

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

ПРИКАЗ
от "___" _____ г. N ___

**ОБ УТВЕРЖДЕНИИ ПОРЯДКА ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ РАБОТ
ПО АТТЕСТАЦИИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ НА СООТВЕТСТВИЕ
ТРЕБОВАНИЯМ О ЗАЩИТЕ ИНФОРМАЦИИ, 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. N 1085 (Собрание законодательства Российской Федерации, 2004, N 34, ст. 3541; 2020, N 35, ст. 5554), приказываю:

1. Утвердить прилагаемый [Порядок](#) организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации, не составляющей государственную тайну.

2. Установить, что указанный в [пункте 1](#) настоящего приказа [Порядок](#) применяется для аттестации объектов информатизации с 1 июня 2021 г.

Директор Федеральной
службы по техническому
и экспортному контролю
В.СЕЛИН

Утвержден
приказом ФСТЭК России
от _____ г. N ___

ПОРЯДОК
ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ РАБОТ ПО АТТЕСТАЦИИ ОБЪЕКТОВ
ИНФОРМАТИЗАЦИИ НА СООТВЕТСТВИЕ ТРЕБОВАНИЯМ О ЗАЩИТЕ
ИНФОРМАЦИИ, 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, установленным ФСТЭК России в соответствии с [частью 5 статьи 16](#) Федерального закона от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (Собрание законодательства Российской Федерации, 2006, N 31, ст. 3448; 2014, N 30, ст. 4243) и [подпунктом 9.1 пункта 8](#) Положения о Федеральной службе по техническому и

экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. N 1085 (Собрание законодательства Российской Федерации, 2004, N 34, ст. 3541; 2018, N 20, ст. 2818) (далее - требования по защите информации), а также требования к форме и содержанию разрабатываемых при проведении таких работ документов.

2. К объектам информатизации, подлежащим аттестации в соответствии с настоящим Порядком, относятся государственные и муниципальные информационные системы, информационные системы управления производством, используемые организациями оборонно-промышленного комплекса, защищаемые помещения, а также значимые объекты критической информационной инфраструктуры и автоматизированные системы 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, для которых при их создании установлены требования к оценке соответствия требованиям по защите информации в форме аттестации.

3. Аттестация объектов информатизации проводится на этапе создания объекта информатизации и предусматривает проведение комплекса организационных и технических мероприятий (аттестационных испытаний), в результате которых подтверждается соответствие объекта информатизации требованиям по защите информации в условиях его эксплуатации.

II. Организация работ по аттестации объектов информатизации

4. Аттестация объектов информатизации проводится 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 (далее - владельцы объектов информатизации).

5. Для проведения аттестационных испытаний владелец объекта информатизации привлекает организацию, имеющую лицензию на осуществление деятельности по технической защите конфиденциальной информации (в части проведения работ и оказания услуг по аттестационным испытаниям и аттестации на соответствие требованиям по защите информации), выданную ФСТЭК России в соответствии с [пунктом 5 части 1 статьи 12](#) Федерального закона от 4 мая 2011 г. N 99-ФЗ "О лицензировании отдельных видов деятельности" (Собрание законодательства Российской Федерации, 2011, N 19, ст. 2716; 2020, N 31, ст. 5029) и [Положением](#) о лицензировании деятельности по технической защите конфиденциальной информации, утвержденным постановлением Правительства Российской Федерации от 3 февраля 2012 г. N 79 (Собрание законодательства Российской Федерации, 2012, N 7, ст. 863; 2020, N 49, ст. 7943) (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, на которое возложены функции по защите информации, после информирования ФСТЭК России о принятом решении и при наличии необходимых для проведения работ по аттестации:

а) средств защиты информации и средств контроля эффективности защиты информации (для аттестации информационных (автоматизированных) систем), контрольно-измерительного, производственного и испытательного оборудования (для аттестации защищаемых помещений);

б) нормативных правовых актов и методических документов ФСТЭК России, 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. N 1085, национальных стандартов;

в) работников, обладающих знаниями и навыками в области технической защиты 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 защиты информации и аттестации объектов информатизации (далее - эксперты органа по аттестации). Члены аттестационной комиссии обязаны обеспечить качество и объективность результатов аттестационных испытаний объекта информатизации. Проведение аттестации объекта информатизации должностными лицами, работниками органа по аттестации, участвующими в проектировании, внедрении системы защиты информации объекта информатизации, не допускается.

8. Срок проведения аттестации объекта информатизации устанавливается владельцем объекта информатизации по согласованию с органом по аттестации.

