



**Частное образовательное учреждение  
дополнительного профессионального образования  
«Профессиональный бухгалтер»  
(ЧОУ ДПО «Профессиональный бухгалтер»)**

**Положение  
по аттестации объекта информатизации  
по требованиям безопасности информации**

г. Саратов

**Положение  
по аттестации объекта информатизации  
по требованиям безопасности информации**

**1. Общие положения**

1.1. Настоящее Положение устанавливает основные принципы, организационную структуру системы аттестации объектов информатизации по требованиям безопасности информации, порядок проведения аттестации, а также контроля и надзора за аттестацией и эксплуатацией аттестованных объектов информатизации.

1.2. Положение разработано в соответствии с Законами Российской Федерации "О сертификации продукции и услуг" и "О государственной тайне", "Положением о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам", "Положением о государственном лицензировании деятельности в области защиты информации", "Положением о сертификации средств защиты информации по требованиям безопасности информации"

1.3. Система аттестации объектов информатизации по требованиям безопасности информации (далее - система аттестации) является составной частью единой системы сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации и подлежит государственной регистрации в установленном Госстандартом России порядке. Деятельность системы аттестации организует федеральный орган по сертификации продукции и аттестации объектов информатизации по требованиям безопасности информации (далее - федеральный орган по сертификации и аттестации), которым является Гостехкомиссия России.

1.4. Под аттестацией объектов информатизации понимается комплекс организационно-технических мероприятий, в результате которых посредством специального документа - "Аттестата соответствия" подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных Гостехкомиссией России.

Наличие на объекте информатизации действующего "Аттестата соответствия" дает право обработки информации с уровнем секретности (конфиденциальности) и на период времени, установленными в "Аттестате соответствия".

1.5. Обязательной аттестации подлежат объекты информатизации, предназначенные для обработки информации, составляющей государственную тайну.

Аттестация по требованиям безопасности информации предшествует началу обработки подлежащей защите информации и вызвана необходимостью официального подтверждения эффективности комплекса используемых на конкретном объекте информатизации мер и средств защиты информации.

1.6. При аттестации объекта информатизации подтверждается его соответствие требованиям по защите информации от несанкционированного доступа, в том числе от компьютерных вирусов, от утечки за счет побочных электромагнитных излучений и наводок при специальных воздействиях на объект (высокочастотное навязывание и облучение, электромагнитное и радиационное воздействие), от утечки или воздействия на нее за счет специальных устройств, встроенных в объекты информатизации.

1.7. Аттестация предусматривает комплексную проверку (аттестационные испытания) защищаемого объекта информатизации в реальных условиях эксплуатации с целью оценки

соответствия применяемого комплекса мер и средств защиты требуемому уровню безопасности информации.

1.8. Аттестация проводится органом по аттестации в установленном настоящим Положением порядке в соответствии со схемой, выбираемой этим органом на этапе подготовки к аттестации из следующего основного перечня работ:

- анализ исходных данных по аттестуемому объекту информатизации;
- предварительное ознакомление с аттестуемым объектом информатизации;
- проведение экспертного обследования объекта информатизации и анализ разработанной документации по защите информации на этом объекте с точки зрения ее соответствия требованиям нормативной и методической документации;
- проведение испытаний отдельных средств и систем защиты информации на аттестуемом объекте информатизации с помощью специальной контрольной аппаратуры и тестовых средств;
- проведение испытаний отдельных средств и систем защиты информации в испытательных центрах (лабораториях) по сертификации средств защиты информации по требованиям безопасности информации;
- проведение комплексных аттестационных испытаний объекта информатизации в реальных условиях эксплуатации;
- анализ результатов экспертного обследования и комплексных аттестационных испытаний объекта информатизации и утверждение заключения по результатам аттестации.

1.9. Органы по аттестации объектов информатизации несут ответственность за выполнение возложенных на них функций, обеспечение сохранности государственных и коммерческих секретов, а также за соблюдение авторских прав разработчиков аттестуемых объектов информатизации и их компонентов.

