"Положение по аттестации объектов информатизации по требованиям безопасности информации" (утв. Гостехкомиссией России 25.11.1994)

I. 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", «Системой сертификации ГОСТ Р».

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, управления экологически опасными объектами, ведения секретных переговоров.

В остальных случаях аттестация носит добровольный характер (добровольная аттестация) и может осуществляться по инициативе заказчика или владельца объекта информатизации.

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 аккредитуются Гостехкомиссией России. Правила аккредитации определяются действующим в системе «Положением об аккредитации испытательных лабораторий и

органов по сертификации средств защиты информации по требованиям безопасности информации».

Гостехкомиссия России может передавать права на аккредитацию отраслевых (ведомственных) органов по аттестации другим органам государственной власти.

1.10. Расходы по проведению всех видов работ и услуг по обязательной и добровольной аттестации объектов информатизации оплачивают заявители.

Оплата работ по обязательной аттестации производится в соответствии с договором по утвержденным расценкам, а при их отсутствии - по договорной цене в порядке, установленном Гостехкомиссией России по согласованию с Министерством финансов Российской Федерации.

Расходы по проведению всех видов работ и услуг по аттестации объектов информатизации оплачивают заявители за счет финансовых средств, выделенных на разработку (доработку) и введение в действие защищаемого объекта информатизации.

1.11. 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 компонент.

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;
- испытательные центры (лаборатории) по сертификации продукции по требованиям безопасности информации;
- заявители (заказчики, владельцы, разработчики аттестуемых объектов информатизации).

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.

Такими 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. Испытательные центры (лаборатории) по сертификации продукции по требованиям безопасности информации по заказам заявителей проводят испытания несертифицированной продукции, используемой на объекте информатики, подлежащем обязательной аттестации, в соответствии с «Положением о сертификации средств защиты информации по требованиям безопасности информации».

2.6. Заявители:
- проводят подготовку объекта информатизации для аттестации путем реализации необходимых организационно-технических мероприятий по защите информации;
- привлекают органы по аттестации для организации и проведения аттестации объекта информатизации;
- предоставляют органам по аттестации необходимые документы и условия для проведения аттестации;
- привлекают, в необходимых случаях, для проведения испытаний несертифицированных средств защиты информации, используемых на аттестуемом объекте информатизации, испытательные центры (лаборатории) по сертификации;
- осуществляют эксплуатацию объекта информатизации в соответствии с условиями и требованиями, установленными в «Аттестате соответствия»;
- извещают орган по аттестации, выдавший «Аттестат соответствия», о всех изменениях в

информационных технологиях, составе и размещении средств и систем информатики, условиях их эксплуатации, которые могут повлиять на эффективность мер и средств защиты информации (перечень характеристик, определяющих безопасность информации, об изменениях которых требуется обязательно извещать орган по аттестации, приводится в «Аттестате соответствия»);
- предоставляют 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;
- испытание несертифицированных средств и систем защиты информации, используемых на аттестуемом объекте (при необходимости);
- разработка программы и методики аттестационных испытаний;
- заключение договоров на аттестацию;
- проведение аттестационных испытаний объекта информатизации;
- оформление, регистрация и выдача «Аттестата соответствия»;
- осуществление государственного контроля и надзора, инспекционного контроля за проведением аттестации и эксплуатацией аттестованных объектов информатизации;
- рассмотрение апелляций.

3.2. Подача и рассмотрение заявки на аттестацию.

3.2.1. Заявитель 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 и принимает решение о проведении аттестации объекта информатизации.

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.

3.4. Испытания несертифицированных средств и систем защиты информации, используемых на аттестуемом объекте информатизации.

3.4.1. При использовании на аттестуемом объекте информатизации несертифицированных средств и систем защиты информации в схему аттестации могут быть включены работы по их испытаниям в испытательных центрах (лабораториях) по сертификации средств защиты информации по требованиям безопасности информации или непосредственно на аттестуемом объекте информатизации с помощью специальной контрольной аппаратуры и тестовых средств.

3.4.2. Испытания отдельных несертифицированных средств и систем защиты информации в испытательных центрах (лабораториях) по сертификации проводятся до аттестационных испытаний объектов информатизации.

В этом случае заявителем к началу аттестационных испытаний должны быть представлены заключения органов по сертификации средств защиты информации по требованиям безопасности информации и сертификаты.

3.5. Разработка программы и методики аттестационных испытаний.

3.5.1. По результатам рассмотрения заявки и анализа исходных данных, а также предварительного ознакомления с аттестуемым объектом органом по аттестации разрабатываются программа аттестационных испытаний, предусматривающая перечень работ и их продолжительность, методики испытаний (или используются типовые методики), определяются количественный и профессиональный состав аттестационной комиссии, назначаемой органом по аттестации объектов информатизации, необходимость использования контрольной аппаратуры и тестовых средств на аттестуемом объекте информатизации или привлечения испытательных центров (лабораторий) по сертификации средств защиты информации по требованиям безопасности информации.

3.5.2. Порядок, содержание, условия и методы испытаний для оценки характеристик и показателей, проверяемых при аттестации, соответствия их установленным требованиям, а также применяемые в этих целях контрольная аппаратура и тестовые средства определяются в методиках испытаний различных видов объектов информатизации.

