ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 58189— 2018

Защита информации

ТРЕБОВАНИЯ К ОРГАНАМ ПО АТТЕСТАЦИИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

Издание официальное

Москва
Стандартинформ
2018

gost.e-ecolog.ru

Предисловие

1 РАЗРАБОТАН Федеральной службой по техническому и экспортному контролю (ФСТЭК России), Федеральным автономным учреждением «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю» (ФАУ «ГНИИИ ПТЗИ ФСТЭК России»)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 362 «Защита информации»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 2 августа 2018 г. № 447-ст

4 ВВЕДЕН ВПЕРВЫЕ

*Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (*gost.e-ecolog.ru

© Стандартинформ, оформление, 2018

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Защита информации

ТРЕБОВАНИЯ К ОРГАНАМ ПО АТТЕСТАЦИИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

Information protection.
Requirements to bodies for certification of informatization objects

Дата введения — 2019—01—01

1 Область применения

Настоящий стандарт устанавливает обязательные требования к органам по аттестации объектов информатизации, предназначенных для обработки информации, содержащей сведения, составляющие государственную тайну, а также к организациям, претендующим на аккредитацию в качестве органа по аттестации.

2 Нормативные ссылки

В настоящем стандарте использована нормативная ссылка на следующий стандарт:
ГОСТ Р 50922 Защита информации. Основные термины и определения

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящем стандарте применены термины по ГОСТ Р 50922, а также следующие термины с соответствующими определениями:

3.1 **аккредитация органа по аттестации объектов информатизации:** Официальное признание уполномоченным федеральным органом исполнительной власти компетентности юридического лица выполнять работы по аттестации объектов информатизации, предназначенных для обработки информации, содержащей сведения, составляющие государственную тайну.

3.2 **аттестация объектов информатизации:** Комплекс организационных и технических мероприятий, в результате которых подтверждается соответствие системы защиты информации объекта информатизации требованиям безопасности информации.

Издание официальное

3.3

объект информатизации; ОИ: Совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров.

[ГОСТ Р 51275-2006, статья 3.1]

3.4 **орган по аттестации объектов информатизации:** Юридическое лицо, выполняющее работы по аттестации объектов информатизации, предназначенных для обработки информации, содержащей сведения, составляющие государственную тайну.

3.5 **уполномоченные федеральные органы исполнительной власти:** Федеральные органы исполнительной власти, устанавливающие в пределах своих полномочий обязательные требования соответствия безопасности информации, а также порядок сертификации продукции, используемой в целях защиты информации, и аттестации объектов информатизации.

4 Обозначения и сокращения

В настоящем стандарте применены следующие сокращения:

АС — автоматизированная система;

БИ — безопасность информации;

НСД — несанкционированный доступ;

ОИ — объект информатизации;

ФОИВ — федеральный орган исполнительной власти.

5 Общие требования к органам по аттестации объектов информатизации

Орган по аттестации ОИ и организация, претендующая на аккредитацию в качестве органа по аттестации ОИ, должны удовлетворять следующим обязательным требованиям к наличию:

- документов, определяющих порядок и правила выполнения работ по аттестации ОИ;
- помещений, предназначенных для размещения работников, измерительных приборов, средств контроля эффективности технической защиты информации и ОИ;
- средств измерений и испытаний, необходимых для выполнения работ по аттестации ОИ;
- работников, имеющих соответствующую квалификацию, стаж работы, знания и навыки;
- лицензий, необходимых для выполнения работ по аттестации ОИ;
- ОИ, предназначенных для обработки информации, содержащей сведения, составляющие государственную тайну;
- организационно-распорядительной документации, определяющей задачи, функции, обязанности, права и ответственность органа по аттестации.

6 Требования к органам по аттестации объектов информатизации

6.1 Требования к наличию документов, определяющих порядок и правила выполнения работ по аттестации объектов информатизации

Орган по аттестации ОИ должен иметь в наличии необходимые для выполнения работ по аттестации ОИ нормативные правовые акты, методические документы и национальные стандарты, определяющие порядок и методики проведения аттестационных испытаний в целях подтверждения соответствия ОИ требованиям БИ. Перечень таких документов определяется соответствующим уполномоченным ФОИВ.

Орган по аттестации ОИ должен обеспечить учет, хранение и актуализацию фонда нормативных правовых актов, методических документов и национальных стандартов в установленном законодательством Российской Федерации порядке.