## **2. Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации**

2.1. Организационную структуру системы аттестации объектов информатизации образуют:

- федеральный орган по сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации - Гостехкомиссия России;
- органы по аттестации объектов информатизации по требованиям безопасности информации;
- заявитель ЧОУ ДПО «Профессиональный бухгалтер»

2.2. Федеральный орган по сертификации и аттестации осуществляет следующие функции:

- организует обязательную аттестацию объектов информатизации;
- создает системы аттестации объектов информатизации и устанавливает правила для проведения аттестации в этих системах;
- устанавливает правила аккредитации и выдачи лицензий на проведение работ по обязательной аттестации;
- организует, финансирует разработку и утверждает нормативные и методические документы по аттестации объектов информатизации;
- аккредитует органы по аттестации объектов информатизации и выдает им лицензии на проведение определенных видов работ;
- осуществляет государственный контроль и надзор за соблюдением правил аттестации и эксплуатацией аттестованных объектов информатизации;
- рассматривает апелляции, возникающие в процессе аттестации объектов

информатизации и контроля за эксплуатацией аттестованных объектов информатизации;

- организует периодическую публикацию информации по функционированию системы аттестации объектов информатизации по требованиям безопасности информации.

2.3. Органы по аттестации объектов информатизации аккредитуются Гостехкомиссией России и получают от нее лицензию на право проведения аттестации объектов информатизации.

Таковыми органами могут быть отраслевые и региональные учреждения, предприятия и организации по защите информации, специальные центры Гостехкомиссии России.

2.4. Органы по аттестации:

- аттестуют объекты информатизации и выдают "Аттестаты соответствия";

- осуществляют контроль за безопасностью информации, циркулирующей на аттестованных объектах информатизации, и за их эксплуатацией;

- отменяют и приостанавливают действие выданных этим органом "Аттестатов соответствия";

- формируют фонд нормативной и методической документации, необходимой для аттестации конкретных типов объектов информатизации, участвуют в их разработке;

- ведут информационную базу аттестованных этим органом объектов информатизации;

- осуществляют взаимодействие с Гостехкомиссией России и ежеквартально информируют его о своей деятельности в области аттестации.

2.5. Заявитель ЧОУ ДПО «Профессиональный бухгалтер»:

- проводит подготовку объекта информатизации для аттестации путем подготовки рабочего места и реализации необходимых организационно-технических мероприятий по защите информации;

- привлекает органы по аттестации для организации и проведения аттестации объекта информатизации;

- предоставляет органам по аттестации необходимые документы и условия для проведения аттестации;

- осуществляет эксплуатацию объекта информатизации в соответствии с условиями и требованиями, установленными в "Аттестате соответствия";

- извещает орган по аттестации, выдавший "Аттестат соответствия", обо всех изменениях в информационных технологиях, составе и размещении средств и систем информатики, условиях их эксплуатации, которые могут повлиять на эффективность мер и средств защиты;

- предоставляет необходимые документы и условия для осуществления контроля и надзора за эксплуатацией объекта информатизации, прошедшего обязательную аттестацию.

### 3. Порядок проведения аттестации и контроля

3.1. Порядок проведения аттестации объектов информатизации по требованиям безопасности информации включает следующие действия:

- подачу и рассмотрение заявки на аттестацию;

- предварительное ознакомление с аттестуемым объектом;

- заключение договора на аттестацию;

- проведение аттестационных испытаний объекта информатизации, а именно, рабочего места ЧОУ ДПО «Профессиональный бухгалтер»;

- оформление, регистрация и выдача "Аттестата соответствия";

- осуществление государственного контроля и надзора, инспекционного контроля за проведением аттестации и эксплуатацией аттестованного объекта информатизации;

3.2. Подача и рассмотрение заявки на аттестацию

3.2.1. Заявитель ЧОУ ДПО «Профессиональный бухгалтер» для получения "Аттестата соответствия" заблаговременно направляет в орган по аттестации заявку на проведение

аттестации с исходными данными по аттестуемому объекту информатизации по форме, приведенной в [приложении 1](#).

3.2.2. Орган по аттестации в месячный срок рассматривает заявку и на основании анализа исходных данных выбирает схему аттестации, согласовывает ее с заявителем ЧОУ ДПО «Профессиональный бухгалтер» и принимает решение о проведении аттестации рабочего места.

### 3.3. Предварительное ознакомление с аттестуемым объектом

При недостаточности исходных данных по аттестуемому объекту информатизации в схему аттестации включаются работы по предварительному ознакомлению с аттестуемым объектом, проводимые до этапа аттестационных испытаний.

3.3.1. По результатам рассмотрения заявки и анализа исходных данных, а также предварительного ознакомления с аттестуемым объектом (рабочее место ЧОУ ДПО «Профессиональный бухгалтер») органом по аттестации разрабатывается программа аттестационных испытаний, предусматривающая перечень работ объекте.

3.3.2. Программа аттестационных испытаний согласовывается с заявителем.

### 3.4. Заключение договора на аттестацию.

3.4.1. Этап подготовки завершается заключением договора между заявителем ЧОУ ДПО «Профессиональный бухгалтер» и органом по аттестации на проведение аттестации.