9. Информация об объекте информатизации, полученная органом по аттестации в ходе аттестации объекта информатизации, подлежит защите в соответствии с законодательством Российской Федерации и требованиями владельца этого объекта информатизации.

III. Проведение работ по аттестации объектов информатизации

10. Аттестация объекта информатизации проводится владельцем объекта информатизации до ввода объекта информатизации в эксплуатацию после проведения мероприятий по разработке и внедрению системы защиты информации объекта информатизации.

11. Для проведения работ по аттестации объекта информатизации владелец объекта информатизации представляет в орган по аттестации копии следующих документов:

а) технический паспорт объекта информатизации;

б) акт классификации информационной (автоматизированной) системы, акт категорирования значимого объекта критической информационной инфраструктуры (далее - акт категорирования значимого объекта);

в) модель угроз безопасности информации (только для информационных (автоматизированных) систем);

г) техническое задание на создание (модернизацию) объекта информатизации или частное техническое задание на создание (модернизацию) системы защиты информации объекта информатизации;

д) проектную документацию на систему защиты информации объекта информатизации;

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

ж) документы по технической защите информации владельца объекта информатизации, регламентирующие обеспечение защиты информации в ходе эксплуатации объекта информатизации, в том числе план мероприятий по защите информации на объекте информатизации, документы по анализу угроз безопасности информации, управлению системой защиты информации, управлению конфигурацией объекта информатизации, реагированию на инциденты, информированию и обучению персонала, контролю за обеспечением уровня защищенности информации.

Дополнительно владелец объекта информатизации представляет в орган по аттестации копии материалов, содержащие результаты анализа уязвимостей информационной (автоматизированной) системы, а также материалы, оформленные по

результатам предварительных и приемочных испытаний системы защиты информации информационной (автоматизированной) системы (протоколы, заключения).

Форма технического паспорта на объект информатизации приведена в приложении N 1 к настоящему Порядку. Форма акта классификации информационной (автоматизированной) системы приведена в приложении N 2 к настоящему Порядку.

По решению владельца объекта информатизации указанные в настоящем пункте копии документов могут быть представлены в орган по аттестации в на бумажном носителе или в электронном виде.

12. На основе анализа документов и материалов, предусмотренных [пунктом 11](#) настоящего Порядка, орган по аттестации разрабатывает программу и методики аттестационных испытаний.

13. Программа и методики аттестационных испытаний может быть уточнена органом по аттестации по согласованию с владельцем объекта информатизации в ходе обследования объекта информатизации в условиях его эксплуатации.

Обследование информационной (автоматизированной) системы, компоненты которой расположены вне границ одной контролируемой зоны (далее - распределенная информационная (автоматизированной) система), и имеющей клиент-серверную архитектуру, в том числе функционирующей на базе информационно-телекоммуникационной инфраструктуры центра обработки данных, должно предусматривать уточнение данных по ее серверной части или информационно-телекоммуникационной инфраструктуре основного и резервного (при наличии) центра обработки данных, информационно-телекоммуникационной сети, используемой для передачи информации, а также не менее чем по 30% типовым клиентским автоматизированным рабочим местам, входящим в состав распределенной информационной (автоматизированной) системы. Выборка обследуемых в условиях эксплуатации клиентских автоматизированных рабочих мест производится органом по аттестации. Обследование остальных клиентских автоматизированных рабочих мест проводится на основе анализа документов, представленных владельцем объекта информатизации в соответствии с [пунктом 11](#) настоящего Порядка.

14. В случае несоответствия сведений, содержащихся в документах, предусмотренных [пунктом 11](#) настоящего Порядка, условиям эксплуатации объекта информатизации, орган по аттестации представляет владельцу объекта информатизации предложения по доработке объекта информатизации, изменения условий эксплуатации или внесению изменений в указанные в [пункте 11](#) настоящего Порядка документы.

15. 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.

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

а) наименование и краткое описание архитектуры объекта информатизации, класс защищенности информационной (автоматизированной) системы, акт категорирования 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) классы угроз безопасности информации, актуальных для объекта информатизации.

15.2. Раздел, касающийся программы аттестационных испытаний объекта информатизации, должен включать перечень работ по аттестации объекта информатизации: 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, сроки выполнения каждой работы по аттестации объекта информатизации, фамилию и инициалы эксперта органа по аттестации, ответственного за проведение каждой работы.