3.5.3. Программа аттестационных испытаний согласовывается с заявителем.

3.6. Заключение договоров на аттестацию.

3.6.1. Этап подготовки завершается заключением договора между заявителем и органом по аттестации на проведение аттестации, заключением договоров (контрактов) органа по аттестации с привлекаемыми экспертами и оформлением предписания о допуске аттестационной комиссии к проведению аттестации.

3.6.2. Оплата работы членов аттестационной комиссии производится органом по аттестации в соответствии с заключенными трудовыми договорами (контрактами) за счет финансовых средств от заключаемых договоров на аттестацию объектов информатизации.

3.7. Проведение аттестационных испытаний объектов информатизации.

3.7.1. На этапе аттестационных испытаний объекта информатизации:
- осуществляется анализ организационной структуры объекта информатизации, информационных потоков, состава и структуры комплекса технических средств и программного обеспечения, системы защиты информации на объекте, разработанной документации и ее соответствия требованиям нормативной документации по защите информации;
- определяется правильность категорирования объектов ЭВТ и классификации АС (при аттестации автоматизированных систем), выбора и применения сертифицированных и несертифицированных средств и систем защиты информации;
- проводятся испытания несертифицированных средств и систем защиты информации на аттестуемом объекте или анализ результатов их испытаний в испытательных центрах (лабораториях) по сертификации;
- 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;
- оформляются протоколы испытаний и заключение по результатам аттестации с конкретными рекомендациями по устранению допущенных нарушений, приведению системы защиты объекта информатизации в соответствие с установленными требованиями и совершенствованию этой системы, а также рекомендациями по контролю за функционированием объекта информатизации.

3.7.2. 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.

К заключению прилагаются протоколы испытаний, подтверждающие полученные при испытаниях результаты и обосновывающие приведенный в заключении вывод.

Протоколы испытаний подписываются экспертами - членами аттестационной комиссии, проводившими испытания.

Заключение и протоколы испытаний подлежат утверждению органом по аттестации.

3.8. Оформление, регистрация и выдача «Аттестата соответствия».

3.8.1. «Аттестат соответствия» на объект информатизации, отвечающий требованиям по безопасности информации, выдается органом по аттестации по форме, приведенной в приложении 2.

3.8.2. «Аттестат соответствия» оформляется и выдается заявителю после утверждения заключения по результатам аттестации.

3.8.3. 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.

Ведение сводных информационных баз аттестованных объектов информатизации осуществляется Гостехкомиссией России или по ее поручению одним из органов надзора за аттестацией и эксплуатацией аттестованных объектов.

3.8.4. «Аттестат соответствия» выдается владельцу аттестованного объекта информатизации органом по аттестации 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.

Владелец аттестованного объекта информатизации несет ответственность за выполнение установленных условий функционирования объекта информатизации, технологии обработки защищаемой информации и требований по безопасности информации.

3.8.5. В случае изменения условий и технологии обработки защищаемой информации владельцы аттестованных объектов обязаны известить об этом орган по аттестации, который принимает решение о необходимости проведения дополнительной проверки эффективности системы защиты объекта информатизации.

3.8.6. 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.

3.9. Рассмотрение апелляций.

В случае несогласия заявителя с отказом в выдаче «Аттестата соответствия» он 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.

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

3.10.1. 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.

Гостехкомиссия России может передавать некоторые из своих функций государственного контроля и надзора по аттестации и за эксплуатацией аттестованных объектов информатизации аккредитованным органам по аттестации.

3.10.2. Объем, содержание и порядок государственного контроля и надзора устанавливаются в нормативной и методической документации по аттестации объектов информатизации.

3.10.3. Государственный контроль и надзор за соблюдением правил аттестации включает проверку правильности и полноты проводимых мероприятий по аттестации объектов информатизации, оформления и рассмотрения органами по аттестации отчетных документов и протоколов испытаний, своевременное внесение изменений в нормативную и методическую документацию по безопасности информации, инспекционный контроль за эксплуатацией аттестованных объектов информатизации.

3.10.4. В случае грубых нарушений органом по аттестации требований стандартов или иных нормативных и методических документов по безопасности информации, выявленных при контроле и надзоре, орган по аттестации может быть лишен лицензии на право проведения аттестации объектов информатизации.

3.10.5. 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.

3.10.6. В случае грубых нарушений органом по аттестации требований стандартов или иных нормативных документов по безопасности информации, утвержденных Гостехкомиссией России, выявленных при контроле и надзоре и приведших к повторной аттестации, расходы по осуществлению контроля и надзора могут быть по решению Госарбитража взысканы с органа по аттестации. Повторная аттестация может быть также осуществлена за счет этого органа по аттестации.

3.10.7. Расходы по осуществлению надзора за обязательной аттестацией и эксплуатацией объектов, прошедших обязательную аттестацию, оплачиваются органом надзора из средств госбюджета, выделенных ему в этих целях.

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.

Начальник Управления
государственной технической комиссии
при президенте Российской Федерации
В. Вирковский
«24» ноября 1994 г.

Приложение 1

Заявка на проведение аттестации объекта информатизации

Приложение к форме "Заявки..."

Исходные данные по аттестуемому объекту информатизации готовятся на основе следующего перечня вопросов

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.

Приложение 2

Аттестат соответствия объекта информатизации требованиям безопасности 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.