

**Федеральное государственное автономное образовательное учреждение
высшего образования «Российский университет транспорта (МИИТ)»**

Институт транспортной техники и систем управления

Кафедра «Управление и защита информации»

Практическая работа на тему:

«Перечень документов для аттестации АС»

По дисциплине:

«Организационное и правовое обеспечение ИБ»

Выполнил:

Студент группы ТКИ-342

Дроздов Антон Дмитриевич

Проверил:

К.Т.Н.

Привалов Александр Андреевич

Москва 2023

Оглавление

1. Введение	3
2. Актуальность работы	3
3. Обзор нормативных документов	4
4. Основная часть	8
5. Вывод	13
6. Список используемых источников	13

1. Введение

Практическая работа по теме «Перечень документов для аттестации АС» выполнена в целях ознакомления с порядком разработки организацией требуемых документов и проведения необходимых работ по аттестации автоматизированных систем (АС), включающих в себя как организационные, так и технические мероприятия.

Аттестация АС подразумевает под собой полный комплекс задач и осуществляется в определенном порядке:

1. Исследование АС по заданным требованиям;
2. Проектирование системы защиты информации и дальнейшее её внедрение;
3. Аттестация АС.

Основная цель аккредитации АС является подтверждение соответствия системы защиты информации АС требованиям нормативных документов Российской Федерации в области защиты информации.

В настоящее время проблематика аттестации АС организации заключается в правильном порядке прохождения аккредитации, своевременном устранении недостатков по рекомендациям аттестационной комиссии.

Для аттестации АС на соответствие требованиям о защите информации привлекается организация, имеющая лицензию ФСТЭК на деятельность по технической защите конфиденциальной информации.

В данной работе далее будут рассматриваться конкретные этапы прохождения аттестации АС и необходимые соответствующие им документы.

2. Актуальность работы

Актуальность данной практической работы связана с тем, что аттестация автоматизированных систем является важным этапом в их эксплуатации. Аттестация позволяет оценить соответствие системы установленным требованиям безопасности и защиты информации, а также выявить возможные уязвимости и недостатки в работе системы.

Перечень документов, необходимых для аттестации АС, является одним из ключевых моментов процесса аттестации. Неправильное или неполное предоставление документации может привести к задержкам в процессе аттестации, а также к отказу в выдаче сертификата соответствия. Поэтому знание перечня документов, необходимых для аттестации АС, является важным для специалистов, занимающихся разработкой, эксплуатацией и аттестацией автоматизированных систем.

3. Обзор нормативных документов

Перечень документов для аттестации автоматизированных систем (АС) регулируется нормативными документами, которые определяют требования к процессу аттестации и документам, необходимым для ее проведения:

1. "(СТР-К) Специальные требования и рекомендации по технической защите конфиденциальной информации", утвержденный приказом председателя Государственной технической комиссией от 30 августа 2002 г.

Пункт 2.2 – "Требования и рекомендации настоящего документа распространяются на защиту:

- конфиденциальной информации ...
- информации о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющей идентифицировать его личность (персональные данные) ..."

Пункт 2.17 – "Объекты информатизации должны быть аттестованы на соответствие требованиям по защите информации"

Пункт 2.3 – "Для защиты конфиденциальной информации, содержащейся в негосударственных информационных ресурсах, режим защиты которой определяет собственник этих ресурсов (например, информации, составляющей коммерческую, банковскую тайну и т.д.) (далее - коммерческая тайна), данный документ носит рекомендательный характер."

Пункт 3.19 – " На стадии ввода в действие объекта информатизации и СЗИ осуществляются: ...

- аттестация объекта информатизации по требованиям безопасности информации."

Пункт 3.20. – "... При положительных результатах аттестации на объект информатизации оформляется "Аттестат соответствия" требованиям по безопасности информации (форма "Аттестата соответствия" для АС приведена в приложении № 2 ..."

2. Приказ ФСТЭК от 29 апреля 2021 г. № 77 "Об утверждении порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну", включающий в себя порядок разработки документов и содержание работ для аттестации АС.

Пункт 1 – "Настоящий Порядок определяет состав и содержание работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа ... а также требования к форме и содержанию разрабатываемых при организации и проведении таких работ документов."

Пункт 4 – "Аттестация объекта информатизации проводится на этапе его создания или развития (модернизации) и предусматривает проведение комплекса организационных и технических мероприятий и работ (аттестационных испытаний) ..."