15.3. Раздел, касающийся методик аттестационных испытаний объекта информатизации, должен включать описание методики проведения каждого аттестационного испытания объекта информатизации: характеристика, параметр требования, на соответствие которому проводится испытание, исходные данные и порядок испытания, методы испытания, применяемые при проведении испытания средства контроля эффективности защиты информации, средства защиты информации, контрольно-измерительное и испытательное оборудование.

16. 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.

17. Аттестационные испытания включают:

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

б) проверку наличия и согласования с ФСТЭК России модели угроз безопасности информации и технического задания на создание (модернизацию) объекта информатизации или частного технического задания на создание (модернизацию) системы защиты информации объекта информатизации (только для государственных и муниципальных информационных систем);

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

г) 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. N 55 (зарегистрирован Минюстом России 11 мая 2018 г., регистрационный N 51063) (в случае наличия требования об обязательном применении сертифицированных средств защиты информации), или иных документов (сведений), подтверждающих проведение оценки соответствия средства защиты информации требованиям по безопасности информации (в случае наличия требования об обязательном применении средств защиты информации, прошедших процедуру оценки соответствия требованиям по безопасности информации);

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

е) оценку информированности и уровня знаний работников владельца объекта информатизации, ответственных за обеспечение защиты информации в ходе эксплуатации объекта информатизации, по вопросам управления (администрирования) системой защиты информации, управления конфигурацией объекта информатизации, реагирования на инциденты, контроля за обеспечением уровня защищенности информации, в соответствии с установленными для них владельцем обязанностями;

ж) 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;

з) оценку соответствия принятых на объекте информатизации 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;

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

18. При проведении аттестационных испытаний органом по аттестации должны применяться следующие методы испытаний (проверок):

а) при проведении мероприятий, предусмотренных [подпунктами "а" - "ж" пункта 17](#) настоящего Порядка, - экспертно-документальный метод;

б) при проведении мероприятий, предусмотренных [подпунктом "з" пункта 17](#) настоящего Порядка, - анализ уязвимостей с использованием средств контроля эффективности защиты информации и испытания системы защиты информации путем осуществления (имитации) попыток несанкционированного доступа (воздействия) в обход системы защиты информации, в том числе с использованием специальных программных тестирующих средств (в случае технической возможности);

в) при проведении мероприятий, предусмотренных [подпунктом "и" пункта 17](#) настоящего Порядка, - экспертно-документальный метод и инструментально-расчетные методы с применением контрольно-измерительного и испытательного оборудования.

Испытания распределенной информационной (автоматизированной) системы, имеющей клиент-серверную архитектуру, в том числе функционирующей на базе информационно-телекоммуникационной инфраструктуры центра обработки данных, проводятся путем анализа уязвимостей и осуществления (имитации) попыток несанкционированного доступа (воздействия) в обход системы защиты информации непосредственно на объекте информатизации или удаленно (при предоставлении владельцем сетевого доступа к объекту информатизации). При этом испытания должны предусматривать анализ и тестирование серверной части или информационно-телекоммуникационной инфраструктуры основного и резервного (при наличии) центра обработки данных, информационно-телекоммуникационной сети, используемой для передачи информации, а также не менее чем 30% типовых клиентских автоматизированных рабочих мест, входящих в состав распределенной информационной (автоматизированной) системы. Выборка тестируемых клиентских автоматизированных рабочих мест производится органом по аттестации. Условия и порядок проведения таких испытаний устанавливаются в программе и методиках аттестационных испытаний.

19. В ходе аттестационных испытаний объекта информатизации в целях его приведения в соответствие требованиям по защите информации владельцем объекта информатизации могут вноситься изменения в состав объекта информатизации, в том числе в состав системы защиты информации объекта информатизации и технический паспорт объекта информатизации, с отметкой о дате и содержании таких изменений.

20. По результатам аттестационных испытаний орган по аттестации оформляет заключение по результатам аттестационных испытаний объекта информатизации, включающее следующие сведения:

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

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

дата утверждения программы и методик аттестационных испытаний объекта информатизации;

срок проведения аттестационных испытаний;

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

результаты испытаний, предусмотренных [пунктом 18](#) 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, заключением о соответствии (несоответствии) требованиям о защите информации по каждому испытанию;

рекомендации по устранению несоответствий системы защиты информации объекта информатизации требованиям по защите информации в случае их выявления при проведении аттестационных испытаний;

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

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

21. По результатам испытаний, предусмотренных [подпунктами "з" и "и" пункта 17](#) настоящего Порядка, органом по аттестации наряду с заключением по результатам аттестационных испытаний оформляются протоколы аттестационных испытаний объекта информатизации, содержащие:

наименование и описание архитектуры объекта информатизации;

дату утверждения программы и методик аттестационных испытаний объекта информатизации;

даты и места проведения аттестационных испытаний, а также состав компонентов распределенной информационной (автоматизированной) системы, прошедших испытания;

описание порядка и условий проведенных испытаний, применяемых при проведении испытаний методов, средств контроля эффективности защиты информации или контрольно-измерительного и испытательного оборудования;

результаты испытаний по каждому испытываемому параметру, характеристике требования к объекту информатизации;

вывод о соответствии (несоответствии) объекта информатизации требованиям по защите информации.

Протоколы аттестационных испытаний объекта информатизации подписываются экспертами органа по аттестации, проводившими аттестацию объекта информатизации.

22. Заключение по результатам аттестационных испытаний объекта информатизации и протоколы аттестационных испытаний объекта информатизации направляются органом по аттестации владельцу объекта информатизации.

23. В случае выявления при проведении аттестационных испытаний несоответствий системы защиты информации объекта информатизации требованиям по защите информации, которые можно устранить в ходе аттестации объекта информатизации, владелец объекта информатизации при необходимости с привлечением организации (структурного подразделения), выполнившей работы по проектированию и (или) внедрению системы защиты информации объекта информатизации, устраняет выявленные несоответствия, а орган по аттестации оценивает качество их устранения. При

необходимости орган по аттестации проводит дополнительные испытания, по результатам которых оформляет протоколы аттестационных испытаний.

24. В случае выявления при проведении аттестационных испытаний несоответствий системы защиты информации объекта информатизации требованиям по защите информации, которые невозможно устранить в ходе аттестации объекта информатизации, копия заключения по результатам аттестационных испытаний объекта информатизации, содержащего вывод о невозможности выдачи аттестата соответствия на объект информатизации, направляется в электронном виде в ФСТЭК России. К заключению по результатам аттестационных испытаний объекта информатизации прилагаются в электронном виде копии следующих документов:

технического паспорта на объект информатизации;

акта классификации информационной (автоматизированной) системы (акта категорирования);

программы и методик аттестационных испытаний объекта информатизации;

протоколов аттестационных испытаний.

Копии технического паспорта на объект информатизации, акта классификации информационной (автоматизированной) системы, акта категорирования значимого объекта передаются в электронном виде владельцем объекта информатизации в орган по аттестации.

Заключение по результатам аттестационных испытаний объекта информатизации, не являющегося федеральной информационной системой или информационной системой, владельцем которой является государственная корпорация, а также прилагаемые к нему копии документов направляются органом по аттестации в территориальный орган ФСТЭК России, на территории которого расположен объект информатизации.

В случае испытаний распределенной информационной (автоматизированной) системы, имеющей клиент-серверную архитектуру (функционирующей на базе информационно-телекоммуникационной инфраструктуры центра обработки данных), заключение по результатам аттестационных испытаний направляется в территориальный орган ФСТЭК России, на территории которого расположена серверная часть (информационно-телекоммуникационная инфраструктура основного центра обработки данных) информационной (автоматизированной) системы.

25. Владелец объекта информатизации в случае несогласия с выявленными при проведении аттестационных испытаний несоответствиями системы защиты информации объекта информатизации требованиям по защите информации и выводами, содержащимися в заключении по результатам аттестационных испытаний объекта информатизации, направляет письменное обращение, содержащее обоснование такого несогласия, в ФСТЭК России (территориальный орган ФСТЭК России).

ФСТЭК России (территориальный орган ФСТЭК России) в течение 10 календарных дней с даты получения обращения осуществляет экспертно-документальный анализ документов, указанных в [пункте 24](#) настоящего Порядка, на предмет соответствия выводов, содержащихся в заключении по результатам аттестационных испытаний требованиям по защите информации. По согласованию с владельцем объекта информатизации работники ФСТЭК России (территориального органа ФСТЭК России) проводят контрольные испытания на объекте информатизации.

ФСТЭК России (территориальный орган ФСТЭК России) оформляет заключение о возможности или невозможности выдачи аттестата соответствия, которое направляет владельцу объекта информатизации и органу по аттестации.

26. Аттестат соответствия оформляется органом по аттестации по [форме](#) согласно приложению N 3 к настоящему Порядку.

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

27. Аттестат соответствия выдается на весь срок эксплуатации объекта информатизации, если иное не установлено требованиями по защите информации, на соответствие которым проводилась аттестация объекта информатизации.