6.2 Требования к наличию помещений

Орган по аттестации ОИ должен иметь помещения, принадлежащие ему на праве собственности или ином законном основании, в которых созданы необходимые условия, установленные требованиями руководящих и нормативных документов, утвержденных соответствующими уполномоченными ФОИВ, для размещения работников, измерительных приборов, средств контроля эффективности технической защиты информации и ОИ, предназначенных для обработки информации, содержащей сведения, составляющие государственную тайну.

6.3 Требования к наличию средств измерений и испытаний

Орган по аттестации ОИ должен иметь принадлежащие ему на праве собственности средства измерений, испытательное оборудование и программные (программно-аппаратные) средства, необходимые для выполнения работ по аттестации ОИ. Примерный перечень средств измерений, испытательного оборудования и программных (программно-аппаратных) средств определяется соответствующим ФОИВ.

Средства измерений должны иметь характеристики, обеспечивающие в процессе аттестации ОИ требуемые измерения, определенные уполномоченным ФОИВ в соответствии с Перечнем измерений, относящихся к сфере государственного регулирования обеспечения единства измерений.

Средства измерений должны иметь действующие свидетельства о поверке, проведенной в установленном законодательством Российской Федерации порядке.

Программные (программно-аппаратные) средства контроля эффективности технической защиты информации должны иметь действующие сертификаты соответствия требованиям безопасности информации, выданные уполномоченным ФОИВ по результатам проведенной оценки (подтверждения) их соответствия в установленном законодательством Российской Федерации порядке.

6.4 Требования к наличию работников и их квалификации

Орган по аттестации ОИ должен иметь подразделение, на которое возложены работы по аттестации ОИ, укомплектованное работниками, для которых работа в органе по аттестации ОИ является основным местом работы.

Орган по аттестации ОИ должен иметь в штате работников, заключивших с ним трудовой договор, которые обладают необходимыми знаниями, умениями и могут выполнять работы по аттестации ОИ, в том числе:

- руководителя или лица, уполномоченного руководить работами по аттестации ОИ, имеющего:

высшее профессиональное образование по направлению подготовки (специальности) «Информационная безопасность» и не менее 5 лет стажа работы в области аттестации ОИ;

или иное высшее профессиональное[1)] образование и не менее 10 лет стажа работы в области аттестации ОИ;

или иное высшее образование и не менее 5 лет стажа работы в области аттестации ОИ, прошедшего обучение по программам профессиональной переподготовки по направлению «Информационная безопасность» (со сроком обучения не менее 360 аудиторных часов);

- не менее трех инженерно-технических работников для проведения работ по аттестации ОИ, имеющих:

высшее профессиональное образование по направлению подготовки (специальности) «Информационная безопасность»;

или иное высшее профессиональное[1)] образование и прошедших обучение по программе повышения квалификации по направлению «Информационная безопасность» (со сроком обучения не менее 40 аудиторных часов);

или иное высшее образование и прошедших обучение по программам профессиональной переподготовки по одной из специальностей в области информационной безопасности (со сроком обучения не менее 360 аудиторных часов).

Работники должны иметь документы установленного образца, подтверждающие квалификацию, практический опыт и уровень подготовки.

[1)] По направлению подготовки (специальности) в области математических и естественных наук, инженерного дела, технологий и технических наук.

Характеристика квалификации, необходимой работнику органа по аттестации для осуществления профессиональной деятельности, определяется действующим профессиональным стандартом «Специалист по технической защите информации».

6.5 Требования к наличию лицензий

Орган по аттестации ОИ должен иметь выданную в установленном законодательством Российской Федерации порядке лицензию на проведение работ, связанных с использованием сведений, составляющих государственную тайну.

Орган по аттестации ОИ должен иметь выданную в установленном законодательством Российской Федерации порядке лицензию на осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны (в части технической защиты информации).

6.6 Требования к наличию объектов информатизации

Орган по аттестации ОИ для обработки информации, содержащей сведения, составляющие государственную тайну, должен иметь принадлежащие ему на праве собственности АС и средства их защиты, прошедшие процедуру оценки соответствия в установленном законодательством Российской Федерации порядке.

Орган по аттестации ОИ для обсуждения информации, содержащей сведения, составляющие государственную тайну, должен иметь принадлежащие ему на праве собственности или на другом законном основании помещение и средства его защиты, прошедшие процедуру оценки соответствия в установленном законодательством Российской Федерации порядке.

6.7 Требования к наличию организационно-распорядительной документации

Орган по аттестации ОИ в своей деятельности должен руководствоваться Положением об органе по аттестации, в котором должны быть определены задачи, функции, обязанности, права и ответственность органа по аттестации.