### 3.5. Проведение аттестационных испытаний объектов информатизации

3.5.1. На этапе аттестационных испытаний объекта информатизации:

- осуществляется анализ организационной структуры объекта информатизации;
- проверяется уровень подготовки кадров и распределение ответственности персонала за обеспечение выполнения требований по безопасности информации;
- проводятся комплексные аттестационные испытания объекта информатизации в реальных условиях эксплуатации путем проверки фактического выполнения установленных требований на различных этапах технологического процесса обработки защищаемой информации;

3.5.2. Заключение по результатам аттестации с краткой оценкой соответствия объекта информатизации требованиям по безопасности информации, выводом о возможности выдачи "Аттестата соответствия" и необходимыми рекомендациями подписывается членами аттестационной комиссии и доводится до сведения заявителя ЧОУ ДПО «Профессиональный бухгалтер».

### 3.6. Оформление, регистрация и выдача "Аттестата соответствия"

3.6.1. "Аттестат соответствия" на объект информатизации, отвечающий требованиям по безопасности информации, выдается органом по аттестации.

3.6.2. "Аттестат соответствия" оформляется и выдается заявителю после утверждения заключения по результатам аттестации.

3.6.3. Регистрация "Аттестатов соответствия" осуществляется по отраслевому или территориальному признакам органами по аттестации с целью ведения информационной базы аттестованных объектов информатизации и планирования мероприятий по контролю и надзору.

3.6.4. "Аттестат соответствия" выдается на период, в течение которого обеспечивается неизменность условий функционирования объекта информатизации и технологии обработки защищаемой информации, могущих повлиять на характеристики, определяющие безопасность информации (состав и структура технических средств, условия размещения, используемое программное обеспечение, режимы обработки информации, средства и меры защиты), но не более чем на 3 года.

ЧОУ ДПО «Профессиональный бухгалтер» несет ответственность за выполнение установленных условий функционирования объекта информатизации, технологии обработки защищаемой информации и требований по безопасности информации.

3.6.5. В случае изменения условий и технологии обработки защищаемой информации ЧОУ ДПО «Профессиональный бухгалтер» обязано известить об этом орган по аттестации, который принимает решение о необходимости проведения дополнительной проверки эффективности системы защиты объекта информатизации.

3.6.6. При несоответствии аттестуемого объекта требованиям по безопасности информации и невозможности оперативно устранить отмеченные аттестационной комиссией недостатки орган по аттестации принимает решение об отказе в выдаче "Аттестата соответствия".

При этом может быть предложен срок повторной аттестации при условии устранения недостатков.

При наличии замечаний непринципиального характера "Аттестат соответствия" может быть выдан после проверки устранения этих замечаний.

### 3.7. Рассмотрение апелляций

В случае несогласия с отказом в выдаче "Аттестата соответствия" заявитель ЧОУ ДПО «Профессиональный бухгалтер» имеет право обратиться в вышестоящий орган по аттестации или непосредственно в Гостехкомиссию России с апелляцией для дополнительного рассмотрения полученных при испытаниях результатов, где она в месячный срок рассматривается с привлечением заинтересованных сторон. Податель апелляции извещается о принятом решении.

3.8. Государственный контроль и надзор, инспекционный контроль за соблюдением правил аттестации и эксплуатации аттестованных объектов информатизации

3.8.1. Государственный контроль и надзор, инспекционный контроль за проведением аттестации объектов информатизации проводится Гостехкомиссией России как в процессе, так и по завершении аттестации, а за эксплуатацией аттестованных объектов информатизации - периодически в соответствии с планами работы по контролю и надзору

3.8.2. При выявлении нарушения правил эксплуатации аттестованных объектов информатизации, технологии обработки защищаемой информации и требований по безопасности информации органом, проводящим контроль и надзор, может быть приостановлено или аннулировано действие "Аттестата соответствия", с оформлением этого решения в "Аттестате соответствия" и информированием органа, ведущего сводную информационную базу аттестованных объектов информатики, и Гостехкомиссии России.

Решение об аннулировании действия "Аттестата соответствия" принимается в случае, когда в результате оперативного принятия организационно-технических мер защиты не может быть восстановлен требуемый уровень безопасности информации.

## **4. Требования к нормативным и методическим документам по аттестации объектов информатизации**

4.1. Объекты информатизации, вне зависимости от используемых отечественных или зарубежных технических и программных средств, аттестуются на соответствие требованиям государственных стандартов или иных нормативных документов по безопасности информации, утвержденных Гостехкомиссией России.

4.2. Состав нормативной и методической документации для аттестации конкретных объектов информатизации определяется органом по аттестации в зависимости от вида и условий функционирования объектов информатизации на основании анализа исходных данных по аттестуемому объекту.

4.3. В нормативную документацию включаются только те показатели, характеристики, требования, которые могут быть объективно проверены.

4.4. В нормативной и методической документации на методы испытаний должны быть ссылки на условия, содержание и порядок проведения испытаний, используемые при

испытаниях контрольную аппаратуру и тестовые средства, сводящие к минимуму погрешности результатов испытаний и позволяющие воспроизвести эти результаты.

4.5. Тексты нормативных и методических документов, используемых при аттестации объектов информатизации, должны быть сформулированы ясно и четко, обеспечивая их точное и единообразное толкование. В них должно содержаться указание о возможности использования документа для аттестации определенных типов объектов информатизации по требованиям безопасности информации или направлений защиты информации.

4.6. Официальным языком системы аттестации является русский язык, на котором оформляются все документы, используемые и выдаваемые в рамках системы аттестации.

Кому: \_\_\_\_\_  
(наименование органа по аттестации его адрес)

**ЗАЯВКА**  
на проведение аттестации объекта информатизации

1. (наименование заявителя) просит провести аттестацию (наименование объекта информатизации) на соответствие требованиям по безопасности информации:

2. Необходимые исходные данные по аттестуемому объекту информатизации прилагаются.

3. Заявитель готов предоставить необходимые документы и условия для проведения аттестации.

4. Заявитель согласен на договорной основе оплатить расходы по всем видам работ и услуг по аттестации указанного в данной заявке объекта информатизации.

5. Дополнительные условия или сведения для договора:

5.1. Предварительное ознакомление с аттестуемым объектом предлагаю провести в период \_\_\_\_\_

5.2. Аттестационные испытания объекта информатики предлагаю провести в период \_\_\_\_\_

5.3. Испытания несертифицированных средств и систем информатизации (наименование средств и систем) предусмотрено провести в испытательных центрах (лабораториях) (наименование испытательных центров) в период \_\_\_\_\_ (или предлагается провести непосредственно на аттестуемом объекте в период \_\_\_\_\_)

Другие условия (предложения).

печать

Руководитель (органа заявителя)

(подпись, дата) (Фамилия, И.О.)



Приложение к форме "Заявки..."

Исходные данные по аттестуемому объекту информатизации

1. Полное и точное наименование объекта информатизации и его назначение.
2. Характер (научно-техническая, экономическая, производственная, финансовая, военная, политическая) и уровень секретности (конфиденциальности) обрабатываемой информации определен (в соответствии с какими перечнями (государственным, отраслевым, ведомственным, предприятия)
3. Организационная структура объекта информатизации.
4. Перечень помещений, состав комплекса технических средств (основных и вспомогательных), входящих в объект информатизации, в которых (на которых) обрабатывается указанная информация (расположенных в помещениях, где она циркулирует).
5. Особенности и схема расположения объекта информатизации с указанием границ контролируемой зоны.
6. Структура программного обеспечения (общесистемного и прикладного), используемого на аттестуемом объекте информатизации и предназначенного для обработки защищаемой информации, используемые протоколы обмена информацией.
7. Общая функциональная схема объекта информатизации, включая схему информационных потоков и режимы обработки защищаемой информации.
8. Наличие и характер взаимодействия с другими объектами информатизации.
9. Состав и структура системы защиты информации на аттестуемом объекте информатизации.
10. Перечень технических и программных средств в защищенном исполнении, средств защиты и контроля, используемых на аттестуемом объекте информатизации и имеющих соответствующий сертификат, предписание на эксплуатацию.
11. Сведения о разработчиках системы защиты информации, наличие у сторонних разработчиков (по отношению к предприятию, на котором расположен аттестуемый объект информатизации) лицензий на проведение подобных работ.
12. Наличие на объекте информатизации (на предприятии, на котором расположен объект информатизации) службы безопасности информации, службы администратора (автоматизированной системы, сети, баз данных).
13. Наличие и основные характеристики физической защиты объекта информатизации (помещений, где обрабатывается защищаемая информация и хранятся информационные носители).
14. Наличие и готовность проектной и эксплуатационной документации на объект информатизации и другие исходные данные по аттестуемому объекту информатизации, влияющие на безопасность информации.

Примечание. Под объектами информатизации, аттестуемыми по требованиям безопасности информации, понимаются автоматизированные системы различного уровня и назначения, системы связи, отображения и размножения вместе с помещениями, в которых они установлены, предназначенные для обработки и передачи информации, подлежащей защите, а также сами помещения, предназначенные для ведения конфиденциальных переговоров.