Пункт 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 целом, перечень документов для аттестации АС может включать следующие документы:

1. Заявление на аттестацию АС;
2. Техническое задание на аттестацию АС;
3. Техническая документация на АС (включая описание функциональности, архитектуру, алгоритмы и т.д.);
4. Результаты тестирования АС;
5. Протоколы проведения аттестации;
6. Отчет об аттестации АС;
7. Сертификат соответствия на АС.

Далее рассмотрим, какой перечень документов должен быть у органа по аттестации:

Выдержка из документа (статья)	Наименование документа	Примечание	Срок действий
Пункт 6.5 ГОСТ Р 58189-2018	Лицензия на проведение работ, связанных с использованием сведений, составляющих гос. тайну	—	Постановление Правительства 333 "О лицензировании деятельности ... гос. тайны, созданием средств защиты" пункт 8 – "Срок действия лицензии устанавливается ... , но не более чем на 5 лет"
	Лицензия на осуществление мероприятий и (или) оказание услуг в области защиты гос. тайны (в частности технической защиты)	—	

Выдержка из документа (статья)	Наименование документа	Примечание	
Пункт 4.3. ГОСТ РО 0043-003-2021	Аттестат аккредитации органа по аттестации объектов информатизации	Документ имеет гриф: Для Служебного Пользования. Применяется в случае аттестации объекта информатизации, на котором осуществляется обработка секретной информации (отнесенной к гос. тайне)	
Информация от ФСТЭК "Лицензирование деятельности по технической защите информации"	Лицензия деятельности по техн. защите конфиденциальной информации	—	5 лет – указано в информации от ФСТЭК
	Лицензия деятельности по разработке и производству средств защиты конф. инф.	—	

Важно отметить, что перечень документов для аттестации АС может варьироваться в зависимости от конкретной отрасли или сферы применения АС, а

также от требований, установленных регулируемыми органами. Поэтому перед началом процесса аттестации необходимо ознакомиться с соответствующими нормативными документами и требованиями.

4. Основная часть

Рассмотрим полный перечень документов для аттестации АС в соответствии с Приказом ФСТЭК № 77:

Пункт 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 N 1 ... к настоящему Порядку;
- б) акт классификации информационной (автоматизированной) системы по форме согласно приложению N 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)."

Весь перечень документов для аттестации АС рассмотрен далее в рис. 1., где пунктиром указаны необязательные для создания документы в процессе аттестации.