Типовое положение об органе по аттестации ОИ приведено в приложении А.

К Положению об органе по аттестации ОИ прилагаются:

- перечень имеющихся у органа по аттестации ОИ документов, необходимых для выполнения работ по аттестации ОИ (в соответствии с требованиями 6.1);
- перечень имеющихся у органа по аттестации ОИ средств измерений, испытательного оборудования и программных (программно-аппаратных) средств, необходимых для выполнения работ по аттестации ОИ (в соответствии с требованиями 6.3, 6.6);
- перечень имеющихся у органа по аттестации ОИ работников, привлекаемых для выполнения работ по аттестации ОИ (согласно должностным инструкциям в соответствии с требованиями 6.4).

Указанные перечни оформляются в соответствии с правилами лицензирования на осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны (в части технической защиты информации).

В ходе аккредитации по заявлению юридического лица, претендующего на выполнение работ по аттестации объектов информатизации, предназначенных для обработки информации, содержащей сведения, составляющие государственную тайну, уполномоченным ФОИВ производится:

- оценка соответствия заявителя всем обязательным требованиям аккредитации, перечисленным в разделе 5;
- принятие решения по результатам оценки соответствия заявителя требованиям аккредитации.

Приложение А
(рекомендуемое)

Типовое положение об органе по аттестации объектов информатизации

УТВЕРЖДАЮ

Уполномоченное лицо федерального органа
исполнительной власти

«____» _____ 20____ г.

П О Л О Ж Е Н И Е

об органе по аттестации объектов информатизации
(полное наименование юридического лица)

Система сертификации средств защиты информации
по требованиям безопасности информации
(№…)

г. _____
20____ г.

Содержание

1 Общие положения . . . . .
2 Задачи и функции органа по аттестации объектов информатизации . . . . .
3 Деятельность аттестационных комиссий . . . . .
4 Права, обязанности и ответственность органа по аттестации объектов информатизации. . . . . .

1 Общие положения

1.1 Настоящее положение устанавливает задачи, функции, права, обязанности и ответственность органа по аттестации ОИ на соответствие требованиям БИ (*полное наименование юридического лица)* (далее — *сокращенное наименование*).

1.2 Положение разработано в соответствии с Типовым положением об органе по аттестации объектов информатизации.

1.3 (*Сокращенное наименование)* в качестве органа по аттестации ОИ на соответствие требованиям БИ аккредитовано уполномоченным ФОИВ и работает под его методическим руководством.

1.4 (*Сокращенное наименование)* как орган по аттестации ОИ в своей деятельности руководствуется нормативными правовыми актами, методическими документами и национальными стандартами, определяющими соответствие ОИ требованиям БИ, а также порядок и методики проведения аттестационных испытаний в целях подтверждения соответствия ОИ требованиям БИ.

2 Задачи и функции органа по аттестации объектов информатизации

2.1 Основными задачами органа по аттестации ОИ (*сокращенное наименование)* являются организация и проведение аттестации ОИ на соответствие требованиям БИ, а также контроль за состоянием и эксплуатацией аттестованных этим органом ОИ.

2.2 Орган по аттестации ОИ (*сокращенное наименование)* осуществляет следующие функции:

- формирует и поддерживает актуальную базу нормативных правовых актов, методических документов и национальных стандартов, используемых при аттестации ОИ;
- участвует в конкурсах на проведение аттестационных испытаний;
- рассматривает заявки на аттестацию ОИ, планирует работы по аттестации ОИ и доводит сроки проведения аттестации до заявителей;
- проводит анализ исходных данных по аттестуемым ОИ и определяет схему аттестации;
- организует работы по аттестации ОИ на основе заключенных договоров;
- разрабатывает программы и методики аттестационных испытаний ОИ;
- назначает аттестационные комиссии из работников органа по аттестации ОИ;
- рассматривает результаты аттестационных испытаний ОИ, утверждает заключения по результатам аттестации и выдает заявителю при условии положительных результатов «Аттестат соответствия»;
- проверяет при осуществлении контроля за состоянием и эксплуатацией аттестованных ОИ соответствие реальных условий эксплуатации объекта и технологию обработки защищаемой информации условиям и технологии, при которых выдан аттестат соответствия;
- аннулирует, приостанавливает и возобновляет действие выданных (*сокращенное наименование)* аттестатов соответствия;
- ведет информационную базу данных об аттестованных ОИ;
- осуществляет взаимодействие с уполномоченным ФОИВ и информирует его о своей деятельности по аттестации ОИ.