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

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

аттестата соответствия объекта информатизации;

технического паспорта на объект информатизации;

акта классификации информационной (автоматизированной) системы (акта категорирования);

программы и методик аттестационных испытаний объекта информатизации;

заклучения по результатам аттестационных испытаний объекта информатизации;

протоколов аттестационных испытаний.

Копии технического паспорта на объект информатизации, акта классификации информационной (автоматизированной) системы, акта категорирования значимого объекта передаются в электронном виде владельцем объекта информатизации в орган по аттестации.

30. ФСТЭК России (территориальный орган ФСТЭК России) в течение 3 рабочих дней со дня получения от органа по аттестации документов, предусмотренных [пунктом 29](#) настоящего Порядка, вносит сведения об аттестованном объекте информатизации в реестр аттестованных объектов информатизации, ведение которого осуществляется ФСТЭК России в соответствии с [подпунктом 20 пункта 9](#) Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. N 1085.

31. ФСТЭК России (территориальный орган ФСТЭК России) проводит экспертно-документальную оценку документов, представленных органом по аттестации в соответствии с [пунктом 29](#) настоящего Порядка.

32. В случае выявления по результатам проведенной оценки несоответствий представленных материалов требованиям настоящего Порядка, а также требованиям по защите информации, ФСТЭК России (территориальный орган ФСТЭК России) оформляет заключение, содержащее описание выявленных несоответствий и рекомендации по их устранению, и направляет его владельцу объекта информатизации и органу по аттестации.

33. В случае утраты аттестата соответствия владелец объекта информатизации вправе обратиться в орган по аттестации с заявлением о выдаче дубликата аттестата соответствия.

В течение 20 рабочих дней со дня получения заявления о выдаче дубликата аттестата соответствия орган по аттестации оформляет дубликат аттестата соответствия с пометкой "дубликат, оригинал аттестата соответствия признается недействующим" и вручает его владельцу объекта информатизации или направляет заказным почтовым отправлением с уведомлением о вручении.

34. Действие аттестата соответствия приостанавливается ФСТЭК России (территориальным органом ФСТЭК России) в случае:

установления факта несоответствия аттестованного объекта информатизации требованиям по защите информации, в результате которого имеется или имелась возможность возникновения угрозы безопасности информации;

обращения владельца объекта информатизации о приостановлении действия аттестата соответствия.

Установление факта несоответствия аттестованного объекта информатизации требованиям по защите информации осуществляется на основании:

результатов контроля за состоянием работ по технической защите информации, осуществляемого ФСТЭК России в соответствии с подпунктом 7 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. N 1085;

результатов контроля за реализацией настоящего Порядка.

35. Решение о приостановлении действия аттестата соответствия оформляется приказом ФСТЭК России (территориального органа ФСТЭК России).

Действие аттестата соответствия может быть приостановлено на срок не более 90 календарных дней.

ФСТЭК России (территориальный орган ФСТЭК России) в течение 5 рабочих дней со дня принятия решения направляет заказным почтовым отправлением с уведомлением о вручении или вручает владельцу объекта информатизации уведомление о приостановлении действия аттестата соответствия.

36. ФСТЭК России (территориальный орган ФСТЭК России) вносит сведения о приостановлении действия аттестата соответствия в реестр аттестованных объектов информатизации.

37. В случае приостановления действия аттестата соответствия владелец объекта информатизации прекращает эксплуатацию объекта информатизации.

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

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

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.

39. Решение о возобновлении действия аттестата соответствия на объект информатизации оформляется приказом ФСТЭК России (территориального органа ФСТЭК России).

ФСТЭК России (территориальный орган ФСТЭК России) в течение 5 рабочих дней со дня принятия решения направляет заказным почтовым отправлением с уведомлением о вручении или вручает владельцу объекта информатизации уведомление о возобновлении действия аттестата соответствия.

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

непредставления владельцем объекта информатизации в установленный в уведомлении о приостановлении действия аттестата соответствия срок материалов, подтверждающих устранение несоответствия объекта информатизации требованиям по защите информации;

обращения владельца объекта информатизации о прекращении действия аттестата соответствия.

41. Решение о прекращении действия аттестата соответствия оформляется приказом ФСТЭК России (территориального органа ФСТЭК России).

Приказ территориального органа ФСТЭК России о прекращении действия аттестата соответствия, оформляемый территориальным органом ФСТЭК России, подлежит согласованию со структурным подразделением ФСТЭК России, на которое возложены вопросы организации аттестации объектов информатизации.

ФСТЭК России (территориальный орган ФСТЭК России) в течение 5 рабочих дней со дня принятия решения направляет заказным почтовым отправлением с уведомлением о вручении или вручает владельцу объекта информатизации уведомление о прекращении действия аттестата соответствия.

42. В случае прекращения действия аттестата соответствия владелец объекта информатизации прекращает эксплуатацию объекта информатизации, если действие аттестата соответствия ранее не было приостановлено.

43. ФСТЭК России (территориальный орган ФСТЭК России) вносит сведения о прекращении действия аттестата соответствия в реестр аттестованных объектов информатизации.

Приложение N 1
к Порядку организации и проведения
работ по аттестации объектов
информатизации на соответствие
требованиям о защите информации,
не составляющей государственную
тайну, утвержденному приказом
ФСТЭК России
от _____ г. N ____

Форма технического паспорта
на объект информатизации

УТВЕРЖДАЮ

(руководитель (уполномоченное лицо)
владельца объекта информатизации)

(подпись, инициалы и фамилия)

"__" _____ 20__ г.

ТЕХНИЧЕСКИЙ ПАСПОРТ
информационной (автоматизированной) системы

(наименование информационной (автоматизированной) системы)

1. Общие сведения об информационной (автоматизированной) системе.

1.1. Наименование и назначение информационной (автоматизированной) системы: _____.

1.2. Расположение программно-технических средств информационной (автоматизированной) системы: _____.
(указываются адреса расположения средств)

1.3. Установленный класс защищенности информационной (автоматизированной) системы (категория значимости): _____.

(указываются реквизиты акта классификации (категорирования))

1.4. Сведения о вводе информационной (автоматизированной) системы в эксплуатацию: _____.

(указываются номер и дата приказа о вводе в эксплуатацию)

2. Условия эксплуатации информационной (автоматизированной) системы

2.1. Сведения об архитектуре информационной (автоматизированной) системы, включающие описание структуры и состава (типовых компонентов), структурную (топологическую) схему с указанием информационных связей между компонентами информационной системы (автоматизированной) системы и иными информационными системами, в том числе с сетью Интернет _____.

2.2. Описание технологического процесса обработки информации и режимы доступа к информационным ресурсам, включающее описание всех типов внешних, внутренних пользователей (привилегированных, непривилегированных), полномочий пользователей и тип доступа к информационным ресурсам _____.

2.3. Сведения об аттестате соответствия информационно-телекоммуникационной инфраструктуры центра обработки данных, на базе которой функционирует информационная (автоматизированная) система, а также о модели услуг, по которой предоставляются вычислительные услуги (заполняется при условии аттестации информационной (автоматизированной) системы на базе аттестованной на соответствие требованиям по защите информации информационно-телекоммуникационной инфраструктуры центра обработки данных): _____.

(указываются реквизиты аттестата соответствия и модель услуг)

3. Состав информационной системы (автоматизированной) системы.

3.1. Состав программно-технических средств информационной (автоматизированной) системы: _____.

(указываются типы технических средств, их наименования и модели)

3.2. Состав общесистемного и прикладного программного обеспечения информационной (автоматизированной) системы: _____.

(указываются типы программного обеспечения, их наименования и основные (мажорные) версии)

3.3. Состав телекоммуникационного оборудования информационной (автоматизированной) системы и используемые для передачи информации линии связи: _____.

(указываются типы оборудования, их наименования и основные (мажорные) версии)

3.4. Состав средств защиты информации, используемых в информационной системе (автоматизированной) системе: _____.

(указываются типы средств их наименования и основные (мажорные) версии, сведения о сертификатах соответствия)

4. Сведения о соответствии информационной (автоматизированной) системы требованиям по безопасности информации.

4.1. Сведения о протоколах сертификационных испытаний информационной (автоматизированной) системы _____.

(реквизиты протоколов и дата их выдачи)

4.2. Сведения о заключении по результатам сертификационных испытаний информационной (автоматизированной) системы _____.

(реквизиты заключения и дата выдачи)

4.3. Сведения об аттестате информационной (автоматизированной) системы на соответствие требованиям о защите информации: _____.

(реквизиты аттестата соответствия, дата выдачи)

5. Сведения о проведении контроля за обеспечением уровня защищенности информации, содержащейся в информационной (автоматизированной) системе, приведены в таблице 1.

Таблица 1

N п/п	Наименование организации (подразделения), проводившей контроль	Дата проведения контроля	Реквизиты документа с выводами о результатах	Вывод по результатам контроля
1.				
2.				