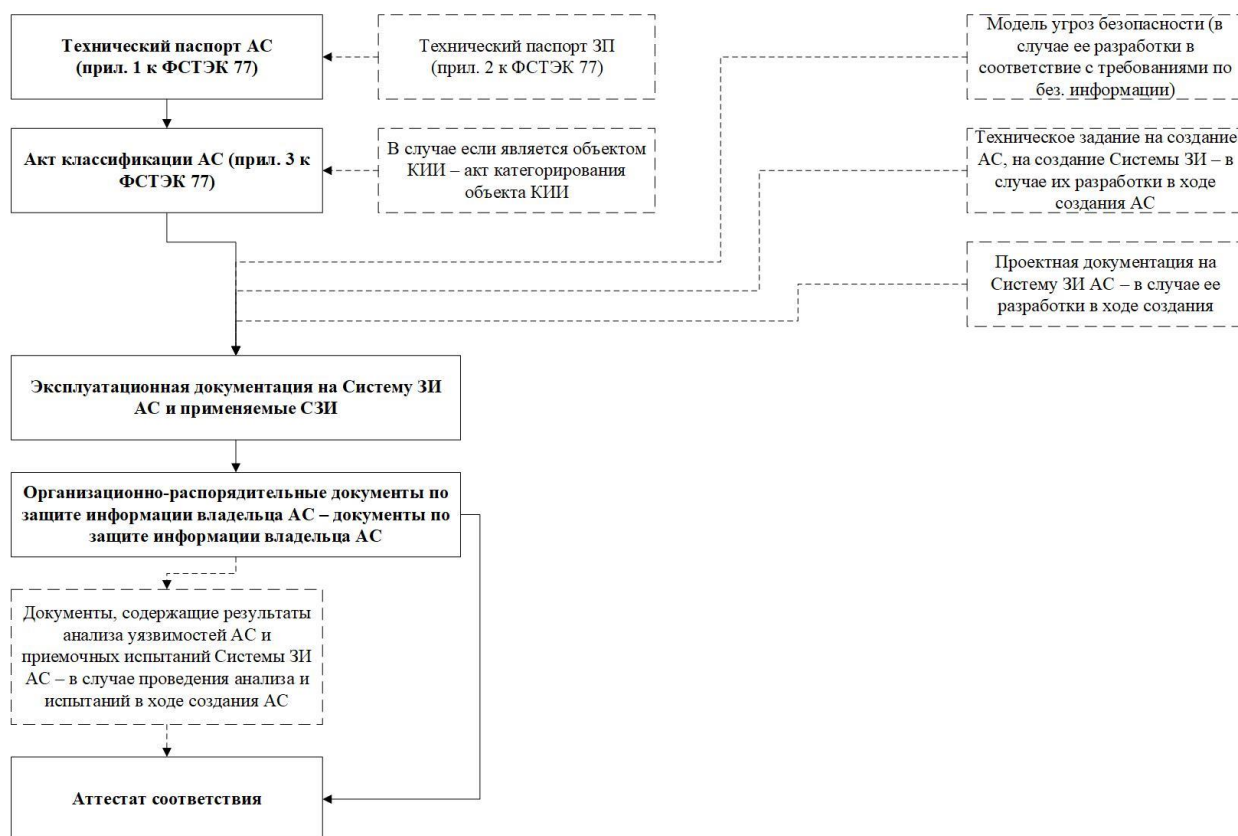


Рисунок 1 – Перечень документов для аттестации АС

В случае, если в процессе проведения аттестационных испытаний выявлены недостатки:

Пункт 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."

Далее, в результате устранения всех недостатков, орган по аттестации выдаёт Аттестат соответствия:

Пункт 22 – "Аттестат соответствия оформляется органом по аттестации по форме согласно приложению N 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."

Рассмотрим каждый документ, относящийся к процессу аттестации, по отдельности для лучшего понимания о составе данных документов:

1. Приложение №1 к Приказу ФСТЭК №77 – технический паспорт на объект информатизации. Содержание документа рассмотрено в таблице 1.

Таблица 1

Номер пункта	Описание
1.	Общие сведения об АС
1.1.	Наименование и назначение АС
1.2.	Расположение программно-технических средств АС
1.3.	Класс защищенности АС
1.4.	Номер и дата приказа о вводе в эксплуатацию
2.	Условия эксплуатации АС
2.1.	Сведения об архитектуре
Номер пункта	Описание
2.2.	Описание технологического процесса обработки информации и режимы доступа
2.3.	Сведения об аттестате соответствия информационно-телекоммуникационная инфраструктура – указываются реквизиты аттестата соответствия и модель услуг
3.	Состав АС
3.1.	Состав программно-технических средств АС

3.2.	Состав общесистемного и прикладного ПО АС
3.3.	Состав телекоммуникационного оборудования АС
3.4.	Состав СЗИ в АС
4.	Сведения о соответствии АС требованиям защите информации
4.1.	Сведения о протоколах аттестационных испытаний АС
4.2.	Сведения о заключении испытаний
4.3.	Сведения об аттестате соответствия АС
5.	Сведения о проведении контроля за обеспечением уровня защиты информации в АС – таблица 1
6.	Сведения об изменениях АС и СЗИ – таблица 2

2. Приложение №3 к Приказу ФСТЭК №77 – акт классификации АС. Содержание в себе следующие сведения:

- Наименование АС;
- Номер приказа о проведении классификации АС;
- Масштаб АС;
- Уровень значимости информации в АС;
- Класс защищенности АС;
- Члены комиссии.

3. Заключительным документов по аттестации автоматизированной системы является Аттестат соответствия, который содержит в себе следующие данные:

- Номер и дату выдачи аттестата соответствия;
- Наименование, класс защищенности и категория значимости АС;
- Наименование владельца АС;
- Наименование требований по защите информации;
- Дата, от которой получен технический паспорт АС;
- Наименование органа аттестации;
- Наименование АС;

- Дата получения результатов аттестационных испытаний в АС;
- Наименование ответственного подразделения (работника).

5. Вывод

Для успешной аттестации АС необходимо учитывать все требования, установленные нормативными документами, и строго следовать процедурам, определенным в перечне документов для аттестации.

6. Список используемых источников

1. Учебно–методическое пособие к практической работе "Организационное и правовое обеспечение информационной безопасности". А.А.Привалов. 2020 г.
2. Приказ ФСТЭК № 77 "Об утверждении порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну".
3. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР–К).
4. ГОСТ Р 58189-2018 "Защита информации. Требования к органам по аттестации объектов информатизации".
5. Постановление Правительства № 333 "О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны".