием средств контроля эффективности защиты информации от несанкционированного доступа, а также испытания системы защиты информации путем осуществления попыток несанкционированного доступа (воздействия) в обход системы защиты информации с использованием средств тестирования;

в) при проведении работ, предусмотренных подпунктом «к» пункта 15 настоящего Порядка, – оценка показателей эффективности защиты информации с применением контрольно-измерительного и испытательного оборудования.

17. В ходе аттестационных испытаний объекта информатизации владельцем объекта информатизации могут вноситься изменения в объект информатизации, в том числе в архитектуру его системы защиты информации, в целях приведения объекта информатизации в соответствие с требованиями по защите информации.

18. По результатам аттестационных испытаний орган по аттестации оформляет заключение по результатам аттестационных испытаний объекта информатизации (далее – заключение), включающее следующие сведения:

а) наименование объекта информатизации и его назначение, состав программно-технических, программных средств и средств защиты информации;

б) класс защищенности информационной (автоматизированной) системы, категория значимости значимого объекта;

в) фамилии, имена, отчества (при наличии), должности экспертов органа по аттестации, проводивших аттестацию объекта информатизации;

г) дату утверждения программы и методик аттестационных испытаний объекта информатизации;

д) срок проведения аттестационных испытаний;

д) наименования и реквизиты документов ФСТЭК России, устанавливающих требования по защите информации, на соответствие которым проводилась аттестация объекта информатизации;

е) результаты испытаний, предусмотренных пунктом 15 настоящего Порядка, с описанием состава проведенных работ и испытаний в соответствии с программой и методикой испытаний, указанием сроков выполнения каждого испытания и экспертов органа по аттестации, ответственных за проведение каждого испытания, используемых экспертами при испытаниях средств, а также заключение о соответствии (несоответствии) требованиям по защите информации по каждой проведенной работе и испытанию;

ж) рекомендации по устранению несоответствий системы защиты информации объекта информатизации требованиям по защите информации (далее – недостатки) в случае их выявления при проведении аттестационных испытаний;

з) вывод о возможности или невозможности выдачи аттестата соответствия или о необходимости доработки системы защиты информации объекта информатизации.

Заключение подписывается экспертами органа по аттестации, проводившими аттестацию объекта информатизации, и утверждается руководителем органа по аттестации.

19. По результатам испытаний, предусмотренных подпунктами «и» и «к» пункта 15 настоящего Порядка, органом по аттестации наряду с заключением по результатам аттестационных испытаний оформляются протоколы аттестационных испытаний объекта информатизации (далее – протоколы), содержащие:

а) наименование испытания в соответствии с программой и методикой испытаний;

б) дату утверждения программы и методик аттестационных испытаний объекта информатизации;

в) дату и место проведения аттестационных испытаний;

г) критерии выполнения требований по защите информации, в отношении которых проводились испытания;

д) условия и исходные данные для проведения испытаний;

е) применяемые при проведении испытаний средства контроля эффективности защиты информации от несанкционированного доступа, а также контрольно-измерительное и испытательное оборудование;

ж) описание порядка испытаний по оценке критериев выполнения требований по защите информации;

з) результаты испытаний по каждому оцениваемому критерию выполнения требований по защите информации.

Протоколы подписываются экспертами органа по аттестации, проводившими аттестационные испытания объекта информатизации.

20. Заключение и протоколы в течение 5 рабочих дней после утверждения органом по аттестации направляются владельцу объекта информатизации.

21. В случае выявления в ходе аттестационных испытаний недостатков, которые можно устранить в процессе аттестации объекта информатизации, владелец объекта информатизации обеспечивает их устранение, а орган по аттестации оценивает качество такого устранения.

По результатам устранения недостатков орган по аттестации повторно оформляет заключение, в которое наряду со сведениями, указанными в пункте 18 настоящего Порядка, включаются сведения об устранении владельцем объекта информатизации всех выявленных недостатков, а также делается вывод о возможности выдачи аттестата соответствия требованиям по защите информации (далее – аттестат соответствия) на объект информатизации.

22. Аттестат соответствия оформляется органом по аттестации по форме согласно приложению № 4 к настоящему Порядку.

Аттестат соответствия подписывается руководителем органа по аттестации и заверяется печатью органа по аттестации (при наличии).

Аттестат соответствия вручается органом по аттестации владельцу объекта информатизации или направляется ему заказным почтовым отправлением с уведомлением о вручении.

23. В случае выявления при проведении аттестационных испытаний недостатков, которые невозможно устранить в процессе аттестации объекта информатизации, работы по аттестации объекта информатизации завершаются, аттестат соответствия не оформляется.

24. Владелец объекта информатизации в случае несогласия с выявленными органом по аттестации недостатками и выводами, содержащимися в заключении и протоколах, направляет в течение 5 рабочих дней с момента получения заключения и протоколов письменное обращение с обоснованием такого несогласия (далее – обращение) в ФСТЭК России. Обращения федеральных органов государственной власти или государственных корпораций направляются в центральный аппарат ФСТЭК России, обращения иных владельцев объектов информатизации направляются в управление ФСТЭК России по федеральному

округу, на территории которого расположен объект информатизации (далее – территориальный орган ФСТЭК России).

К обращению прилагаются в электронном виде копии следующих документов:

а) технического паспорта на объект информатизации;

б) акта классификации информационной (автоматизированной) системы (акта категорирования значимого объекта);

в) программы и методик аттестационных испытаний объекта информатизации;

г) заключения и протоколов.

25. ФСТЭК России (территориальный орган ФСТЭК России) в течение 10 календарных дней с даты получения обращения проводит оценку документов, указанных в пункте 24 настоящего Порядка, на предмет соответствия проведенных органом по аттестации аттестационных испытаний и выводов, содержащихся в заключении, требованиям по защите информации и настоящему Порядку. По согласованию с владельцем объекта информатизации работники ФСТЭК России (территориального органа ФСТЭК России) проводят контрольные испытания на объекте информатизации в соответствии с пунктами 15 и 16 настоящего Порядка.

26. Если по результатам оценки, проведенной в соответствии с пунктом 25 настоящего Порядка, установлено несоответствие аттестационных испытаний и (или) выводов, содержащихся в заключении или протоколах, требованиям по защите информации или настоящему Порядку, ФСТЭК России (территориальный орган ФСТЭК России) направляет в орган по аттестации уведомление о необходимости устранения выявленных недостатков в указанный в уведомлении срок. Копия уведомления направляется владельцу объекта информатизации. Орган по аттестации обязан устранить недостатки, выявленные ФСТЭК России по результатам оценки документов, в указанный в уведомлении срок и оформить аттестат соответствия.

Если по результатам оценки, проведенной в соответствии с пунктом 25 настоящего Порядка, ФСТЭК России (территориальным органом ФСТЭК России) подтвержден вывод органа по аттестации о невозможности выдачи аттестата соответствия, аттестат соответствия на объект информатизации органом по аттестации не оформляется. Результаты проведенной оценки направляются ФСТЭК России (территориальным органом ФСТЭК России) владельцу объекта информатизации для устранения недостатков, выявленных органом по аттестации.

27. Орган по аттестации в течение 5 рабочих дней после подписания аттестата соответствия представляет в ФСТЭК России (территориальный орган ФСТЭК России) в электронном виде копии следующих документов:

а) аттестата соответствия объекта информатизации;

б) технического паспорта на объект информатизации;

в) акта классификации информационной (автоматизированной) системы, акта категорирования значимого объекта;

г) программы и методик аттестационных испытаний объекта информатизации;