6. Сведения об изменениях состава, условий эксплуатации информационной (автоматизированной) системы и средств защиты информации приведены в таблице 2.

Таблица 2

N п/п	Дата внесения изменения	Документ, на основании которого внесены изменения	Пункт технического паспорта, в который внесены изменения	Краткая характеристика изменений	Подпись лица, внесшего изменения
1.					
2.					

Ответственный за обеспечение защиты информации в ходе эксплуатации информационной (автоматизированной) системы

_____ (должность)

_____ (подпись, фамилия и инициалы)

" ___ " _____ 20__ г.

УТВЕРЖДАЮ

_____ (руководитель (уполномоченное лицо) владельца объекта информатизации)

_____ (подпись, инициалы и фамилия)

" ___ " _____ 20__ г.

ТЕХНИЧЕСКИЙ ПАСПОРТ
защищаемого помещения

_____ (наименование защищаемого помещения)

1. Общие сведения о защищаемом помещении

- 1.1. Наименование и назначение защищаемого помещения: _____.
- 1.2. Расположение защищаемого помещения: _____.
(указываются адрес, строение, этаж, номер)
- 1.3. Сведения о проведении проверок защищаемого помещения с целью выявления возможно внедренных электронных устройств перехвата информации ("закладок"): _____.
(указываются реквизиты заключения, наименование организации, проводившей проверки <*>)
- 1.4. Сведения об аттестации защищаемого помещения:

(указываются реквизиты аттестата соответствия требованиям по безопасности информации)

- 1.5. Сведения о вводе защищаемого помещения в эксплуатацию:

(указываются номер и дата приказа о вводе в эксплуатацию защищаемого помещения)

2. Условия расположения и эксплуатации защищаемого помещения

2.1. Сведения и схема расположения защищаемого помещения относительно границ контролируемой зоны с указанием расстояний до ее границ, сведения и схема основных технических средств и систем (в случае их наличия), вспомогательных технических средств и систем, средств защиты информации, а также линий, имеющих выход за пределы контролируемой зоны, относительно границ контролируемой зоны с указанием расстояний до ее границ.

2.2. Сведения и схемы электроснабжения и заземления основных технических средств и систем (в случае их наличия) и вспомогательных технических средств и систем, установленных в защищаемом помещении, включая место расположения трансформаторной подстанции и заземляющего устройства, с указанием расстояний до границ контролируемой зоны, сведения о сопротивлении заземляющего устройства (при наличии основных технических средств и систем).

3. Состав защищаемого помещения

3.1. Состав основных технических средств и систем, установленных в защищаемом помещении, представлен в таблице 1.

Таблица 1

N п/п	Наименование основного технического средства и системы, заводской (инвентарный) номер	Минимальное расстояние до границы контролируемой зоны, м	Сведения о специальных проверках <*>	Сведения о специальных исследованиях или сертификатах соответствия <***>
1.				
2.				

3.2. Состав вспомогательных технических средств и систем, установленных в защищаемом помещении, представлен в таблице 2.

Таблица 2

N п/п	Наименование вспомогательного технического средства и системы, заводской (инвентарный) номер	Минимальное расстояние до основных технических средств и систем, м	Сведения о специальных проверках <*>	Сведения о специальных исследованиях или сертификатах соответствия <***>
1.				
2.				

3.3. Состав средств защиты информации, используемых в защищаемом помещении, представлен в таблице 3.

Таблица 3

N п/п	Наименование и тип средства защиты информации, заводской (инвентарный) номер	Сведения о сертификате соответствия <***>	Номер знака соответствия	Место установки
1.				
2.				

4. Сведения о периодическом контроле защищаемого помещения представлены в таблице 4.

Таблица 4

N п/п	Дата проведения контроля	Вывод по результатам контроля
1		
2		

5. Сведения об изменениях состава, условий размещения и эксплуатации защищаемого помещения представлены в таблице 5.

Таблица 5

N п/п	Дата внесения изменений	Наименование документа, на основании которого внесены изменения	Пункт технического паспорта, в который внесены изменения	Краткая характеристика изменений	Подпись лица, внесшего изменения
1					
2					

Ответственный за эксплуатацию защищаемого помещения

_____ (должность)

_____ (подпись, фамилия и инициалы)

" ___ " _____ 20__ г.

<*> В случае отсутствия необходимости специальной проверки технических средств пункт не заполняется.

<***> В случае отсутствия необходимости применения сертифицированных средств защиты информации пункт не заполняется.

Приложение N 2
к Порядку организации и проведения
работ по аттестации объектов
информатизации на соответствие
требованиям о защите информации,
не составляющей государственную
тайну, утвержденному приказом
ФСТЭК России
от _____ г. N ____

Форма акта
классификации информационной (автоматизированной) системы

УТВЕРЖДАЮ

(руководитель (уполномоченное лицо)
владельца объекта информатизации)

(подпись, инициалы и фамилия)

" ___ " _____ 20__ г.

АКТ
классификации информационной (автоматизированной) системы

(наименование информационной системы
(автоматизированной) системы)

Комиссия, назначенная приказом _____, провела
классификацию информационной (автоматизированной) системы

Комиссия установила:

1. Масштаб информационной (автоматизированной) системы _____

2. Уровень значимости информации, содержащейся в информационной
(автоматизированной) системе _____

3. Класс защищенности информационной (автоматизированной) системы _____

Члены комиссии:

_____	_____
(должность)	(подпись, фамилия и инициалы)
_____	_____
(должность)	(подпись, фамилия и инициалы)

Приложение N 3
к Порядку организации и проведения
работ по аттестации объектов
информатизации, утвержденному
приказом ФСТЭК России
от _____ г. N ____

Форма аттестата
соответствия объекта информатизации

АТТЕСТАТ СООТВЕТСТВИЯ
требованиям по защите информации

N _____
(номер аттестата соответствия в формате АААА.ББББ.ВВВВ
(А - номер выданной органу по аттестации лицензии
на деятельность по технической защите конфиденциальной
информации, Б - порядковый номер объекта информатизации,
аттестованного органом по аттестации, В - год,
в котором выдан аттестат)

Выдан: _____.
(дата выдачи аттестата соответствия)

Настоящий аттестат удостоверяет, что _____

_____,
наименование объекта информатизации, класс защищенности
информационной (автоматизированной) системы)
принадлежащий _____,
(наименование владельца объекта информатизации)
соответствует _____.
(наименование требований по защите информации,
на соответствии которым проводилась аттестация)

Аттестат соответствия выдан на основании результатов аттестационных
испытаний, проведенных органом по аттестации

(наименование и адрес местонахождения органа по аттестации)

Заключение по результатам аттестационных испытаний

(дата утверждения заключения)

Руководитель органа по аттестации

М.П.

СПРАВКА
К ПРОЕКТУ ПРИКАЗА ФЕДЕРАЛЬНОЙ СЛУЖБЫ ПО ТЕХНИЧЕСКОМУ
И ЭКСПОРТНОМУ КОНТРОЛЮ "ОБ УТВЕРЖДЕНИИ ПОРЯДКА ОРГАНИЗАЦИИ
И ПРОВЕДЕНИЯ РАБОТ ПО АТТЕСТАЦИИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ
НА СООТВЕТСТВИЕ ТРЕБОВАНИЯМ О ЗАЩИТЕ ИНФОРМАЦИИ,
НЕ СОСТАВЛЯЮЩЕЙ ГОСУДАРСТВЕННУЮ ТАЙНУ"

Порядок организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации, не составляющей государственную тайну, разработан во исполнение поручения Президента Российской Федерации от 11 июля 2019 г. N Пр-1261 и поручения Правительства Российской Федерации от 18 июля 2019 г. N МА-П10-6116.

Проект нормативного правового акта издан в соответствии с [подпунктом 13.1 пункта 8](#) Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. N 1085 (Собрание законодательства Российской Федерации, 2004, N 34, ст. 3541; 2006, N 49, ст. 5192; 2008, N 43, ст. 4921, N 47, ст. 5431; 2012, N 7, ст. 818; 2013, N 26, ст. 3314; N 52, ст. 7137; 2014, N 36, ст. 4833; N 44, ст. 6041; 2015, N 4, ст. 641; 2016, N 1, ст. 211; 2017, N 48, ст. 7198; 2018, N 20, ст. 2818) и [частью 1 статьи 5](#) Федерального закона "О техническом регулировании" от 27 декабря 2002 г. N 184-ФЗ (Собрание законодательства Российской Федерации, 2002, N 52, ст. 5140; 2007, N 19, ст. 2293; 2011, N 49, ст. 7025).

Проектом приказа ФСТЭК России определяется состав и содержание работ по аттестации объектов информатизации на соответствие требованиям о защите информации, не составляющей государственную тайну, а также требования к форме разрабатываемых при проведении таких работ документов.