

**Об утверждении Правил проведения аттестации государственных информационных систем на соответствие требованиям информационной безопасности**

***Утративший силу***

Постановление Правительства Республики Казахстан от 17 января 2008 года N 24. Утратило силу постановлением Правительства Республики Казахстан от 30 декабря 2009 года N 2280

      *Сноска. Утратило силу постановлением Правительства РК от 30.12.2009* N 2280 *(порядок введения в действие см.* п. 3*).*

      В соответствии со статьей 5 Закона Республики Казахстан от 11 января 2007 года "Об информатизации" Правительство Республики Казахстан **ПОСТАНОВЛЯЕТ:**

      1. Утвердить прилагаемые Правила проведения аттестации государственных информационных систем на соответствие требованиям информационной безопасности.

      2. Настоящее постановление вступает в силу со дня подписания.

*Премьер-Министр*

*Республики Казахстан*

Утверждены

постановлением Правительства

Республики Казахстан

от 17 января 2008 года

N 24

**ПРАВИЛА**

**проведения аттестации государственных информационных систем на**

**соответствие требованиям информационной безопасности**

**1. Общие положения**

      1. Настоящие Правила проведения аттестации государственных информационных систем на соответствие требованиям информационной безопасности (далее - Правила) разработаны в соответствии с Законом Республики Казахстан от 11 января 2007 года "Об информатизации" и определяют порядок организации и проведения работ по аттестации государственных информационных систем на соответствие требованиям информационной безопасности.

      2. Доступ к государственной информационной системе определяется правилами, разрабатываемыми владельцами государственной информационной системы.

      3. Под аттестацией государственных информационных систем на соответствие требованиям информационной безопасности понимается процедура, результатом которой является документальное удостоверение соответствия государственной информационной системы требованиям информационной безопасности.

      Цель аттестации государственных информационных систем - показать, что она является полной, непротиворечивой, технически правильной и поэтому пригодна для изложения требований к одной или нескольким оцениваемым информационным системам.

      4. Соответствие государственной информационной системы требованиям информационной безопасности проводится в соответствии с требованиями нормативных документов, устанавливающих параметры и методы проведения аттестации с учетом соотношения затрат на организацию защиты информации и величины ущерба, который может быть нанесен собственнику информационных ресурсов.

      5. Эксплуатация государственных информационных систем и (или) принятие государственной информационной системы осуществляется по результатам аттестации на соответствие требованиям информационной безопасности.

      6. Регулирование процессов аттестации, а также порядок их проведения выполняется уполномоченным органом в сфере информатизации.

**2. Порядок проведения аттестации**

      7. Устанавливается следующий порядок проведения аттестации:

      1) подача заявителем в организацию проводящей аттестацию заявки по форме, согласно приложению к настоящим Правилам, с приложением документов, указанных в пункте 6 настоящих Правил;

      2) предварительная оценка и принятие решения по заявке организацией проводящей аттестацию;

      3) проведение организацией проводящей аттестацию аттестационного обследования;

      4) принятие решения и выдача (отказ в выдаче) аттестата.

      8. К заявке прилагаются следующие документы:

      1) учредительные документы заявителя;

      2) свидетельство о государственной регистрации юридического лица;

      3) перечень средств, примененных при обеспечении информационной безопасности информационной системы;

      4) сертификаты соответствия по требованиям информационной безопасности технических и программных средств, входящих в состав информационной системы и подлежащих подтверждению соответствия в соответствии с законодательством Республики Казахстан ;

      5) перечень нормативно-технических документов по информационной безопасности;

      6) акт инспекционного обследования организации - заявителя (при условии его проведения);

      7) утвержденная схема (план) взаимодействия информационной системы с ее компонентами;

      8) проектно-техническая документация информационной системы;

      9) эксплуатационная документация информационной системы.

      9. В случае если заявка и (или) прилагаемые к заявке документы не соответствуют требованиям Правил или прилагаемые к заявке документы представлены не в полном объеме, такая заявка подлежит возврату в течение десяти календарных дней, с указанием причин возврата.

**3. Аттестационное обследование**

      10. Аттестационное обследование проводится на основании методик и программ испытаний, разработанных организацией проводящей аттестацию и согласованных с заявителем, а также с уполномоченными органами в сфере информатизации, по защите государственных секретов и обеспечению информационной безопасности, органами национальной безопасности.

      11. Для технических и программных средств обработки и защиты информации, входящих в состав аттестуемой информационной системы, необходима аттестация на соответствие требованиям информационной безопасности.

      12. Приказом органа по подтверждению соответствия создается Комиссия для проведения аттестационного обследования (далее - Комиссия).

      13. При обследовании прикладного программного обеспечения организацией проводящей аттестацию изучаются:

      методы защиты информации с общим доступом;

      запись регистрации событий;

      защищенность данных системных журналов;

      запись регистрации сбоев;

      управление доступом к системе.

      14. При обследовании баз данных орган по подтверждению соответствия изучает:

      методы защиты информации с общим доступом;

      запись регистрации событий;

      защищенность данных системных журналов;

      запись администратора и оператора;

      запись регистрации сбоев;

      управление доступом к системе.

      15. При обследовании специальных программных средств, предназначенных для защиты информации, орган по подтверждению соответствия изучает:

      методы защиты информации с общим доступом;

      запись регистрации событий;

      запись регистрации сбоев;

      защиту средств аудита;

      управление доступом к системе.

      16. При обследовании операционных систем орган по подтверждению соответствия изучает:

      методы защиты информации с общим доступом;

      запись регистрации событий;

      запись администратора и оператора;

      запись регистрации сбоев;

      управление доступом к системе;

      мониторинг использования системы.

      17. Срок аттестационного обследования объекта Комиссией проводится в течение тридцати календарных дней с момента прибытия Комиссии к месту аттестационного обследования.

      18. На основании решения Комиссии орган по подтверждению соответствия выдает заявителю акт об итогах аттестационного обследования.

      19. Акт составляется в двух экземплярах (по одному для заявителя и организации проводящей аттестацию), с указанием фактического состояния государственной информационной системы, выводов, рекомендаций и заключения о возможности (невозможности) выдачи аттестата.

      20. Аттестат соответствия оформляется и выдается заявителю после положительного решения Комиссии по результатам аттестации.

      21. Организация, проводящая аттестацию ведет реестр выданных аттестатов. Государственные информационные системы регистрируются в государственном регистре электронных информационных ресурсов и информационных систем в порядке, установленном законодательством Республики Казахстан об информатизации .

Приложение

к Правилам проведения аттестации

государственных информационных

систем, на соответствие требованиям

информационной безопасности

Кому\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

      (наименование органа по аттестации)

**ЗАЯВКА**

на проведение аттестации государственной информационной системы

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

                             (наименование заявителя)

просит провести аттестацию \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

                              (наименование объекта информатизации или СВТ)

на соответствие требованиям по информационной безопасности.

      1. Исходные данные по государственной информационной системе на \_\_\_ листах прилагаются.

      2. Заявитель готов представить необходимые документы и создать условия для проведения аттестации.

      3. Заявитель согласен, на договорной основе, оплатить расходы по всем видам работ и услуг по аттестации информационной системы.

      М.П.

      \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_             \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

      (Ф.И.О. руководителя органа заявителя)             (подпись, дата)

 © 2012. РГП на ПХВ «Институт законодательства и правовой информации Республики Казахстан» Министерства юстиции Республики Казахстан