3 Деятельность аттестационных комиссий

3.1 Аттестационные комиссии формируются (*сокращенное наименование)* из числа работников органа по аттестации ОИ таким образом, чтобы обеспечить комплексную проверку ОИ с целью оценки его соответствия требованиям БИ.

3.2 Персональный состав аттестационных комиссий определяется руководителем органа по аттестации ОИ и приводится в Программе аттестационных испытаний ОИ.

3.3 Работники органа по аттестации ОИ, включенные в состав аттестационных комиссий, осуществляют свою деятельность в соответствии с должностными инструкциями и должны обладать необходимой квалификацией и компетентностью.

4 Права, обязанности и ответственность органа по аттестации объектов информатизации

4.1 Орган по аттестации ОИ (*сокращенное наименование)* имеет право:

- устанавливать сроки и договорные цены на проведение аттестации ОИ, а также иные условия взаимодействия с заявителем;
- отказывать заявителю в аттестации ОИ, указав при этом причины отказа и конкретные рекомендации по устранению этих причин;
- участвовать в контроле за состоянием и эксплуатацией аттестованного ОИ;
- проводить аттестацию собственных ОИ;
- аннулировать аттестат соответствия или приостанавливать его действие в случае нарушения заявителем условий функционирования ОИ, технологии обработки защищаемой информации и его соответствия требованиям БИ.

4.2 Орган по аттестации ОИ (*сокращенное наименование)* обязан:

- соблюдать в полном объеме все правила и порядок аттестации ОИ, установленные нормативными правовыми актами, методическими документами и национальными стандартами;
- информировать уполномоченный ФОИВ обо всех изменениях, которые могут привести к необходимости рассмотрения вопроса о переоформлении, приостановлении и прекращении действия аттестата аккредитации (*сокращенное наименование)*;
- уведомлять уполномоченный ФОИВ об изменениях в кадровом составе органа по аттестации;
- представлять на согласование в уполномоченный ФОИВ программы, методики и заключения по результатам аттестационных испытаний ОИ первой категории, а также собственных ОИ, аттестованных своими силами, используемых при проведении работ по аттестации;
- информировать уполномоченный ФОИВ о несоответствии средств защиты информации, применяемых на аттестуемых ОИ, требованиям безопасности информации;
- организовывать и проводить аттестацию ОИ в установленные договором с заявителем сроки;
- обеспечивать сохранность государственной и коммерческой тайны в процессе и по завершении аттестации ОИ, соблюдение авторского права;
- вести информационную базу данных об аттестованных ОИ;
- представлять ежеквартально (до двадцатого числа последнего месяца квартала) в уполномоченный ФОИВ информацию о результатах деятельности по аттестации ОИ за прошедший период;
- допускать в установленном порядке представителей уполномоченного ФОИВ для осуществления инспекционного контроля деятельности органа по аттестации.

4.3 Орган по аттестации ОИ (*сокращенное наименование)* несет ответственность за:

- соответствие проведенных им аттестационных испытаний ОИ требованиям нормативных правовых актов, методических документов и национальных стандартов, а также достоверность и объективность результатов испытаний;
- полноту и качество выполнения задач, функций прав и обязанностей, возложенных на орган по аттестации ОИ;
- формирование состава и квалификацию работников аттестационных комиссий;
- соблюдение установленных сроков и условий проведения аттестации ОИ, зафиксированных в договоре с заявителем;
- обеспечение сохранности государственной и коммерческой тайны;
- соблюдение установленного законодательством Российской Федерации порядка в области технической защиты информации.

Руководитель органа по аттестации объектов информатизации
(сокращенное наименование организации) _____

(подпись руководителя)

УДК 004.056:057.86:006.354 ОКС 35.020

Ключевые слова: орган по аттестации, объект информатизации, аккредитация органа по аттестации

БЗ 7—2018/58

Редактор *Н.А. Аргунова*
Технический редактор *В.Н. Прусакова*
Корректор *Е.Д. Дульнева*
Компьютерная верстка *И.А. Налейкиной*

Сдано в набор 03.08.2018. Подписано в печать 09.08.2018. Формат 60×84 1/8. Гарнитура Ариал.
Усл. печ. л. 1,40. Уч.-изд. л. 1,24.
Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении ФГУП «СТАНДАРТИНФОРМ» для комплектования Федерального информационного фонда стандартов, 123001 Москва, Гранатный пер., 4.

gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru